NCIA/ACQ/2018/854
28 March 2018

To: All Nominated Prospective Bidders

Subject: **INVITATION FOR BID**

Provision of a Service Oriented Architecture (SOA) and Identity Management Platform (IdM) IFB-CO-14176-SOA-IDM

Reference: A. AC/4-D/2261 (1996 Edition) and AC/4-D/2261-ADD2 (1996 Edition)

                 B. AC/4-D(2008)0002-REV1-AS1 and AC/4(2008)0002-REV2

                 C. NSIP Project Serial 2014/0IS03094-0

                 D. AC/4(PP)D/27047-ADD2

                 E. AC/4-DS(2015)0024

                 F. AC/4(PP)D/27047-ADD3

                 G. AC/4-DS(2017)0017

                 H. NCI Agency NOI NCIA/ACQ/2017/2096 dated 6 November 2017

Dear Madam/Sir,

1.   Your company is hereby invited to participate in an International Competitive Bid under the Best Value procedures set forth in References A and B for the provision of a Service Oriented Architecture (SOA) & Identity Management (IdM) Platform.

2.   The full requirements of the project are described in the Prospective Contract (Book II), part of the Invitation for Bid (IFB) package.

3.   The NCI Agency intends placing one Contract to cover the entire scope of the project. No partial bidding will be allowed.

4.   Contract will be based on the proposal evaluated as the Best Values in accordance with the selection criteria set forth in the Bidding Instructions (Book I) which follow the procedures for International Competitive Bidding set forth in References A and B.

5.   The reference for this IFB is **IFB-CO-14176-SOA-IDM**. All correspondence related to this IFB shall reference this number.
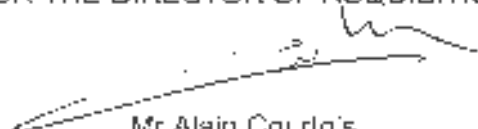
6. **THE CLOSING TIME FOR SUBMISSION OF BIDS IN RESPONSE TO THIS IFB IS 15:00 HOURS (BRUSSELS TIMES) ON 12 JUNE 2018.**

7. This IFB consists of the Bidding Instructions, including Administrative Certificates and Bidding Sheets (Book I) and the Prospective Contract (Book II). The Prospective Contract contains the Schedule of Supplies and Services (Part I), Contract Special Provisions (Part II), Contract General Provisions (Part III), as well as the Statement of Work (Part IV) and the Annexes thereto set forth detailed specifications governing the performance requirements of the Contract.

8. The overall security classification of this IFB is "NATO UNCLASSIFIED". This IFB remains the property of the NCI Agency and shall be protected in accordance with the applicable national security regulations.

9. The successful Bidder will be required to handle and store classified information up to the level of "NATO SECRET". In addition, Contractors' personnel working on NATO sites will be required to hold 'NATO SECRET' individual security clearances, and Contractors' personnel who need System Administrator privileges or access when working on NATO SECRET systems will be required to hold 'NATO CTS' (Cosmic Top Secret) clearance. Contractor personnel will be required to work unescorted in Class II and Class I Security areas and therefore access can only be permitted to cleared individuals. Only companies maintaining such cleared industrial facilities and the appropriate personnel clearances will be able to perform the resulting Contract.

10. Recipients are requested to complete and return the enclosed "Acknowledgement of Receipt" at Attachment A within 14 days of receipt of this IFB, informing the NCI Agency of their intention to bid or not to bid. Companies are not bound by their initial decision, and should a firm decide to reverse its stated intention at a later date, it is requested to advise the NCI Agency by separate letter

11. Bidders are advised that the NCI Agency reserves the right to cancel this IFB at any time in its entirety and bears no liability for bid preparation costs incurred by firms or any other collateral costs if bid cancellation occurs

12. The Contracting Officer responsible for this solicitation is Mr. Phil Chulick, and all Correspondence regarding this IFB should solely be addressed to Mr. Curtis Day, IFB-CO-14176-SOA-IDM.Clarifications@ncia.nato.int

FOR THE DIRECTOR OF ACQUISITION

Mr Alain Courtois
Chief of Contracts

Attachment(s):

A. Acknowledgement of Receipt of IFB-CO-14176-SOA-IDM

B. Distribution List of IFB-CO-14176-SOA-IDM

C. Final Bidders List for IFB-CO-14176-SOA-IDM

D. Invitation for Bid IFB-CO-14176-SOA-IDM

ATTACHMENT A

**ACKNOWLEDGEMENT OF RECEIPT OF INVITATION FOR BIDS
IFB-CO-14176-SOA-IDM**

Please complete, sign and return by email (scanned to pdf) within 14 days to IFB-CO-14176-SOA-IDM.Clarifications@ncia.nato.int

We hereby advise that we have received Invitation For Bids IFB-CO-14176-SOA-IDM on ...., together with all enclosures listed in its Table of Contents.

PLEASE CHECK ONE

☐　　　As of this date and without commitment on our part we **do intend** to submit a bid.

☐　　　We **do not intend** to submit a bid

☐　　　We are reviewing the requirements of the IFB and will notify you of our decision as soon as possible.

Signature:　＿＿＿＿＿＿＿＿＿＿＿

Printed Name:　＿＿＿＿＿＿＿＿＿＿＿

Title:　＿＿＿＿＿＿＿＿＿＿＿

Date:　＿＿＿＿＿＿＿＿＿＿＿

Company:　＿＿＿＿＿＿＿＿＿＿＿

Address:　＿＿＿＿＿＿＿＿＿＿＿

POC:　＿＿＿＿＿＿＿＿＿＿＿

Tel.:　＿＿＿＿＿＿＿＿＿＿＿

E-mail:　＿＿＿＿＿＿＿＿＿＿＿

ATTACHMENT B
Distribution List of IFB-CO-14176-SOA-IDM

All Nominated Prospective Bidders

NATO Delegations and Embassies

NCI Agency – All NATEXs

NATO HQ:

NATO Office of Resources
Management and Implementation Branch – Attn: Deputy Branch Chief

Director, NATO HQ C3 Staff
Attn: Executive Co-ordinator

SACTREPEUR

Att.: Investment Assistant

Strategic Commands

Major General Walter Huhn, ACO/DCOS CIS & Cyber Defence

Lieutenant General Jeffery Lofgren, ACT/DCOS Capability Development

NCI Agency:

ACQ Director of Acquisition (Mr Peter Scaruppe)

ACQ Deputy Director of Acquisition (Mrs Agata Szydelko)

ACQ Contract Award Board Administrator (Ms Marie-Louise Le Bourlot)

ACQ Chief of Contracts (Mr Alain Courtois)

ACQ Principal Contracting Officer (Mr Philip Chulick)

ACQ Senior Contracting Officer (Mr Curtis Day)

DIS/CES - Chief (Mr Pierre Pradier)

DIS/CES - Project Manager (Mr Cedric Salson)

NLO (Mr Xavier Desfougeres)

ILS (Mr Carlo Oroni)

Cost Analyst (Mr Ryan Feeks)

Finance (Mr Mariano Ippolito)

Legal (Ms Simona Rocchi)

Registry

ATTACHMENT C

Final Bidders List for IFB-CO-14176-SOA-IDM

Country	Vendors
BELGIUM	ATOS
	BT Limited
	CISCO Systems Limited
	DXC Technology
	Hewlett-Packard Belgium
	IBM Belgium
	Microsoft
	Oracle
	Proximus
	Securitas
	SOPRASTERIA
	Vitrociset Belgium
BULGARIA	Index-Bulgaria Ltd
	Kontrax JSC
	Lirex Bg Ltd
	S&T Bulgaria Ltd
CANADA	MDA Systems Ltd.
	MDOS Consulting Inc.
	RIMPAC CONSULTANTS INC.
	Terida Systems Ltd
	QinetiQ
CROATIA	King ICT d.o.o
	SPAN d.o.o
CZECH REPUBLIC	AMI Praka a.s.
	S.ICZ a.s.
FRANCE	Airbus Defence and Space
	Global Technologies
	Sopra Steria Limited

GERMANY	Airbus Defence and Space GmbH
	Atos Information
	CGI Deutschland Ltd. and Co. KG
	Euromicron Deutschland GmbH
	INFODAS GmbH
	IABG MbH
GREECE	European Dynamics SA
	Intrasoft Int'nal SA
ITALY	Altran Italia S.p.A.
	Engineering Ingegneria Informatica S.p.A.
	Hitrac Engineering Group SpA
	Leonardo S.p.A.
	Next-Ingegneria Dei Sistemi S. p. A.
	Vitrociset S.p.A.
LITHUANIA	UAB "ELSIS PRO"
NETHERLANDS	NCIM Groep
POLAND	Comp Spolka Akcyjna and Enigma Systemy Ochrong Informacji Spa z.o.o
	Vector Synergy Sp. z.o.o.
ROMANIA	Siemens Convergence Creators SRL
SPAIN	Everis
	GMV
	Indra Sistemas, S.A.
UK	AIRBUS Defence and Space
	Fujitsu
	QinetiQ Group Ltd
	Sopra Steria Limited
TURKEY	ATOS
	C Tech Bilisim Teknolojileri
	Havelsan Hava Electronik
	Milsoft
	STM Savunma Teknolojileri
USA	Ardent Technologies, Inc.
	Booz Allen Hamilton, Inc.

	Business Integra Technology Solutions, Inc.
	Creative Information Technology, Inc.
	EMW, Inc.
	PlanIT
	Raytheon Corporation
	U.S. International Development Consortium, Inc.

INVITATION FOR BID

IFB-CO-14176- SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

AUTHORISATION/SERIAL NOs

2014/0IS03094-0
AC/4(PP)D/27047-ADD3, AC/4-DS(2017)0017
AC/4(PP)D/27047-ADD2, AC/4-DS(2015)0024

BOOK I

BIDDING INSTRUCTIONS

Page Intentionally Left Blank

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this Invitation For Bid (IFB) is to award a Contract for the provision of a Service Oriented Architecture and Identity management (SOA & IdM) Platform.

1.1.2 This project is identified as Project 2014/0IS03094-0 and originates from the Capability Package 9C0150.

1.2 Project Scope

1.2.1 The current authorisation and consequently any Contract resulting from this Invitation for Bid (IFB) shall address **solely** Project 2014/0IS03094-0.

1.2.1.1 The entire project scope consist of 12 (twelve) Work Packages. This IFB covers only four (4) Work Packages: WP-2 (two), WP-4 (four), WP-6 (six) and WP-7 (seven).This IFB shall address only above mentioned four (4) Work Packages as shown below. Overall project schedule is described in Book II SoW, Section 4.2.

Work package	Base Contract	Evaluated Priced Options
#	CLIN Numbers	CLIN Numbers
2	2.1-2.6 (Wave 1)	2.7-2.14 (Wave 2)
4	4.1-4.6 (Wave 1)	4.7- 4.14 (Wave 2)
6	6.1-6.2 (Wave 1)	6.3-6.4 (Wave 2)
7		7 (Wave 1)

1.2.1.2 The scope of the SOA & IdM project of this IFB includes four (4) Work Packages splitt in two Waves as shown below and also described in para 4.3.4.1.1.1:

Wave 1	Wave 2 (Option)
Work Package 2 - Basic SOA Platform	Work Package 2 - Extended SOA Platform
Work Package 4 - Basic IdM Platform	Work Package 4 - Extended IdM Platform
Work Package 6 - Support pilot Integration cases	Work Package 6 - Support pilot Integration cases
Work Package 7 - Support Integration of other projects (Option)	

1.2.1.3   Waves:

1.2.1.3.1 Wave 1 shall be Costed and Evaluated;

1.2.1.3.2 Wave 1 O&M (Operations and Maintenace shall be Costed and Evaluated Option;

1.2.1.3.3 Wave 2 shall be Costed and Evaluated Option;

1.2.1.3.4 Wave 2 O&M shall be Costed and Evaluated Option.

1.2.1.4   Work Packages:

1.2.1.4.1 Work Package 2: This work package will provide a common platform to existing and new systems to enable the migration towards a Service Oriented Architecture (SOA), on both: Operational Network (ON) and Protected Business Network (PBN).

1.2.1.4.2 Work Package 4. This work package will provide a common Identity Management (IdM) Platform to existing and new systems.

1.2.1.4.3 Work Package 6. This work package will provide consultancy and on-demand support to a 3rd party Contractor and developers working under on implementing the pilot integration cases with the SOA & IdM Platform.

1.2.1.4.4 Work Package 7. This work package will provide a not-to-exceed on-demand support (including post-implementation support) for 3rd party Contractors working for other projects that will integrate their systems with the SOA&IdM Platform.

1.3   Overview of the Prospective Contract

1.3.1   The Prospective Contract (Book II) requires the selected Contractor to deliver the scope of the project described above. This will be achieved within the framework of the Contract resulting from this IFB by means of performance of Contract requirements and Work Packages that are further defined in the Statement of Work (SOW), Part IV to the Prospective Contract.

1.3.2   A Contract will be awarded for the work defined in the SOW for two Waves, with Wave 1 being the Basic Contract, and the work defined in Wave 2 being included as Firm Fixed Price options to the Contract.

1.4   Governing Rules, Eligibility, and Exclusion Provisions

1.4.1   This solicitation is an International IFB and is issued in accordance with the procedures for International Competitive Bidding set forth in the NATO document AC/4-D/2261 (1996 Edition) including Annex X. Pursuant to these procedures, Bidding is restricted to companies from participating NATO

member nations for which a Declaration of Eligibility (DoE) has been issued by their respective government authorities.

1.4.2   The evaluation method to be used in the selection of the successful Bidder under this solicitation will follow the Best Value Procedures set forth in AC/4-D/2261-ADD2 dated 24 July 2009, AC/4-D(2008)0002-REV1-AS1 dated 23 July 2009 and AC/4(2008)0002-REV2 dated 15 July 2015.

1.4.3   The Bid evaluation criteria and the detailed evaluation procedures are described in Section 4 BID EVALUATION AND CONTRACT AWARD.

1.4.4   This IFB will not be the subject of a public Bid opening.

1.4.5   The Bidder shall refer to the Purchaser all queries for resolution of any conflicts found in information contained in this document in accordance with the procedures set forth in paragraph 2.6 "Request for IFB Clarifications".

1.5   Security

1.5.1   This Invitation For Bid has been classified as NATO UNCLASSIFIED.

1.5.2   Contractor will be required to handle and store classified material to the level of "NATO SECRET" and the Contractor shall have the appropriate facility and personnel clearances. Should a Contractor be unable to perform the Contract due to the fact that the facility clearance has not been provided by their respective national security agency, this lack of clearance cannot be the basis for a claim of adjustment or an extension of schedule, nor the lack of clearance be considered a mitigating circumstance in the case of an assessment of Liquidated Damages or a determination of Termination For Default by the Purchaser.

1.5.3   Contractor personnel working at NATO sites are required to possess a security clearance of "NATO SECRET". Contractor personnel without such a clearance, confirmed by the appropriate national security authority and transmitted to the cognisant NATO security officer at least fourteen (14) days prior to the site visit, will be denied access to the site. Denial of such access by the Purchaser may not be used by the Contractor as the basis for a claim of adjustment or an extension of schedule nor can the denial of access be considered a mitigating circumstance in the case of an assessment of Liquidated Damages or a determination of Termination for Default by the Purchaser. Contractor personnel who need System Administrator privileges when working on NATO SECRET systems shall be required to hold NATO CTS clearances (see SoW 13.1).

1.5.4   Bidders are advised that Contract signature will not be delayed in order to allow the processing of security clearances for personnel or facilities and, should the otherwise successful Bidder not be in a position to accept the offered Contract within a reasonable period of time, due to the fact that its personnel or facilities do not possess the appropriate security clearance(s), the Purchaser may

determine the Bidder's Offer to be non-compliant and offer the Contract to the next ranking Bidder. In such a case, the Bidder who would not sign the Contract shall be liable for forfeiture of the Bid Guarantee.

1.5.5   All documentation, including the IFB itself, all applicable documents and any reference documents provided by the Purchaser are solely to be used for the purpose of preparing a response to this IFB. They are to be safeguarded at the appropriate level according to their classification and reference documents are provided "as is, without any warranty" as to quality or accuracy.

2 GENERAL BIDDING INFORMATION

2.1 Definitions

2.1.1 In addition to the definitions and acronyms set in the Clause 2 entitled "Definitions of Terms and Acronyms" of the NCI Agency Contract General Contract Provisions Book II, (Part III), the following terms and acronyms, as used in this IFB, shall have the meanings specified below:

2.1.1.1 "Bidder": a firm, consortium, or joint venture which submits an offer in response to this solicitation. Bidders are at liberty to constitute themselves into any form of Contractual arrangements or legal entity they desire, bearing in mind that in consortium-type arrangements a single judicial personality shall be established to represent that legal entity. A legal entity, such as an individual, Partnership or Corporation, herein referred to as the "Principal Contractor", shall represent all members of the consortium with the NCI Agency and/or NATO. The "Principal Contractor" shall be vested with full power and authority to act on behalf of all members of the consortium, within the prescribed powers stated in an irrevocable Power of Attorney or equivalent issued to the "Principal Contractor" by all members associated with the consortium. Evidence of authority to act on behalf of the consortium by the "Principal Contractor" shall be enclosed and sent with the Bid. Failure to furnish proof of authority shall be a reason for the Bid being declared non-compliant.

2.1.1.2 "Compliance": strict conformity to the requirements and standards specified in this IFB and its attachments.

2.1.1.3 "Contractor": the awardee of this solicitation of offers, which shall be responsible for the fulfilment of the requirements established in the prospective Contract.

2.1.1.4 "Firm of a Participating Country": a firm legally constituted or chartered under the laws of, and geographically located in, or falling under the jurisdiction of a Participating Country.

2.1.1.5 "IFB": Invitation for Bid.

2.1.1.6 ''Purchaser'': The Purchaser is defined as the current NCI Agency or its legal successor.

2.1.1.7 "Quotation" or "Bid": a binding offer to perform the work specified in the attached prospective Contract (Book II).

2.2 Eligibility and Origin of Equipment and Services

2.2.1 As stated in paragraph 1.4.1 above only firms from a Participating Country are eligible to engage in this competitive Bidding process. In addition, all Contractors, sub-Contractors and manufacturers, at any tier, must be from Participating Countries.

2.2.2 In addition, all Contractors, sub-Contractors and manufacturers, at any tier, must be from Participating Countries.

2.2.3 None of the work, including project design, labour and services shall be performed other than by firms from and within Participating Countries.

2.2.4 No materials or items of equipment down to and including identifiable Sub-assemblies shall be manufactured or assembled by a firm other than from and within a Participating Country.

2.2.5 Unless otherwise authorised by the terms of the prospective Contract, the Intellectual Property Rights (IPR) to all design documentation and related system operating software shall reside in NATO member countries, and no license fees or royalty charges shall be paid by the Contractor to firms, individuals or governments other than within the NATO member community.

2.3 Bid Delivery and Bid Closing

2.3.1 All Bids shall be in the possession of the Purchaser at the address given below in paragraph 2.3.2 on/or before 15:00 hours (Brussels Time) on **12 June 2018** at which time and date Bidding shall be closed.

2.3.2 Bids shall be delivered to the following email address, which will generate an automatic confirmation of receipt: IFB-CO-14176-SOA-IDM.Bids@ncia.nato.int. Delivery POCs are shown at 2.5.1.

2.3.3 Late Bids

2.3.3.1 Bids which are delivered to the Purchaser after the specified time and date set forth above for Bid Closing are "Late Bids" and shall not be considered for award.Upon receipt of a late bid. The sender shall be notified that hteir bid arrived after bid closing.

2.3.3.2 *Consideration of Late Bid* – The Purchaser considers that it is the responsibility of the Bidder to ensure that the Bid submission arrives by the specified Bid Closing Date and Time.

2.4 Requests for Extension of Bid Closing Date

2.4.1 Bidders are informed that requests for extension to the closing date for the IFB shall be submitted by the Bidder only through its respective country's NATO Delegation or Embassy to the Purchaser POC indicated in paragraph 2.5.1

below. In accordance with AC/4-D/2261 Final (July 1996 Edition) any request for extension shall be submitted by the respective NATO Delegation or Embassy **no later than fourteen (14) days** prior to the established Bid closing date. The Purchaser is under no obligation to answer requests submitted after this time. Bidders are advised to submit their request in sufficient time as to allow their respective NATO Delegation or Embassy to deliver the formal request to the Purchaser within the above time limit.

2.5 Purchaser's Point of Contact

2.5.1 The Contracting Officer (CO) responsible for this solicitation is Mr. Philip Chulick. All Correspondence regarding this IFB should solely be addressed to:

> Mr. Curtis Day
> NATO Communications and Information Agency
> Tel: +32.2.707.8155
> Acquisition Directorate
> Avenue du Bourget 140 Bâtiment Z
> B-1110 Brussels - Belgium

> Alternate:

> Mrs. Emira Kapetanovic
> Tel: +32.2.707.8582
> Acquisition Directorate
> Avenue du Bourget 140 Bâtiment Z
> B-1110 Brussels - Belgium

> Bid Delivery E-mail
> IFB-CO-14176-SOA-IDM.Bids@ncia.nato.int

> Questions/Clarifications E-Mail
> IFB-CO-14176-SOA-IDM.Clarifications@ncia.nato.int

2.6 Request for IFB Clarifications

2.6.1 Bidders, at the earliest stage possible during the solicitation period, are encouraged to query and seek clarification of any matters of a Contractual, administrative and technical nature pertaining to this IFB.

2.6.2 All questions and requests for clarification shall be forwarded to the Purchaser via email using the Clarification Request Form provided at Annex E of this Book I. Such questions shall be forwarded to the point of contact specified in paragraph 2.5.1 above and shall arrive **not later than twenty eight (28)**

calendar days prior to the stated "Bid Closing Date". The Purchaser is under no obligation to answer requests for clarification submitted after this time. Requests for clarification must address the totality of the concerns of the Bidder, as the Bidder will generally not be permitted to revisit areas of the IFB for additional clarification except as noted in paragraph 2.6.3, below.

2.6.3   Additional requests for clarification are limited only to the information provided as answers by the Purchaser to Bidder requests for clarification. Such additional requests shall arrive not later than fourteen (14) calendar days before the established Bid Closing Date.

2.6.4   It is the responsibility of the Bidders to ensure that all Clarification Requests submitted bear no mark, logo or any other form or sign that may lead to reveal the Bidders' identity in the language constituting the clarification itself. This prescription is not applicable to the means used for the transmission of the clarification (i.e. email or form by which the clarification is forwarded).

2.6.5   The Purchaser declines all responsibilities associated to any and all circumstances regardless of the nature or subject matter arising from the Bidders' failure or inability to abide to the prescription in paragraph 2.6.4.

2.6.6   The Purchaser may provide for the removal of any form of identification in the body of the clarification request in those instances in which such practice is feasible as well as providing for a re-wording of the clarification request in those cases in which the original language submitted is deemed ambiguous, unclear, subject to different interpretation or revelatory of the Bidder's identity.

2.6.7   Bidders are advised that subsequent questions and/or requests for clarification included in a Bid shall neither be answered nor considered for evaluation and may be considered by the Purchaser as grounds for a determination of non-compliance.

2.6.8   Except as provided above, all questions will be answered by the Purchaser and the questions and answers (but not the identity of the questioner) will be issued in writing to all prospective Bidders. The Bidders shall immediately inform the Purchaser in the event that submitted question are not reflected in the answers published.

2.6.9   The published answers issued by the Purchaser shall be regarded as the authoritative interpretation of the IFB. Amendment to the language of the IFB included in the answers shall be incorporated by the Bidder in his offer.

2.6.10 Where the extent of the changes implied by the response to a clarification request is of such a magnitude that the Purchaser deems necessary to issue revised documentation, the Purchaser will do so by the mean of the issuance of a formal IFB Amendment in accordance with paragraph 2.8 below.

2.6.11 The Purchaser reserves the right to reject clarification requests clearly devised or submitted for the purpose of artificially obtaining an extension of the Bidding time (i.e. clarifications re-submitted using different wording where such wording does not change the essence of the clarification being requested).

2.7   Requests for Waivers and Deviations

2.7.1   Bidders are informed that requests for alteration to, waivers, or deviations from the terms and conditions of this IFB and attached Prospective Contract (Book II) will not be considered after the request for clarification process. Requests for alterations to the other requirements, terms or conditions of the IFB or the Prospective Contract may only be considered as part of the clarification process set forth in paragraph 2.6 above. Requests for alterations to the specifications, terms and conditions of the Contract which are included in a Bid as submitted may be regarded by the Purchaser as a qualification or condition of the Bid and may be grounds for a determination of non-compliance.

2.8   Amendment of the IFB

2.8.1   The Purchaser may revise, amend or correct the terms, conditions and/or specifications and provisions of the IFB at any time prior to the date set for the Bid Closing. Any and all modifications will be transmitted to all Bidders by an official Amendment designated as such and signed by the Contracting Authority. Such Amendment may be accompanied by an acknowledgement of receipt which the Bidder shall complete and forward to the Purchaser. This process may be part of the clarification procedures set forth in paragraph 2.6 above or may be an independent action on the part of the Purchaser.

2.8.2   The Purchaser will consider the potential impact of Amendments on the ability of prospective Bidders to prepare a proper Bid within the allotted time. The Purchaser may extend the "Bid Closing Date" at its discretion and such extension will be set forth in the Amendment document.

2.8.3   All revision or Amendments issued by the Purchaser shall also be acknowledged by the Bidder in its Bid by completing the "Annex B-2 – Acknowledgement of Receipt of IFB Amendments and Responses to Clarification Requests" at Annex B-2, 6.2. Failure to acknowledge receipt of all Amendments may be grounds to determine the Bid to be non-compliant.

2.9   Modification and Withdrawal of Bids

2.9.1   Bids, once submitted, may be modified by Bidders, but only to the extent that the modifications are in writing, conform to the requirements of the IFB, and are received by the Purchaser prior to the exact time and date established for Bid Closing. Such modifications shall be considered as an integral part of the submitted Bid.

2.9.2   Modifications to Bids which arrive after the Bid Closing Date will be considered as "Late Modifications" and will be processed in accordance with the procedure set forth above concerning "Late Bids", except that unlike a "Late Bid", the Purchaser will retain the modification until a selection is made. A modification to a Bid which is determined to be late will not be considered in the evaluation and selection process. If the Bidder submitting the modification is determined to be the successful Bidder on the basis of the unmodified Bid, the modification may then be opened. If the modification makes the terms of the Bid more favourable to the Purchaser, the modified Bid may be used as the basis of Contract award. The Purchaser, however, reserves the right to award a Contract to the apparent successful Bidder on the basis of the Bid submitted and disregard the late modification.

2.9.3   A Bidder may withdraw its Bid at any time prior to Bid Opening without penalty. In order to do so, an authorised agent or employee of the Bidder must provide an original statement of the firm's decision to withdraw the Bid and remove the Bid from the Purchaser's premises.

2.9.4   Except as provided in paragraph 2.10.4.2 below, a Bidder may withdraw its Bid after Bid Opening only by forfeiture of the Bid Guarantee.

2.10 Bid Validity

2.10.1   Bidders shall be bound by the term of their Bids for a period of twelve (12) months starting from the Bid Closing Date specified in paragraph 2.3.1 above.

2.10.2   In order to comply with this requirement, the Bidder shall complete the Certificate of Bid Validity set forth in paragraph 6.4. Bids offering less than the period of time referred to above for acceptance by the Purchaser may be determined to be non-compliant.

2.10.3   The Purchaser will endeavour to complete the evaluation and make an award within the period referred to above. However, should that period of time prove insufficient to render an award, the Purchaser reserves the right to request an extension of the period of validity of all Bids which remain under consideration for award.

2.10.4   Upon notification by the Purchaser of such a request for a time extension, the Bidders shall have the right to:

2.10.4.1   accept this extension of time in which case Bidders shall be bound by the terms of their offer for the extended period of time and the Bid Guarantee and Certificate of Bid Validity extended accordingly; or

2.10.4.2   refuse this extension of time and withdraw the Bid, in which case the Purchaser will return to the Bidder its Bid Guarantee in the full amount without penalty.

2.10.5 Bidders shall not have the right to modify their Bids due to a Purchaser request for extension of the Bid validity unless expressly stated in such request.

2.11 Bid Guarantee

2.11.1 The Bidder shall furnish with its Bid a guarantee in an amount equal to **Three Hundred Thousand EURO (€300,000)** with a validity equal to that of the Bid as expressed in paragraph 2.10.1. The Bid Guarantee shall be substantially similar to paragraph 7BOOK I - ANNEX C as an irrevocable, unqualified and unconditional Standby Letter of Credit (SLC) issued by a Belgian banking institution fully governed by Belgian legislation or issued by a non-Belgian financial institution and confirmed by a Belgian banking institution fully governed by Belgian legislation. In the latter case signed original letters from both the issuing institution and the confirming institution must be provided. The confirming Belgian bank shall clearly state that it will guarantee the funds, the drawing against can be made by the NCI Agency at its premises in Belgium. Bid Guarantees shall be made payable to the Treasurer, NCI Agency.

2.11.2 Alternatively, a Bidder may elect to post the required Guarantee by certified cheque. If the latter method is selected, Bidders are informed that the Purchaser will cash the cheque on the Bid Closing Date.

2.11.3 If the Bid Closing Date is extended after a Bidder's financial institution has issued a Bid Guarantee, it is the obligation of the Bidder to have such Bid Guarantee (and confirmation, as applicable) extended to reflect the revised Bid Validity date occasioned by such extension.

2.11.4 Failure to furnish the required Bid Guarantee in the proper amount, and in the proper form and for the appropriate duration by the Bid Closing Date may be cause for the Bid to be determined non-compliant.

2.11.5 In the event that a Bid Guarantee is submitted directly by a banking institution, the Bidder shall furnish a copy of said document in the Bid Administration Package.

2.11.6 The Purchaser will make withdrawals against the amount stipulated in the Bid Guarantee under the following conditions:

2.11.6.1 The Bidder has submitted a Bid and, after Bid Closing Date (including extensions thereto) and prior to the selection the compliant Bid determined to represent the best value, withdraws its Bid, or states that he does not consider its Bid valid or agree to be bound by his Bid; or

2.11.6.2 The Bidder has submitted a compliant Bid determined by the Agency to represent the best value, but the Bidder declines to sign the Contract offered by the Agency, such Contract being consistent with the terms of the IFB;

2.11.6.3 The Purchaser has offered the Bidder the Contract for execution but the Bidder has been unable to demonstrate compliance with the security requirements of the Contract within a reasonable time; or

2.11.6.4 The Purchaser has entered into the Contract with the Bidder but the Bidder has been unable or unwilling to provide the Performance Guarantee required under the terms of the Contract within the time frame required.

2.11.7 Bid Guarantees will be returned to Bidders as follows:

2.11.7.1 to non-compliant Bidders forty-five (45) days after notification by the Purchaser of a non-compliant Bid (except where such determination is challenged by the Bidder; in which case the Bid Guarantee will be returned forty-five (45) days after a final determination of non-compliance);

2.11.7.2 to all other unsuccessful Bidders within thirty (30) days following the award of the Contract to the successful Bidder;

2.11.7.3 to the successful Bidder upon submission of the Performance Guarantee required by the Contract or, if there is no requirement for such a Performance Guarantee, upon Contract execution by both parties;

2.11.7.4 pursuant to paragraph 2.10.4.2 above.

2.11.8 "Standby Letter of Credit" or "SLC" as used herein, means a written commitment by a Belgian financial institution either on its own behalf or as a confirmation of the Standby Letter of Credit issued by a non-Belgian bank to pay all or part of a stated amount of money, until the expiration date of the letter, upon presentation by the Purchaser of a written demand therefore. Neither the financial institution nor the Contractor can revoke or condition the Standby Letter of Credit. The term "Belgian financial institution" includes non-Belgian financial institutions licensed to operate in Belgium.

2.12 Cancellation of IFB

2.12.1 The Purchaser may cancel, suspend or withdraw for re-issue at a later date this IFB at any time prior to Contract award. No legal liability on the part of the Purchaser for payment of any sort shall arise and in no event will any Bidder have cause for action against the Purchaser for the recovery of costs incurred in connection with preparation and submission of a Bid in response to this IFB.

2.13 Electronic Transmission of Information and Data

2.13.1 The Purchaser will endeavour to communicate answers to requests for clarification and Amendments to this IFB to the prospective Bidders as soon as practicable.

2.13.2 Bidders are cautioned that the Purchaser will rely exclusively on electronic mail communication to manage all correspondence related to this IFB, including IFB Amendments and clarifications.

2.14 Supplemental Agreements

2.14.1 Bidders are required, in accordance with the certificate in paragraph 6.7 of these Instructions to Bidders, to disclose any prospective Supplemental Agreements that are required by national governments to be executed by NATO/NCI Agency or successor organisations as a condition of Contract performance.

2.14.2 Supplemental Agreements are typically associated with, but not necessarily limited to, national export control regulations, technology transfer restrictions and end user agreements or undertakings.

2.14.3 Bidders are cautioned that failure to provide full disclosure of the anticipated requirements and the terms thereof, to the best of the Bidder's knowledge and experience, may result in the Purchaser withholding award of the Contract or cancelling an executed Contract if it is discovered that the terms of such Supplemental Agreements contradict salient conditions of the Prospective Contract to the extent that either key objectives cannot be accomplished or basic Contract principles and Purchaser rights have been abridged.

2.15 Notice of Limitations on Use of Intellectual Property Delivered to the Purchaser

2.15.1 Bidders are instructed to review Clause 30 of the Contract General Provisions set forth Part III of Book II herein. This Clause sets forth the definitions, terms and conditions regarding the rights of the Parties concerning Intellectual Property developed and/or delivered under this Contract or used as a basis of development under this Contract.

2.15.2 Bidders are required to disclose, in accordance with paragraph 6.10, 6.11, the Intellectual Property proposed to be used by the Bidder that will be delivered with either Background Intellectual Property Rights or Third Party Intellectual Property Rights. Bidders are required to identify such Intellectual Property and the basis on which the claim of Background or Third Party Intellectual Property is made.

2.15.3 Bidders are further required to identify any restrictions on Purchaser use of the Intellectual Property that is not in accordance with the definitions and rights set

forth in the Contract concerning use or dissemination of such Intellectual Property.

2.15.4 Bidders are reminded that restrictions on use or dissemination of Intellectual Property conflicting with the objectives and purposes of the Purchaser as stated in the Prospective Contract may result in a determination of non-compliant Bid.

2.16 Receipt of an unreadable electronic bid

2.16.1 If a bid received at the NCI Agency's facility by electronic data interchange

is unreadable to the degree that conformance to the essential requirements of the solicitation cannot be ascertained, the CO immediately shall notify the Bidder that the bid will be rejected unless the Bidder provides clear and convincing evidence:

a) of the content of the bid as originally submitted; and,
b) that the unreadable condition of the bid was caused by Purchaser software or hardware error, malfunction, or other Purchaser mishandling.

2.16.2 A Bid that fails to conform to the above requirements may be declared noncompliant and may not be evaluated further by the Purchaser.

2.16.3 If it is discovered, during either the Price or Technical evaluation, that the Bidder has taken exception to the Terms and Conditions of the Prospective Contract, has qualified and/or otherwise conditioned his offer on a modification or alteration of the Terms and Conditions or the language of theStatement of Work, or has submitted an unreadable electronic bid, the Bidder may be determined to have submitted a non compliant bid.

3 BID PREPARATION INSTRUCTIONS

3.1 General

3.1.1 Bidders shall prepare and submit their Bid in accordance with the requirements and format set forth in this IFB. Compliance with all Bid submission requirements is mandatory. Failure to submit a Bid in conformance with the stated requirements may result in a determination of non-compliance by the Purchaser and the elimination of the Bid from further consideration.

3.1.2 Bidders shall prepare their bid in three (3) parts in the following quantities:

(a) Administrative Package Electronic: 1 scanned PDF copy
sent via e-mail, with physical (nondigital) signatures

(b) Technical Proposal (Part II): Electronic: 1 PDF copy sent via email

(c) Price Proposal (Part III): Electronic: 1 Excel copy sent via email
on the provided template(s)

3.1.3 Bidders shall not simply restate the IFB requirements. A Bid shall demonstrate that the Bidder understands the terms, conditions and requirements of the IFB and shall demonstrate the Bidder's ability to provide all the services and deliverables listed in the Schedules of the prospective Contract.

3.1.4 Bidders are informed that the quality, thoroughness and clarity of the Bid will affect the overall scoring of the Bid. Although the Purchaser may request clarification of the Bid, it is not required to do so and may make its assessment on the content of the Bid as written. Therefore, Bidders shall assume that inconsistencies, omissions, errors, lack of detail and other qualitative deficiencies in the submitted Bid will have a negative impact on the final Best Value score.

3.1.5 Partial Bids will be declared non-compliant.

3.1.6 Bidders are advised that the Purchaser reserves the right to incorporate the successful Bidder's Offer in whole or in part by reference in the resulting Contract.

3.1.7 If no specific format has been established for electronic versions, Bidders shall deliver documentation in an electronic format which is best suited for review and maintenance by the Purchaser (e.g., Project Master Schedule in MS Project format, Project Highlight Reports in MS Word).

3.1.8 Bids and all related documentation shall be submitted in the English language.

3.1.9 All documentation submitted as part of the Bid shall be classified no higher than "NATO UNCLASSIFIED".

3.2 Bid Package Content

3.2.1 The complete Bid shall consist of three distinct and separated parts each of which will be send as an individual electronic submission as described in the following subparagraphs. Detailed requirements for the structure and content of each of these packages are contained in these Bidding Instructions.

3.2.2 Part 1 is the Bid Administration Package, containing the documents specified in paragraph 3.3 below. This shall be provided as a single PDF file, with scanned (non-digital) signatures.

3.2.3 Part 2 is the Technical Proposal consisting of three volumes as specified below. This shall be provided as a PDF files separately for each Volume.

    3.2.3.1 Volume 1 – Management and Risk with the Executive Summary with Technical Proposal Cross Reference Matrix and Management and Risk, and shall also include:
- a) Bidder Qualifications and Key Personnel;
- b) Project Milestone with delivery schedule;
- c) Initial Project Management Plan (PMP) and Work Breakdown Structure;
- d) Project Management Communication plan showing in particular: approach to status reporting, communications tool and web space;
- e) Initial Risk Management Plan with Risk Log.

    3.2.3.2 Volume 2 – Engineering shall include (but not be limited to):
- a) Initial System Design Specifications (SDS);
- b) Initial Project Implementation Plan (PIP);
- c) Initial Security Risk Assessment (SRA) as a part of PIP;
- d) Initial Test Acceptance Plan (TAP).

    3.2.3.3 Volume 3 – Supportability shall include (but not be limited to):
- a) Initial Itegrated Logistic Support Plan (ILSP);
- b) Initial Configuration Management Plan (CMP);
- c) Initial Quality Assurance Plan (QAP);
- d) Maintenance and Support Concept.

3.2.4 Part 3 is the Price Quotation. This shall be provided as a completed Excel file, using the Excel file provided in the IFB.

3.2.5 Bidding instructions describing the expected contents of each of the Bid Parts follows in this Section of the Bidding Instructions.

3.3 Part 1 – Bid Administration Package

3.3.1 The Bid Administration Package must include the original of the Bid Guarantee required by paragraph 2.11 of the Bidding Instructions. If the Bid Guarantee is sent to the Purchaser directly from the Bidder's bank, a letter, in lieu of the actual Guarantee, shall be included specifying the details of the transmittal and a copy of the Guarantee. Bidders are reminded that the Bid Guarantee shall

reflect any extensions to the Bid Validity Date due to extensions in the Bid Closing Date.

3.3.2 Bidders shall complete and return the IFB/ Bid Requirements Cross Reference Matrix (BRCM) (see instructions in paragraph 8 Annex D) covering the full Prospective Contract and Bidding Instructions where required. It is the Bidders responsibility to ensure that the submitted IFB Cross-Reference Table covers all sections of the IFB technical requirements.

3.3.3 The Package shall include the Certificates set forth in paragraph 6 Annex B to these Bidding Instructions, signed in the original by an authorised representative of the Bidder. The Certificates are as follows:

3.3.3.1 Annex B-1 – Certificate of Legal Name of Bidder;

3.3.3.2 Annex B-2 – Acknowledgement of Receipt of IFB Amendments and Responses to Clarification Requests;

3.3.3.3 Annex B-3 – Certificate of Independent Determination;

3.3.3.4 Annex B-4 – Certificate of Bid Validity;

3.3.3.5 Annex B-5 – Certificate of Exclusion of Taxes, Duties and Charges;

3.3.3.6 Annex B-6 – Comprehension and Acceptance of Contract Special and General Provisions;

3.3.3.7 Annex B-7 – Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements with the prospective text of such Agreements, as applicable;

3.3.3.8 (Annex B-8 – Certificate of Compliance AQAP 2110:2016 or ISO 9001:2015 or Equivalent) with a copy of the relevant quality certification attached to it;

3.3.3.9 Annex B-9 – List of Prospective SubContractors;

3.3.3.10 Annex B-10 – Bidder Background IPR);

3.3.3.11 Annex B-11 – List if SubContractors IPR;

3.3.3.12 Annex B-12 – Certificate of Origin of Equipment, Services, and Intellectual Property;

3.3.3.13 Annex B-13 – List of Proposed Key Personnel;

3.3.3.14 Annex B-14 – Certificate of Price Ceilings;

3.3.3.15 Annex B-15 – Copies of Power of Attorney or equivalent (where relevant) for Principle Contractor as required by Book 1 paragraph 2.1.1 (if relevant);

3.3.3.16   Annex B-16 – Disclosure of Involvement of Former NCI Agency Employment;

3.3.3.17   Annex B-17 – Comprehension and Intention to Comply with PMIC Exclusion Clause and Conflict of Interest.

3.3.4   In accordance with paragraph 3.2.2, the administrative package shall be contained on a single email submission.

3.4   Part 2 – Technical Proposal

3.4.1   Bidders shall provide all the information required by these Bid Preparation Instructions. To facilitate Bidding and the subsequent evaluation of the Bidder's response to the various sections of the SOW, the Bidders Technical Proposal shall be organised and submitted in three volumes as described in the paragraphs that follow.

3.4.2   The Bidders shall assure Bid compliance with SoW and SRS requirements

3.4.3   Pages of each and every document shall be clearly readable and use a font no smaller than 12 point.

3.4.4   Bidding instructions related to each of the three (3) volumes are provided in Sections 3.4.5 through 3.4.7.

3.4.5   Volume 1 - Management and Risk (including the Executive Summary)

    3.4.5.1   As well as an Executive Summary and Table of Contents for the whole Technical Bid this volume addresses the Bidder's understanding of the strategic aims of the SOA & IdM Platform project and the high level requirements related to vision, purpose, objectives and scope. The Purchaser requires that all 'shall' statements from all sections SOW be addressed in this volume.

    3.4.5.2   This volume also addresses requirements for Milestones, Project Management, Risk, and Documentation contained in SOW Sections 4, 5 and Annex F and G.

    3.4.5.3   This volume shall also contain a Bid Requirements Cross Reference Matrix (BRCM), indicating where in the Bid the Bidder addresses each of the 'shall' statements in the SOW, in the format indicated in paragraph 8 BOOK I - ANNEX D.

  3.4.5.4 Executive Summary

    3.4.5.4.1 Bidders shall provide an overview of the salient features of their technical Bid in the form of an executive summary.

    3.4.5.4.2 This summary shall provide a general description of the major points contained in each of the required sections of the technical Bid and shall demonstrate the depth of the Bidder's understanding of: the

project, the implementation environment, the problems and risks of project implementation foreseen by the Bidder, as well as the Bidder's ability to communicate high level concepts in an appropriate and succinct manner. The Bidder shall highlight the strengths which it and its team bring to the project in terms of minimising the problems and reducing the risks, and the key points of the technical approach. This summary shall not exceed 15 pages.

3.4.5.4.3 Bidders shall explicitly state in the Executive Summary of their Bid that, should their firm be selected and awarded the Contract resulting from this solicitation, the delivered product(s) and services will comply with the requirements of the SOW.

3.4.5.5 Table of Contents

3.4.5.5.1 Bidders shall compile a detailed Table of Contents which lists not only the section headings but also the major sub-sections, and topic headings of the Bid. Heading, section and subsection titles should be appropriately descriptive in order to permit the Purchaser's Bid evaluation team to locate relevant material expeditiously.

3.4.5.6 Overall Understanding of Requirements

3.4.5.6.1 The Bid must demonstrate the Bidder's understanding of the Purchaser's technical requirements as described in the SOW and specifically address requirements stated in entire SOW and annexes. The strategic vision behind the SOA & IdM Platform project, the objectives, constraints, purpose and scope must all be addressed and related to the technical solution described in the Bid.

3.4.5.7 Bidder Qualifications

3.4.5.7.1 The Bidder shall provide a section which describes the company structure and activities of the prime Contractor. The country in which the prime Contractor is registered shall be identified and the size and location(s) of the company headquarters and subsidiary branches described. Within that structure the location and organizational unit of the office which will manage this Contract shall be identified. This section shall also describe the major activities of the company and how they are distributed across the organisation.

3.4.5.7.2 The Bid shall provide a description of the corporate capabilities of the Bidder, including corporate experience, corporate structure and individual skills and experience. The Bidder shall provide evidence of relevant and recent experience in the design and implementation of projects similar to the SOA & IdM Platform project. The Bidder shall provide a section which describes how the experience and expertise of the prime Contractor and all nominated sub-Contractors will contribute to the successful execution of the Contract.

3.4.5.7.3 The Bidder shall provide a section which identifies its major proposed sub-Contractors for the Project. Major proposed sub-Contractors, for purposes of this section, refer to the criteria set forth in Clause 10 of the Prospective Contract General Provisions entitled "Sub-Contracts". The Bidder shall identify the firm and the nation of origin and describe the contribution which the sub - Contractor is expected to make to the execution of the project. The Bidder shall also provide rationale for the selection of the sub-Contractor and describe the added value the sub-Contractor will bring to the execution of the project.

3.4.5.7.4 Volume 1 shall provide a description of individual skills and experience in relation to the project of all project team members and Subject Matter Experts (SMEs) foreseen to support the project team. The description shall include how each individual expertise and experience will add value to the team.

3.4.5.7.5 Volume 1 shall provide the resumes / Curricula Vitae (CV) and supporting certification documentation (e.g. Prince 2 certificates) of each proposed Key Personnel that meet or exceed the requirements in SOW Section 13.

3.4.5.7.6 The Bidder, except CVs for all personnel nominated to fill Key Roles, shall also provide rationale to explain why each individual nominated for a Key Role has been proposed, having due regard for the requirements for each role expressed in the SOW.

3.4.5.7.7 While the previous paragraphs ask that the Bidder provide descriptions of the individual team members (including the prime) and the expertise and experience they bring to the team, the Bidder shall also present an overall organisational description for its team that makes clear how the team will function, including, as a minimum:

a) evidence that the team is balanced to ensure that the right team composition has been selected from a technical, experience, and managerial point of view;

b) evidence that there are no missing skills or other gaps in the team that would increase risk or otherwise adversely affect the execution of the project;

c) a description of how the work is organised across the team;

d) a description of the internal team management measures, including company executive relationships that ensure that team members perform;

e) evidence that appropriate Contractual and managerial checks are in place to ensure that the team functions in a manner appropriate to deliver the SOA & IdM Platform project, and;

     f)   any other material that will make clear that the Bidder understands how to manage the selected team, that the team composition is optimal, and will remain functional throughout the execution period, to respond to the demands of the SOA & IdM Platform project.

3.4.5.8 Project Management

3.4.5.8.1 In order to demonstrate how the Bidder plans to meet all requirements contained in Sections 5 and 6 of the SOW, and to demonstrate its approach to the management of the execution of the work, the Bidder shall submit initial versions of the following three (3) project management documents called for in the SOW, in a format based on that called for in Annex G of the SOW:

    a)   the Project Management Plan (PMP), including the Work Breakdown Structure called for therein;

    b)   the Risk Management Plan (RMP) with initial Risk Log;

    c)   the Project Management Communications Plan (part of PMP).

3.4.5.8.2 The submitted documents shall include sufficient information to demonstrate the Bidder's understanding of the key challenges involved in the SOA & IdM Platform project, and demonstrate that the Bidder is proposing an approach that can deal with these challenges.

3.4.5.8.3 The Bidder shall demonstrate in the submitted initial three (3) plans how the Project Management Controls required under SOW Section 5 will be implemented during the life of the Contract. In particular the Bidder shall demonstrate that the Project Management Methodology proposed for the project is suitable to the successful execution of the project and shall further describe its approach to achievement of milestones, configuration management and quality assurance.

3.4.5.8.4 The Bidder shall describe its approach to Project Management Communications and explain how requirements for Formal Meetings, Informal Meetings, Status Reports, Project Communications Tools and Project Web Space will be met.

3.4.5.9 Schedule of Project Milestones

3.4.5.9.1 The Bidder shall provide a section which demonstrates its commitment to the achievement of project milestones as described in Section 4 of the SOW. This section shall address the two (2) Waves of the SOA & IdM Platform implementation and be consistent with the schedule information presented in the draft Project Implementation Plan provided above and described in Section 5 and 6 of SOW.

3.4.5.9.2 In its response, the Bidder should include additional subordinate milestones that they plan to achieve which make clear the extent of

parallel activities and the detailed phasing and dependencies of different activities.

3.4.5.9.3 For purposes of Bidding the milestones described in SOW Section 4 must be adhered to. The Purchaser cannot consider a Bid which is predicated on an alternative schedule.

3.4.5.10 Risk

3.4.5.10.1 The Bidder shall submit an initial Risk Management Plan with draft Risk Log describing a minimum of six (6) and a maximum of ten (10) most important risks to the successful completion of the project from its perspective.

3.4.5.10.2 For each risk identified the Bidder shall state the perceived likelihood of the risk becoming a reality, the impact of risk manifesting itself and assess the severity of the impact should that come to pass.

3.4.5.10.3 For each risk identified the Bidder shall describe its proposed mitigation of that risk in the event of it becoming a reality.

3.4.5.10.4 The Bidder shall describe how risks will be managed throughout the execution of the Contract in response to the requirements of SOW Sections 5 and 11.

3.4.5.11 Documentation

3.4.5.11.1 Throughout the SOW, and more in particular Annex G, guidelines are provided on how SOA & IdM Platform documents shall be formatted, delivered, distributed and reviewed. For Bidding purposes, in this volume, a simple affirmation that all requirements will be met is sufficient. Other sections of these Bidding Instructions will indicate where portions of the Bid need to be submitted in accordance with the formats and content described in Annex G.

3.4.6 Volume 2 – Engineering

3.4.6.1 This volume covers the engineering activity in the SOA & IdM Platform project from analysis and design through to delivery, testing and acceptance, and implementation. A substantial response is expected to the design requirements in SOW Section 7 and Annex A, implementation requirements in SOW Section 6 and testing and acceptance requirements of SOW Section 8.

3.4.6.2 System Design Specification

3.4.6.2.1 The Bidder shall provide an initial System Design Specification (SDS), which describes its proposed technical solution and demonstrates its understanding of the requirements in Section 7 and Annex A of the SOW.

3.4.6.2.2 The Bid shall demonstrate a comprehensive understanding of all of the requirements of Section 7 and Annex A of the SOW and describe how every requirement is addressed in the Contractor's SOA & IdM Platform proposed solution.

3.4.6.2.3 The Bid shall describe in the SDS how the following Architecture Principles (see Annex A, SRS, Section 2) have been treated:

3.4.6.2.3.1 Service Orientation;

3.4.6.2.3.2 Runtime Environment;

3.4.6.2.3.3 Enterprise Application Integration;

3.4.6.2.3.4 Microservices;

3.4.6.2.3.5 Service Composition;

3.4.6.2.3.6 Multi-tenancy;

3.4.6.2.3.7 Performance and Scalability;

3.4.6.2.3.8 Event-driven Architecture;

3.4.6.2.3.9 Common Security;

3.4.6.2.3.10 Federated Integration;

3.4.6.2.3.11 Documentation and Guidance.

3.4.6.2.4 The Bid shall describe in the SDS the design solution proposed for the SOA & IdM Platform services.

3.4.6.2.5 The Service Management and Control Toolset must be comprehensively described in the SDS provided with the Bid. In particular requirements related to integration with Enterprise SMC interfaces.

3.4.6.2.6 The Bid must demonstrate a clear understanding of all internal and external interface requirements.

3.4.6.2.7 The Bid shall describe in the SDS how requirements for Continuity of Service, Disaster Recovery and Availability are met.

3.4.6.2.8 The Bid shall comprehensively address all system requirements.

3.4.6.2.9 The Bidder shall describe how the Purchaser Furnished Information and As Is Information provided in Annex C of the SOW have been taken into account in the SDS included in the Bid.

3.4.6.2.10   The Bidder shall demonstrate that he has understood the design process imposed in the SOW by describing his support of the cycle of design reviews and approvals.

3.4.6.2.11   The Bid must include an example of system design documentation which shows an understanding of the Design Deliverable requirements described in SOW: Section 7 and Annex A. Such examples shall include already designed and working solution.

3.4.6.3 Security Accreditation

3.4.6.3.1 The Bidder shall propose in his Bid initial Project Management Plan (PMP), which shall include Security Accreditation (SA) process (see Section SOW 10).

3.4.6.3.2 The Bid shall demonstrate the Bidder's clear and complete understanding of the Security Accreditation process described in SOW Section 10 and describe the role the Contractor will play in providing input to security documentation.

3.4.6.4 Security Measures

3.4.6.4.1 The Bid shall include initial Security Risk Assessment (SRA) as described in SOW Sections 8 and 10.

3.4.6.4.2 The Bidder shall demonstrate an understanding of the Security Measures described in SOW Section 10 and explain how they will feature in SOA & IdM Platform design and implementation.

3.4.6.4.3 The Bidder must assume responsibility for all security measures marked for implementation by the SOA & IdM Platform Contractor and for the integration of those security measures marked as provided by the Purchaser for integration by the SOA & IdM Platform Contractor. The manner in which this will be accomplished must be a feature of the Bidder's SDS.

3.4.6.5 Implementation

3.4.6.5.1 The Bid shall include initial Project Implementation Plan (PIP).

3.4.6.5.2 The Bidder shall provide a detailed account of how the implementation requirements in Section 6 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the services to be implemented.

3.4.6.5.3 The Bid must show clear traceability between the Contractor's design and the implementation activity to be undertaken.

3.4.6.5.4 The Bidder shall assume that all elements of its design must be provided in full at the implementation stage and that no software or business processes exist on site in a reusable form.

3.4.6.5.5 The Bidder shall describe its approach to site surveys as mentioned in Section 9 of SOW, identify the issues to be checked on site and relate the site survey to the overall implementation effort in terms of timing and purpose.

3.4.6.5.6 The Bidder shall describe its Bid for the implementation of a SOA & IdM Platform Reference Environment.

3.4.6.5.7 In all descriptions provided, the Bidder should be clear regarding how its approach minimises disruption to all services.

3.4.6.6   Test and Acceptance

3.4.6.6.1 The Bidder shall include a section in its Bid which takes a comprehensive approach to the testing and acceptance requirements in Section 8 of the SOW and describes how each requirement will be met.

3.4.6.6.2 The Bidder shall describe how the SOA & IdM Platform Reference Environment will be used to support testing activity.

3.4.6.6.3 The Bidder shall describe its Test Strategy and include in its Bid an initial draft Test and Acceptance Plan (TAP), in accordance with the template provided in Annex G of the SOW.

3.4.6.6.4 The test plan shall address how each of the defined requirements shall be tested, the acceptance criteria, the types of testing to be undertaken and the locations at which testing will occur.

3.4.6.6.5 The Bidder shall describe how testing will be conducted, the test documentation to be provided and how test results will be validated and recorded.

3.4.6.6.6 The Bidder shall describe how failures and off specifications will be dealt with during testing.

3.4.6.6.7 The Bidder shall demonstrate a comprehensive understanding of the acceptance procedures at site, wave and full system acceptance levels.

3.4.6.6.8 Test Scenarios

3.4.6.6.8.1 The Bid shall describe the test scenarios which will be developed to support service based testing and provide evidence that processes within services and activities within processes will be tested. The Bid shall describe how test scenarios shall demonstrate that trained Users can exercise the processes successfully within the full range of services to be developed as part of the Contractor's design and within each service that processes for service design, service transition and service operation will all be tested.

3.4.6.7 Purchaser Furnished Information, Equipment (PFI, PFE), Infrastructure and Services referenced at SOW Annex C.

    3.4.6.7.1 The Bid shall demonstrate a clear understanding of Purchaser Furnished Information, Equipment, Infrastructure and Services (PFE) and shall describe how the Bidder proposes to make use of PFE during the execution of the Contract.

3.4.7 Volume 3 – Supportability

    3.4.7.1 This volume of the Technical Bid describes the Bidder's approach to support and supportability requirements as described in SOW Section 14.

    3.4.7.2 Integrated Logistics Support (ILS)

        3.4.7.2.1 The Bidder shall provide a detailed account of how the Integrated Logistics Support (ILS) requirements in Section 14 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Logistics Support Analysis (LSA) process and Reliability, Availability, Maintainability and Testability (RAMT) activities.

        3.4.7.2.2 The Bidder shall include in its Bid a draft Integrated Logistics Support Plan (ILSP) which describes how the Bidder shall fulfil all ILS requirements during the life of the project. The Bidder shall describe its ILS organisation and responsibilities in relation to other disciplines in the project.

        3.4.7.2.3 The Bidder shall describe its ILS procedures regarding how the Maintenance and Support Concept described in the ILS will be designed, implemented, demonstrated and delivered.

        3.4.7.2.4 The Bidder shall demonstrate how the supply support and how the PHST (Packaging, Handling Storage and Transportation) activities are designed and integrated in the Maintenance and Support Concept, also described in SOW Section 14 and Annex B.

        3.4.7.2.5 The Bidder shall demonstrate how the Technical documentation and training are designed, implemented validated and delivered.

        3.4.7.2.6 The Bidder shall include in the ILS Plan the CLS plan as described in the SOW (Section 14), which describes how the optional CLS Contract will be managed and implemented.

        3.4.7.2.7 The Bidder shall demonstrate that all ILS activities and milestones are integrated into the project's master schedule.

        3.4.7.2.8 The Bidder shall include the draft ILS Plan how the required LSA support cases will be developed. The Bidder shall describe its approach to all the LSA required analysis. The Bidder shall explain how the LSA activities are integrated into the analysis, design and test activities of the project. The Bidder shall demonstrate that all LSA

activities and milestones are integrated into the project's master schedule. The Bidder shall also demonstrate that its RAMT activities are consistent with the RAMT requirements in the System Requirements Specification.

3.4.7.3   Configuration Management (CM)

3.4.7.3.1 The Bidder shall provide a detailed account of how the Configuration Management requirements in Section 12 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Configuration Management Process and Configuration Baseline management

3.4.7.3.2 The Bidder shall include in its Bid a draft Configuration Management Plan (CMP) which describes how the Bidder shall fulfil all configuration Management requirements during the life of the project. The Bidder shall describe its configuration Management organisation and responsibilities in relation to other disciplines in the project. The Bidder shall describe its CM procedures regarding Configuration Item Identification and documentation; configuration Control; Engineering Change Process, configuration Status Accounting, Versioning and auditing. The Bidder shall demonstrate that all CM activities and milestones are integrated into the project's master schedule.

3.4.7.4   Quality Assurance and Control

3.4.7.4.1 The Bidder shall provide a detailed account of how the Quality Assurance requirements in Section 11 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Quality Assurance Process management.

3.4.7.4.2 The Bidder shall include in its Bid a draft Quality Assurance Plan (QAP) which describes how the Bidder shall fulfil all QA requirements during the life of the project. The Bidder shall describe its configuration QA organisation and responsibilities in relation to other disciplines in the project. The Bidder shall describe its QA procedures related to the design, development, verification and qualification and of the support of the product. The Bidder shall demonstrate that all QA activities and milestones are integrated into the project's master schedule.

3.4.7.5   Training

3.4.7.5.1 The Bidder shall provide a detailed account of how the Training requirements in Section 14.7 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Training Process Management.

3.4.7.5.2 The Bidder shall include in its Bid a draft Training Plan which describes how the Bidder shall fulfil all Training requirements during

the life of the project. The Bidder shall describe its configuration Training organisation and responsibilities in relation to other disciplines in the project. The Bidder shall provide some Training example from similar training programmes. The Bidder shall demonstrate that all Training activities and milestones are integrated into the project's master schedule.

3.4.7.6   Maintenance and Support

3.4.7.6.1 The Bidder shall include in its Bid a draft Maintenance and Support Concept as described in SOW Section 14.3-14.4 and SOW Annex B.

3.5   Part 3 – Price Quotation

3.5.1   The Price Quotations shall be submitted in electronic form and contain the following documentation and media:

3.5.1.1 Annex A-1 (paragraph 5) "Bidding Sheets" and, as an Annex, the complete set of sheets contained in the electronic file "2- IFB-CO-14176-SOA-IDM - Bidding Sheets.xls" submitted as part of this IFB; and

3.5.2   Bidders shall prepare their Price Quotation by completing the Bidding Sheets referred in paragraph 3.5.1.1 above, in accordance with the Bid Package Content instructions specified in paragraph 3.2.4.

3.5.3   The structure of the Bidding Sheets shall not be changed, other than as indicated elsewhere, nor should any quantity or item description in the Bidding Sheets. The currency(ies) of each Contract Line Item and sub-item shall be indicated by the Bidder. The prices provided shall be intended as the comprehensive total price offered for the fulfilment of all requirements as expressed in the IFB documentation including but not limited to those expressed in the SOW.

3.5.3.1 Bidders shall furnish Firm Fixed Prices for all required items in accordance with the format set forth in the Instructions for preparation of the Bidding Sheets.

3.5.3.2 Bidders shall furnish Firm Fixed Prices for the Work Packages of Wave 1 and the each Optional Work Package of Wave 2. Purchaser evaluation of the submitted Bids will be on the basis of the complete submission including administrative, price and technical components for the two (2) Waves.

3.5.3.3 Offered prices shall not be "conditional" in nature. Any comments supplied in the Bidding Sheets which are conditional in nature, relative to the offered prices, may result in a determination that the Bid is non-compliant.

3.5.3.4 Bidders are responsible for the accuracy of their Price Quotations. Price Quotations that have apparent computational errors may have such errors resolved in the Purchaser's favour or, in the case of gross omissions, inconsistencies or errors, may be determined to be non-compliant.

3.5.3.5 Bidders shall quote in their own national currency. Bidders may also quote in other than their national currency if it can be demonstrated that the Bidder is expected to incur equivalent costs in that/those currency(ies), for example through sub-Contracts or purchased materials/services. In these cases, a Bidder may express its Bid price in multiple currencies.

3.5.3.6 Bidders are informed that the Purchaser, by virtue of its status stipulated in the provisions of the NATO Communication and Information Organisation (NCIO) Charter, Article 67(e)(3), is exempt from all direct and indirect taxes (e.g., VAT), and all customs duties on merchandise imported or exported. The stated provision reads as follows:

> *"Each participating nation undertakes to grant to NCI Agency under the terms of Articles 9 and 10 of the Ottawa Agreement, exemption from all direct taxes (except rates, taxes and dues which are no more than charges for public utility services) from the taxes on the sale of movable and immovable properties, and from customs and excise duties in respect of equipment imported or exported by NCI Agency or its appointed agents."*

3.5.3.7 Bidders shall therefore exclude from their price Bid all taxes, duties and customs charges from which the Purchaser is exempted by international agreement and are required to certify that they have done so through execution of the Certificate at 6.5.

3.5.3.8 Unless otherwise specified in the instructions for the preparation of Bidding Sheets, all prices quoted in the Bid shall be on the basis that all deliverable items shall be delivered on the basis of Delivery Duty Paid (DDP) in accordance with the International Chamber of Commerce INCOTERMS.

3.5.3.9 The Bidder's attention is directed to the fact that Price Quotation shall contain no document and/or information other than the priced copies of the Bidding Sheets. Any other document will not be considered for evaluation.

3.5.3.10 All prices Bid shall be clearly traceable in the detailed Bidding Sheets.

3.5.3.11 Any adjustment or discount to prices should be clearly traceable to the lowest level of break down in the Bidding Sheets and should not be aggregated or summed. Any lack of clarity or traceability may render the Bid non-compliant.

4 BID EVALUATION AND CONTRACT AWARD

4.1 General

4.1.1 The evaluation of Bids will be made by the Purchaser solely on the basis of the requirements specified in this IFB.

4.1.2 All Bids will be evaluated solely using the formulae, evaluation criteria and factors contained herein. Technical Bids will be evaluated strictly against the technical criteria and not against other Technical Bids submitted.

4.1.3 The evaluation of Bids and the determination as to the Best Value Score will be based only on that information furnished by the Bidder and contained in its Bid. The Purchaser shall not be responsible for locating or securing any information that is not identified in the Bid.

4.1.4 The Bidder shall furnish with its Bid all information requested by the Purchaser in Book 1, Section 3 Bid Preparation Instructions. Significant omissions and/or cursory submissions will result in a reduced Best Value Score and may result in a determination of non-compliance without recourse to further clarification. The information provided by the Bidder in its Bid shall be to a level of detail necessary for the Purchaser to fully comprehend exactly what the Bidder proposes to furnish as well as its approach and methodologies.

4.1.5 During the evaluation, the Purchaser may request clarification of the Bid from the Bidder and the Bidder shall provide sufficient detailed information in connection with such requests as to permit the Purchaser to make a final assessment of the Bid based upon the facts. The purpose of such clarifications will be to resolve ambiguities in the Bid and to permit the Bidder to state its intentions regarding certain statements contained therein. The purpose of the clarification stage is not to elicit additional information from the Bidder that was not contained in the original submission or to allow the Bidder to supplement cursory answers or omitted aspects of the Bid. The Bidder is not permitted any cardinal alteration of the Bid regarding technical matters and shall not make any change to its price quotation at any time.

4.1.6 The Purchaser reserves the right, during the evaluation and selection process, to verify any statements made concerning experience, facilities, or existing designs or materials by making a physical inspection of the Bidder's facilities and capital assets. This includes the right to validate, by physical inspection, the facilities and assets of proposed subContractors.

4.1.7 The evaluation will be conducted in accordance with NATO Infrastructure Bidding Procedures as set forth in the document, and the Best Value evaluation procedures set forth in AC /4-D/2261-ADD2 dated 24 July 2009, AC/4-D(2008)0002-REV1-AS1 dated 23 July 2009 and AC/4(2008)0002-REV2 dated 15 July 2015. "Procedures and Practices for Conducting NSIP International Competitive Bidding Using Best Value Methodology". The Bid evaluation methodology to be followed, including the top-level evaluation criteria and their weighting factors, were agreed by the NATO Infrastructure Committee.

4.2 Best Value Award Approach and Bid Evaluation Factors

4.2.1 The Contract resulting from this IFB will be awarded to the Bidder whose conforming offer provides the Best Value to NATO, as evaluated by the Purchaser in compliance with the requirements of this IFB and according to the evaluation method specified in this Bid Evaluation and Contract Award.

4.2.2 The overall score for each compliant Bidder will be derived using the following formula:

Best Value Score = ((M + R) + E + S)*60%+P*40%

where the following is the breakdown of the non-price element:

M = Management Weighted Score (20% of the non-price element);

R = Risk (10% of the non-price element)

E = Engineering Weighted Score (50% of the non-price element);

S = Supportability Weighted Score (20% of the non-price element).

4.2.3 The maximum possible Best Value Score is 100; the minimum possible is zero. The Bid with the highest Best Value Score will be will be recommended to be the Apparent Successful Bidder.

4.2.4 Technical Evaluation Criteria

4.2.4.1 The Second Level Evaluation Criteria shown above are further divided into Third Level Criteria in each area. These Third Level Criteria are provided in paragraph 4.3 and its subparagraphs in descending order of importance under each of the Second Level Criteria. The Third Level Criteria are also weighted and aggregate to the total weight of the respective Second Level. The exact weights are not published, nor are these weights made available to the Purchaser evaluation team. These weights are kept sealed until after the price evaluation and known only to the Chairman of the Agency Contracts Award Board and the technical lead who proposed the numerical weighting factors. The technical lead is not on the Evaluation Team.

4.2.5 Price Evaluation

4.2.5.1 Price (P): 40% weight, with the Weighted Price Score (P) derived using the following formula:

*Price Score = 100 * (1-(Bid Price / 2*Average Bid Price))*

4.2.5.1.1 Using this formula, a price quotation that is exactly equal to the average price of all Bids would receive a score of 20 of the 40 points available. A price quotation that is one-half of the average price of all Bids would receive a score of 30 of the 40 points available, and a price quotation of two times the average Bid price would receive a score of 0. Price Quotations in excess of two times the average Bid price would likewise receive a score of 0, even though the formula would generate a negative figure.

4.2.5.1.2 Bidders are advised that the total price of CLINs Comprising Waves 1 and 2 and the associated Operation and Support CLINs should not exceed 48,974,593 Euro (Best Value Ceiling - BVC), as described in

6.14: Annex B-14 – Certificate of Price . Bids submitted in excess of <u>one or more</u> of the stated thresholds will be deemed as non-compliant and disqualified..

4.2.5.2 Technical ((M + R) + E + S): 60% weight

4.2.5.2.1 The technical evaluation will be based on the high level criteria indicated at the beginning of Section 4.2.

4.2.5.2.2 The Purchaser's priorities in the evaluation of the Technical Bid are described in the form of sub criteria in Section 4.3.3 of this document. The sub criteria are listed in an order that reflects the relative importance that the Purchaser places on each sub criterion, from highest importance to lowest.

4.3 Evaluation Procedure

4.3.1 The evaluation will be done in a four step process, as described below:

4.3.1.1 Step 1: Administrative Compliance

4.3.1.1.1 Bids received shall be reviewed for compliance with the mandatory Administrative requirements specified in paragraph 4.3.2. Bids not meeting all of the mandatory requirements may be determined to be non-compliant and not further considered in the evaluation or for award.

4.3.1.1.2 All Bid Bid Guarantees shall be reviewed for compliance with the mandatory Administrative requirements specified in paragraphs 4.3.2 and 2.11.

4.3.1.2 Step 2: Technical Evaluation

4.3.1.2.1 In Step 2 Bids will have their Technical Bids Packages evaluated against predetermined top-level criteria and identified sub-criteria (see paragraph below), and scored accordingly. This evaluation will result in "raw" or not weighted technical scores against the criteria.

4.3.1.2.2 Bidders are advised that any Bid whose Technical Bid receives a score of less than 20% of the not weighted raw score possible in any of the sub-criteria listed in Section 4.3 of this document may be determined by the Purchaser to be non-compliant and not further considered for award.

4.3.1.3 Step 3: Price Evaluation

4.3.1.3.1 The Price Quotations of all Bids remaining after Step 2 will be opened, evaluated and scored in accordance with paragraph 4.3.4 and 4.3.5.

4.3.1.4 Step 4: Determination of Apparently Successful Bidder

4.3.1.4.1 Upon completion of the Price Evaluation, the Apparent Successful Bid will be determined in accordance with paragraph 4.3.5 hereafter.

4.3.2 Evaluation Step 1 – Administrative Compliance

4.3.2.1 Bids will be reviewed for compliance with the formal requirements for Bid submission as stated in this IFB and the content of the Administrative Documentation Package. The evaluation of the Administrative Documentation Package will be made on its completeness, conformity and compliance to the requested information. This evaluation will not be scored in accordance with Best Value procedures but is made to determine if a Bid complies with the requirements of the Bidding Instructions and Prospective Contract. Specifically, the following requirements shall be verified:

4.3.2.1.1 The Bid was received by the Bid Closing Date and Time;

4.3.2.1.2 The Bid is packaged and marked properly;

4.3.2.1.3 The Bid Administration Package contains the documentation listed in paragraph 3.3 above and complies with the formal requirements established in paragraph 3.1 above;

4.3.2.1.4 The Bidder has not taken exception to the Terms and Conditions of the Prospective Contract or has not qualified or otherwise conditioned its offer on a modification or alteration of the Terms and Conditions or the language of the SOW; and

4.3.2.1.5 Evaluation of Conflict of Interest Documentation:

4.3.2.1.5.1 The Purchaser will evaluate the Bidder submission as detailed in Book I Section 3 and resort to the disqualification of the Bid in those cases in which it is deemed that the Bidder's relationships with the industrial entities identified in Book I Section 3 could constitute a real or apparent conflict of interest, could in any manner or form influence or appear to influence the capacity of the Bidder to render unbiased service or otherwise result in an advantage during the course of the performance under the prospective Contract and any proposed conflict of interest mitigation plan proposed by the Bidder does not satisfactory resolve the conflict of interest in place.

4.3.2.1.5.2 Conversely, should the Purchaser deem that the Bidder's Conflict of Interest Mitigation Plan adequately addresses the concerns relevant to any conflict of interest, it will make such plan part of any awarded Contract and subject to the stipulation of Clause 29 of the prospective Contract Special Provisions. Equally in those cases where the Bidder declares that no apparent or real conflict of interest exists such condition shall be reflected in any resulting Contract and made subject to the prescription of Clause 29 of the prospective Contract Special Provisions.

4.3.2.1.5.3   In the event that, during the evaluation of the Bids, the Purchaser would determine or suspect that the Bidder has not disclosed a real or apparent conflict of interest of which it was knowledgeable at the time of Bid submission, in breach of above paragraphs 4.3.2.1.5.1 and 4.3.2.1.5.2, the Purchaser reserves the right to declare the Bid non-compliant.

4.3.2.2   A Bid that fails to conform to the above requirements may be declared non-compliant and may not be evaluated further by the Purchaser.

4.3.2.3   Bids that are determined to be administratively compliant will proceed to Step 2, Technical Evaluation.

4.3.2.4   Notwithstanding paragraph 4.3.2.3, if it is later discovered in the evaluation of the Administrative Package, Technical Bid or the Price Quotation that the Bidder has taken exception to the Terms and Conditions of the Prospective Contract, or has qualified and/or otherwise conditioned its offer on a modification or alteration of the Terms and Conditions or the language of the SOW, the Bidder may be determined to have submitted a non-compliant Bid at the point in time of discovery.

4.3.2.5   All Bid Bid Guarantees shall be reviewed for compliance with the mandatory Administrative requirements specified in paragraphs 2.11 and 4.3.2.1.

4.3.3   Evaluation Step 2 – Technical Evaluation

4.3.3.1   The Technical Bid will be evaluated against the criteria set forth in paragraph 4.2 above. In this section those criteria will be expanded to identify third-level criteria considered important by the Purchaser during Bid evaluation. Sub criteria appear in descending order of importance within the criterion of which they form a part. Within each of the three volumes of the Technical Bid the criteria and their sub criteria are identified as follows:

4.3.3.2   Volume 1 – Management and Risk (including the Executive Summary)

4.3.3.2.1   Criteria – Management (20% of the Technical Bid): third-level sub criteria in descending order of importance:

4.3.3.2.1.1 Understanding of the strategic aims, objectives and scope;

4.3.3.2.1.2 Bidder Qualifications and Key Personnel;

4.3.3.2.1.3 Commitment to Project Milestones and a schedule which shows how they will be achieved;

4.3.3.2.1.4 Quality and completeness of the initial Project Management Plan and Work Breakdown Structure;

4.3.3.2.1.5 Quality of the Project Management Communications proposed in the bid. In particular the approach to status reporting, communications tools and web space;

4.3.3.2.1.6 Compliance with requirements. In particular completeness and quality of the PFE list, and commitment to integrate with PFE.

4.3.3.2.1.7 Adequacy of the Project Management Controls proposed in the bid. In particular the management methodology to be used and the approach to configuration management and quality control;

4.3.3.2.1.8 Quality of the Executive Summary.

4.3.3.2.2 Criteria – Risk (10% of the Technical Bid): third-level sub criteria in descending order of importance.

4.3.3.2.2.1 Overall level of risk according to the initial Risk Log;

4.3.3.2.2.2 Quality of the draft Risk Log submitted with the Bid and the relevance of the risks identified;

4.3.3.2.2.3 Adequacy and pertinence of the mitigation measures proposed for the risks identified in the initial Risk Log;

4.3.3.2.2.4 Adequacy of the Bidder's proposal to manage risk throughout the project.

4.3.3.3 Volume 2 – Engineering

4.3.3.3.1 Criteria – Engineering (50% of the Technical Bid): sub criteria in descending order of importance:

4.3.3.3.1.1 Quality and completeness of the initial System Design Specification (SDS);

4.3.3.3.1.2 Quality and completeness of the initial Project Implementation Plan (PIP), including site survey process;

4.3.3.3.1.3 Quality and completeness of the testing process and initial Test and Acceptance Plan (TAP);

4.3.3.3.1.4 Quality and completeness of the initial Security Risk Assessment;

4.3.3.3.1.5 Quality and completeness of the Bidder's approach to meeting the Security Accreditation process requirements.

4.3.3.4 Volume 3 – Supportability

4.3.3.4.1 Criteria – Supportability (20% of the Technical Bid); Third-level sub criteria in descending order of importance:

4.3.3.4.1.1 Sound supportability approach and Operation & Maintenance approach in line with SOW;

4.3.3.4.1.2 Completeness and robustness approach to the Maintenance and Support Concept, in accordance with SOW and SRS;

4.3.3.4.1.3 Completeness and quality of the initial ILSP ensuring that proposed ILS arrangements are optimized and acceptable, and in line with SOW;

4.3.3.4.1.4 Realistic and credible initial Training Plan, and in line with SOW;

4.3.3.4.1.5 Completeness and Quality of the initial CMP, and in line with SOW;

4.3.3.4.1.6 Initial Quality Assurance Plan testifies that QA processes are mature and comprehensive, and in line with SOW.

4.3.4 Evaluation Step 3 – Price Evaluation

4.3.4.1 The Bidder's Price Quotation will be first assessed for compliance against the following criteria:

4.3.4.1.1 The Bid price complies with the requirement relevant to the Bid Ceiling Price.

4.3.4.1.1.1 Total price offered in the price quotation of this Bid in Section 1 of the Bidding Sheets shall not exceed amounts, as described below:

Waves	*Status*	*Cost ceiling*
Wave 1	Costed and Evaluated	€ 10,440,458
Wave 1 O&M	Costed and Evaluated Option	€ 8,903,606
Wave 2	Costed and Evaluated Option	€15,446,725
Wave 2 (O&M)	Costed and Evaluated Option	€ 14,183,804

and 48,974,593 Euro in total as described in paragraph 4.2.5 of Book I. If any one or more of the prices proposed by the Bidders are above the ceilings- then the Bid will be declared non-compliant.

4.3.4.1.2 In particular, the Bidders shall note that the total price stated in Section 1 of the Bidding Sheets shall not exceed the figure quoted in paragraph 4.2.5.1.2. for two Waves. The Price Quotation meets the requirements for preparation and submission of the Price Quotation set forth in the Bid Preparation Section and the Instructions for Preparation of the Bidding Sheets in Annex A-2.

4.3.4.1.3 Detailed pricing information has been provided and is adequate, accurate, traceable, and complete; and

4.3.4.1.4 The Price Quotation meets requirements for price realism and balance as described below in paragraph 4.3.4.4.

4.3.4.2 A Bid which fails to meet the compliance standards defined in this section may be declared non-compliant and may not be evaluated further by the Purchaser.

4.3.4.3 Basis of Price Comparison

4.3.4.3.1 For quotation submitted in other than EURO currency, for the purposes of price comparison, the Purchaser will proceed as follows: The Purchaser will convert all prices quoted into EURO for purposes of comparison and computation of price scores. The exchange rate to be utilised by the Purchaser will be the average of the official buying and selling rates of the European Central Bank at close of business on the last working day preceding the Bid Closing Date.

4.3.4.3.2 The Evaluated Bid Price to be inserted into the formula specified at paragraph 4.2.5.1 will be calculated as follows:
a) Total cumulative amount derived from the sum of the Total Firm Fixed Prices offered for all CLINs;
b) Total cumulative amount derived from the sum of Prices offered for the Total Price of the predetermined optional CLINs.

4.3.4.4 Price Balance and Realism

4.3.4.4.1 In those cases in which the prices quoted in relation with this Invitation for Bid appear to be unreasonably low in relation to the performance required under the prospective Contract and/or the level of effort associated with the tasks, the Purchaser will reserve the right to request the Bidder clarifications aimed to demonstrate the rationale for such circumstances.

4.3.4.4.2 Indicators of an unrealistically low Bid may be the following, amongst others:

4.3.4.4.2.1 Labour Costs that, when amortised over the expected or proposed direct labour hours, indicate average labour rates far below those prevailing in the Bidder's locality for the types of labour proposed;

4.3.4.4.2.2 Direct Material costs that are considered to be too low for the amounts and types of material proposed, based on prevailing market prices for such material; or

4.3.4.4.2.3 Numerous Line Item prices for supplies and services that are provided at no cost or at nominal prices.

4.3.4.4.3 If the Purchaser has reason to suspect that a Bidder has artificially debased its prices in order to secure Contract award, the Purchaser will request clarification of the Bid in this regard and the Bidder shall provide explanation on one of the following bases:

4.3.4.4.3.1 An error was made in the preparation of the price quotation. In such a case, the Bidder must document the nature of the error and show background documentation concerning the preparation of the price quotation that makes a convincing case that a mistake was made by the Bidder. In such a case, the Bidder shall petition the Purchaser to either remain in the competition and accept the Contract at the offered price, or to withdraw from the competition;

4.3.4.4.3.2 The Bidder has a competitive advantage due to prior experience or industrial/technological processes that demonstrably reduce the costs of Bidder performance and therefore the price offered is realistic. Such an argument must support the technical Bid offered and convincingly and objectively describe the competitive advantage and the net savings achieved by this advantage over standard market practices and technology; or

4.3.4.4.3.3 The Bidder recognises that the submitted price quotation is unrealistically low compared to its cost of performance and, for business reasons, the Bidder is willing to absorb such a loss. Such a statement can only be made by the head of the business unit submitting the Bid and will normally be made at the level of Chief Operating Officer or Chief Executive Officer. In such a case, the Bidder shall estimate the potential loss and show that the financial resources of the Bidder are adequate to withstand such reduction in revenue.

4.3.4.4.4 If a Bidder fails to submit a comprehensive and compelling response on one of the basis above, the Purchaser may determine the Bid submitted as non-compliant. If the Bidder responds on the basis of 4.3.4.4.2 above and requests to withdraw from the competition, the Purchaser may, depending on the nature and gravity of the mistake, allow the Bidder to withdraw.

4.3.4.4.5 If the Purchaser accepts the Bidder's explanation of mistake in paragraph 4.3.4.4.3.1 and allows the Bidder to accept the Contract at the offered price, or the Purchaser accepts the Bidder's explanation pursuant to paragraph 4.3.4.4.3.3 above, the Bidder shall agree that the supporting pricing data submitted with its Bid will be incorporated by reference in the resultant Contract. The Bidder shall agree as a condition of Contract signature, that the pricing data will be the basis of determining fair and reasonable pricing for all subsequent negotiations for modifications of or additions to the Contract and that no revisions of proposed prices will be made.

4.3.4.4.6 If the Bidder presents a convincing rationale pursuant to paragraph 4.3.4.4.3.2 above, no additional action will be warranted. The Purchaser, however, reserves its right to reject such an argument if the rationale is not compelling or capable of objective analysis. In such a case the Bid may be determined to be non-compliant.

4.3.4.4.7   The Agency reserves the right to request prime Contractors, or the subContractor to separately identify each of the direct/indirect costs, advise why each is required, and provide supporting documentation to substantiate each charge, such as: 1) catalogue price lists and any applicable discounts, 2) copies of the subContractor's orders from others for the same or similar items, including explanations for cost variations, or 3) subContractor's internal cost estimate, or documentation of whatever means the subContractor used to arrive at the charge.

4.3.4.5   Once the offered prices as described in paragraph 4.3.4.3.2 have been calculated and checked, the formula set forth in paragraph 4.2.5.1 above will be applied to derive the Price Score of each Bid.

4.3.5   Evaluation Step 4 – Calculation of Best Value Scores

4.3.5.1   Upon conclusion and approval of the Price Evaluation results, the pre-determined weighting scheme for the Technical Evaluation will be unsealed and the scores for the Management, Risk, Engineering, and Supportability factors will be calculated for each compliant Bid. Then all partial scores will be fed into the formula stated in paragraph 4.2.2 in order to obtain the Best Value Score of each Bid.

4.3.5.2   The highest scored Bid will be recommended as the Apparent Successful Bid.

4.3.5.3   Should the calculation of the Best Value Scores result in a Statistical Tie between two or more Bids, the Purchaser will recommend among those as Apparent Successful Bid, that which offers the lowest price. For the purpose of this paragraph the term Statistical Tie shall be construed to indicate the situation where the total weighted score of the highest scoring Bid, that is, the weighted score of price and technical combined, is within 1.0% of the total weighted score of one or more of the other Bidders.

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

5   BOOK I - ANNEX A

BIDDING SHEETS

Page Intentionally Left Blank

Annex A Bidding Sheets

See separate Excel Workbook attached
"2- IFB-CO-14176-SOA-IDM -Bidding Sheets.xls"

Bidding Sheets

On behalf of the firm stated below I hereby offer the Purchaser the services and deliverables (collectively referred as "ITEMS") set forth in the attached schedules[1], at the specified prices, and subject to the terms and conditions stated in IFB-CO-14176-SOA-IDM.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Bid Reference _____

---

[1] Bidders shall submit in electronic form the cover page and an electronic copy of the worksheets contained in the file "2- IFB-CO-14176-SOA-IDM -Bidding Sheets.xls" that was submitted to them as part of the IFB package.

5.1 Instructions for the Preparation of Bidding Sheets

5.1.1 INTRODUCTION

Bid pricing requirements as addressed in this Annex are mandatory. Failure to abide to the prescriptions of Bid submission referred in this section may lead to the Bid being declared non-compliant and not being taken into consideration for award.

No alteration of the Bidding sheets including but not limited to quantity indications, descriptions or titles are allowed with the sole exception of those explicitly indicated as allowed in this document. Additional price columns may be added if multiple currencies are Bid, including extra provisions for all totals.

The Purchaser reserves the right to request additional and/or clarifying pricing information after the initial pricing evaluation, and reserves the right to incorporate this information into the resultant Contract. Failure to provide timely and accurate information as requested could lead to a determination of price non-compliance.

5.1.2 GENERAL REQUIREMENTS

Bidders shall follow the specific instructions provided in each worksheet.

Bidders shall insert information in all yellow cells.

The prices and quantities entered on the document shall reflect the total items required to meet the Contractual requirements. The total price shall be indicated in the appropriate columns.

In preparing the Bidding Sheets, Bidders shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part.

All metrics (e.g., cost associated with labour) will be assumed to be standard or normalised to 7.6 hour/day, for a five day working week at NATO sites and Contractor facilities located within Europe and 8 hours/day at NATO sites and Contractor facilities located in the United States.

Should the Bid be in other than Euro currency, the award of the Contract will be made in the currency or currencies of the Bid.

Bidders are advised that formulae are designed to ease evaluation of the Bidders Bid have been inserted in the electronic copies of the Bidding Sheets. Notwithstanding this the Bidder remains responsible for ensuring that their figures are correctly calculated and should not rely on the accuracy of the formulae electronic copies of the Bidding Sheets.

If the Bidder identifies an error in the spreadsheet, it should notify the Purchaser who will make a correction and notify all the Bidders of the update.

Any discounted or reduced prices offered by the Bidder must be traceable to a CLIN or CLINs at the lowest level. Prices and detail of the traceability of application of the discount shall be clearly identified in the supporting detail sheets and applied at the unit price level.

5.1.3   STRUCTURE OF BIDDING SHEETS

The Bidding Sheets provided in MS Office Excel format are organised according to the following structure:

a) Instructions;
b) Section 1. Offer & CLIN Summary sheets;
c) Section 2. Detailed Bidding sheetsfor;
d) Labour,Material,Travel,ODC and Rates.

5.1.4   COMPLETING SECTION 1 (Offer & CLIN Summary Sheets)

5.1.4.1 Section 1 corresponds to the Schedule of Supplies and Services of the Prospective Contract. Each Work Package (WP) included in the Contract is represented by a detailed schedule showing the Contract Line Items (CLINs) included within the scope of the Work Package (Detailed Bidding sheet tabs) and a detailed cost breakdown attached to each WP schedule.

5.1.4.2 Filling in the Offer Summary

Bidders shall fill in the Offer Summary sheet based on the information provided in the CLIN summary sheet. The Offer Summary is a high level summary that separates the offer prices for the each wave, and separates the investment and the Operations and Maintenance offers. CLINs 2.7 and 4.5 are to be summed as the Operations and Maintenance offer. All other CLINs are to be considered investment.

5.1.4.3 Filling the CLIN Summary Sheet

Bidders shall fill in the CLIN summary sheet based on the information provided in the detailed Bidding sheets (CLIN Price Breakdown sheets). The detailed Bidding sheets are broken down in to the categories listed in Section 5. Bidders are expected to aggregate the prices in the detailed Bidding sheets that make up the line items in the CLIN summary sheet. The line items in the CLIN Summary Sheet shall be all INCLUSIVE of the price being Bid in order to fulfil the requirement for the line item in the CLIN Summary Sheet. Bidders shall make sure that the total price indicated in the Detailed Bidding Sheets matches the price stated in the CLIN summary sheet for the same corresponding CLIN or sub-CLIN.

Bidders shall make sure that they have filled all delivery dates in yellow and that these dates comply with the time limits specified in each worksheet and are in accordance with the dates proposed in the proposed Project Master Schedule (Book II, Part 4 – SOW, Sections 4, 5, 7, 8).

5.1.5   COMPLETING SECTION 2 (Detailed Bidding Sheets)

Bidders are instructed to prepare their cost Bids in sufficient detail to permit thorough and complete evaluation. For each of the CLINs the Bidder shall use the separate Sheets as provided, adding additional sheets if multiple currencies are used. Change the currency in the header of the Sheets if necessary.

5.1.5.1 MATERIAL

5.1.5.1.1 Purchased Parts: Provide a consolidated priced summary of individual material quantities included in the various tasks, orders, or Contract line items being proposed and the basis for pricing.

a) Raw Material: Consists of material in a form or state that requires further processing. Provide priced quantities of items required for the Bid. Show total cost.

b) Standard Commercial Items: Consists of items that the Bidder normally fabricates, in whole or in part, and that are generally stocked in inventory. Provide an appropriate explanation of the basis for pricing on attached schedule.

c) The Bidder shall provide a level of detail down the unique sellable item level (e.g.: a server, a laptop, a printer)

d) The Bidder shall provide unit prices that shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the MATERIAL LABOUR OVERHEAD section of the detailed Bidding sheet to the total cost of material.

5.1.5.2 DIRECT LABOUR

Show the hourly rate by year and the total hours for the categories and disciplines of direct labour proposed. Unit prices shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the DIRECT LABOUR OVERHEAD section of the detailed Bidding sheet to the total cost of direct labour.

5.1.5.3   SUBCONTRACT LABOUR

Show the hourly rate by year and the total hours for the categories and disciplines of subContract labour proposed. Unit prices shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the SUBCONTRACT LABOUR OVERHEAD section of the detailed Bidding sheet to the total cost of subContract labour.

5.1.5.4 TRAVEL

Show the number of trips being made, the number of people travelling, the number of days per trip, the cost of traveling (e.g. flight costs), and the daily per diem rate. Insert comments/descriptions/references/explanation of calculation method under the 'Notes' column including the location & reference to SOW.

5.1.5.5 OTHER DIRECT COSTS

5.1.5.5.1 Special Tooling/Equipment. Identify and support specific equipment and unit prices. Use a separate schedule if necessary.

5.1.5.5.2 Individual Consultant Services. Identify and support the proposed contemplated consulting. State the amount of services estimated to be required and the consultant's quoted daily or hourly rate.

5.1.5.5.3 Other Costs. List all other direct charge costs not otherwise included in the categories described above (e.g., services of specialized trades, computer services, preservation, packaging and packing, leasing of equipment, ex-pat costs etc.) and provide bases for pricing.

5.1.6 SPECIAL INSTRUCTIONS

The Biddings sheets have columns for both Wave 1 & 2 activities as referenced at 1.2.2.1 and Annex B-14 (6.14) Wave 1 is the base Contract and subject to the price ceiling for both investment and Operations and Maintenance. Some elements, such a project management, will be common to both waves. The Bidder is expected to fill in these elements that are common the both Wave 1 & 2, in such a manner that only the requirements within each wave are considered for Wave 1 & 2 columns in the Bidding sheets. The Bidder may not place the entirety of a price of an element in Wave 1 column when Wave 2 will require effort/cost. Front loading of the cost in such a manner can make the Bid be determined to be non-compliant. Elements that are inherently only to Wave 1 or just Wave 2, the Bidder shall only fill in the CLIN summary for that element in the appropriate wave.

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

6 BOOK I - ANNEX B

Prescribed Administrative Forms and Certificates

Page Intentionally Left Blank

Annex B Prescribed Administrative Forms and Certificates

6.1   Annex B-1 – Certificate of Legal Name of Bidder

This Bid is prepared and submitted on behalf of the legal corporate entity specified below:

FULL NAME OF CORPORATION: _____

DIVISION (IF APPLICABLE): _____

SUB DIVISION (IF APPLICABLE): _____

OFFICIAL MAILING ADDRESS

_____
_____
_____
_____

E-MAIL ADDRESS: _____

TELEFAX No: _____

POINT OF CONTACT REGARDING THIS BID:

NAME: _____
POSITION: _____
TELEPHONE: _____

ALTERNATIVE POINT OF CONTACT:

NAME: _____
POSITION: _____
TELEPHONE: _____

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.2 Annex B-2 – Acknowledgement of Receipt of IFB Amendments and Responses to Clarification Requests

I confirm that the following Amendments and responses to Clarification Requests to Invitation for Bid CO-14176-SOA-IDM have been received and the Bid, as submitted, reflects the content as such.

Amendment no./Responses to CR release no.	Date of Issued	Date of receipt	Initials

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.3 Annex B-3 – Certificate of Independent Determination

It is hereby stated that:

a) we have read and understand all documentation issued as part of CO-14176-SOA-IDM. Our Bid submitted in response to the referred solicitation is fully compliant with the provisions of the IFB and the prospective Contract.
b) our Bid has been arrived at independently, without consultation, communication or agreement, for the purpose of restricting competition, with any other Bidder or with any competitor;
c) the contents of our Bid have not been knowingly disclosed by the Bidder and will not knowingly be disclosed by the Bidder prior to award, directly or indirectly to any other Bidder or to any competitor; and
d) no attempt has been made, or will be made by the Bidder to induce any other person or firm to submit, or not to submit, a Bid for the purpose of restricting competition.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Bid Reference _____

6.4   Annex B-4 – Certificate of Bid Validity

I, the undersigned, as an authorised representative of the firm submitting this Bid, do hereby certify that the pricing and all other aspects of our Bid will remain valid for a period of twelve months from the Bid Closing Date of this Invitation for Bid.

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.5   Annex B-5 – Certificate of Exclusion of Taxes, Duties and Charges

I hereby certify that the prices offered in the price quotation of this Bid exclude all taxes, duties and customs charges from which the Purchaser has been exempted by international agreement.

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.6 Annex B-6 – Comprehension and Acceptance of Contract Special and General Provisions

The Bidder hereby certifies that he has reviewed the Special Contract Provisions and the NCI Agency General Provisions set forth in the Prospective Contract, Book II of this Invitation for Bid. The Bidder hereby provides its confirmation that he fully comprehends the rights, obligations and responsibilities of the Contractor as set forth in the Articles and Clauses of the Prospective Contract. The Bidder additionally certifies that the offer submitted by the Bidder is without prejudice, qualification or exception to any of the Terms and Conditions and he will accept and aBide by the stated Special and General Provisions if awarded the Contract as a result of this Invitation for Bid.

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.7 Annex B-7 – Disclosure of Requirements for NCI Agency Execution of Supplemental Agreements

I, the undersigned, as an authorised representative of _____, certify the following statement:

All supplemental agreements, defined as agreements, documents and/or permissions outside the body of the Contract but are expected to be required by my Government, and the governments of my subContractors, to be executed by the NCI Agency, or its legal successors, as a condition of my firm's performance of the Contract, have been identified, as part of the Bid.

These supplemental agreements are listed as follows:

Examples of the terms and conditions of these agreements have been provided in our Offer. The anticipated restrictions to be imposed on NATO, if any, have been identified in our offer along with any potential conflicts with the terms, conditions and specifications of the Prospective Contract. These anticipated restrictions and potential conflicts are based on our knowledge of and prior experience with such agreements and their implementing regulations. We do not certify that the language or the terms of these agreements will be exactly as we have anticipated.

The processing time for these agreements has been calculated into our delivery and performance plans and contingency plans made in the case that there is delay in processing on the part of the issuing government(s).

We recognise that additional supplemental agreements, documents and permissions presented as a condition of Contract performance or MOU signature after our firm would be selected as the successful Bidder may be cause for the NCI Agency, or its legal successors, to determine the submitted Bid to be non-compliant with the requirements of the IFB;

We accept that should the resultant supplemental agreements issued in final form by the government(s) result in an impossibility to perform the Contract in accordance with its schedule, terms or specifications, the Contract may be terminated by the Purchaser at no cost to either Party.

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.8 Annex B-8 – Certificate of Compliance AQAP 2110:2016 or ISO 9001:2015 or Equivalent

I hereby certify that _____ (name of Company) possesses and applies Quality Assurance Procedures/Plans that are equivalent to the AQAP 2110 or ISO 9001:2015 as evidenced through the attached documentation[1].

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

---

[1] Bidders must attach copies of any relevant quality certification.

6.9 Annex B-9 – List of Prospective SubContractors

Name and Address of Sub-Bidder	DUNS Number [3]	Primary Location of Work	Items/Services to be Provided	Estimated Value of Sub-Contract

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

---

[3] Data Universal Numbering System (DUNS). Bidders are requested to provide this data in order to help NCI AGENCY to correctly identify SubContractors. If a SubContractor's DUNS is not known this field may be left blank.

6.10 Annex B-10 – Bidder Background IPR

I, the undersigned, as an authorised representative of Bidder _____, warrant, represent, and undertake that:

A. The Contractor Background IPR specified in the table below will be used for the purpose of carrying out work pursuant to the prospective Contract.

ITEM	DESCRIPTION

B. The stated Bidder has and will continue to have, for the duration of the prospective Contract, all necessary rights in and to the Background IPR specified above.

C. The Background IPR stated above complies with the terms specified in Clause 32 of the Special Contract Provisions and shall be licensed to the Purchaser according to the terms and conditions specified in the prospective Contract, and more particularly, in accordance with Clause 32 of the Special Contract Provisions and Clause 30 of the NCIA General Contract Provisions.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Bid Reference _____

6.11 Annex B-11 – List if SubContractors IPR

I, the undersigned, as an authorised representative of Bidder
_____, warrant, represent, and undertake that:

A. The SubContractor IPR specified in the table below will be used for the purpose of carrying out work pursuant to the prospective Contract.

ITEM	DESCRIPTION

B. The stated Bidder has and will continue to have, for the duration of the prospective Contract, all necessary rights in and to the IPR specified above necessary to perform the Contractor's obligations under the Contract.

C. The SubContractor IPR stated above complies with the terms specified in Clause 32 of the Special Contract Provisions and shall be licensed to the Purchaser according to the terms and conditions specified in the prospective Contract, and more particularly, in accordance with Clause 32 of the Special Contract Provisions and Clause 30 of the NCIA General Contract Provisions.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Bid Reference _____

6.12 Annex B-12 – Certificate of Origin of Equipment, Services, and Intellectual Property

The Bidder hereby certifies that, if awarded the Contract pursuant to this solicitation, he will perform the Contract subject to the following conditions:

A. none of the work, including project design, labour and services shall be performed other than by firms from and within participating NATO member countries;

B. no material or items of equipment down to and including identifiable sub-assemblies shall be manufactured or assembled by a firm other than from and within a participating NATO member country. (A sub-assembly is defined as a portion of an assembly consisting of two or more parts that can be provisioned and replaced as an entity); and

C. The intellectual property rights to all design documentation and related system operating software shall reside in NATO member countries, and no license fees or royalty charges shall be paid by the Bidder to firms, individuals or Governments other than within the NATO member countries.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: _____

Bid Reference _____

6.13 Annex B-13 – List of Proposed Key Personnel

Position	SOW/Work Package Reference	Labour Category	Name	Designation Period
Project Manager				EDC thru Contract expiration date
Senior System Engineer Lead (Technical Lead)				EDC thru Contract expiration date
Test Director / Test Engineer				EDC thru Contract expiration date
Quality Assurance Manager				EDC thru Contract expiration date
Other (tbd by Bidder):				EDC thru Contract expiration date

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.14 Annex B-14 – Certificate of Price Ceilings

I hereby certify that the total price offered in the price quotation of this Bid in Section 1 of the Bidding Sheets does not exceed amounts, as described below:

	Status	Cost ceiling
Wave 1	Costed and Evaluated	€ 10,440,458
Wave 1 O&M	Costed and Evaluated Option	€ 8,903,606
Wave 2	Costed and Evaluated Option	€15,446,725
Wave 2 (O&M)	Costed and Evaluated Option	€ 14,183,804

and 48,974,593 Euro in total as described in paragraph 4.2.4 of Book I. If any one or more of the prices proposed by the Bidders are above the ceilings - then the Bid will be declared non-compliant.

Note: no price information of your Bid should be disclosed in the Bid Administration Package nor the Technical Bid Package.

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

6.15 Annex B-15 – Copies of Power of Attorney or equivalent (where relevant)

6.16 Annex B-16 – Disclosure of Involvement of Former NCI Agency Employment

A. The Bidder hereby certifies that, in preparing its Bid, the Bidder did not have access to solicitation information prior to such information been authorized for release to Bidders (e.g., draft statement of work and requirement documentation).

B. The Bidder hereby acknowledges the post-employment measures applicable to former NCI Agency Personnel as per the NCI Agency Code of Conduct.

C. The Bidder hereby certifies that its personnel working as part of the company's team, at any tier, preparing the Bid:

☐ Have not held employment with NCI Agency within the last two years.

☐ Has obtained a signed statement from the former NCI Agency personnel below, who departed the NCI Agency within the last two years, that they were not previously involved in the project under competition (as defined in the extract of the NCI Agency Code of Conduct provided in Annex B of the prospective Contract Provisions):

Employee Name	Former NCIA Position	Current Company Position

D. The Bidder also hereby certifies that it does not employ and/or receive services from former NCI Agency Personnel at grades A5 and above or ranks OF-5 and above, who departed the NCI Agency within the last 12 months. This prohibitions covers negotiations, representational communications and/or advisory activities.

Date   :   ....

Signature   :   ....

Name & Title   :   ....

Company   :   ....

Bid Reference   :   ....

6.17 Annex B-17 – Comprehension and Intention to Comply with PMIC Exclusion Clause and Conflict of Interest

A. I, the undersigned, as an authorised representative of the firm submitting this Bid, do hereby certify that the _____ (FIRM NAME) and its sub-Contractors have not participated in support of CO-14171-PMIC Provide Programme Management and Integration Capability (PIMIC) and are eligible for Contract award.

B. The NCI Agency shall not consider mitigation plans regarding this exclusion.

C. This exclusion clause does not apply to parent companies of the Contractor and their wholly owned subsidiaries provided that the parent company or its subsidiaries provides proof to the satisfaction of the Purchaser that they operate as a separate legal entity in a completely distinguishable and different business domain. Proof as mentioned above may consist of:

    i. company's structure
    ii. roles and responsibilities within structure
    iii. business domain
    iv. ownership and control
    v. and any other proof that will fulfil the purpose of the exclusion clause

D. The Contractor shall insert the substance of of this clause in all subContracts for work performed under this Contract. It is the responsibility of the Contractor to ensure that their subContractor(s) are made aware of this exclusion clause prior to the subContractor(s) commencing performance under this Contract.

E. The Contractor agrees that compliance with this exclusion clause is of the essence and that failure to abide to these terms shall constitute sufficient grounds for the Termination for Default of the Contract in accordance with Clause 39 of the NCI Agency Contract General Provisions.

Signature of authorised Representative:

_____

Printed Name: _____

Title: _____

Date: _____

Company: _____

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

7 BOOK I - ANNEX C

Bid Guarantee - Standby Letter of Credit

Page Intentionally Left Blank

Annex C Bid Guarantee - Standby Letter of Credit

Standby Letter of Credit Number:

Issue Date: _____

Beneficiary: NCI Agency, Financial Management Office
                                Boulevard Leopold III, B-1110, Brussels
                                Belgium

Expiry Date: _____

A. We, (issuing bank) hereby establish in your favour our irrevocable standby letter of credit number {number} by order and for the account of (NAME AND ADDRESS OF BIDDER) in the original amount of € 300,000.00 (Three Hundred Thousand Euro). We are advised this Guarantee fulfils a requirement under Invitation for Bid IFB CO-14176-SOA-IDM dated _____.

B. Funds under this standby letter of credit are available to you upon first demand and without question or delay against presentation of a certificate from the NCI Agency Contracting Officer that:

1) (NAME OF BIDDER) has submitted a Bid and, after Bid Closing Date (including extensions thereto) and prior to the selection of the lowest priced, technically compliant Bid, has withdrawn its Bid, or stated that he does not consider its Bid valid or agree to be bound by its Bid, or

2) (NAME OF BIDDER) has submitted a Bid determined by the Agency to be the lowest priced, technically compliant Bid, but (NAME OF BIDDER) has declined to execute the Contract offered by the Agency, such Contract being consistent with the terms of the Invitation for Bid, or

3) The NCI Agency has offered (NAME OF BIDDER) the Contract for execution but (NAME OF BIDDER) has been unable to demonstrate compliance with the security requirements of the Contract within a reasonable time, or

4) The NCI Agency has entered into the Contract with (NAME OF BIDDER) but (NAME OF BIDDER) has been unable or unwilling to provide the Performance Guarantee required under the terms of the Contract within the time frame required.

C. This Letter of Credit is effective the date hereof and shall expire at our office located at   (Bank Address) on _____. All demands for payment must be made prior to the expiry date.

D. It is a condition of this letter of credit that the expiry date will be automatically extended without Amendment for a period of sixty (60) calendar days from the current or any successive expiry date unless at least thirty (30) calendar days prior to the then current expiry date the NCI Agency Contracting Officer notifies us that the Letter of Credit is not required to be extended or is required to be extended for a shorter duration.

E. We may terminate this letter of credit at any time upon sixty (60) calendar days notice furnished to both (NAME OF BIDDER) and the NCI Agency by registered mail.

F. In the event we (the issuing bank) notify you that we elect not to extend the expiry date in accordance with paragraph 4 above, or, at any time, to terminate the letter of credit, funds under this credit will be available to you without question or delay against presentation of a certificate signed by the NCI Agency Contracting Officer which states

G. "The NCI Agency has been notified by {issuing bank} of its election not to automatically extend the expiry date of letter of credit number {number} dated {date} pursuant to the automatic renewal clause (or to terminate the letter of credit). As of the date of this certificate, no suitable replacement letter of credit, or equivalent financial guarantee has been received by the NCI Agency from, or on behalf of (NAME OF BIDDER), and the NCI Agency, as beneficiary, hereby draws on the standby letter of credit number _____ in the amount of € (Amount up to the maximum available under the LOC), such funds to be transferred to the account of the Beneficiary number _____ (to be identified when certificate is presented)."

H. Such certificate shall be accompanied by the original of this letter of credit and a copy of the letter from the issuing bank that it elects not to automatically extend the standby letter of credit, or terminating the letter of credit.

I. The Beneficiary may not present the certificate described in paragraph 6 above until 20 (twenty) calendar days prior to a) the date of expiration of the letter of credit should {issuing bank} elect not to automatically extend the expiration date of the letter of credit, b) the date of termination of the letter of credit if {issuing bank} notifies the Beneficiary that the letter of credit is to be terminated in accordance with paragraph 6 above.

J. Multiple drawings are allowed.

K. Drafts drawn hereunder must be marked, "Drawn under {issuing bank} Letter of Credit No. {number}" and indicate the date hereof.

L. This letter of credit sets forth in full the terms of our undertaking, and this undertaking shall not in any way be modified, amended, or amplified by reference to any document, instrument, or agreement referred to herein (except the International Standby Practices (ISP 98) hereinafter defined) or in which this letter of credit is referred to or to which this letter of credit relates, and any such reference shall not be deemed to incorporate herein by reference any document, instrument, or agreement.

M. We hereby engage with you that drafts drawn under and in compliance with the terms of this letter of credit will be duly honoured upon presentation of documents to us on or before the expiration date of this letter of credit.

N. This Letter of Credit is subject to The International Standby Practices-ISP98 (1998 Publication) International Chamber of Commerce Publication No.590.

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

8 BOOK I - ANNEX D

Bid Requirements Cross Reference Matrix (BRCM)

Page Intentionally Left Blank

Annex D Bid Requirements Cross Reference Matrix (BRCM)

8.1 Volume 1 shall contain a Bid Requirements Cross Reference Matrix (BRCM), indicating where in the Bid the Bidder addresses each of the '*SHALL*' statements in the SOW.

8.1.1 Bidders shall provide the BRCM in Excel format according to the template "Book I Annex D BRCM".

8.1.2 Optionally the BRCM may also contain a brief description of how the Bidder meets the requirement, to facilitate the reading, but any such descriptions will not form part of the formal evaluation.

8.2 The BRCM shall be completed as per the following instructions:

8.2.1 "Reference Document", the document from which the requirement is defined.

8.2.2 "Reference ID", the reference of the section/requirement under consideration. The "Reference ID" column shall cover:

8.2.2.1 "Bidding Instruction" references covering section 3 of this document. "Bidding Instruction" references shall be provided in the format [BI - #] where "#" represents the actual paragraph number.

8.2.2.2 "SOW Requirement" references covering all "*SHALL*" statement of the SOW (including SRS annexes A). SOW Requirement References shall be provided in the following format:

8.2.2.2.1 For the SOW: [SOW - #] where "#" represents the actual requirement (i.e. paragraph or "*SHALL"* statement) number.

8.2.2.2.2 For the SOW Annex A (SRS): [SRS - #] where "#" represents the actual requirement number (i.e. paragraph or "*SHALL"* statement) number.

8.2.3 "Description": the actual text of the section/requirement under consideration.

8.2.4 "Bid Reference" indicating where in their Bid the associated Bid Instruction Reference and/or SOW Requirement Reference is/are addressed. Bid Reference shall be provided in the form "Volume # - Doc # - Section #"

8.2.5 "Remarks", as applicable. The column "Remarks" might be used by the Bidders to provide a brief description of how the Bidder meets the requirement, to facilitate the reading, but any such descriptions will not form part of the formal evaluation.

8.2.6 "Compliance statement": the way and extent the Bid covers and complies with the section/requirement under consideration, using the following classifications:

8.2.6.1 "Provided/Detailed": The Bidder states providing a document or details at the mentioned reference. Such a classification is expected for all BIs and the majority of the SOW and SRS requirements.

8.2.6.2 "Partial": The Bidder states fulfilling the requirement but only describes part of it. Such a classification is expected for a small number of SOW and SRS requirements.

8.2.6.3 "Deviation proposed": The Bidder states tacking and describing an alternative approach to fulfil the section/requirement under consideration. Such a classification is expected for a very limited amount of SOW and/or SRS requirements.

8.2.6.4 "Not detailed": The Bidder states fulfilling the requirement, but does not detail/justify how. It is expected that some requirements from the SOW or SRS cannot be justified/detailed at the Bidding stage.

8.3 One copy of the duly completed BRCM shall be included in the Bid Administration Package, as well as the Technical Bid Package (Volume 1).

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

9   BOOK I - ANNEX E

Clarification Request Form

Page Intentionally Left Blank

Annex E Clarification Request Form

**INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE**

INVITATION FOR BID
IFB CO-14176-SOA-IDM

Provide a Service Oriented Architecture

CLARIFICATION REQUEST FORM

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

ADMINISTRATION or CONTRACTING				
Serial NR	IFB REF	QUESTIONS	ANSWERS	Status
A.1.				
A.2.				
A.3.				
A.4.				

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

PRICE				
Serial NR	IFB REF	QUESTIONS	ANSWERS	Status
P.1				
P.2				
P.3				
P.4				
P.5				
P.6				

INSERT COMPANY NAME HERE
INSERT SUBMISSION DATE HERE

TECHNICAL				
Serial NR	IFB REF	QUESTIONS	ANSWERS	Status
T.1				
T.2				
T.3				

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

SERVICE-ORIENTED ARCHITECTURE & IDENTITY MANAGEMENT PLATFORM

BOOK II

PROSPECTIVE CONTRACT
SIGNATURE PAGE

Page Intentionally Left Blank

SIGNATURE SHEET

CONTRACT CO-14176-SOA-IDM

**Between
NCI Organisation, as
represented by the General Manager NCI Agency
(Purchaser)**

and

(Contractor)

IN WITNESS HEREOF the parties hereto have caused this agreement to be executed by their duly authorised officers on the date shown hereunder:

Signature of Contractor: ………………………………

Name of Signer: ………………………………..

Title of Signer: ……………………………….

Date: ……………………………….

Signature of Purchaser: ………………………………

Name of Signer: ………………………………..

Title of Signer: ………………………………...

Date: ………………………………....

EFFECTIVE DATE OF CONTRACT: [TBD]

TOTAL CONTRACT VALUE: [TBD]

Page Intentionally Left Blank

TABLE OF CONTENTS

THE PROSPECTIVE CONTRACT – BOOK II

Page Intentionally Left Blank

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

SERVICE-ORIENTED ARCHITECTURE & IDENTITY MANAGEMENT PLATFORM

BOOK II - PART I

PROSPECTIVE CONTRACT

SCHEDULES OF SUPPLIES AND SERVICES (SSS)

Page Intentionally Left Blank

CLIN	Description	Price requirements - caps	Qty/MD Total	Unit Price / Base Cost	Total Price [Indicate Currency Here]	Delivery Date	SoW reference: Sections #
Total					100.00		
Work Package 2 -Implement SOA (basic) Wave 1					25.00		
2.1	Project Management	<= 3% of total price of CLIN2	1	1.00	1.00	based on bidding sheets	5.3, 5.4, 11.5, 11.6, 12.3, G.2, G.3
2.2	Engineering				7.00		7
2.2.1	Orientation Workshop	<= 5% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	7.2
2.2.2	System Requirements Analysis and Review	<= 15% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	4.4, 7.3
2.2.3	Design & Review	<= 25% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.4	Basic SOA Platform	<= 70% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	6.9
2.2.5	Tests (during Product Baseline and before Operational Baseline)	<= 10% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	5., 6., 8., 12., 14., G.4.
2.2.6	Site Surveys for PSA sites	<= 5% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	3.1., 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.
2.2.7	Engineering Documentation	<= 10% of total price of CLIN2.2	1	1.00	1.00	based on bidding sheets	5.4., 5.5. 5.6., 7., G.2
2.3	Implementation				5.00		6
2.3.1	Implementation Plan	<= 5% of total price of CLIN2.3	1	1.00	1.00	based on bidding sheets	3., 4., 5.3., 6., 8.4, 8.5, 9., 10., 13.2.
2.3.2	Reference System Implementation	<= 30% of total price of CLIN2.3	1	1.00	1.00	based on bidding sheets	4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.3.3	Site Survey	<= 5% of total price of CLIN2.3	1	1.00	1.00	based on bidding sheets	3.1., 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.
2.3.4	Implementation (PSA and FSA sites)	<= 50% of total price of CLIN2.3	1	1.00	1.00	based on bidding sheets	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.3.5	Baselines for Wave 1	<= 50% of total price of CLIN2.3	1	1.00	1.00	based on bidding sheets	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
2.4	System Testing and Acceptance	<= 10% of total price of CLIN2	1	1.00	1.00	based on bidding sheets	6., 7., 8, 9.5., 10., G.2, G.8
2.5	Integrated Logistics Support (ILS)				5.00		3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
2.5.1	Integrated Logistics Support Plan (ILSP) +	<= 5% of total price of CLIN2.5	1	1.00	1.00	based on bidding sheets	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 14.
2.5.2	Technical Documentation	<= 15% of total price of CLIN2.5	1	1.00	1.00	based on bidding sheets	12.5., 12.6., 14.6., G.7
2.5.3	Training	<= 10% of total price of CLIN2.5	1	1.00	1.00	based on bidding sheets	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., G.7.
2.5.4	Configuration, Issues and Changes Management Package	<= 40% of total price of CLIN2.5	1	1.00	1.00	based on bidding sheets	3., 4., 5., 8., 9.4, 10.2., 11., 12., 14., G.2
2.5.5	Warranty	<= 30% of total price of CLIN2.5	1	1.00	1.00	based on bidding sheets	6.12., 14.4., 14.6., 14.8, 14.10.
2.6	Software/Equipment		1	1.00	1.00	based on bidding sheets	3.1.2., 4.6., 4.9., 5.2., 6.4., 6.5., 6.8., 7., 8.2., 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1., 14.8., 14.9.4., 14.10.
2.7	Operations and Maintanace (OPTIONAL)				5.00		9.4.1., 12.2.4., 14.
2.7.1	Initial Operational Support (Year 1)	= 20% of total price of CLIN2.7	1	1.00	1.00	from PSA of Wave1 + 1year	9.4.1., 12.2.4., 14.
2.7.2	Follow-on Support (Year 2)	= 20% of total price of CLIN2.7	1	1.00	1.00	From PSA of Wave1 +1year to PSA + 2year	9.4.1., 12.2.4., 14.
2.7.3	Follow-on Support (Year 3)	= 20% of total price of CLIN2.7	1	1.00	1.00	From PSA of Wave1 + 2year to PSA + 3years	9.4.1., 12.2.4., 14.
2.7.4	Follow-on Support (Year 4)	= 20% of total price of CLIN2.7	1	1.00	1.00	From FSA of Wave1 + 3year to PSA + 4year	9.4.1., 12.2.4., 14.
2.7.5	Follow-on Support (Year 5)	= 20% of total price of CLIN2.7	1	1.00	1.00	From PSA of Wave1 + 4years to PSA + 5year	9.4.1., 12.2.4., 14.
Total - Work Package 2 Wave 1					25.00		
Work Package 2 -Implement SOA (extended) Wave 2					25.00		
2.8	Project Management	<= 3% of total price of CLIN2	1	1.00	1.00	based on bidding sheets	5.4., 11.5, 11.6, 12.3, G.2., G.3
2.9	Engineering				7.00		
2.9.1	Orientation Workshop	<= 5% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	7.2
2.9.2	System Requirements Analysis and Review	<= 15% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	4.4, 7.3
2.9.3	Design & Review	<= 25% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	4.1., 4.5., 5.5., 5.6., 7.4.
2.9.4	Extended SOA Platform	<= 70% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	6.9
2.9.5	Tests (during Product Baseline and before Operational Baseline)	<= 10% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	5., 6., 8., 12., 14., G.4.
2.9.6	Site Surveys for PSA sites	<= 5% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	3.1., 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.
2.9.7	Engineering Documentation	<= 10% of total price of CLIN2.9	1	1.00	1.00	based on bidding sheets	5.4., 5.5. 5.6., 7., G.2
2.10	Implementation				5.00		6
2.10.1	Implementation Plan	<= 5% of total price of CLIN2.10	1	1.00	1.00	based on bidding sheets	3., 4., 5.3., 6., 8.4, 8.5, 9., 10., 13.2.
2.10.2	Reference System Implementation	<= 30% of total price of CLIN2.10	1	1.00	1.00	based on bidding sheets	4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.10.3	Site Survey	<= 5% of total price of CLIN2.10	1	1.00	1.00	based on bidding sheets	3.1., 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.
2.10.4	Implementation (PSA and FSA sites)	<= 50% of total price of CLIN2.10	1	1.00	1.00	based on bidding sheets	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.5	Baselines for Wave 2	<= 50% of total price of CLIN2.10	1	1.00	1.00	based on bidding sheets	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 8.5.1., 14.7.
2.11	System Testing and Acceptance	<= 10% of total price of CLIN2	1	1.00	1.00	based on bidding sheets	6., 7., 8, 9.5., 10., G.2, G.8
2.12	Integrated Logistics Support (ILS)				5.00		3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
2.12.1	Integrated Logistics Support Plan (ILSP) +	<= 5% of total price of CLIN2.12	1	1.00	1.00	based on bidding sheets	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 14.
2.12.2	Technical Documentation	<= 15% of total price of CLIN2.12	1	1.00	1.00	based on bidding sheets	12.5., 12.6., 14.6., G.7
2.12.3	Training	<= 10% of total price of CLIN2.12	1	1.00	1.00	based on bidding sheets	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., G.7.
2.12.4	Configuration, Issues and Changes Management Package	<= 40% of total price of CLIN2.12	1	1.00	1.00	based on bidding sheets	3., 4., 5., 8., 9.4, 10.2., 11., 12., 14., G.2
2.12.5	Warranty	<= 30% of total price of CLIN2.12	1	1.00	1.00	based on bidding sheets	6.12., 14.4., 14.6., 14.8, 14.10.
2.13	Software/Equipment		1	1.00	1.00	based on bidding sheets	3.1.2., 4.6., 4.9., 5.2., 6.4., 6.5., 6.8., 7., 8.2., 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1., 14.8., 14.9.4., 14.10.
2.14	Operations and Maintanace (OPTIONAL)				5.00		9.4.1., 12.2.4., 14.
2.14.1	Initial Operational Support (Year 1)	= 20% of total price of CLIN2.14	1	1.00	1.00	from PSA of Wave2 + 1year	9.4.1., 12.2.4., 14.
2.14.2	Follow-on Support (Year 2)	= 20% of total price of CLIN2.14	1	1.00	1.00	From PSA of Wave2 +1year to PSA + 2year	9.4.1., 12.2.4., 14.
2.14.3	Follow-on Support (Year 3)	= 20% of total price of CLIN2.14	1	1.00	1.00	From PSA of Wave2 + 2year to PSA + 3years	9.4.1., 12.2.4., 14.
2.14.4	Follow-on Support (Year 4)	= 20% of total price of CLIN2.14	1	1.00	1.00	From FSA of Wave2 + 3year to PSA + 4year	9.4.1., 12.2.4., 14.
2.14.5	Follow-on Support (Year 5)	= 20% of total price of CLIN2.14	1	1.00	1.00	From PSA of Wave2 + 4years to PSA + 5year	9.4.1., 12.2.4., 14.
Total - Work Package 2 Wave 2					25.00		

Work Package 4 -Implement IdM (basic) Platform Wave 1					21.00		
4.1	Project Management	<= 3% of total price of CLIN4	1	1.00	1.00	based on bidding sheets	5., 11.5, 11.6, 12.3, G.2., G.3
4.2	Engineering				6.00		
4.2.1	Orientation Workshop	<= 5% of total price of CLIN4.2	1	1.00	1.00	based on bidding sheets	7.2
4.2.2	Sytem Requirements Analysis (and Review)	<= 15% of total price of CLIN4.2	1	1.00	1.00	based on bidding sheets	4.4., 7.3
4.2.3	Design & Review (PDR and CDR)	<= 25% of total price of CLIN4.2	1	1.00	1.00	based on bidding sheets	4.1., 4.5., 5.5., 5.6., 7.4
4.2.4	Basic IdM Platform (Wave 1)	<= 70% of total price of CLIN4.2	1	1.00	1.00	based on bidding sheets	6.10
4.2.5	Tests (during Product Baseline and before Operational Baseline)	<= 10% of total price of CLIN4.2	1	1.00	1.00	based on bidding sheets	5., 6., 8., 12., 14., G.4.
4.2.6	Engineering Documentation	<= 10% of total price of CLIN4.2	1	1.00	1.00	based on bidding sheets	5.4., 5.5 5.6., 7., G.2
4.3	Implementation				2.00		6
4.3.1	Implementation Plan	<= 10% of total price of CLIN4.3	1	1.00	1.00	based on bidding sheets	3., 4., 5., 6., 8.4, 8.5, 9., 10., 13.2.
4.3.2	Baselines for Wave 1		1	1.00	1.00	based on bidding sheets	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.4	System Testing and Acceptance	<= 10% of total price of CLIN4	1	1.00	1.00	based on bidding sheets	6., 7., 8., 9.5., 10., G.2, G.8
4.5	Integrated Logistics Support				5.00		3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
4.5.1	Integrated Logistics Support Plan (ILSP) +	<= 5% of total price of CLIN4.5	1	1.00	1.00	based on bidding sheets	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 14.
4.5.2	Technical Documentation	<= 15% of total price of CLIN4.5	1	1.00	1.00	based on bidding sheets	12.5., 12.6., 14.6., G.7
4.5.3	Training	<= 10% of total price of CLIN4.5	1	1.00	1.00	based on bidding sheets	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., G.7
4.5.4	Configuration, Issues and Changes Management Package	<= 40% of total price of CLIN4.5	1	1.00	1.00	based on bidding sheets	3., 4., 5., 8., 9.4, 10.2., 11., 12., 14., G.2
4.5.5	Warranty	<= 30% of total price of CLIN4.5	1	1.00	1.00	based on bidding sheets	6.12., 14.4., 14.6., 14.8., 14.10.
4.6	Software/Equipment		1	1.00	1.00	based on bidding sheets	3.1.2., 4.6., 4.9., 5.2., 6.4., 6.5., 6.8., 7., 8.2., 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1., 14.8., 14.9.4., 14.10.
4.7	Operations and Maintanance (OPTIONAL)				5.00		9.4.1., 12.2.4., 14.
4.7.1	Initial Operational Support (Year 1)	= 20% of total price of CLIN4.7	1	1.00	1.00	from PSA of Wave1 + 1year	9.4.1., 12.2.4., 14.
4.7.2	Follow-on Support (Year 2)	= 20% of total price of CLIN4.7	1	1.00	1.00	From PSA of Wave1 +1year to PSA + 2year	9.4.1., 12.2.4., 14.
4.7.3	Follow-on Support (Year 3)	= 20% of total price of CLIN4.7	1	1.00	1.00	From PSA of Wave1 + 2year to PSA + 3years	9.4.1., 12.2.4., 14.
4.7.4	Follow-on Support (Year 4)	= 20% of total price of CLIN4.7	1	1.00	1.00	From PSA of Wave1 + 3year to PSA + 4year	9.4.1., 12.2.4., 14.
4.7.5	Follow-on Support (Year 5)	= 20% of total price of CLIN4.7	1	1.00	1.00	From PSA of Wave1 + 4years to PSA + 5year	9.4.1., 12.2.4., 14.
Total - Work Package 4 Wave 1					21.00		

Work Package 4 -Implement IdM (extended) Platform Wave 2					21.00		
4.8	Project Management	<= 3% of total price of CLIN4	1	1.00	1.00	based on bidding sheets	5., 11.5, 11.6, 12.3, G.2., G.3
4.9	Engineering				6.00		
4.9.1	Orientation Workshop	<= 5% of total price of CLIN4.9	1	1.00	1.00	based on bidding sheets	7.2
4.9.2	Sytem Requirements Analysis (and Review)	<= 15% of total price of CLIN4.9	1	1.00	1.00	based on bidding sheets	4.4., 7.3
4.9.3	Design & Review (PDR and CDR)	<= 25% of total price of CLIN4.9	1	1.00	1.00	based on bidding sheets	4.1., 4.5., 5.5., 5.6., 7.4
4.9.4	Extended IdM Platform (Wave 2)	<= 70% of total price of CLIN4.9	1	1.00	1.00	based on bidding sheets	6.10
4.9.5	Tests (during Product Baseline and before Operational Baseline)	<= 10% of total price of CLIN4.9	1	1.00	1.00	based on bidding sheets	5., 6., 8., 12., 14., G.4.
4.9.6	Engineering Documentation	<= 10% of total price of CLIN4.9	1	1.00	1.00	based on bidding sheets	5.4., 5.5 5.6., 7., G.2
4.10.	Implementation				2.00		6
4.10.1	Implementation Plan	<= 10% of total price of CLIN4.10	1	1.00	1.00	based on bidding sheets	3., 4., 5.3., 6., 8.4, 8.5, 9., 10., 13.2.
4.10.3	Baselines for Wave 2		1	1.00	1.00	based on bidding sheets	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.11	System Testing and Acceptance	<= 10% of total price of CLIN4	1	1.00	1.00	based on bidding sheets	6., 7., 8., 9.5., 10., G.2, G.8
4.12	Integrated Logistics Support				5.00		3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
4.12.1	Integrated Logistics Support Plan (ILSP) +	<= 5% of total price of CLIN4.12	1	1.00	1.00	based on bidding sheets	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4 8.2., 9.5., 14.
4.12.2	Technical Documentation	<= 15% of total price of CLIN4.12	1	1.00	1.00	based on bidding sheets	12.5., 12.6., 14.6., G.7
4.12.3	Training	<= 10% of total price of CLIN4.12	1	1.00	1.00	based on bidding sheets	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., G.7
4.12.4	Configuration, Issues and Changes Management Package	<= 40% of total price of CLIN4.12	1	1.00	1.00	based on bidding sheets	3., 4., 5., 8., 9.4, 10.2., 11., 12., 14., G.2
4.12.5	Warranty	<= 30% of total price of CLIN4.12	1	1.00	1.00	based on bidding sheets	6.12., 14.4., 14.6., 14.8., 14.10.
4.13	Software/Equipment		1	1.00	1.00	based on bidding sheets	3.1.2., 4.6., 4.9., 5.2., 6.4., 6.5., 6.8., 7., 8.2., 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1., 14.8., 14.9.4., 14.10.
4.14	Operations and Maintanance (OPTIONAL)				5.00		9.4.1., 12.2.4., 14.
4.14.1.	Initial Operational Support (Year 1)	= 20% of total price of CLIN4.14	1	1.00	1.00	from PSA of Wave2 + 1year	9.4.1., 12.2.4., 14.
4.14.2.	Follow-on Support (Year 2)	= 20% of total price of CLIN4.14	1	1.00	1.00	From PSA of Wave2 +1year to PSA + 2year	9.4.1., 12.2.4., 14.
4.14.3.	Follow-on Support (Year 3)	= 20% of total price of CLIN4.14	1	1.00	1.00	From PSA of Wave2 + 2year to PSA + 3years	9.4.1., 12.2.4., 14.
4.14.4.	Follow-on Support (Year 4)	= 20% of total price of CLIN4.14	1	1.00	1.00	From PSA of Wave2 + 3year to PSA + 4year	9.4.1., 12.2.4., 14.
4.14.5.	Follow-on Support (Year 5)	= 20% of total price of CLIN4.14	1	1.00	1.00	From PSA of Wave2 + 4years to PSA + 5year	9.4.1., 12.2.4., 14.
Total - Work Package 4 Wave 2					21.00		

Work Package 6 - Support Pilot Integration Cases (Wave 1)					3.00		
6.1	Project Management	<= 5% of total price of CLIN6	1	1.00	1.00	based on bidding sheets	5.3., 5.4., 5.5 5.6., 6.11., G.2.
6.2	Support				2.00		
6.2.1	Training	<= 5% of total price of CLIN6.2	1	1.00	1.00	based on bidding sheets	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 6.11., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., 14.10., G.7.2.
6.2.2	Contractor Logistics Support		1	1.00	1.00	As required	6.11., 14
Total - Work Package 6 (Wave 1)					3.00		

Work Package 6 - Support Pilot Integration Cases (Wave 2)					3.00		
6.3	Project Management	<= 5% of total price of CLIN6	1	1.00	1.00	based on bidding sheets	5.3., 5.4., 5.5 5.6., 6.11., G.2.
6.4	Support				2.00		
6.4.1	Training	<= 5% of total price of CLIN6.4	1	1.00	1.00	based on bidding sheets	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 6.11., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., 14.10., G.7.2.
6.4.2	Contractor Logistics Support		1	1.00	1.00	As required	6.11., 14
Total - Work Package 6 (Wave 2)					3.00		

Work Package 7 - Support integration of other projects					2.00		

7.1	Project Management	<= 10% of total price of CLIN7	1	1.00	1.00	based on bidding sheets	5.3, 5.4., 5.5., 6.12., G.2.
7.2	Contractor Logistics Support		1	1.00	1.00	As required	6.12., 14.
Total - Work Package 7					2.00		

Work Package	Milestones	Affected CLINs	Milestone Payment	Milestone Date
WP 2 **Wave 1 - Basic SOA Platform** **Wave 2 - Extended SOA Platform** **WP 4** **Wave 1 - Basic IdM Platform** **Wave 2 - Extended IdM Platform**	**M1** (CDR - Wave 1)	CLIN 2.1 - 30% CLIN 2.2.1 - 100% CLIN 2.5.1/2.5.2 - 60% CLIN 4.1 - 30% CLIN 4.2.1 - 100% CLIN 4.5.1/4.5.2 - 60%	5.00	EDC + 1 month
	M2 (PSA Wave 1)	CLIN 2.1 - 50% CLIN 2.2.2/2.2.3/2.2.4/2.2.5/2.2.6/2.2.7 - 80% CLIN 2.3/2.4 - 80% CLIN 2.5.1/2.5.2 - 30% CLIN 2.5.3/2.5.4 - 80% CLIN 4.1 - 50% CLIN 4.2.2/4.2.3/4.2.4/4.2.5/4.2.6 - 80% CLIN 4.3/4.4 - 80% CLIN 4.5.1/4.5.2 - 30% CLIN 4.5.3/4.5.4 - 80%	21.40	EDC + 17 months
	M3 (FSA Wave 1)	CLIN 2.1 - 20% CLIN 2.2.2/2.2.3/2.2.4/2.2.6/2.2.7/ - 20% CLIN 2.3/2.4 - 20% CLIN 2.5.1/2.5.2 - 10% CLIN 2.5.3/2.5.4 - 20% CLIN 2.5.5 - billed quarterly CLIN 2.6 - 100% CLIN 4.1 - 20% CLIN 4.2.2/4.2.3/4.2.4/4.2.6/ - 20% CLIN 4.3/4.4 - 20% CLIN 4.5.1/4.5.2 - 10% CLIN 4.5.3/4.5.4 - 20% CLIN 4.5.5 - billed quarterly CLIN 4.6 - 100%	9.60	EDC + 18 months
	Option **M4** (CDR Wave 2)	CLIN 2.8 - 30% CLIN 2.9.1 - 100% CLIN 2.12.1/2.12.2 - 60% CLIN 4.8 - 30% CLIN 4.9.1 - 100% CLIN 4.12.1/4.12.2 - 60%	5.00	EDC + 20 months
	Option **M5** (PSA Wave 2)	CLIN 2.8- 50% CLIN 2.9.2/2.9.3/2.9.4/2.9.5/2.9.6/2.9.7- 80% CLIN 2.10/2.11 - 80% CLIN 2.12.1/2.12.2 - 30% CLIN 2.12.3/2.12.4- 80% CLIN 4.8 - 50% CLIN 4.9.2/4.9.3/4.9.4/4.9.5/4.9.6- 80% CLIN 4.10/4.11 - 80% CLIN 4.12.1/4.12.2 - 30% CLIN 4.12.3/4.12.4- 80%	21.40	EDC + 32 months

	Option **M6** (FSA Wave 2)	CLIN 2.8 - 20% CLIN 2.9.2/2.9.3/2.9.4/2.9.5/2.9.6/2.9.7 - 20% CLIN 2.10/2.11 - 20% CLIN 2.12.1/2.12.2 - 10% CLIN 2.12.3/2.12.4 - 20% CLIN 2.12.5 - billed quarterly CLIN 2.13 - 100% CLIN 4.8 - 20% CLIN 4.9.2/4.9.3/4.9.4/4.9.5/4.9.6 - 20% CLIN 4.10/4.11 - 20% CLIN 4.12.1/4.12.2 - 10% CLIN 4.12.3/4.12.4 - 20% CLIN 4.12.5 - billed quarterly CLIN 4.13 - 100%	9.60	EDC + 33 months
	Option **M7** (O&M Waves 1 and 2)	CLINs 2.7.1-2.7.5, billed quarterly is arrears for 25% of the subCLIN price CLINs 2.14.1-2.14.5, billed quarterly is arrears for 25% of the subCLIN price CLINs 4.7.1-4.7.5, billed quarterly is arrears for 25% of the subCLIN price CLINs 4.14.1-4.14.5, billed quarterly is arrears for 25% of the subCLIN price	20.00	billed quarterly after first quarter from O&M begins
WP 6 **Waves 1/2 - Support Pilot Integration Cases**	**M8** (Project Management Plan(s) and Documents approval)	CLIN 6.1 - 100%	1.00	EDC + 18 months
	Option **M9** (Training)	CLIN 6.2.1 - 100%	1.00	EDC + 18 months
	Option **M10** (Support)	CLIN 6.2.2 - billed quarterly is arrears for based on time and material expenditure	1.00	billed quarterly after first quarter from support start date
	Option **M11** (Project Management Plan(s) and Documents approval)	CLIN 6.3 - 100%	1.00	EDC + 19 months
	Option **M12** (Training)	CLIN 6.4.1 - 100%	1.00	EDC + 20 months
	Option **M13** (Support)	CLIN 6.4.2 - billed quarterly is arrears for based on time and material expenditure	1.00	billed quarterly after first quarter from support start date
WP 7 **Waves 1/2 - Support Integration of other projects**	**M14** (Project Management Plan(s) and Documents approval)	CLIN 7.1 - 100%	1.00	EDC + 17 months (not earlier than first integration of toher FAS)
	M15 (Support)	CLIN 7.2 - billed quarterly is arrears for based on time and material expenditure	1.00	EDC + 17 months (not earlier than first integration of toher FAS)
			100.00	

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

BOOK II – PART II

CONTRACT SPECIAL PROVISIONS

PART II
CONTRACT SPECIAL PROVISIONS - INDEX OF CLAUSES

1. ORDER OF PRECEDENCE

1.1 In the event of any inconsistency in this Contract, the inconsistency shall be resolved by giving precedence in the following order:

- a.   Signature sheet
- b.   Part I - The Schedule of Supplies and Services (SSS)
- c.   Part II - The Contract Special Provisions (CSP)
- d.   Part III – The Contract General Provisions
- e.   Part IV – The Statement of Work (SOW) and SOW Annexes
- f.   The Contractor's Bid including any clarifications thereto, incorporated by reference, and the formal documentation of pre-Contract discussions.

2. TYPE OF CONTRACT

2.1 This is a Firm Fixed Price Contract established for the supplies and services defined in Part I - Schedule of Supplies and Services and Part IV – Statement of Work.

2.2 The Purchaser assumes no liability for costs incurred by the Contractor in excess of the stated Firm Fixed Price except as provided under other provisions of this Contract.

2.3 The Total Contract price is inclusive of all expenses related to the performance of the present contract.

3. SCOPE OF WORK

3.1 The current authorisation and consequently any Contract resulting from this Invitation for Bid (IFB) shall address **solely** Project 2014/0IS03094-0.

3.1.1   The scope of the SOA & IdM project includes four work packages in two waves as shown below.

Wave 1	Wave 2
Work Package 2 – Basic SOA Platform	Work Package 2 – Extended SOA Platform
Work Package 4 – Basic IdM Platform	Work Package 4 – Extended IdM Platform
Work Package 6 – Support pilot Integration cases	Work Package 6 – Support pilot Integration cases
Work Package 7 – Support Integration of other projects	

3.2 Work Package 2: This work package will provide a common platform to existing and new systems to enable the migration towards a Service Oriented

Architecture (SOA), on both: Operational Network (ON) and Protected Business Network (PBN).

3.3 Work Package 4. This work package will provide a common Identity Management (IdM) Platform to existing and new systems. The scope of this Work Package will be delivered in two subsequent Work Packages corresponding to the implementation Waves.

3.4 Work Package 6. This work package will provide consultancy and on-demand support to a 3rd party contractor and developers working under on implementing the pilot integration cases with the SOA&IdM Platform.

3.5 Work Package 7. This work package will provide a not-to-exceed on-demand support (including post-implementation support) for 3rd party contractors working for other projects that will integrate their systems with the SOA&IdM Platform.

4. COMPREHENSION OF CONTRACT AND SPECIFICATIONS

4.1 The Contractor warrants that he has read, understood and agreed to each and all terms, clauses, specifications and conditions specified in the Contract and that this signature of the Contract is an acceptance, without reservations, of the said Contract terms within their normal and common meaning.

4.2 The specifications set forth the performance requirements for the Contractor's proposed work as called for under this Contract. Accordingly, notwithstanding any conflict or inconsistency which hereafter may be found between achievement of the aforesaid performance requirements and adherence to the Contractor's proposed design for the work, the Contractor hereby warrants that the work to be delivered will meet or exceed the performance requirements of the said specifications.

4.3 The Contractor hereby acknowledges that he has no right to assert against the Purchaser, its officers, agents or employees, any claims or demands with respect to the aforesaid specifications as are in effect on the date of award of this Contract.

4.4 Based upon impossibility of performance, defective, inaccurate, impracticable, insufficient or invalid specifications, implied warranties of suitability of such specifications, or

4.5 Otherwise derived from the aforesaid specifications, and hereby waives any claims or demands so based or derived as might otherwise arise.

4.6 Notwithstanding the "Changes" clause or any other clause of the Contract, the Contractor hereby agrees that no changes to the aforesaid specifications which may be necessary to permit achievement of the performance requirements specified herein for the Contractor's proposed work shall entitle the Contractor either to any increase in the firm fixed price as set forth in this Contract or to any extension of the delivery times for the work beyond the period of performance in the Schedule of Supplies and Services.

5. PLACE AND TERMS OF DELIVERY

5.1 Deliverables under this Contract shall be delivered DDP (Delivered Duty Paid) in accordance with the International Chamber of Commerce INCOTERMS 2010 to the destination(s) and at such times as set forth in the Schedule of Supplies and Services. The Contractor shall note that the Purchaser is exempt from customs duties and VAT. The Purchaser shall not be liable for any storage, damage, accessorial or any other charges involved in such transporting of supplies.

6. PARTICIPATING COUNTRIES

6.1 This Clause supplements Clause 9 (Participating Countries) of the Contract General Provisions.

6.2 Participating countries are as follows NATO nations in ALBANIA, BELGIUM, BULGARIA, CANADA, CROATIA, THE CZECH REPUBLIC, DENMARK, ESTONIA, FRANCE, GERMANY, GREECE, HUNGARY, ICELAND, ITALY, LATVIA, LITHUANIA, LUXEMBOURG, THE NETHERLANDS, NORWAY, POLAND, PORTUGAL, ROMANIA, SLOVAKIA, SLOVENIA, SPAIN, TURKEY, THE UNITED KINGDOM and THE UNITED STATES.

7. TRANSPORTATION OF EQUIPMENT

7.1 All supplies covered under this Contract, including Purchaser Furnished Equipment (PFE), once handed over to the Contractor, and items shipped under warranty for repair or otherwise, shall be transported to and from all destinations at the responsibility of the Contractor. The Purchaser shall not be liable for any storage, damage, accessorial or any other charges involved in such transporting of supplies.

8. INSPECTION AND ACCEPTANCE

8.1 Acceptance is the action by which the Purchaser formally acknowledges that the Contractor has fully demonstrated that Contract Deliverables are complete or have been performed according to the requirements set in the Contract.

8.2 Inspection and Acceptance procedures are described in Clause 21 of the NCIO General Contract Provisions ("Inspection and Acceptance of work").

9. CONTRACTOR'S RESPONSIBILITY

9.1 The Contractor shall monitor changes and/or upgrades to commercial off the shelf (COTS) software or hardware to be utilized under subject Contract.

9.2 For COTS items which are or could be impacted by obsolescence issues, as changes in technology occur, the Contractor will propose substitution of new products/items for inclusion in this Contract. The proposed items should provide at least equivalent performance and/or lower life-cycle support costs, or enhanced performance without a price or cost increase.

9.3 The Contractor will provide evidence with respect to price and performance of the equipment being proposed as well as data proving an improvement in

performance and/or a reduction in price and/or life-cycle support costs. If necessary for evaluation by the Purchaser, the Contractor shall provide a demonstration of the proposed items. Should the Purchaser decide that the proposed item(s) should be included in the Contract, an equitable price adjustment will be negotiated and the proposed item(s) shall be added to the Contract by bilateral modification under the authority of this Article.

9.4 The Contractor shall notify the Purchaser of any proposed changes in the commercial off the shelf software or hardware to be utilized. Such notification shall provide an assessment of the changes and the impact to any other items to be delivered under this Contract.

10. PRICING OF CHANGES, MODIFICATIONS, FOLLOW-ON CONTRACTS AND CLAIMS

10.1   The Purchaser may at any time, by written order designated or indicated to be a change order, and without notice to the sureties, if any, make changes within the scope of any Contract or Task Order, in accordance with Clause 16 (Changes) of the Contract General Provisions.

10.2   Changes, modifications, follow-on Contracts of any nature, and claims shall be priced in accordance with Clause 19 (Pricing of Changes, Amendments and Claims) of the Contract General Provisions, and with the "Purchaser's Pricing Principles" as set out in the Annex 1 to the Contract General Provisions.

10.3   Except otherwise provided for in this Contract, prices quoted for the above-mentioned changes, modifications, etc shall have a minimum validity period of twelve (12) months from the date of purchaser acceptance of proposal

11. INVOICES AND PAYMENTS

11.1   Following Purchaser acceptance, in writing, payment for supplies and services furnished shall be made in the currency specified for the relevant portion of the Contract.

11.2   The term of the Contract may not be exceeded without prior approval of the Purchaser. In no case will the Purchaser make payment above the total of the corresponding CLINs.

11.3   No payment will be made if CLIN items agreed for delivery before milestones are not complete as described in bidding sheets, SSS and SoW.

11.4   No payment shall be made with respect to undelivered supplies; works not performed, services not rendered and/or incorrectly submitted invoices.

11.5   No payment will be made for additional items delivered that are not specified in the contractual document.

11.6   The invoice amount shall be exclusive of VAT and exclusive of all Taxes and Duties as per Clause 26 (Taxes and Duties) of the Contract General Provisions.

11.7   CLINs will be paid as below based on Purchaser milestone approval in writing.

11.8   The Contractor shall be entitled to submit invoices as in IFB-CO-14176-SOA-IDM - Book 2 - Part 1 – SSS spreadsheet.

11.9   Evidence of the acceptance by the Purchaser shall be attached to all invoices.

11.10 The Purchaser is released from paying any interest resulting from any reason whatsoever.

11.11 The Contractor shall render all invoices in a manner, which shall provide a clear reference to the Contract. Invoices in respect of any service and/or deliverable shall be prepared and submitted as specified hereafter and shall contain:

11.11.1   Contract number CO-14176-SOA

11.11.2   Purchase Order number (TBD at Contract Award)

11.11.3   Contract Amendment number (if any)

11.11.4   Contract Line Item(s) (CLIN) as they are defined in the priced Schedule of Supplies and Services.

11.11.5   Bank Account details for International wire transfers

11.12 The invoice shall contain the following certificate:
"I certify that the above invoice is true and correct, that the delivery of the above described items has been duly effected and/or that the above mentioned services have been rendered and the payment therefore has not been received". The certificate shall be signed by a duly authorised company official on the designated original.

11.13 Invoices referencing "CO-14176-SOA/ PO (TBD at Contract Award)" shall be submitted in electronic format to:

   AccountsPayable@NCIA.NATO.int

An Electronic copy shall be sent to the Contracting Officer, at the email address specified in the clause ''Contract Administration''.

11.14 NCI Agency will make payment within 60 days of receipt by NCI Agency of a properly prepared and documented invoice.

12. LIQUIDATED DAMAGES

12.1   This Clause replaces Clause 38 (Liquidated Damages) of the Contract General Provisions.

12.2   If the Contractor fails to:

12.2.1 meet the delivery schedule of the Deliverables or any specified major performance milestones or required performance dates specified in the Schedule of Supplies and Services to this Contract, or any extension thereof, or

12.2.2 deliver and obtain acceptance of the Deliverables or to acceptably perform the services as specified in the Schedule of Supplies and Services to this Contract,

the actual damage to the Purchaser for the delay will be difficult or impossible to determine. Therefore, in lieu of actual damages the Contractor shall pay to the Purchaser, for each day of delinquency in achieving the deadline or milestone, fixed and agreed liquidated damages of 1% (one per cent) per day of the associated payment set forth in the schedule of payments provided in Clause 11 of the Contract Special Provisions.

12.3   In addition to the liquidated damages, the Purchaser shall have the possibility of terminating this Contract in whole or in part, as provided in Clause 39 (Termination for Default) of the Contract General Provisions. In the event of such termination, the Contractor shall be liable to pay the excess costs provided in Clause 39.5 (Termination for Default) of the Contract General Provisions.

12.4   The Contractor shall not be charged with liquidated damages when the delay arises out of causes beyond the control and without the fault or negligence of the Contractor as defined in Clause 39.6 (Termination for Default) of the Contract General Provisions. In such event, subject to the provisions of Clause 41 (Disputes) of the Contract General Provisions, the Purchaser shall ascertain the facts and extent of the delay and shall extend the time for performance of the Contract when in his judgement the findings of the fact justify an extension.

12.5   Liquidated damages shall be payable to the Purchaser from the first day of delinquency and shall accrue at the rate specified in Clause 12.2.2 above to 15% of the value of each line item individually and an aggregate sum of all delinquent items not to exceed 15% of the value of the total Contract. These liquidated damages shall accrue automatically and without any further notice being required.

12.6   The amount of Liquidated Damages due by the Contractor shall be recovered by the Purchaser in the following order of priority:

   a) By deducting such damages from the amounts due to the Contractor against the Contractor's invoices.

   b) By proceeding against any surety or deducting from the Performance Guarantee if any

   c) By reclaiming such damages through appropriate legal remedies.

12.7   The rights and remedies of the Purchaser under this clause are in addition to any other rights and remedies provided by law or under this Contract.

13. SERVICES MODIFICATIONS

13.1   The Purchaser shall have the right to increase or decrease the services as he deems necessary.

13.2   The Purchaser shall inform the Contractor about a change in the services by issuing a service request. Each change in services shall be

formalized by means of a Contract Amendment in accordance with Clause 16 (Changes) of the Contract General Provisions.

13.3   The delivery date for a new service / effective date of reduction of services will be stipulated in the service request and shall become contractually binding by means of the relevant Contract Amendment.

14. SUPPLEMENTAL AGREEMENT(S), DOCUMENTS AND PERMISSIONS

14.1   If any supplemental agreements, documents and permissions are introduced after Contract award, the execution of which by the Purchaser is/ are required by national law or regulation, and it is determined that the Contractor failed to disclose the requirement for the execution of such agreement from the Purchaser prior to Contract signature, the Purchaser may terminate this Contract for Default, in accordance with Clause 39 (Termination for Default) of the Contract General Provisions.

14.2   Supplemental agreement(s), documents and permissions, the execution of which by the Purchaser is/are required by national law or regulation and that have been identified by the Contractor prior to the signature of this Contract, but have not yet been finalised and issued by the appropriate governmental authority, are subject to review by the Purchaser. If such supplemental agreement(s), documents and permissions are contrary to cardinal conditions of the signed Contract between the Parties, and the Parties and the appropriate governmental authority cannot reach a mutual satisfactory resolution of the contradictions, the Purchaser reserves the right to terminate this Contract and the Parties agree that in such case the Parties mutually release each other from claim for damages and costs of any kind, and any payments received by the Contractor from the Purchaser will be refunded to the Purchaser by the Contractor.

15. SECURITY

15.1   This Clause supplements Clause 11 (Security) of the Contract General Provisions.

15.2   The security classification of this Contract is NATO UNCLASSIFIED.

15.3   In the performance of all works under this Contract it shall be the Contractor's responsibility to ascertain and comply with all applicable NATO and National security regulations as implemented by the Purchaser and by the local authorities.

15.4   Contractor and /or Subcontractor personnel employed under this Contract that will require access to locations, such as sites and headquarters, where classified material and information up to and including "NATO SECRET" are handled shall be required to have a NATO security clearance up to this level.

15.5   All NATO CLASSIFIED material entrusted to the Contractor shall be handled and safeguarded in accordance with applicable security regulations.

15.6   The Contractor will be required to handle and store classified material to the level of "NATO SECRET".

15.7   It shall be the Contractor's responsibility to obtain the appropriate personnel and facility clearances to the levels stated in the preceding paragraphs and to have such clearances confirmed to the Purchaser by the relevant National security authority for the duration of the Contract in its entirety.

15.8   Failure to obtain or maintain the required level of security for Contractor personnel and facilities for the period of performance of this Contract shall not be grounds for any delay in the scheduled performance of this Contract and may be grounds for termination under Clause 39 (Termination for Default) of the Contract General Provisions.

15.9   The Contractor shall note that there are restrictions regarding the carriage and use of electronic device (e.g. laptops) in Purchaser secured locations. The Contractor shall be responsible for satisfying and obtaining from the appropriate site authorities the necessary clearance to bring any such equipment into the facility.

16. KEY PERSONNEL

16.1   The designated Contractor personnel fulfilling the roles as described in Statement of Work are considered Key Personnel for successful Contract performance and are subject to the provisions of this Clause as set forth in the following paragraphs

16.2   The following individuals are identified as Key Personnel under this Contract:

Role	Name
Project Manager (PM)	To be completed based on proposal
Quality Manager	To be completed based on proposal
I&T Lead (Technical Lead / Senior Sytem Engineer)	To be completed based on proposal
Test Director / Test Engineer	To be completed based on proposal
Other (TBD by Bidder)	To be completed based on proposal

16.3   Under the terms of this Clause, Key Personnel may not be voluntarily diverted by the Contractor to perform work outside the Contract unless approved by the Purchaser. In cases where the Contractor has no control over the individual's non-availability (e.g. resignation, sickness, incapacity, etc.), the Contractor shall notify the Purchaser immediately of a change of Key Personnel and offer a substitute with equivalent qualifications at no additional costs to the Purchaser within 21 days of the date of knowledge of the prospective vacancy.

16.4   The Contractor shall take all reasonable steps to avoid changes to Key Personnel assigned to this project except where changes are unavoidable or are of a temporary nature. Any replacement personnel shall be of a similar

grade, standard and experience as the individual to be substituted and must meet the minimum qualifications and required skills cited in the attached Statement of Work.

16.5   In the event of a substitution of any Key Personnel listed above and prior to commencement of performance, the Contractor shall provide a CV for the personnel proposed. The CV shall clearly stipulate full details of professional and educational background, and evidence that the personnel is qualified in pertinent Contract related areas of the SOW.

16.6   The Purchaser reserves the right to interview any Contractor personnel proposed in substitution of previously employed Contractor Key Personnel to verify their language skills, experience and qualifications, and to assess technical compliance with the requirements set forth in the SOW.

16.6.1 The interview, if required, may be conducted as a telephone interview, or may be carried out at the Purchaser's premises in Brussels, Belgium.

16.6.2 If, as a result of the evaluation of the CV and/or interview the Purchaser judges that the proposed replacement Key Personnel does not meet the required skills levels, he shall have the right to request the Contractor to offer another qualified individual in lieu thereof.

16.6.3 All costs to the Contractor associated with the interview(s) shall be borne by the Contractor, independently from the outcome of the Purchaser's evaluation.

16.7   The Purchaser Contracting Authority will confirm any consent given to a substitution in writing and only such written consent shall be deemed as valid evidence of Purchaser consent. Each of the replacement personnel will also be required to sign the Non-Disclosure Declaration at Annex A hereto prior to commencement of work.

16.8   Furthermore, even after acceptance of Contractor personnel on the basis of his/her CV and/or interview, the Purchaser reserves the right to reject Contractor personnel, if the individual is not meeting the required level of competence. The Purchaser will inform the Contractor, in writing, in cases where such a decision is taken and the Contractor shall propose and make other personnel available within ten working days after the written notification. The Purchaser shall have no obligation to justify the grounds of its decision and the Purchaser's acceptance of Contractor personnel shall in no way relieve the Contractor of his responsibility to achieve the contractual and technical requirements of this Contract nor imply any responsibility of the Purchaser.

16.9   The Purchaser may, for just cause, require the Contractor to remove his employee. Notice for removal will be given to the Contractor by the Purchaser in writing and will state the cause justifying the removal. The notice will either demand substitution for the individual involved and/or contain a notice of default and the remedies to be sought by the Purchaser.

16.10 In those cases where, in the judgement of the Purchaser, the inability of the Contractor to provide a suitable replacement in accordance with the terms of this Clause may potentially endanger the progress under the Contract, the

Purchaser shall have the right to terminate the Contract as provided under Clause 39 (Termination for Default) of the Contract General Provisions.

17. INDEPENDENT CONTRACTOR

17.1   The Personnel provided by the Contractor are at all times employees of the Contractor and not the Purchaser. In no case shall Contractor personnel act on behalf of or as an agent for NATO or any of its bodies. In no way shall the Contractor personnel claim directly or indirectly to represent NATO in an official capacity or claim themselves to be NATO employees.

17.2   The Purchaser shall not be responsible for securing work permits, lodging, leases nor tax declarations, driving permits, etc., with national or local authorities. Contractors personnel employed under this Contract are not eligible for any diplomatic privileges or for NATO employee benefits.

18. NON DISCLOSURE AGREEMENT

18.1   All Contractor and Subcontractor personnel working at any NATO Organisation / Commands premises or having access to NATO classified / commercial-in-confidence information must certify and sign the Declaration attached hereto at Annex A and provide it to the NCI Agency Contracting Officer prior to the commencement of any performance under this Contract.

19. CARE AND DILIGENCE OF PROPERTY

19.1   The Contractor shall use reasonable care to avoid damaging buildings, walls, equipment, and vegetation (such as trees, shrub and grass) on the work site.

19.2   If the Contractor damages any such buildings, walls, equipment or vegetation on the work site, he shall fix or replace the damage as directed by the Purchaser and at no expense to the Purchaser. If he fails or refuses to make such repair or replacement, the Contractor shall be liable for the cost thereof, which may be deducted from the Contract price.

19.3   The Purchaser will exercise due care and diligence for the Contractor's furnished equipment and materials on site. The Purchaser will, however, not assume any liability except for gross negligence and wilful misconduct on the part of the Purchaser's personnel or agents.

19.4   The Contractor shall, at all times, keep the site area, including storage areas used by the Contractor, free from accumulations of waste. On completion of all work the Contractor is to leave the site area and its surroundings in a clean and neat condition.

20. RESPONSIBILITY OF THE CONTRACTOR TO INFORM EMPLOYEES OF WORK ENVIRONMENT

20.1   The Contractor shall inform his employees under this Contract of the terms of the Contract and the conditions of the working environment.

20.2   Specifically, personnel shall be made aware of all risks associated with the performance under this Contract, the conditions of site in which the

performance is to take place and living conditions while performing within the boundaries of the Contract. The selection of adequate personnel shall remain sole responsibility of the Contractor.

21. CONTRACTOR LOGISTICS SUPPORT (CLS)

21.1 Clause 27 (Warranty of Work) and Clause 31 (Software Warranty) of the Contract General Provisions are supplemented with the following:

21.1.1 CLS, including any warranty, shall start after Site-PSA, for each Site, as indicated in the SOW. Until a warranty period is complete, software (except for PFE Software) to be provided under this Contract shall be the Contractor's responsibility.

21.1.2 The CLS period for all hardware and for all services shall be 60 months from Site-PSA.

21.1.3 The CLS period for all software shall be 60 months from Site-PSA.

21.2 Sub-Clause 27.4 of the Contract General Provisions is replaced with the following:

21.2.1 Any hardware or parts thereof corrected or furnished in replacement and any services re-performed shall also be subject to the conditions of Clause 27 (Warranty of Work) of the Contract General Provisions to the same extent as hardware and services initially accepted. The CLS, including any warranty, with respect to these hardware and services, or parts thereof shall run from the date of delivery of the corrected or replaced hardware and services and shall cover the remaining period until expiration of the initial warranty period stated in Clause 21.1 above.

22. SOFTWARE

22.1 The Purchaser reserves the right to exclude from the awarded Contract the purchase of software licenses for which NATO has established centralized Contracts. In this case, the Contract terms, schedule and prices will be modified accordingly, and the software licenses will be provided to the Contractor in the form of "Purchaser Furnished Property (including software)".

22.2 Where the term Purchaser Furnished Equipment (PFE) is used it should be interpreted as Purchaser Furnished Property as defined in the Contract General Provisions.

23. WARRANTY

23.1 The Contractor shall provide warranty on all material provided under this Contract and in accordance with paragraph 14 and Annex B of Book II, Part IV of the Statement of Work or a minimum one (1) year warranty where no period is specified.

23.2 For this purpose the Contractor shall provide exact warranty conditions by type of equipment and detailed handling instructions, including information of points of contact to be contacted in case of a warranty claim.

24. OBSOLESCENCE

24.1   It is the responsibility of the Contractor to ensure that adequate supplies of replacement parts and equipment are available to perform the services for the duration of the Period of Performance. It is recognised that in some cases, the end of production of certain items of hardware and/or the end of support for certain software and software tools may occur suddenly and/or with limited or no warning. In the case where limited or no warning has been provided or where the acquisition of logistics stocks is not an adequate response, the Contractor shall notify the Purchaser of the event in writing as early as practicable after the Contractor has first knowledge. The notification shall provide a brief description of the nature of the event and the potential impact of the event on the ability of the Contractor to meet the performance requirements of the SOW, or a SLA. The Contractor shall further provide recommendations in the form of one or more Engineering Change Proposals (ECPs) as to the solution(s) to the potential impacts. These recommendations shall provide a full life cycle cost of implementation and support as well as the technical risks and impacts involved if the solution(s) or each of the solutions were implemented (trade off analysis).

24.2   ECPs issued pursuant to this Clause may also include proposals for Optimisation as set forth in Clause 25 below.

24.3   After review and analysis, the Purchaser will inform the Contractor of the acceptance of one or more Enginering Change Proposals (ECP(s)) and the changes and the agreed adjustment to the price of the Contract which will be incorporated into the Contract by formal Amendment. Such adjustment shall cover the Contractor's cost associated to the in depth obsolescence study when applicable. The Purchaser may also decide to take no action and accept the impact on system performance/supportability as detailed by the Contractor. In such a case, an Amendment to the Contract will be executed changing the aspects of the SOW or SLA and SOW as required to reflect the impact of not taking any action, and the recovery of the cost associated to the in depth obsolescence study if applicable.

25. OPTIONS

25.1   Operations and Maintanace (O&M) of Wave 1 is optional and is available for exercise by the Purchaser at any time and in any combination from the date of Contract execution to Wave 1 Acceptance plus one (1) year. If the Purchaser exercises such options, the Contractor shall deliver such specified quantities of additional or alternative supplies and services at such times and to such destinations as specified in the Contract.

25.2   Wave 2 is optional and is available for exercise by the Purchaser at any time and in any combination from the date of Contract execution to Wave 1 Acceptance plus one (1) year. If the Purchaser exercises such options, the Contractor shall deliver such specified quantities of additional or alternative supplies and services at such times and to such destinations as specified in the Contract.

25.3   Operations and Maintanace (O&M) of Wave 2 is optional and is available for exercise by the Purchaser at any time and in any combination

from the date of Contract execution to Wave 2 Acceptance plus one (1) year. If the Purchaser exercises such options, the Contractor shall deliver such specified quantities of additional or alternative supplies and services at such times and to such destinations as specified in the Contract.

25.4   Prices for all optional line items shall have a validity period that corresponds to the option exercise period cited above.

25.5   The Contractor understands that there is no obligation under this Contract for the Purchaser to exercise any of the optional line items and that the Purchaser bears no liability should he decide not to exercise the options (totally or partially). Further, the Purchaser reserves the right to request another Contractor (or the same), to perform the tasks described in the optional line items of the current Contract through a new Contract with other conditions.

25.6   Any options exercised shall be exercised by written Amendment to the Contract.

26. OPTIMISATION

26.1   The Contractor is encouraged to examine methods and technology that may increase efficient operation and management of the system(s) on which the required services are provided to the Purchaser, thus reducing operating and manpower costs and the overall cost to the Purchaser.

26.2   The Contractor may, during the Period of Performance, introduce Engineering Change Proposals (ECPs) offering innovations and/or technology insertion with a view towards reducing the Total Cost of Ownership TCO to the Purchaser.

26.3   Any such ECP submitted shall cite this Clause as the basis of submission and provide the following information:

26.3.1 A detailed description of the technical changes proposed, the advantages, both long and short term, and an analysis of the risks of implementation;

26.3.2 A full analysis of the prospective savings to be achieved, in the form of a TCO Assessment Report, in both equipment and manpower, including, as appropriate, utility and fuel consumption and NATO manpower, travel, etc.;

26.3.3 A full impact statement of changes that the Purchaser would be required to make, if any, to its operational structure and management procedures;

26.3.4 A fully detailed proposal of any capital investment necessary to achieve the savings;

26.3.5 A schedule of how the changes would be implemented with minimal negative impact to on-going performance and operations.

27. CONTRACT ADMINISTRATION

27.1   The Purchaser is the NATO Communications and Information Agency (NCI Agency). The Purchaser is the Point of Contact for all contractual and

technical issues. The Contractor shall accept Contract modifications only in writing from the Purchaser's Contracting Authority.

27.2   All notices and communications between the Contractor and the Purchaser shall be written and conducted in English. Contract modifications only become valid when received in writing from the General Manager, NCI Agency, and his authorised representative.

27.3   Formal letters and communications shall be personally delivered or sent by mail, registered mail, courier or other delivery service, to the official points of contact quoted in this Contract. Telefax or other electronic means may be used to provide an advance copy of a formal letter or notice which shall subsequently be delivered through the formal communications means.

27.4   Informal notices and informal communications may be exchanged by any other communications means including telephone and e-mail.

27.5   All notices and communications shall be effective upon receipt.

27.6   Official points of contact are:

PURCHASER	
Contractual issues:	**Technical issues:**
NCI Agency	NCI Agency
Batiment Z	Batiment Z
Acquisition	
Boulevard Léopold III	Boulevard Léopold III
B-1110 Brussels	B-1110 Brussels
Belgium	Belgium
POC: Curtis Day	POC: Cedric Salson
Tel: +32 2-707-8155	Tel: +32 6544-7238
Email: IFB-CO-14176-SOA-IDM.Clarifications@ncia.nato.int	E-mail: Cedric.Salson@ncia.nato.int

CONTRACTOR	
Contractual issues:	**Technical issues:**
Company Name	*Company Name*
Address	*Address*
POC:	POC:
Tel:	Tel:
Fax:	Fax:
E-mail:	E-mail:

28. TECHNICAL DIRECTION

28.1   The Contract will be administered by the Purchaser in accordance with the Clause 26 of these Contract Special Provisions entitled "Contract Administration".

28.2   The individuals working on this Contract shall perform the effort within the general scope of work identified in the Contract Part III - Statement of Work (SOW). This effort will be directed on a more detailed level by the Purchaser's Project Manager who will provide detailed tasking and instruction on how to proceed.

28.3   The Purchaser reserves his right to assign a Technical Representative who will provide the Contractor personnel with instruction and guidance, within the general scope of work, in performance of their duties and working schedule.

28.4   Neither the Purchaser's Project Manager as identified in Clause 27 of these Contract Special Provisions, nor any Technical Representative has the authority to change the terms and conditions of the Contract. If the Contractor has reason to believe that the Project Manager/Technical Representative is requesting products and services on terms inconsistent with that in the scope of the Contract, the Contractor shall immediately inform the Purchaser's Contracting Authority for confirmation of the actions. Failure to obtain confirmation that the action of the Project Manager is under the authority of the Contract shall render any subsequent claim null and void.

28.5   Upon receipt of such notification above, the Purchaser's Contracting Authority will:

  a) confirm the effort requested is within scope, or

  b) confirm that the instructions received constitute a change and request a quotation for a modification of scope and/or price, or

  c) rescind the instructions.

29. CONFLICT OF INTEREST

29.1   A conflict of interest means that because of other activities or relationships with other persons or entities, a Contractor is unable, or potentially unable to render impartial assistance or advice to the Purchaser, or the Contractor's objectivity in performing the Contract work is, or might be otherwise impaired, or the Contractor has an unfair competitive advantage. Conflict of interest includes situations where the capacity of a Contractor (including the Contractor's executives, directors, consultants, subsidiaries, parent companies or Subcontractors) to give impartial, technically sound advice or objective performance is or may be impaired or may otherwise result in a biased work product or performance because of any past, present or planned interest, financial or otherwise in organizations whose interest may substantially affected or be substantially affected by the Contractor's performance under the Contract.

29.2   The Contractor is responsible for maintaining and providing up-to-date conflict of interest information to the Purchaser. If, after award of this Contract

or any task order herein, the Contractor discovers a conflict of interest with respect to this Contract or task order which could not reasonably have been known prior to award, or if any additional conflicts or potential conflicts arise after award, the Contractor shall give written notice to the Purchaser as set forth below.

29.3   If, after award of this Contract or any task order herein, the Purchaser discovers a conflict of interest with respect to this Contract or task order, which has not been disclosed by the Contractor, the Purchaser may at its sole discretion request additional information from the Contractor, impose mitigation measures, or terminate the Contract for default in accordance with Clause 39 (Termination for Default) of the Contract General Provisions.

29.4   The Contractor's notice called for in paragraph 29.3 above shall describe the actual, apparent, or potential conflict of interest, the action(s) the Contractor has taken or proposes to take to avoid or mitigate any conflict, and shall set forth any other information which the Contractor believes would be helpful to the Purchaser in analysing the situation. Any changes to the Contractor's conflict of interest mitigation plan, if any is incorporated in the Contract, should be also detailed.

29.5   The Contractor has the responsibility of formulating and forwarding a proposed conflict of interest mitigation plan to the Purchaser, for review and consideration. This responsibility arises when the Contractor first learns of an actual, apparent, or potential conflict of interest.

29.6   If the Purchaser in its discretion determines that the Contractor's actual, apparent, or potential conflict of interest remains, or the measures proposed are insufficient to avoid or mitigate the conflict, the Purchaser will direct a course of action to the Contractor designed to avoid, neutralize, or mitigate the conflict of interest. If the parties fail to reach agreement on a course of action, or if having reached such agreement, the Contractor fails to strictly adhere to such agreement during the remaining period of Contract performance, the Purchaser has the discretion to terminate the Contract for default or alternatively refrain from exercising any further Option or Work Package under the Contract.

29.7   The Contractor's misrepresentation of facts in connection with a conflict of interest reported, or a Contractor's failure to disclose a conflict of interest as required shall be a basis for default termination of this Contract.

30. INCOTERMS

30.1   This Clause replaces Clause 20.1 of the Contract General Provisions.

30.2   Delivery of all items under this Contract shall be made by the Contractor on the basis of "Delivery Duty Paid" (DDP) as defined by the INCOTERMS 2010 (International Chamber of Commerce). It shall be noted, however, that because the Purchaser is exempted from direct taxes and duty as set forth in Clause 26 (Taxes and Duties) of the Contract General Provisions, there is no duty to be paid by the Contractor.

31. EXCLUSION CLAUSE

31.1   This This Contract has an exclusion clause and it is as follows:

31.1.1 The Contractor and its sub-Contractors that supported the award of CO-14171-PMIC shall be excluded from award of this contract of future Contract(s) and sub-Contract(s) for consultancy, hardware or software implementation under the Bi-Strategic Automated Information Systems (Bi-SC AIS) and NATO General Communication Services (NGCS) Programmes.

31.1.2 The Contractor and its sub-Contractors are also excluded from currently holding any other Contract(s) or sub-Contract(s) for consultancy, hardware or software implementation under the Bi-Strategic Automated Information Systems (Bi-SC AIS) and NATO General Communication Services (NGCS) Programmes.

31.2   For informational purposes, the current list of BI-SC AIS and NGCS projects will be available upon request. This list is subject to frequent updates (with newly approved Bi-SC and NGCS Capability Packages (CPs)) via amendments to the Contract.

31.3   The NCI Agency shall not consider mitigation plans regarding this exclusion.

31.4. This exclusion clause does not apply to parent companies of the Contractor and their wholly owned subsidiaries provided that the parent company or its subsidiaries provides proof to the satisfaction of the Purchaser that they operate as a separate legal entity in a completely distinguishable and different business domain. Proof as mentioned above may consist of:

31.4.1. Company's structure

31.4.2. Roles and responsibilities within structure

31.4.3. Business domain

31.4.4. Ownership and control

31.4.5. And any other proof that will fulfil the purpose of the exclusion clause

31.5. This exclusion clause shall remain valid for a period of two (2) years after Contract completion.

31.6. Once the validity period of this exclusion clause has expired, the limitations imposed by this exclusion clause shall no longer apply.

31.7. The Contractor shall insert the substance of paragraphs 31.1 through 31.6 of this clause in all subcontracts for work performed under this Contract. It is the responsibility of the Contractor to ensure that their subcontractor(s) are made aware of this exclusion clause prior to the subcontractor(s) commencing performance under this Contract.

31.8. The Contractor agrees that compliance with this exclusion clause is of the essence and that failure to abide to these terms shall constitute sufficient grounds for the Termination for Default of the Contract in accordance with Clause 39 of the NCI Agency Contract General Provisions.

32. INTELLECTUAL PROPERTY

32.1   This Article augments Clause 30 of the Contract General Provisions.

32.2   Any use of Contractor Background IPR and Third Party IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to Purchaser. The Contractor hereby grants to NATO and NATO Nations a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Contractor Background IPR for the purpose of exploiting or otherwise using the Foreground IPR.

33. INTELLECTUAL PROPERTY RIGHT INDEMNITY AND ROYALTIES

33.1   This Article augments Clauses 29 of the Contract General Provisions.

33.2   The Contractor shall assume all liability and indemnify the Purchaser, its officers, agents and employees against liability, including costs for the infringement of any patents or copyright in force in any countries arising out of the manufacture, services performed or delivery of supplies, or out of the use or disposal by or for the account of the Purchaser of such supplies. The Contractor shall be responsible for obtaining any patent or copyright licences.

34. TIME AND MATERIALS (T&M) OPTIONAL OPERATIONAL SUPPORT

34.1   T&M for IFB-14176-SOA-IDM T&M support will consist of payment for services and materials used provided in the accomplishment of operational support as outlined below.

34.2   The amounts will be computed through the use of direct labour hours at the established labour rates agreed in the SSS and Bidding sheets. The rates shall include wages, indirect costs, general and administrative expense and profit.

CLIN	WORK PACKAGE	WAVE
2.7	2	1
2.7.1 Initial Operational Support		
2.7.2 Follow on Support Year 2		
2.7.3 Follow on Support Year 3		
2.7.4 Follow on Support Year 4		
2.7.5 Follow on Support Year 5		
2.14	2	2
2.14.1 Initial Operational Support		
2.14.2 Follow on Support Year 2		
2.14.3 Follow on Support Year 3		
2.14.4 Follow on Support Year 4		
2.14.5 Follow on Support Year 5		
4.7	4	1
4.7.1 Initial Operational Support		

4.7.2 Follow on Support Year 2		
4.7.3 Follow on Support Year 3		
4.7.4 Follow on Support Year 4		
4.7.5 Follow on Support Year 5		
4.14	4	2
4.14.1 Initial Operational Support		
4.14.2 Follow on Support Year 2		
4.14.3 Follow on Support Year 3		
4.14.4 Follow on Support Year 4		
4.14.5 Follow on Support Year 5		

ANNEX A: DECLARATION

We, the undersigned........(Company) duly represented by ..... (hereinafter "Contractor") do hereby certify that we shall ensure that the following conditions be accepted and observed by all (Contractor) employees working under CO-14176-SOA-IDM.

_____

(Signature)

_____

(Full name in block capitals)

_____

(Date)
==

TO BE SIGNED BY THE CONTRACTOR'S EMPLOYEES WORKING IN THE NATO'S PREMISES UPON COMMENCEMENT OF THEIR WORK.

I UNDERSTAND:

That I must preserve the security of all classified /commercial-in-confidence information which comes to my knowledge as a result of this Contract with NATO and that I undertake to comply with all relevant security regulations.

That I must not divulge to any unauthorised person, any classified/commercial-in confidence information gained by me as a result of my Contract with NATO, unless prior permission for such disclosure has been granted by the General Manager of the NCI Agency or by his designated representative.

That I must not, without the approval of the General Manager of the NCI Agency publish (in any document, article, book, CD, video, film, play, or other form) any classified /commercial-in-confidence information which I have acquired in the course of my work under CO-14176-SOA-IDM.

That, at the end of Contract and after performance of all required tasks, I must surrender any official document or material made or acquired by me in the course of my work under CO-14176-SOA-IDM, save such as I have been duly authorised to retain.

That the provisions of the above Declaration apply not only during the period of work under CO-14176-SOA-IDM, but also after my Contract has ceased and that I am liable to prosecution if either by intent or negligence I allow classified/commercial-in-confidence information to pass into unauthorised hands.

ANNEX B: INVOLVEMENT OF FORMER NCI AGENCY EMPLOYMENT

NCI Agency Personnel are required to maintain unquestionable integrity and impartiality in relation to procurements initiated by the NCI Agency.

NCI Agency Personnel shall not disclose any proprietary or contract related information regarding procurement directly or indirectly to any person other than a person authorized by the NCI Agency to receive such information. NCI Agency Personnel shall not disclose any documentation related to a procurement action to any third party without a need to know1 (e.g., draft statement of work, statement of requirements) unless this is expressly provided under NATO Procurement Regulations or authorized in writing by the Director of Acquisition. During an on-going selection, NCI Agency Personnel shall not disclose any information on the selection procedure unless authorized by the Chairman of the award committee/board. The NCI Agency Personnel concerned will ensure that proper access controls are put in place to prevent disclosure of procurement information that has not yet been authorized for release for outside distribution, including draft statements of work and requirement documentations.

NCI Agency Personnel will not participate in a source selection if an offer has been provided by a friend, family member, a relative, or by a business concern owned, substantially owned, or controlled by him/her or by a friend, family member or a relative. NCI Agency Personnel appointed as part of an evaluation shall report such links to the Director of Acquisition immediately upon becoming aware of it.

Contractors and consultants shall not be allowed to participate in the drafting of the statement of work or in the source selection process unless they and their company/employer will be excluded from competition of the related contract. The same will apply to contractors and consultants involved in the definition and development of requirements.

Contractors will be given specific and coherent statements of work, providing precise explanation of how she/he is going to be employed. Tasks to be performed and minimum qualifications are to be well defined from the start. In addition, supervisors will ensure that contractors do not occupy managerial positions within the Agency.

NCI Agency Personnel shall not enter into authorized commitments in the name of NCI Agency or NATO unless specifically authorized. NCI Agency Personnel must abstain from making promises or commitment to award or amend a contract or otherwise create the appearance of a commitment from the NCI Agency unless properly authorized by the NCI Agency.

NCI Agency Personnel shall not endorse directly or indirectly products from industry. Therefore, NCI Agency Personnel shall not name or make statements endorsing or appearing to endorse products of specific companies.

Industry partners will need to abide with the post-employment measures under this Directive upon submission of their bids / Bids to the NCI Agency. As part of the selection process, industry will be requested to agree with an ethical statement.

INDUSTRY INITIATIVES

Industry initiatives may include loans, displays, tests or evaluation of equipment and software, requesting NCI Agency speakers at industry gatherings and conferences, inviting speakers from industry to NCI Agency events, consultancy or studies of technical or organizational issues, etc. These initiatives are usually at no cost to the NCI Agency and take place at a pre-contractual phase or before the development of requirements and specifications. While there are benefits associated with the early involvement of industry in the definition of requirements and specifications, this also raises the potential for unfair treatment of potential competitors.

Industry initiatives which go beyond routine interaction in connection with on-going contracts must be reported to and coordinated by the NCI Agency Acquisition Directorate for approval. Industry initiatives shall be properly documented and governed by written agreements between the NCI Agency and the company concerned where relevant. Such agreements may contain provisions describing the nature of the initiative, the non-disclosure of NCI Agency/NATO information, NCI Agency ownership of any resulting work, the NCI Agency's right to release such work product to future competitors for any follow-on competition or contract, the requirement that any studies must provide non-proprietary solutions and/or an acknowledgement that the participating companies will not receive any preferential treatment in the contracting process.

Any authorized industry initiatives must be conducted in such a way that it does not confer an unfair advantage to the industry concerned or create competitive hurdles for potential competitors.

POST EMPLOYMENT MEASURES

The NCI Agency will not offer employment contracts to former NCI Agency Personnel who departed less than 2 years earlier, unless prior approval by the General Manager has been received.

Former NCI Agency Personnel will not be accepted as consultants or commercial counterpart for two (2) years after finalization of their employment at NCI Agency, unless the General Manager decides otherwise in the interest of the Agency and as long as NATO rules on double remuneration are observed. Such decision shall be recorded in writing. Commercial counterparts include owners or majority shareholders, key account managers, or staff member, agent or consultant of a company and/or subcontractors seeking business at any tier with the NCI Agency in relation to a procurement action in which the departing NCI Agency staff member was involved when he/she was under the employment of the NCI Agency. As per the Prince 2 Project

methodology, a Project is defined as a "temporary organization that is created for the purpose of delivering one or more business products according to an agreed business case". For the purpose of this provision, involvement requires (i) drafting, review or coordination of internal procurement activities and documentation, such as statement of work and statement of requirement; and/or (ii) access to procurement information that has not yet been authorized for release for outside distribution, including draft statements of work and requirement documentations; and/or (iii) being appointed as a representative to the Project governance (e.g., Project Board) with access to procurement information as per (ii) above; and/or (iv) having provided strategic guidance to the project, with access to procurement information as per (ii) above.

In addition to Section 17.2 above, former NCI Agency Personnel at grades A5 and above or ranks OF-5 and above are prohibited during twelve months following the end of their employment with the NCI Agency to engaging in negotiations, representational communications and/or advisory activities with the NCI Agency on behalf of a private entity, unless this has been agreed in advance by the NCI Agency General Manager and notified to the ASB.

NCI Agency Personnel leaving the Agency shall not contact their former colleagues in view of obtaining any information or documentation about procurement activities not yet authorized' release. NCI Agency Personnel shall immediately report such contacts to the Director of Acquisition.

The ASB Chairman will be the approving authority upon recommendation by the Legal Adviser when the NCI Agency Personnel concerned by the above is the NCI Agency General Manager and will notify the ASB.

NCI Agency Personnel leaving the Agency shall sign a statement that they are aware of the post-employment measures set out in this Directive.

The post-employment measures set out in this Directive shall be reflected in the NCI Agency procurement documents, such as IFBs, and Contract provisions.

NATO UNCLASSIFIED

NATO COMMUNICATIONS AND INFORMATION AGENCY

CONTRACT GENERAL PROVISIONS

V 1.0 dated 16 Oct 2014

Index of Clauses

The Contract General Provisions

NATO UNCLASSIFIED

The Contract General Provisions

1. ORDER OF PRECEDENCE

In the event of any inconsistency in language, terms or conditions of the various parts of this Contract, precedence will be given in the following order:

1.1.   The Signature Page;

1.2.   The Contract Schedules, Part I;

1.3.   The Contract Contract Special Provisions, Part II;

1.4.   The Contract General Provisions, Part III;

1.5.   The Statement of Work, Part IV of the Contract;

1.6.   The Annexes to the Statement of Work.

2. DEFINITIONS OF TERMS AND ACRONYMS

2.1   ***Assembly***-   An item forming a portion of equipment that can be provisioned and replaced as an entity and which normally incorporates replaceable parts or groups of parts.

2.2   ***Acceptance-*** Acceptance is the act by which the Contracting Authority recognises in writing that the delivered Work meets the Contract requirements..

2.3   ***Claims-***   A written demand or written assertion by one of the Parties seeking, as a matter of right, the payment of money in a sum certain, the adjustment or interpretation of Contract terms, or other relief arising under or in relation to this Contract.

2.4   ***Clause-***   A provision of the Special or General Provisions of this Contract.

2.5   ***Codification Authority-***   The National Codification Bureau (NCB) or authorised agency of the country in which the Work is produced.

2.6   ***Commercial Off-the-Shelf Items (COTS)-***   The term "Commercially Off-the-Shelf Item (COTS)" means any item that:is a commercial item, customarily used by the general public, that has been sold, leased, or licensed to the general public or has been offered for sale, lease or license to the general public;

   a) is sold in substantial quantities in the commercial marketplace; and

   b) is offered to the Purchaser, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace.

2.7   ***Component-***   A part or combination of parts, having a specific function, which can be installed or replaced only as an entity.

The Contract General Provisions

2.8 **Contractor Background IPR-**   Any IPR owned by the Contractor and/or any Sub-contractor or licensed by a third party to the Contractor which is not created in relation to or as the result of work undertaken for any purpose contemplated by the Contract and which is needed for the performance of the Contract or for the exploitation of Foreground IPR.

2.9 **Correction-** Elimination of a Defect.

2.10 **Contract-**   The agreement concluded between the Purchaser and Contractor, duly signed by both contracting parties. The Contract includes the documents referred to in Clause 1 (Order of Preference).

2.11 **Contracting Authority-**   The General Manager of the NCI Agency, the Director of Acquisition, the Chief of Contracts of the NCI Agency or the authorised representatives of the Chief of Contracts of the NCI Agency.

2.12 **Contractor-** The person or legal entity from a Participating Country which has signed this Contract and is a Party thereto.

2.13 **Day-** A calendar day

2.14 **Defect-** Any condition or characteristic in any Work furnished by the Contractor under the Contract that is not in compliance with the requirements of the Contract.

2.15 **Deliverable-** Any and all goods (including movable and immovable goods) to be delivered pursuant to the terms of this Contract including, without limitation, building, raw materials, components, intermediate Assemblies, Parts, end products, equipment, documentation, data, software.

2.16 **Design Defect-** Defect attributable to incompatibility, unsuitability or erroneous application of theory, drawings or formula.

2.17 **Effective Date of Contract (or "EDC")-**   The date upon which this Contract is deemed to start. Unless otherwise specified, a Contract enters into force on the date of the last signature of the Contract by the Parties.

2.18 **Failed Component-**   A part or combination of parts, having a specific function, which can be installed or replaced only as an entity which ceases to perform in a manner consistent with its intended use and specifications of the Contract.

2.19 **Foreground IPR** -   Any IPR created by the Contractor or any subcontractor of the Contractor in the course of or as the result of work undertaken for any purpose contemplated by the Contract.

2.20 **IPR-**   Any intellectual property rights of any qualification irrespective of their stage of development or finalisation, including but not limited to patents, trademarks (registered of not), designs and models (registered or not) and applications for the same, copyright (including on computer software), rights in databases, know-how, confidential information and rights in records (whether or not stored on computer) which includes technical and other data and documents.

The Contract General Provisions

2.21 **Manufacturing Defect-**   Defect attributable to improper manufacturing processes, testing or quality control procedures.

2.22 **NATO-** The North Atlantic Treaty Organisation. For the purpose of this contract, the term NATO includes NATO bodies, the NATO military command structure, agencies and NATO nations.

2.23 **NCI AGENCY-** The NATO Communications and Information Agency. The NCI Agency is part of the NCIO. The General Manager of the Agency is authorised to enter into contracts on behalf of the NATO CI Organisation.

2.24 **NATO COMMUNICATIONS AND INFORMATION ORGANISATION (NCIO)-** The NATO Communications and Information Organisation. The NCI Organisation constitutes an integral part of the North Atlantic Treaty Organisation (NATO) The NCI Organisation is the legal personality from whence flows the authority of its agent, the NCI Agency, to enter into contracts.

2.25 **NATO Purposes-**   Activities conducted by or on behalf of NATO to promote the common defence and common interests of NATO, such as, among others, NATO operations, NATO procurement, NATO training and NATO maintenance.

2.26 **Part-** An item of an assembly or sub-assembly, which is not normally further broken down.

2.27 **Participating Country-** A NATO member country that participates in financing the effort.

2.28 **Parties-** The Contracting Parties to this Contract, i.e., the Purchaser and the Contractor.

2.29 **Purchaser**- The NCI Organisation, as represented by the General Manager, NCI Agency. The Purchaser is the legal entity who awards and administers the Contract on behalf of NATO and stands as one of the Contracting Parties.

2.30 **Purchaser Background IPR-**   Any IPR owned by the Purchaser as of the Effective Date of Contract and which has been developed by, assigned to or licensed to the Purchaser prior to the Effective Date of Contract.

2.31 **Purchaser Furnished Property-** Any item of equipment, material, document, technical data, information and Software or any other item of property furnished by the Purchaser to the Contractor required or useful for the performance of the Contract. The Purchaser Furnished Property, if any, shall be detailed in the Contract.

2.32 **Software (Computer Software)-** A computer program comprising a series of instructions, rules, routines regardless of the media in which it is recorded, that allows or cause a computer to perform a specific operation or a series of operations.

2.33 **Software Defect-**   Any condition or characteristic of Software that does not conform with the requirements of the Contract.

The Contract General Provisions

2.34 **Sub-Assembly-** A portion of an Assembly consisting of two or more parts that can be provisioned and replaced as an entity. The definition purposely excludes Components and/or Parts.

2.35 **Sub-contract-** Any agreement made by the Contractor with any third party in order to fulfil any part of the obligations under this Contract. Sub-contracts may be in any legal binding form, *e.g.*, contract, purchase order, etc.

2.36 **Sub-contractor-** Any person or legal entity directly or indirectly under Sub-contract to the Contractor in performance of this Contract.

2.37 **Third Party IPR-** Any IPR owned by a third party not being the Purchaser or the Contractor or its Subcontractor, which is needed for the performance of the Contract or for the exploitation of Foreground IPR. This includes, for example, third party software, including open source software.

2.38 **Work-** Any deliverable, project design, labour or any service or any other activity to be performed by the Contractor under the terms of this Contract.

3. AUTHORITY

3.1. All binding contractual instruments and changes, including amendments, additions or deletions, as well as interpretation of and instructions issued pursuant to this Contract shall be valid only when issued in writing by the Purchaser and signed by the Contracting Authority only.

3.2. No direction which may be received from any person employed by the Purchaser or a third party shall be considered as grounds for deviation from any of the terms, conditions, specifications or requirements of this Contract except as such direction may be contained in an authorised amendment to this Contract or instruction duly issued and executed by the Contracting Authority. Constructive change may not be invoked by the Contractor as a basis for Claims under this Contract.

3.3. The entire agreement between the Parties is contained in this Contract and is not affected by any oral understanding or representation, whether made previously to or subsequently to this Contract.

3.4. Personal notes, signed minutes of meetings, comments to delivered documentation and letters, e-mails and informal messages from project or other Purchaser staff which may indicate the intent and willingness to make changes to the Contract, do not implement the change to the Contract and shall not be used as a basis for claiming change to the Contract by the Contractor.

NATO UNCLASSIFIED

The Contract General Provisions

4. APPROVAL AND ACCEPTANCE OF CONTRACT TERMS

4.1.   By his signature of the Contract, the Contractor certifies that he has read and unreservedly accepts and approves of all terms and conditions, specifications, plans, drawings and other documents which form part of and/or are relevant to the Contract. The Contractor further agrees that the terms of the Contract take precedence over any proposals or prior commitments made by the Contractor in order to secure the Contract. Contractor also hereby waives any and all rights to invoke any of the Contractor's general and special terms and conditions of sales and/or supply.

5. LANGUAGE

5.1.   All written correspondence, reports, documentation and text of drawings delivered to the Purchaser by the Contractor shall be in the English language.

6. AUTHORISATION TO PERFORM/CONFORMANCE TO NATIONAL LAWS AND REGULATIONS

6.1.   The Contractor warrants that he and his Sub-contractors are duly authorised to operate and do business in the country or countries in which this Contract is to be performed and that he and his Sub-contractors have obtained or will obtain all necessary licences and permits required in connection with the Contract. No claim for additional monies with respect to any costs or delay to obtain the authorisations to perform shall be made by the Contractor.

6.2.   The Contractor acknowledges that he and his Sub-contractors are responsible during the performance of this Contract for ascertaining and complying with all applicable laws and regulations, including without limitation: labour standards, environmental laws, health and safety regulations and export controls laws and regulations in effect at the time of Contract signature or scheduled to go into effect during Contract performance.   Failure to fully ascertain and comply with such laws, regulations or standards shall not be the basis for claims for change to the specifications, terms, conditions or monetary value of this Contract.

7. FIRM FIXED PRICE CONTRACT

7.1   This is a Firm Fixed Price Contract. The Firm Fixed Price of this Contract is as stated on the signature page of the Contract or any amendments thereto. The Purchaser assumes no liability for costs incurred by the Contractor in excess of the stated Firm Fixed Price except as may be authorised under certain provisions of this Contract.

The Contract General Provisions

8. PERFORMANCE GUARANTEE

8.1.   As a guarantee of performance under the Contract, the Contractor shall deposit with the Purchaser within thirty (30) calendar days from the Effective Date of Contract a bank guarantee (the "Performance Guarantee") denominated in the currency of the Contract, to the value of ten per cent (10%) of the total Contract price.

8.2.   The Performance Guarantee, the negotiability of which shall not elapse before the expiration of the warranty period, or such other period as may be specified in the Contract, shall be made payable to the Purchaser and shall be in the form of certified cheques or a Standby Letter of Credit subject to the agreement of the Purchaser. In the case of a Standby Letter of Credit, payment shall be made to the Purchaser without question and upon first demand by the Purchaser against a certificate from the Purchaser's Contracting Authority that the Contractor has not fulfilled its obligations under the Contract. The Contractor shall have no right to enjoin or delay such payment.

8.3.   Certified Cheques issued to fulfil the requirements of the Performance Guarantee will be cashed by the Purchaser upon receipt and held in the Purchaser's account until the term of the Performance Guarantee has expired.

8.4.   The standby letter of credit shall be subject to Belgian Law and shall be issued by (i) a Belgian bank, (ii) the Belgian subsidiary of a foreign bank licensed to provide financial services in Belgium; or (iii) an insurance company licensed to do business in Belgium and belonging to a Belgian banking institution provided the banking institution guarantees explicitly the demand for payment, unless otherwise specified by the Purchaser.

8.5.   The Contractor shall request in writing relief from the Performance Guarantee upon expiration of the warranty period or such other period as may be specified in the Contract and such relief may be granted by the Purchaser.

8.6.   The Contractor shall be responsible, as a result of duly authorised adjustments in the total contract price and/or period of performance by the Purchaser, for obtaining a commensurate extension and increase in the Performance Guarantee, the value of which shall not be less than ten per cent (10%) of the total contract price (including all amendments), and for depositing such guarantee with the Purchaser, within thirty (30) calendar days from the effective date of aforesaid duly authorised adjustment.

8.7.   The failure of the Contractor to deposit and maintain such Performance Guarantee with the Purchaser within the specified time frame, or any extension thereto granted by the Purchaser's Contracting Authority, is a material breach of the Contract terms and conditions subject to the

The Contract General Provisions

provisions of the Contract regarding Termination for Default.

8.8.   The rights and remedies provided to the Purchaser under the present Clause are in addition to any other rights and remedies provided by law or under this Contract. The certificate described in Clause 8.2 above shall not be regarded as a Termination for Default and this Clause is in addition to and separate from the Clause of the Contract detailing termination for default.

8.9.   If the Contractor elects to post the Performance Guarantee by Standby Letter of Credit, the form of the document shall be substantially as follows:

PERFORMANCE GUARANTEE STANDBY LETTER OF CREDIT

Standby Letter of Credit Number: _____

Issue Date: _____

Initial Expiry Date: _____

Final Expiry Date: _____

Beneficiary: NCI Agency, Finance, Accounting & Operations
                    Boulevard Leopold III, B-1110, Brussels
                    Belgium

1.   We hereby establish in your favour our irrevocable standby letter of credit number {number} by order and for the account of (NAME AND ADDRESS OF CONTRACTOR)   in   the   amount   of _____.   We   are   advised   this undertaking represents fulfilment by (NAME OF CONTRACTOR) of certain performance requirements under Contract No. _____ dated _____ between the NCI Agency ("NCIA and (NAME OF CONTRACTOR).

2.   We hereby engage with you that drafts drawn under and in compliance with the terms of this letter of credit will be duly honoured upon presentation of documents to us on or before the expiration date of this letter of credit.

3.   Funds under this letter of credit are available to you without question or delay against presentation of a certificate signed by the NCI Agency Contracting Officer which states:

            "(NAME OF CONTRACTOR) has not fulfilled its obligations under Contract No. _____ dated _____ between NCI Agency and (NAME OF CONTRACTOR) (herein called the "Contract"), and the NCI Agency, as beneficiary, hereby draws on the standby letter of credit number _____ in the amount denominated in the currency of the Contract, Amount up to the maximum available under the LOC), such funds to be transferred to the account of the Beneficiary

The Contract General Provisions

number _____(to be identified when certificate is presented)."

Such certificate shall be accompanied by the original of this letter of credit.

4. This Letter of Credit is effective the date hereof and shall expire at our office located at ____(Bank Address)____ on _____. All demands for payment must be made prior to the expiry date.

5. It is a condition of this letter of credit that the expiry date will be automatically extended without amendment for a period of one (1) year from the current or any successive expiry date unless at least 90 (ninety) calendar days prior to the then current expiry date we notify you by registered mail and notify (NAME OF CONTRACTOR) that we elect not to extend this letter of credit for such additional period. However, under no circumstances will the expiry date extend beyond _____ ("Final Expiry Date") without amendment.

6. We may terminate this letter of credit at any time upon 90 (ninety) calendar days notice furnished to both (NAME OF CONTRACTOR) and the NCI Agency by registered mail.

7. In the event we (the issuing bank) notify you that we elect not to extend the expiry date in accordance with paragraph 6 above, or, at any time, to terminate the letter of credit, funds under this credit will be available to you without question or delay against presentation of a certificate signed by the NCI Agency Contracting Officer which states:

> "The NCI Agency has been notified by {issuing bank} of its election not to automatically extend the expiry date of letter of credit number {number} dated {date} pursuant to the automatic renewal clause (or to terminate the letter of credit). As of the date of this certificate, no suitable replacement letter of credit, or equivalent financial guarantee has been received by the NCI Agency from, or on behalf of (NAME OF CONTRACTOR). (NAME OF CONTRACTOR) has, therefore, not fulfilled its obligations under Contract No. _____ dated _____ between NCI Agency and (NAME OF CONTRACTOR), and the NCI Agency, as beneficiary, hereby draws on the standby letter of credit number _____ in the amount of (Amount up to the maximum available under the LOC), such funds to be transferred to the account of the Beneficiary number _____ (to be identified when certificate is presented)."

Such certificate shall be accompanied by the original of this letter of credit and a copy of the letter from the issuing bank that it elects not to automatically extend the standby letter of credit, or terminating the letter of credit.

8. The Beneficiary may not present the certificate described in paragraph 7 above

8

The Contract General Provisions

until 20 (twenty) calendar days prior to a) the date of expiration of the letter of credit should {issuing bank} elect not to automatically extend the expiration date of the letter of credit, b) the date of termination of the letter of credit if {issuing bank} notifies the Beneficiary that the letter of credit is to be terminated in accordance with paragraph 6 above.

9.   Multiple partial drawings are allowed to the maximum value of the standby letter of credit.

10.   This letter of credit sets forth in full the terms of our undertaking, and this undertaking shall not in any way be modified, amended, or amplified by reference to any document, instrument, or agreement referred to herein (except the International Standby Practices (ISP 98) hereinafter defined) or in which this letter of credit is referred to or to which this letter of credit relates, and any such reference shall not be deemed to incorporate herein by reference any document, instrument, or agreement.

11.   This Letter of Credit is subject to The International Standby Practices-ISP98 (1998 Publication) International Chamber of Commerce Publication No.590.

9.   PARTICIPATING COUNTRIES

9.1   Unless prior written authorisation of the Purchaser has been obtained, none of the Work, shall be performed other than by firms from and within NATO Participating Countries. Unless otherwise specified in the Contract Special Provisions, the Participating Countries are the twenty-eight (28) Member Nations of the North Atlantic Treaty Organisation.

9.2   Unless prior written authorisation of the Purchaser has been obtained, no material or items of equipment down to and including identifiable Sub-Assemblies shall be manufactured or assembled by a firm other than from and within a NATO Participating Country.

9.3   The Contractor shall not place any Sub-contracts outside the NATO Participating Countries without the prior written authorisation of the Purchaser.

9.4   Unless prior written authorisation of the Purchaser has been obtained, the intellectual property rights for all software and documentation incorporated by the Contractor and/or its Sub-contractors into the Work shall vest with persons or legal entities from and within NATO participating nations and no royalties or licence fees for such software and documentation shall be paid by the Contractor to any source that does not reside within a NATO participating nation.

9.5   Any modification in the nationality, ownership and/or change of control of the Contractor and/or its Sub-contractor(s) shall be immediately notified in writing to the Purchaser with all necessary details to allow the Purchaser to determine whether or not the Contractor and/or its Sub-contractors continue

to comply with the Clauses above. Non-compliance with the Clauses above, by the Contractor and/or its Subcontractor may constitute ground for termination of this Contract under Clause 39 (Termination for Default).

10.   SUB-CONTRACTS

10.1   The Contractor shall place and be responsible for the administration and performance of all Sub-contracts including terms and conditions which he deems necessary to meet the requirements of this Contract in full.

10.2   Prior to the Sub-contractors being given access to any classified information, the Contractor shall ensure that any Sub-contractor that has a need to access classified information for the performance of any part of this Contract has been granted the appropriate facility and personnel security clearances by the Sub-contractor's national authorities and that such clearances are still in effect at the time the information is disclosed and remains in effect throughout the performance of the work to be carried out under the Sub-contract concerned.

10.3   The Contractor shall seek the approval in writing of the Purchaser prior to the placing of any Sub-contract if:

10.3.1   the Sub-contract was not part of the Contractor's original proposal;

and

10.3.2   the value of the Sub-contract is known or estimated to exceed 15 per cent of the total Contract value; or

10.3.3   the Sub-contract is one of a number of Sub-contracts with a single Sub-contractor for the same or related Work under this Contract that in the aggregate are known or expected to exceed 15 per cent of the total Contract value.

10.4   The Contractor shall inform the Purchaser of any change in Sub-contractors for Sub-contracts of a value known or estimated to exceed 15 per cent of the total Contract value.

10.5   The Contractor shall submit a copy of any such proposed Sub-contract including prices when seeking approval to the Contracting Authority but such approval by the Contracting Authority shall in no way relieve the Contractor of his responsibilities to fully achieve the contractual and technical requirements of this Contract.

10.6   The Contractor shall, as far as practicable, select Sub-contractors on a competitive basis consistent with the objectives and requirements of the Contract.

NATO UNCLASSIFIED

The Contract General Provisions

11.   SECURITY

11.1   The Contractor shall comply with all security measures as are prescribed by the Purchaser and the national security authority or designated security agency of each of the NATO countries in which the Contract is being performed.   The Contractor shall be responsible for the safeguarding of classified information, documentation, material and equipment entrusted to him or generated by him in connection with the performance of the Contract.

11.2   In particular the Contractor undertakes to:

11.2.1   appoint an official responsible for supervising and directing security measures in relation to the Contract and communicating details of such measures to the Purchaser on request;

11.2.2   maintain, preferably through the official responsible for security measures, a continuing relationship with the national security authority or designated security agency charged with ensuring that all NATO classified information involved in the Contract is properly safeguarded;

11.2.3   abstain from copying by any means, without the authorisation of the Purchaser, the national security authority or designated security agency, any classified documents, plans, photographs or other classified material entrusted to him;

11.2.4   furnish, on request, information to the national security authority or designated security agency pertaining to all persons who will be required to have access to NATO classified information;

11.2.5   maintain at the work site a current record of his employees at the site who have been cleared for access to NATO classified information.   The record should show the date of issue, the date of expiration and the level of clearance;

11.2.6   deny access to NATO classified information to any person other than those persons authorised to have such access by the national security authority or designated security agency;

11.2.7   limit the dissemination of NATO classified information to the smallest number of persons ("need to know basis") as is consistent with the proper execution of the Contract;

11.2.8   comply with any request from the national security authority or designated security agency that persons entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding both of their obligations under national legislation affecting the safeguarding of classified information, and of their comparable obligations

The Contract General Provisions

under the laws of the other NATO nations in which they may have access to classified information;

11.2.9 report to the national security authority or designated security agency any breaches, suspected breaches of security, suspected sabotage, or other matters of security significance which would include any changes that may occur in the ownership, control or management of the facility or any changes that affect the security arrangements and security status of the facility and to make such other reports as may be required by the national security authority or designated security agency, e.g. reports on the holdings of NATO classified material;

11.2.10 apply to the Purchaser for approval before Sub-contracting any part of the work, if the Sub-contract would involve that the Sub-contractor would have access to NATO classified information, and to place the Sub-contractor under appropriate security obligations no less stringent than those applied to his own contract;

11.2.11 undertake not to utilise, other than for the specific purpose of the Contract, without the prior written permission of the Purchaser or his authorised representative, any NATO classified information furnished to him, including all reproductions thereof in connection with the Contract, and to return all NATO classified information referred to above as well as that developed in connection with the Contract, unless such information has been destroyed, or its retention has been duly authorised with the approval of the Purchaser. Such NATO classified information will be returned at such time as the Purchaser or his authorised representative may direct;

11.2.12 classify any produced document with the highest classification of the NATO classified information disclosed in that document.

12. **RELEASE OF INFORMATION**

12.1 Except as otherwise specified elsewhere in the Contract and to the extent that it is demonstratively unavoidable and without prejudice to the Clause 11 (Security), the Contractor and/or his employees shall not, without prior authorisation from the Purchaser, release to third parties any information pertaining to this Contract, its subject matter, performance there under or any other aspect thereof.

12.2 The Contractor shall seek the prior written approval of the Purchaser before publishing any press release or disclosing any other information, orally or in writing, in relation to the Contract. The approval of the Purchaser shall be required for both the opportunity and the content of the information.

12.3   This provision shall remain in effect after the termination of the Contract and shall cease to apply to any particular piece of information once that information becomes public knowledge other than through an act, default or omission of the Contractor or its Sub-contractors.

13.   **PURCHASER FURNISHED PROPERTY**

13.1   The Purchaser shall deliver to the Contractor, for use only in connection with this Contract, the Purchaser Furnished Property at the times and locations stated in the Contract. In the event that Purchaser Furnished Property is not delivered by such time or times stated in the Schedule, or if not so stated, in sufficient time to enable the Contractor to meet such delivery or performance dates the Purchaser shall, upon timely written request made by the Contractor, and if the facts warrant such action, equitably adjust any affected provision of this Contract pursuant to Clause 16 (Changes).

13.2   In the event that Purchaser Furnished Property is received by the Contractor in a condition not suitable for its intended use, the Contractor shall immediately notify the Purchaser. The Purchaser shall within a reasonable time of receipt of such notice replace, re-issue, authorise repair or otherwise issue instructions for the disposal of Purchaser Furnished Property agreed to be unsuitable. The Purchaser shall, upon timely written request of the Contractor, equitably adjust any affected provision of this\ Contract pursuant to Clause 16 (Changes).

13.3   Title to Purchaser Furnished Property will remain in the Purchaser. The Contractor shall maintain adequate property control records of Purchaser Furnished Property in accordance with sound industrial practice and security regulations.

13.4   Unless otherwise provided in this Contract, the Contractor, upon delivery to him of any Purchaser Furnished Property, assumes the risk of, and shall be responsible for, any loss thereof or damage thereof except for reasonable wear and tear, and except to the extent that Purchaser Furnished Property is consumed in the performance of this Contract.

13.5   Upon completion of this Contract, or at such earlier dates as may be specified by the Purchaser, the Contractor shall submit, in a form acceptable to the Purchaser, inventory schedules covering all items of Purchaser Furnished Property.

13.6   The inventory shall note whether:

13.6.1   The property was consumed or incorporated in fabrication of final deliverable(s);

The Contract General Provisions

13.6.2 The property was otherwise destroyed;

13.6.3 The property remains in possession of the Contractor;

13.6.4 The property was previously returned

13.7 The Contractor shall prepare for shipment, deliver DDP at a destination agreed with the Purchaser, or otherwise dispose of Purchaser Furnished Property as may be directed or authorised by the Purchaser. The net proceeds of any such disposal shall be credited to the Contract price or paid to the Purchaser in such other manner as the Purchaser may direct.

13.8 The Contractor shall not modify any Purchaser Furnished Property unless specifically authorised by the Purchaser or directed by the terms of the Contract.

13.9 The Contractor shall indemnify and hold the Purchaser harmless against claims for injury to persons or damages to property of the Contractor or others arising from the Contractor's possession or use of the Purchaser Furnished Property. The Contractor shall indemnify the Purchaser for damages caused by the Contractor to the Purchaser, its property and staff and arising out of the Contractor's use of the Purchaser Furnished Property.

14. **CONTRACTOR'S PERSONNEL WORKING AT PURCHASER'S FACILITIES**

14.1 The term "Purchaser Facilities" as used in this Clause shall be deemed to include sites, property, utilities, ships or vessels and the term "Facility Representative" shall be deemed to refer to the authority designated by the Purchaser responsible for the site, property, utility, ship or vessel.

14.2 The Facility Representative shall provide such available administrative and technical facilities for Contractor's personnel working at Purchaser's Facilities for the purpose of the Contract as in the opinion of the Facility Representative may be necessary for the effective and economical discharge of Work. The Facility Representative shall also determine whether these facilities will be provided free of charge to the Contractor or determine what charges are payable. The Contractor shall have no claim against the Purchaser for any such additional cost or delay or any additional cost or delay occasioned by the closure for holidays of said facilities, or other reasons, where this is generally published or made known to the Contractor by the Purchaser or his authorised representatives.

14.3 The Contractor shall, except as otherwise provided for in the Contract, make good or, at the option of the Purchaser, pay compensation for all damage occurring to any Purchaser's Facilities occasioned by the Contractor, his servants, agents or Sub-contractors, arising from his or their presence and activities in, and use of, the Purchaser's Facilities; provided that this

Condition shall not apply to the extent that the Contractor is able to show that any such damage was not caused or contributed to, by his neglect, or default or the neglect or default of his servants, agents or Sub-contractors, or by any circumstances within his or their control.

14.4 All property of the Contractor while at a Purchaser Facility shall be at the risk of the Contractor, and the Purchaser shall accept no liability for any loss or damage, except to the extent that any loss or damage is the result of a wilful act or gross negligence on the part of the Purchaser's employees or agents.

15. HEALTH, SAFETY AND ACCIDENT PREVENTION

15.1 If the Purchaser notifies the Contractor in writing of any non-compliance in the performance of this Contract with safety and health rules and requirements prescribed on the date of this Contract by applicable national or local laws, ordinances and codes, and the Contractor fails to take immediate corrective action, the Purchaser may order the Contractor to stop all or part of the Work until satisfactory corrective action has been taken. Such an order shall not entitle the Contractor to an adjustment of the Contract price or other reimbursement for resulting increased costs, or to an adjustment of the delivery or performance schedule.

16. CHANGES

16.1 The Purchaser may at any time, by written order of the Contracting Authority designated or indicated to be a change order ("Change Order") make changes within the general scope of this Contract, including, without limitation, in any one or more of the following:

16.1.1 Specifications (including drawings and designs);

16.1.2 Method and manner of performance of the work, including engineering standards, quality assurance and configuration management procedures;

16.1.3 Marking and method of shipment and packing;

16.1.4 Place of delivery;

16.1.5 Amount, availability and condition of Purchaser Furnished Property.

16.2 The Purchaser shall submit a proposal for Contract amendment describing the change to the Contract.

The Contract General Provisions

16.3   If any such Change Order causes an increase in the Contractor's cost of, or the time required for, the performance of any part of the Work under this Contract, whether or not changed by any such order, the Contractor shall submit a written proposal for adjustment to the Purchaser describing the general nature and amount of the proposal for adjustment. The Contractor shall submit this proposal for adjustment within thirty (30) days after receipt of a written Change Order under (a) above unless this period is extended by the Purchaser.

16.4   If any such Change Order causes a decrease in the Contractor's cost of, or the time required for, the performance of any part of the Work under this Contract, whether or not changed by any such order, the Purchaser shall submit a proposal for adjustment within thirty (30) days from the issuance of the Change Order by submitting to the Contractor a written statement describing the general nature and amount of the proposal for adjustment.

16.5   Where the cost of property made obsolete or in excess as a result of a change is included in the Contractor's claim for adjustment, the Purchaser shall have the right to prescribe the manner of disposition of such property.

16.6   The Purchaser reserves the right to reject the introduction of the change, after the evaluation of the change proposal, even if the Purchaser initiated such change.

16.7   Failure to agree to any requested adjustment shall be a dispute within the meaning of the Clause 41 (Disputes). However, nothing in this Clause shall excuse the Contractor from proceeding with the Contract as changed.

16.8   No proposal for adjustment by the Contractor for an equitable adjustment shall be allowed if asserted after final payment and acceptance under this Contract.

16.9   Any other written or oral order (which, as used in this paragraph includes direction, instruction, interpretation, or determination) from the Purchaser that causes a change shall be treated as a Change Order under this Clause, provided, that the Contractor gives the Purchaser a written notice within thirty (30) Days after receipt of such order stating (i) the date, circumstances, and source of the order; (ii) that the Contractor regards the order as a Change Order; and (iii) a detailed cost and time analysis of the impact of the change, and that the Order is accepted in writing by the Purchaser as a Change Order. The timely written notice requirement, as detailed above, remains in force in all cases, even where, for example, the Purchaser has positive knowledge of the relevant facts.

16.10   All tasks and activities carried out by the Contractor in relation to the processing of the Change Order or in relation to this Clause shall form part of the Contractor's routine work and cannot be charged as additional work.

The Contract General Provisions

17. STOP WORK ORDER

17.1   The Purchaser may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the Work called for by this Contract for a period of ninety (90) days after the order is delivered to the Contractor, and for any further period to which the Parties may agree.

17.2   Any such stop work order shall be specifically identified as a stop work order issued pursuant to this Clause (the "Stop Work Order"). The Stop Work Order may include a description of the Work to be suspended, instructions concerning the Contractor's issuance of further orders for material or services, guidance to the Contractor on actions to be taken on any Sub-contracts and any suggestion to the Contractor for minimizing costs.

17.3   Upon receipt of such a Stop Work Order, the Contractor shall forthwith comply with its terms and take all reasonable steps to minimise costs incurred allocable to the Work covered by the Stop Work Order during the period of work stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to the Contractor, or within any extension of that period to which the Parties shall have agreed, the Purchaser shall either:

17.3.1 cancel the Stop Work Order; or

17.3.2 terminate the Work covered by such Stop Work Order as provided in Clause 40 (Termination for Convenience of the Purchaser).

17.4   If a Stop Work Order issued under this Clause is cancelled or the period of the Stop Work Order or any extension thereof expires, the Contractor shall resume work.

17.5   An equitable adjustment shall be made in the delivery schedule or Contract price, or both, and the Contract shall be modified in writing accordingly, if:

17.5.1   the Stop Work Order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this Contract, and;

17.5.2   the Contractor asserts a Claim for such adjustment within thirty (30) days after the end of the period of work stoppage; provided that, if the Purchaser decides the facts justify such action, he may receive and act upon any such claim asserted at a later date but prior to final payment under this Contract.

17.6   If a Stop Work Order is not cancelled and the Work covered by such Stop Work Order is terminated for the convenience of the Purchaser the reasonable costs resulting from the Stop Work Order shall be allowed in

The Contract General Provisions

arriving at the termination settlement.

18.   CLAIMS

18.1   The Contractor shall specifically identify the Contract Clause(s) under which the Claim(s) is/are based.

18.2   Claims shall be specifically identified as such and submitted:

18.2.1 within the time specified in the Clause under which the Contractor alleges to have a Claim. If no time is specified in the Clause under which the Contractor intends to base his Claim, the time limit shall be sixty (60) days from the date the Contractor has knowledge or should have had knowledge of the facts on which he bases his Claim; and

18.2.2 before final payment, pursuant to and with the exceptions specified in Clause 33 entitled" Release of Claims".

18.2.3 Section 18.2.2 above shall only apply to those Claims for which the Contractor could not have had earlier knowledge and were not foreseeable.

18.3   The Contractor shall be foreclosed from his Claim unless he presents complete documentary evidence, justification and costs for each of his Claims within ninety (90) calendar days from the assertion date of such Claims. Claims shall be supported by specifically identified evidence (including applicable historical and planned cost and production data from the Contractor's books and records). Opinions, conclusions or judgmental assertions not supported by such evidence will be rejected by the Purchaser.

18.4   An individual breakdown of cost is required for each element of Contractor's Claims at the time of claim submission or for any material revision of the Claim.

18.5   The Contractor shall present, at the time of submission of a Claim, an attestation as follows:

> I ....the responsible senior company official authorised to commit the .... with respect to its claims dated .... being duly sworn, do hereby depose and say that: (i) the facts described in the claim are current, complete and accurate; and (ii) the conclusions in the claim accurately reflect the material damages or contract adjustments for which the Purchaser is allegedly liable.

....………..

NATO UNCLASSIFIED

The Contract General Provisions

………………………..

SIGNATURE   Date

18.6   Failure to comply with any of the above requirements shall result in automatic foreclosure of the Claim. This foreclosure takes effect in all cases and also where, for example, the Claim is based on additional orders, where the facts are known to the Purchaser, where the Claim is based on defective specifications of the Purchaser or an alleged negligence in the pre-contractual stage.

18.7   Claims submitted by the Contractor will be reviewed by the Contracting Authority. The Contracting Authority will respond within sixty (60) days with a preliminary decision, based on an assessment and evaluation of the facts presented by the Parties, as to whether the Contracting Authority considers the Claim to have merit for consideration. If the preliminary decision of the Contracting Authority is that the Claim, as submitted is without merit, the Contractor shall have fourteen (14) days to present a rebuttal to the Contracting Authority and request reconsideration of the Contracting Authority's decision. Within thirty (30) days receipt of the Contractor's request for reconsideration, the Contracting Authority will issue a decision. The time requirements stated herein may be extended by the Contracting Authority in order to accommodate additional preparation efforts and fact finding discussions but the Contracting Authority may not unreasonable extend such a period. A decision that the submitted claim is without merit will be identified as such, will be issued in writing by the Contracting Authority and will be conclusive. A decision may only be challenged by the Contractor through the Disputes provisions described herein.

18.8   A decision by the Purchaser that the claim has merit will result in a Contracting Authority request to enter into negotiations with the Contractor to arrive at a mutually agreed fair and equitable settlement. The Contracting Authority's decision will contain a target date for the commencement and conclusion of such operations. If the Parties are unable to arrive at an agreement on a fair and reasonable settlement by the target date for conclusion, or any extension thereto made by the Contracting Authority, the latter may declare that negotiations are at an impasse and issue a preliminary decision as to the fair and reasonable settlement and the reasons supporting this decision. The Contractor shall have a period of thirty (30) days to present a rebuttal to the Contracting Authority and request reconsideration of the Contracting Authority's decision. Within sixty (60) days of receipt of the Contractor's request for reconsideration, the Contracting Authority will issue its decision on the request for reconsideration. This timeframe will be respected unless an authorisation is needed from a NATO or other authority , the schedule for which is beyond the Contracting Authority's control. A

The Contract General Provisions

decision of the Contracting Authority on the reconsideration of the matter will be identified as such, will be issued in writing by the Contracting Authority and will be conclusive. A decision on the reconsideration may only be challenged by the Contractor through the Disputes provisions described herein.

18.9 No Claim arising under this Contract may be assigned by the Contractor without prior approval of the Purchaser.

18.10 The Contractor shall proceed diligently with performance of this Contract, pending final resolution of any request for relief, claim appeal, or action arising under the Contract, and comply with any decision of the Contracting Authority.

19. PRICING OF CHANGES, AMENDMENTS AND CLAIMS

19.1 Contractor's pricing proposals for Changes, amendments and Claims shall be priced in accordance with the Purchaser's Pricing Principles (Annex 1 hereto and the sample spreadsheet and its " Instructions to Complete" at Appendix 1) or the national government pricing rules and regulations for the Contractor's own country, where in force. The Contractor shall provide cost information accompanied by appropriate substantiation as required by the Purchaser in accordance with Purchaser's Pricing Principles, or such other format as may be agreed between the Contractor and the Purchaser.

19.2 With respect to Clause 19.1 above, when the price or price adjustment is based on adequate price competition, established catalogue or market price of commercial items sold in substantial quantities to the general public, or prices set by law or regulation, the Contractor shall be responsible for substantiation of such cases to the satisfaction of the Purchaser.

19.3 For the purposes of verifying that the cost or pricing data submitted in conjunction with Clause 19.1 above are accurate, complete and current, the Purchaser or any Purchaser authorised representative shall have the right of access to the Contractor's facilities to examine, until the expiration of three (3) years from the date of final payment of all sums due under the Contract:

19.3.1 those books, records, documents and other supporting data which will permit adequate evaluation and verification of the cost or pricing data submitted; and/or

19.3.2 the computations and projections which were available to the Contractor as of the date of the Contractor price proposal.

19.4 The Contractor, subject to the provisions of this Clause, shall require Sub-contractors to provide to the Purchaser, either directly or indirectly:

19.4.1 cost or pricing data;

19.4.2 access to Sub-contractor's facilities and records for the purposes of verification of such cost or pricing data; and

19.4.3 a Certificate of Current Cost or Pricing Data, when required.

NATO UNCLASSIFIED

The Contract General Provisions

19.5   If any price, including profit, negotiated in connection with this Contract was proposed, taking any of the following into account:

19.5.1   the Contractor furnished cost or pricing data which was not complete, accurate and current as certified in the Contractor's Certificate of Current Cost or Pricing Data provided in accordance with Clause 19.6 below;

19.5.2   a Sub-contractor, pursuant to Clause 19.4 above or any Sub-contract clause therein required, furnished cost or pricing data which was not complete, accurate and current as certified in the Sub-contractor's Certificate of Current Cost or Pricing Data;

19.5.3   a Sub-contractor or prospective Sub-contractor furnished cost or pricing data which was required to be complete, accurate and current and to be submitted to support a Sub-contract cost estimate furnished by the Contractor but which was not complete, accurate and current as of the date certified in the Contractor's Certificate of Current Cost or Pricing Data; or

19.5.4   the Contractor or a Sub-contractor or prospective Sub-contractor furnished any data, not within 19.5.1 through 19.5.3 above, which, as submitted, was not complete, accurate and current;

19.5.5   then the price and/or cost shall be adjusted accordingly and the Contract shall be modified in writing as may be necessary to reflect such.

19.6   At the time of negotiating any price, including profit, which is based upon the submission of cost or pricing data by the Contractor, the Contractor shall be required to submit a certificate of current cost or pricing data ("Certificate").

19.6.1   Such Certificates will certify that, to the best of the Contractor's knowledge and belief, cost or pricing data submitted to the Purchaser in support of any proposal for a price, price adjustment or claim, are accurate, complete and current, as per the completion of the negotiations or, in the case of a claim, as per the submission date of the claim.

19.6.2   All such Certificates shall be in the format shown below and shall be dated and signed by a responsible officer of the company:

The Contract General Provisions

CERTIFICATE OF CURRENT COST OR PRICING DATA

This is to certify that cost or pricing data as submitted, either actually or by specific identification in writing to the Purchaser or his representative in support of..*(Claim, Amendment, ECP#, etc.,)* are accurate, complete and current as of ....*(Date)*.

By submitting the price proposal, the Contractor/sub-Contractor or prospective sub-Contractor grant the Purchaser or his authorized representative(s) the right to examine those records, data and supporting information, used as a basis for the pricing submitted.

_____
Name of Company

_____
Signature

_____
Printed Name of Signatory

_____
Title of Signatory

_____
Date of Signature

19.6.3   The Contractor shall insert the substance of this Clause 19.7 in each Sub-contract.

19.7   For all additional or follow-up agreements which are made for Work which are furnished to the Purchaser without competition, the Contractor shall offer prices on a "Preferred Customer" basis, that is offer prices which are as favourable as those extended to any Government, Agency, Company, Organisation or individual purchasing or handling like quantities of

equipment and/or Parts covered by the Contract under similar conditions. In the event that prior to completing delivery under this Contract the Contractor offers any of such items in substantially similar quantities to any customer at prices lower than those set forth herein, the Contractor shall so notify the Purchaser and the prices of such items shall be correspondingly reduced by a supplement to this Contract. Price in this sense means "Base Price" prior to applying any bonus, export tax reduction, turn-over tax exemptions and other reductions based on National Policies.

20.   **NOTICE OF SHIPMENT AND DELIVERY**

20.1   Except as may be specified in the Contract Special Provisions, delivery of all items under this Contract shall be made by the Contractor on the basis of "Delivery Duty Paid" (DDP) as defined by the INCOTERMS 2000 (International Chamber of Commerce Publication No. 560). It shall be noted, however, that because the Purchaser is exempted from direct taxes and duty as set forth in Clause 26 (Taxes and Duties), there is no duty to be paid by the Contractor.

20.2   "Delivery" of required Work by the Contractor does not constitute "Acceptance" by the Purchaser for purposes of meeting the requirements of the Contract Schedule where Purchaser acceptance is the stated payment or schedule milestone.

20.3   Thirty (30) Days, or such other period as specified in the Contract, prior to the delivery of any shipment of Work, the Contractor shall give prepaid notice of shipment to the Purchaser. The Notice of Shipment shall contain, as appropriate, the request for customs form 302, or equivalent document, which shall enable any carrier to conduct duty free import/export clearance through customs for the Purchaser on behalf of NATO.

20.4   The customs form 302 is an official customs clearance declaration issued in advance of shipment by the Purchaser to provide certified information as to the duty free import, export, or transit of NATO consignments between NATO countries.

20.5   The Notice of Shipment and request for Form 302 or equivalent document shall contain the following information:

20.5.1   Purchaser's Contract number;

20.5.2   Contract item number, designation and quantities;

20.5.3   destination;

20.5.4   number and description of the packages (gross and net weight);

20.5.5   description of the goods and their value (for custom purpose only, not commercial value)

20.5.6   consignor's name and address;

20.5.7   consignee's name and address;

20.5.8   method of shipment (i.e. road, rail, sea, air, etc.);

20.5.9   name and address of freight forwarder.

20.6   Forwarding Agents, Carriers or other responsible organisations shall be informed by the Contractor of the availability of Form 302 or equivalent document and how the form shall be utilised to avoid the payment of custom duties. Form 302 or equivalent document shall be incorporated in all shipping documents provided to the carrier.

20.7   Upon receipt of the Notice of Shipment from the Contractor, the Purchaser may require the Contractor to send copies of the Notice of Shipment to the receiving parties and the Contractor shall comply with this requirement.

21.   INSPECTION AND ACCEPTANCE OF WORK

21.1   For the purposes of this Clause, Work does not include documentation which is addressed in Clause 22 (Inspection and Acceptance of Documentation) hereafter.

21.2   Unless otherwise specifically provided for in the Contract, all Work and all Parts and equipment incorporated in the Work are to be new and of the most suitable grade of their respective kinds for the purpose, notwithstanding the requirements for testing, inspection and performance as required under this Contract. All workmanship shall be as specified under the Contract or, if no workmanship standards are specified, best commercial or "state of the art" complying with relevant (National and International) standards.

21.3   All Work may be subject to inspection and test by the Purchaser or his authorised representative(s) to the extent practicable at all times and places prior to Acceptance, including the period of manufacture, or after delivery or as otherwise specified in the Contract. For the purposes of inspection and testing the Purchaser may delegate as his representative the authorised National Quality Assurance Representative (NQAR) in accordance with STANAG 4107.

21.4   No representative or NQAR appointed by the Purchaser for the purpose of determining the Contractor's compliance with the technical requirements of the Contract shall have the authority to change any of the specifications. Such changes may only be made by the Contracting Authority in writing in accordance with Clause 16 (Changes).

21.5   The presence or absence of an NQAR or other Purchaser representative shall not relieve the Contractor from conforming to the requirements of this Contract.

21.6   Acceptance or rejection of the Work shall be made as promptly as practicable after delivery, except as otherwise provided in the Contract. Failure to timely

The Contract General Provisions

accept or reject the Work shall neither relieve the Contractor from responsibility for such Work nor impose liability on the Purchaser.

21.7 In the event that any Work, or lots thereof, or services are defective in design, material, workmanship or manufacturing quality, or as a result of undue wear and tear or otherwise not in conformity with the requirements of this Contract, including any characteristic or condition which is or becomes at variance to the performance specifications, to the intended function of the Work or the function to which it could reasonably be expected that the Work would perform, the Purchaser shall have the right either to reject them (with or without instructions as to their disposition) or to require their correction or replacement. Work which has been rejected or required to be corrected or replaced shall, at the expense of the Contractor, be removed, or, if permitted or required by the Contracting Authority, corrected in place by the Contractor promptly after notice, and shall not thereafter be tendered for acceptance by the Contractor unless the former rejection or requirement of correction or replacement is withdrawn. If the Contractor fails promptly to remove, replace or correct such Work the Purchaser may either:

21.7.1 by contract or otherwise return, replace or correct such Work or services and charge to the Contractor the cost incurred by the Purchaser; and/or

21.7.2 terminate this Contract for default as provided in Clause 39 (Termination for Default).

21.8 When NQAR is not applicable based on the scale of the project, the Purchaser reserves the right to perform inspections through his own staff in accordance with the latest ISO standard at the time of inspection.

21.9 Unless the Contractor corrects or replaces such Work within the delivery schedule, the Purchaser may require the delivery of such Work at a reduction in price which is equitable under the circumstances. Failure to agree to such reduction of price shall be a dispute within the meaning of Clause 41 (Disputes).

21.10 If any inspection or test is made by the Purchaser's representatives on the premises of the Contractor or Sub-contractor, the Contractor, without additional charge, shall provide all reasonable facilities and assistance for the safety and convenience of the Purchaser's representatives in the performance of their duties. The NQAR or other Purchaser representatives shall have the right of access to any area of the Contractor's or his Sub-contractor's premises where any part of the contractual work is being performed.

21.11 If Purchaser inspection or test is made at a point other than the premises of the Contractor or Sub-contractor, it shall be at the expense of the Purchaser except as otherwise provided in this Contract; provided, that in case of rejection the Purchaser shall not be liable for any reduction in value of samples used in connection with such inspection or test.

21.12 All inspections and tests by the Purchaser shall be performed in such a

The Contract General Provisions

manner as not to unduly delay the Work.

21.13 The Purchaser reserves the right to charge to the Contractor any additional cost of Purchaser inspection and test when Work is not ready at the time such inspection and test is requested by the Contractor or when re-inspection or retest is necessitated by prior rejection.

21.14 Acceptance or rejection of the Work shall be made as promptly as practicable after delivery, except as otherwise provided in this Contract, but failure to inspect and accept or reject Work shall neither relieve the Contractor from responsibility for such Work as are not in accordance with the Contract requirements nor impose liability on the Purchaser thereof.

21.15 The inspection and test by the Purchaser of any Work or lots thereof, or services, does not relieve the Contractor from any responsibility regarding defects or other failures to meet the Contract requirements which may be discovered prior to acceptance.

21.16 Acceptance of Work shall take place when the Contracting Authority confirms acceptance in writing of the Work in accordance with the procedure specified in the Contract, or if none is so specified then the Contracting Authority shall be deemed to have accepted the Work without prejudice to any other remedies, when and as soon as any of the following events have occurred:

21.16.1 the Purchaser has taken the Work into use, except as specifically provided by Clause 23 (Use and Possession Prior to Acceptance);

21.16.2 the Purchaser has not exercised its right of rejection of the Work within any period specified for that purpose in the Contract;

21.16.3 there being no period for exercising the right of rejection specified in the Contract, a reasonable time, all the circumstances having been taken into account, has elapsed since inspection of the Work was effected in accordance with the Contract.

21.17 Except as otherwise provided in this Contract, acceptance shall be conclusive except as regards latent defects, fraud, or such gross mistakes as amount to fraud.

21.18 Unless otherwise specified in this Contract, the Contractor shall have or establish, implement and maintain an effective and economical quality control system necessary to satisfy the Contract requirement. The system shall provide for the early and prompt detection of deficiencies, trends and conditions which could result in unsatisfactory quality and for timely and effective corrective action. Objective evidence that the system is effective shall be readily available to the Purchaser and its authorised representatives. Records of all inspection and testing work by the Contractor shall be kept complete and available to the Purchaser's representatives during the performance of this Contract and for such longer periods as may be specified elsewhere in this Contract.

22. <u>INSPECTION AND ACCEPTANCE OF DOCUMENTATION</u>

22.1   The Contractor shall provide to the Purchaser a draft version of the required documentation as provided by the Contract Schedule and the Statement of Work. Review of draft documentation under this Contract will be made by the Purchaser upon the delivery of these items by the Contractor. The review will be conducted by the Purchaser through duly authorised representatives.

22.2   Upon delivery of the draft documentation, the Purchaser will have a period of review as provided by the Statement of Work. At the end of the review period or before if deemed practical by the Purchaser, the Purchaser's comments will be presented to the Contractor in writing. The substance of such comments will pertain to items of error, non-conformity, omission and guidance in relation to the requirements of the Statement of Work.

22.3   Purchaser Review of the delivered items will emphasise the conformity with the requirements of the Statement of Work, thoroughness of analysis, logical bases of conclusions and models and coherence and completeness of presentation. The review process will also examine editorial and grammatical correctness and the suitability and accuracy of graphics supporting the text.

22.4   The Contractor shall, after receipt of Purchaser comments, incorporate changes, revisions and corrections required by the Purchaser and present the revised documentation in final form to the Purchaser for inspection in accordance with the delivery date specified in the Schedule.

22.5   During the review process the Contractor is not required to halt efforts on further tasks as identified in the Statement of Work. The Purchaser, however, shall not be held liable for any work carried out by the Contractor which is based on draft documentation yet to be reviewed.

22.6   Upon receipt of the items in final form, the Purchaser will inspect the items for a period not exceeding two weeks (or as otherwise stated in the Statement of Work). At the end of the inspection, the Purchaser will notify the Contractor that:

22.6.1   the items have been accepted;

22.6.2   the acceptance of the items is deferred pending further revision;

or

22.6.3   The items are rejected and significantly fail to meet Contract requirements.

22.7   In the case of Clause 22.6.2 above, the Contractor shall only be responsible for those revisions and corrections requested by the Purchaser and the

Purchaser may not request additional revisions during inspection after required revisions have been made. However, if the Purchaser determines that a directed revision has not been made or if such directed revision was cause for revision of other portions of content which were not made by the Contractor, the Purchaser may withhold acceptance until such revisions are made by the Contractor.

22.8 The Contractor shall provide to the Purchaser on request supporting technical data, computer software, databases and background analyses in order to validate findings contained in the delivered items.

22.9 Purchaser acceptance shall be made in writing by the Contracting Authority.

23. USE AND POSSESSION PRIOR TO ACCEPTANCE

23.1 Except as otherwise provided in the Contract Special Provisions, the Purchaser shall have the right to take possession of, or use, any completed or partially completed Work under the Contract at any time, when notified by the Contracting Authority, however such possession or use shall not constitute Acceptance by the Purchaser, as defined in the Contract.

23.2 While the Purchaser has such use or is in such possession, the Contractor shall be relieved of the responsibility for loss or damage to the Work concerned other than that resulting from the Contractor's fault, negligence or defect to the Work.

23.3 If such prior possession or use by the Purchaser delays the progress of the Work or causes additional expense to the Contractor, an equitable adjustment in the Contract price or the time of delivery will be made, in accordance with the Clause 16 (Changes), and the Contract shall be modified in writing accordingly.

24. OWNERSHIP AND TITLE

24.1 Except as may be otherwise stated in the Contract Special Provisions and Clause 23 (Use and Possession prior to Acceptance), ownership and title to all Work will pass to the Purchaser only upon Acceptance by the Contracting Authority in writing. Where the Contract provides for Provisional Acceptance and Final Acceptance, ownership and title will pass to the Purchaser upon written notification of Final Acceptance.

25. INVOICES AND PAYMENT

25.1 Unless otherwise specified in the Contract Special Provisions, invoices shall only be submitted after delivery and Acceptance of the Work and for the total prices and currency(ies) as set out under the Schedule of Work.

25.2 Invoices in respect of any Work or services shall be prepared and submitted

The Contract General Provisions

to the Purchaser and shall contain all of the elements listed below:

25.2.1   Contract number;

25.2.2   Purchaser's Purchase Order number ;

25.2.3   accounting codes (as specified in this Contract);

25.2.4   item number (as defined in the Contract);

25.2.5   Contract description of Work or services, sizes, quantities, unit prices, and extended totals (exclusive of taxes and duties for which relief is available); and

25.2.6   extended totals. Details of Bills of Lading or Freight Warrant numbers and weight of shipment shall be identified on each invoice as appropriate.

25.3   In addition, documentary evidence of Acceptance including copies of certificates of conformity shall be submitted together with each invoice. Invoices shall not be submitted to the Purchaser without Acceptance having been previously made by the Purchaser.

25.4   Each copy of the invoice shall contain the following certificate which shall be signed by a duly authorised company official on the designated original invoice:

> *"I certify that the above invoice is true and correct, that the delivery of the above described items has been duly carried out and the payment thereof has not been received.*
>
> *Order placed for official use. Exemption from VAT Article 42,§3&3*of VAT Code for Belgium or Article 151, §1b of the Council Directive 2006/112/EC dd. 28 November 2006 on intra-community purchases and/or services.".*

25.5   All invoices shall be addressed to the NCI Agency - Financial Management

Either at the following addresses:

NCI Agency * If used for NCI Agency Brussels

NATO Communications and Information Agency
Finance, Accounting & Operations
Batiment Z
Av du Bourget 140
B-1140 Belgium

The Contract General Provisions

OR

shall be addressed to Financial Management at the following electronic address:
"NCIA-CAPDEV-FMU-BEL_E-INVOICES@NCIA.NATO.INT (note there is an underscore between BEL and E-INVOICES)

Note: When used for NCI Agency The Hague or Mons the addresses shall be dictated in the Contract Special Provisions

Once the manner of forwarding the invoice is chosen, the contractor shall keep this manner throughout the contract.

25.6   All invoices submitted shall include the address of the bank to which payment shall be made, together with **either** pertinent information concerning the International Bank Account Number (IBAN) and BIC/SWIFT address **or** pertinent information concerning transit number/sort code, account number and SWIFT address. The Purchaser makes payment only by wire transfer and therefore wire transfer particulars shall be included on the invoice.

25.7   Invoices will be settled by the Purchaser within sixty (60) days of receipt of a properly prepared and submitted invoice.

25.8   The Contractor shall mention on the invoice the payment conditions in line with the Contract.

26.   **TAXES AND DUTIES**

26.1   The Purchaser, by virtue of his status under the terms of Article IX and X of the Ottawa Agreement, is exempt from all direct taxes (incl. VAT) and all customs duties on merchandise imported or exported. The Contractor, therefore, certifies that the prices stipulated in this Contract do not include amounts to cover such direct taxes or customs duties.

26.2   The Contractor shall be responsible for ensuring that his respective Sub-contractors are aware that the Purchaser is exempt from taxes and customs duties. The Contractor (and his respective Sub-contractors) shall be responsible for complying with all applicable national and local legal and administrative procedures to ensure that authorities do not attempt to assess taxes and customs duties on goods and property imported or exported through NATO member nation frontiers under this Contract nor assess direct taxation (VAT) on goods sold to the NCI Agency under this Contract.

26.3   The Purchaser shall give reasonable assistance in providing evidence/documents which might be required by the Contractor to ensure that NCI Agency receives tax exemption by virtue of its status under the Ottawa Agreement.

26.4   If, after complying with all national and local legal and administrative

The Contract General Provisions

procedures, the authorities persist in attempting to impose taxes or duties on goods provided under this Contract, the Contractor shall inform the Contracting Authority providing the particulars of the situation, the procedures which have been followed and the point of contact at the national authority which is attempting to impose taxation or duty. The Contracting Authority will examine the situation and attempt to clarify the legal and administrative basis of the difficulty. If the Contracting Authority so directs, the Contractor shall pay the required taxes and duties and file for reimbursement or rebate from the national authorities in accordance with national legislative and administrative procedures.

26.5   In the event that the petition for reimbursement or rebate is denied by the national authorities concerned and providing that the Contractor and/or his Sub-contractor have complied with the national legislative and administrative procedures, the Purchaser shall reimburse the full amount of the payment(s) upon receipt of the Contractor's invoice indicating such tax or duty as a separate item of cost and fully identified by reference to any governmental law, regulation and/or instruction pursuant to which such tax or duty is enforced. The Contractor shall offer assistance and execute any such document that may be useful or required to ensure that Purchaser obtains the reimbursement of any tax or duty retained by a national authority.

26.6   In the event of the Contractor and/or Sub-contractor not complying with national legislative or administrative procedures, taxes and duties paid by the Contractor and/or Sub-contractors shall not be reimbursed by the Purchaser.

26.7   Following payment by the Purchaser of the taxes and/or duties pursuant to Clause 26.4 above, should the Contractor subsequently receive a rebate of any amount paid by the Purchaser, the Contractor shall immediately notify the Purchaser and the amount of such rebate shall be credited or reimbursed to the Purchaser, as directed. The Contractor shall be responsible for taking any and all action that could reasonably be required in order to obtain such rebate.

26.8   The Contractor shall be liable for all other taxes, assessments, fees, licences, administrative charges or other Government assessments or charges which are applicable to the performance of this Contract. It is the Contractor's responsibility to inform himself of his liability in each country where such liability may arise.

27.   WARRANTY OF WORK (Exclusive of Software)

27.1   For the purpose of this Clause:

27.1.1   "Acceptance" shall mean the act of an authorised representative of the Purchaser by which the Purchaser

31

The Contract General Provisions

assumes title and ownership of delivered Work rendered as partial or complete performance of the Contract. "Acceptance" in this regard, unless specifically provided otherwise in the Contract Contract Special Provisions, means final Acceptance where the Contract provides for Provisional or Partial Acceptance;

27.1.2 "Correction" shall mean the elimination of a defect;

27.1.3 "Work" shall not include software.

27.2 The Contractor shall not be responsible under this Clause for the Correction of Defects in Purchaser Furnished Property, except for Defects in Contractor performed installation, unless the Contractor performs, or is obligated to perform, any modifications or other work on Purchaser Furnished Property. In that event, the Contractor shall be responsible for Correction of Defects that result from the modifications or other Work.

27.3 Unless another period of time is indicated in the Contract Contract Special Provisions, the duration of the warranty provided by the Contractor and its Subcontractors shall be twelve (12) months from the date of Acceptance under this Contract as notified in writing by the Contracting Authority.

27.4 Any Work or parts thereof corrected or furnished in replacement and any services re-performed shall also be subject to the conditions of this Clause 27 to the same extent as Work initially accepted. The warranty, with respect to these Work, or parts thereof shall be equal in duration to that set forth in Clause 27.3, and shall run from the date of delivery of the corrected or replaced Work.

27.5 If the Contractor becomes aware at any time before Acceptance by the Purchaser (whether before or after tender to the Purchaser) or at a later time, that a Defect exists in any Work, the Contractor shall either promptly correct the Defect or promptly notify the Purchaser, in writing, of the Defect, using the same procedures prescribed in Clause 27.8.

27.6 The Purchaser will notify in writing the Contractor of the existence of a Failed Component and return to the Contractor the Failed Component within thirty (30) Days of the discovery of such failure. The transport of the Failed Component shall be at the expense of the Purchaser. The notification of the failure will include as much information as practicable about the circumstances and operating environment at the time of the failure. Upon receipt of such notification by the Purchaser (which may precede receipt of the Failed Component), the Contractor shall ship to the location of the Failed Component an identical component for installation by Purchaser personnel. The Contractor shall ship such replacement component(s) Delivery Duty Paid. Such transportation and replenishment charges are included in the cost of line item of the Contract identified as the warranty.

27.7 In such rare cases where the Failed Component is either too large to be

easily transported or the Failed Component cannot be readily identified and isolated within the larger entity, the Contractor shall be notified by the Purchaser of the failure immediately by telephone, fax or e-mail. The Contractor shall provide technical support to the Purchaser personnel in identifying the Failed Component so as to afford the Purchaser the opportunity to return the Failed Component. In such a case where the Failed Component cannot be identified or is not cost effective or practical to ship to the Contractor's facility, the Contractor may elect to send field service personnel to the site of the failure and repair such equipment on location. In this event, such field service personnel shall be dispatched to the site of the failure within forty-eight (48) hours of initial notification. The expense of the technical support and field service shall be borne by the Contractor.

27.8 The Contractor shall conduct analysis of all Failed Components which are returned to him by the Purchaser or repaired in the field by Contractor field service personnel to determine the cause of the failure. The Contractor shall issue a report to the Purchaser within thirty (30) days of receipt of a returned item or field repair which contains the results of the analysis. The report shall contain the conclusion of the Contractor as to whether the cause of the failure was due to a Manufacturing Defect or a Design Defect and declare what course of remedial action the Contractor shall implement to prevent further failures of a similar nature. Repetitive failures of the same component may be grounds for a de facto determination by the Purchaser that a Design Defect exists.

27.9 If the Purchaser determines that a Design Defect exists in any of the Work accepted by the Purchaser under this Contract, the Purchaser shall promptly notify the Contractor of the Defect, in writing, within ninety (90) days after discovery of the Defect. Upon timely notification of the existence of a Defect, or if the Contractor independently discovers a Design Defect or Manufacturing Defect in accepted Work, the Contractor shall submit to the Purchaser, in writing within thirty (30) days, a recommendation for corrective actions, together with supporting information in sufficient detail for the Purchaser to determine what corrective action, if any, shall be undertaken.

27.10 The Contractor shall also prepare and furnish to the Purchaser data and reports applicable to any Correction required under this Clause (including revision and updating of all other affected data and already accepted documentation called for under this Contract) at no increase in the Contract price.

27.11 In the event of timely notice of a decision not to correct or only to partially correct, the Contractor shall submit a technical and cost proposal within forty-five (45) days to amend the Contract to permit Acceptance of the affected Work in accordance with the revised requirement, and an equitable reduction in the Contract price shall promptly be negotiated by the Parties and be reflected in a supplemental agreement to this Contract.

27.12 Within thirty (30) days after receipt of the Contractor's recommendations for corrective action and adequate supporting information in accordance with

The Contract General Provisions

Clause 27.9, the Purchaser using sole discretion, shall give the Contractor written notice not to correct any Defect, or to correct or partially correct any Defect within a reasonable time.

27.13 The Contractor shall promptly comply with any timely written direction from the Purchaser to correct or partially correct a manufacturing or Design Defect, at no increase in the Contract price.

27.14 The Purchaser shall give the Contractor a written notice specifying any failure or refusal of the Contractor to:

27.14.1 conduct analyses of Failed components and implement a course of remedial action as required by Clauses 27.7 and 27.8;

27.14.2 provide replacement components, technical support or on-location field repair service in accordance with Clauses 27.6 and 27.7; or

27.14.3 prepare and furnish data and reports as required by Clause 27.10.

27.15 The notice referred to in Clause 27.14 shall specify a period of time following receipt of the notice by the Contractor in which the Contractor must remedy the failure or refusal specified in the notice.

27.16 If the Contractor does not comply with the Purchaser's written notice in Clause 27.14, the Purchaser may by Contract or otherwise:

27.16.1 Obtain detailed recommendations for corrective action from its own resources or third parties and either:

27.16.2 correct the Work;

27.16.3 replace the Work, and if the Contractor fails to furnish timely disposition instructions, the Purchaser may dispose of the non-confirming Work for the Purchaser's account in a reasonable manner, in which case the Purchaser is entitled to reimbursement from the Contractor, or from the proceeds, for the reasonable expenses of care and disposition, as well as for excess costs incurred or to be incurred;

27.16.3.1 obtain applicable data and reports; and/or

27.16.3.2 charge the Contractor for the costs incurred by the Purchaser.

27.17 In no event shall the Purchaser be responsible for any extension or delays in the scheduled deliveries or periods of performance under this Contract as a result of the Contractor's obligations to correct Defects, nor shall there be any adjustment of the delivery schedule or period of performance as a result of the Correction of Defects unless provided by a supplemental agreement with adequate consideration.

The Contract General Provisions

27.18 The rights and remedies of the Purchaser provided in this Clause shall not be affected in any way by any terms or conditions of this Contract concerning the conclusiveness of inspection and Acceptance and are in addition to, and do not limit, any rights afforded to the Purchaser by any other Clause of this Contract or applicable law.

28. **RIGHT OF ACCESS, EXAMINATION OF RECORDS**

28.1 The Contractor shall give to the Purchaser and/or his representative(s) full and free access to his premises as and when required for the purpose of this Contract and shall ensure the same right of access to the premises of his Sub-contractors, by the inclusion in any such Sub-contracts of a provision substantially as set forth in this Clause.

28.2 The Purchaser and/or his representative(s) shall continue to have such right of access and examination of records as set forth in Clause 28.1 above until final payment under the Contract or the end of the warranty provisions under the Contract, whichever occurs later.

28.3 The expiration of the Purchaser's rights as set forth in Clause 28.2 is further subject to the provisions of Clause 19 (Pricing of Changes, Amendments and Claims), where a three (3) year right is established following the agreement of contractual amendments or the settlement of claims based upon the submission of cost and pricing data.

28.4 The period of access and examination described in Clause 28.1 above for records not related to cost aspects of a dispute or claim but which relate to issues of fact arising under either proceedings under Clause 41 (Disputes) or Clause 42 (Arbitration), or the settlement of claims made by either Party pursuant to the performance of this Contract, shall continue until such appeals, litigation or claims have been disposed of.

29. **PATENT AND COPYRIGHT INDEMNITY**

29.1 The Contractor shall assume all liability against any and all third party claims that the services, Work and/or parts thereof, in whole or in part, infringe(s) an IPR in force in any countries, arising out of the manufacture, import, export, performance of the services or delivery of Work and/or out of the use or disposal by, or for the account of, the Purchaser of such Services and/or Work. The Contractor shall reimburse and/or indemnify the Purchaser, its officers, agents, employees and/or consultants: (i) for all costs, fees, damages, awards, settlement amounts and any other expenses awarded to the third party right holder against Purchaser and/or the final beneficiaries of the Work in relation to said third party claim; and (ii) for the costs and expenses incurred by the Purchaser in relation to said third party claims, including attorney fees. The Contractor shall be responsible for obtaining any licences necessary for the performance of this Contract and for making all other arrangements required to indemnify

The Contract General Provisions

the Purchaser from any liability for IPR infringement in said countries.

29.2 Each Party shall immediately notify the other of any intellectual property infringement claims of which he has knowledge and which pertain to the Work under this Contract.

29.3 This indemnity shall not apply under the following circumstances:

29.3.1 Patents or copyright which may be withheld from issue by order of the applicable government whether due to security regulations or otherwise;

29.3.2 An infringement resulting from specific written instructions from the Purchaser under this Contract;

29.3.3 An infringement resulting from changes made to the Work by the Purchaser without the Contractor prior written consent;

29.3.4 An infringement resulting from changes or additions to the Work subsequent to final delivery and Acceptance under this Contract.

30. **INTELLECTUAL PROPERTY**

30.1 *Purchaser Background IPR*

30.1.1 The Contractor is licensed to use, non-exclusively and royalty-free any Purchaser Background IPR that is or will be made available for the sole purpose of carrying out the Work.

30.1.2 The Contractor shall not use any Purchaser Background IPR other than for the purpose of carrying out the Work without the prior written agreement of the Purchaser. Any such agreement shall include the terms relating to such use.

30.1.3 The Purchaser gives no warranty as to the validity of any Purchaser Background IPR. The Contractor shall not do anything or act in any way which is inconsistent with or prejudicial to the ownership by the Purchaser of any Purchaser Background IPR.

30.2 *Contractor Background IPR*

30.2.1 Any use of Contractor Background IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to Purchaser. The Contractor hereby grants to NATO a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Contractor Background IPR for the purpose of exploiting or otherwise using the Foreground IPR.

The Contract General Provisions

30.2.2   Any use of Contractor Background IPR is not limited to the number of users or the number of licenses required by the Contract for the use of system. The Purchaser reserves the right to use the Contractor Background IPR for any number of users and number of licenses as required, at no additional cost to the Purchaser.

30.3   *Foreground IPR*

30.3.1   All Foreground IPR is the property of the Purchaser on behalf of NATO. Consequently, no statement shall be made restricting the rights of the Purchaser in the Foreground IPR.

30.3.2   The Contractor shall ensure that suitable arrangements are in place between its employees, agents, consultants and itself regarding Foreground IPR generated by said employees, agents, Subcontractors and consultants to allow the Contractor to fulfil its obligations under Clause 30.3.1 above.

30.3.3   The Contractor shall be entitled to use Foreground IPR on a non-exclusive, royalty free basis solely for the purpose of carrying out the Work.

30.3.4   The Contractor shall not use any Foreground IPR other than for the purpose of carrying out the Work without the Purchaser's prior written agreement. Any such agreement shall include terms relating to such use.

30.3.5   The Contractor shall provide the Purchaser, at the latest upon delivery of the Work and thereafter for the duration of the warranty and any purchased CLS agreement period, with full documented records of information in relation to the Work, including but not limited to, all drawings, specifications and other data that is necessary or useful to further develop, maintain and operate the Work.

30.3.6   The Contractor shall:

30.3.6.1   do all things necessary and sign all necessary or useful documents to enable the Purchaser to obtain the registration of the Foreground IPR as the Purchaser may require and select; and

30.3.6.2   to execute any formal assignment or other documents as may be necessary or useful to vest title to any Foreground IPR in the Purchaser.

The Contract General Provisions

30.3.7   The Contractor undertakes:

30.3.7.1   to notify the Purchaser promptly of any invention or improvement to an invention or any design conceived or made by the Contractor; and

30.3.7.2   to provide the Purchaser with such information as the Purchaser may reasonably request in order to: (i) determine the patentability of such invention or improvement; (ii) assess the need for registering such invention or improvement; and (iii) evaluate the potential value to the Purchaser of such a patent or registration if issued.

30.3.8   If the Purchaser determines that it wishes to apply for one or more patents for the disclosed invention or improvement or for a registration for the disclosed design, it will prosecute such application(s) at its own expense. The Contractor undertakes to provide the Purchaser, at the Purchaser's expense, with such information and assistance as the Purchaser shall reasonably require to prosecute such application(s).

30.4 *Third Party IPR*

30.4.1   Any use of Third Party IPR for the purpose of carrying out the Work pursuant to the Contract shall be free of any charge to the Purchaser. The Contractor hereby grants to NATO a non-exclusive, royalty-free and irrevocable licence to use and authorise others to use any Third Party IPR for the purpose of exploiting or otherwise using the Foreground IPR.

30.4.2   With the exception of COTS items, any use of Third Party IPR is not limited to the number of users or the number of licenses required by the Contract for the use of system. With the exception of COTS items, the Purchaser reserves the right to use the Third Party IPR for any number of users and number of licenses as required, at no additional cost to the Purchaser.

30.4.3   For COTS items, the Contractor shall be responsible for obtaining licences from the Third Party in line with the requirements of the Statement of Work (including numbers and locations of licences).

30.4.4   Where Third Party IPR is the subject of a licence or other agreement between the third party and the Purchaser or the Contractor, the Contractor shall not use any Third Party IPR for the purposes of carrying out work pursuant to the Contract

without the prior written approval of the Purchaser. Contractor shall inform Purchaser in advance of any restrictions on the Purchaser's use.

30.4.5   If, after the award of the Contract, the Contractor becomes aware of the existence of any Third Party IPR which the Contractor is using or believes is needed for the performance of the Contract, the Contractor shall immediately give the Purchaser a written report identifying such IPR and if they are compliant with the other provisions in the contract. Any Third Party IPR under this clause is subject to the prior written approval by the Purchaser.

30.4.6   The Purchaser may consider open source solutions alongside proprietary ones in developments provided that such solutions are fully compliant with the requirements of this Contract. Contractor shall disclose in advance the open source license associated with the contemplated open source solution. The Purchaser reserves the right to refuse the incorporation of open source solutions that are deemed inadequate for incorporation in a NATO application (e.g. post-back obligations).

30.5 *Subcontractor IPR*

30.5.1   When placing a Sub-contract which is concerned with or involves the creation of IPR, the Contractor shall ensure that the Sub-contractor enters into the same agreement for the use of the IPR as stipulated in this Contract in such a way that the Purchaser will be entitled to use the IPR as agreed between the Purchaser and the Contractor. The Contractor shall include in the Sub-contract the content of the provisions of this Clause.

31. **SOFTWARE WARRANTY**

31.1 *Statement of the Warranties*

31.1.1   The Contractor warrants that each Software delivered under this Contract will conform to all requirements specified in the Contract. This will also include Software design specifications, including software configuration.

31.1.2   Regardless of the Purchaser initiation of or participation in developing Software design or specifications, each Software delivered under this Contract will conform to the essential Performance requirements set forth in this Contract, as those essential Performance requirements measured,

The Contract General Provisions

tested, and verified by tests and procedures set forth in this Contract.

31.2 *Notification Requirement*

31.2.1 The Contractor agrees to notify the Purchaser in writing immediately after he first discovers that a defect(s) may exist in Software delivered under this Contract, unless the Purchaser has first notified the Contractor, in writing, of the same defect(s).

31.2.2 The Purchaser shall notify the Contractor upon discovery that a defect(s) may exist in any Software accepted by the Purchaser under this Contract, unless the Contractor has first notified the Purchaser, in writing of the same defect(s).

31.3 Duration of the Warranty

31.3.1 For each Software delivered under this Contract, the Contractor Warranties stated in paragraph 31.1 above shall extend to all defects discovered within 12 months from the date of acceptance of the Software by the Purchaser.

31.4 Purchaser Remedies for Breach

31.4.1 The rights and remedies of the Purchaser under this Software Warranty:

31.4.2 Are in addition to any rights and remedies of the Purchaser under any other provision of this Contract, including, but not limited to, the Purchaser's rights in relation to latent defects, fraud, or gross mistakes that amount to fraud; and

31.4.3 Shall apply notwithstanding inspection, acceptance, or any other clauses or terms of this Contract;

31.4.4 In the event of any defect as defined herein with respect to a Software delivered under this Contract, the Purchaser, in its sole discretion may:

31.4.4.1 Require the Contractor to take such action as may be necessary to eliminate the defect, at no additional cost to the Purchaser for materials, labour, transportation, or otherwise;

31.4.4.2 Require the Contractor to supply, at no additional cost to the Purchaser, all materials and instructions necessary for the Purchaser to eliminate the defect and to pay costs reasonably incurred by the Purchaser in taking such action as

40

The Contract General Provisions

may be necessary to eliminate the defect, or;

31.4.4.3   Equitably reduce the contract price

31.4.5   The Purchaser may elect the remedies provided in paragraph 31.4.4.1 or 31.4.4.2 above notwithstanding any dispute respecting the existence of or responsibility for any alleged defect as defined herein with respect to any Software delivered under this contract, provided that the Contractor will not be required to pay costs incurred by the Purchaser under paragraph 31.4.4.2 until final determination of the defect. In the event that the alleged defect is subsequently determined not to be a defect subject to this warranty but the Contractor has incurred costs under paragraph 31.4.4.1 and 31.4.4.2 as required by the Contract by virtue of this paragraph 31.4.3, the contract price under this contract shall be equitably adjusted.

31.4.6   Election by the Purchaser of the remedy provided under paragraph 31.4.4.1 and 31.4.4.2 above shall not preclude subsequent election of a different remedy under paragraph 31.4.4 if the defect is not successfully eliminated under the prior election with one month of the notification under paragraph 31.4.2 above.

31.5   Limitations and Exclusions from Warranty Coverage

31.5.1   This Software Warranty shall not apply to alleged defects that the Contractor demonstrates to be in or otherwise attributable to the Purchaser furnished property as determined, tested, and verified by the tests and procedures set forth in this Contract. Notwithstanding this paragraph , a defect is not attributable to Purchaser furnished property if it is the result of installation or modification of Purchaser furnished property by the Contractor or of the integration of Purchaser furnished property into any Software delivered under this Contract.

31.5.2   Any Purchaser Furnished Property needs to be checked and approved by the Contractor. Approval is implied once the Contractor starts using the Purchaser Furnished Property.

31.6   Markings

31.6.1   All Deliverables under this Contract will identify the owner of the Deliverable and if applicable, will prominently include notice of the existence of its warranty, its substance, its duration, and instructions to notify the Purchaser promptly if the Software is found to be defective. The markings should also be included in

The Contract General Provisions

the operating and/or maintenance manuals or instructions accompanying such Software.

31.6.2 All Deliverables regardless of the media they are delivered onto and which are subject to export control restrictions shall be clearly marked indicating the type and nature of restriction as well as the national law imposing such restrictions. Nothing in this provision is intended to invalidate, void, or otherwise limit the rights of the Purchaser under this Contract.

32. NATO CODIFICATION

32.1 For the purposes of this Clause "Technical Data" means the drawings, specifications and technical documentation of those items designated by the Purchaser to support the equipment covered by the Contract, and required to fully identify the items and, if applicable, draft item identifications to the extent and in the form to be agreed between the Codification Authority and the Contractor.

32.2 In order to ensure the orderly identification of equipment, the Contractor shall furnish at the request of the Codification Authority the Technical Data required for the identification of the items of supply to the NATO codification system in the time scale stated in this Contract.

32.3 A recommended spare parts list or a similar data carrier prepared in accordance with instructions provided by the Purchaser as the basis for codification shall be supplied by the Contractor by the date established in this Contract.

32.4 The Contractor shall supply or require his Sub-contractor(s)/supplier(s) to supply on request for the period of time specified in the Contract the relevant Technical Data for all items and sub-contracted items to the Codification Authority and the Purchaser. The Contractor shall require that each Sub-contractor/supplier shall include identical conditions in any subsequent order which he may place.

32.5 The drawings, specifications, related documentation and, if applicable, draft item identifications, prepared when possible by the true manufacturer of the item, shall be supplied by the Contractor or his Sub-contractor(s)/supplier(s) direct to the Codification Authority and, if required, to the Purchaser as and when they become available or, at the latest within the time limits specified in the Contract. The Contractor shall inform the Codification Authority and Purchaser within 21 Days of receipt of the request if the required Technical Data are not immediately available, and shall impose a similar obligation upon his Sub-contractor(s)/supplier(s).

The Contract General Provisions

32.6   Except as hereinafter provided, the Contractor shall require the Sub-

contractor(s)/supplier(s) to furnish on request the information direct to the
Codification Authority in the Sub-contractor(s)/supplier(s)' country, but the
Contractor shall remain responsible for ensuring that the information is so
furnished. In the event of a Sub-contract order being placed with a
manufacturer in a non-NATO country, the Contractor shall be responsible
for obtaining Technical Data from the Sub-contractor/supplier and furnishing
it to the Purchaser.

32.7   Technical Data relating to any Sub-contractor's/supplier's items shall include
but not be limited to the name and address of the true manufacturer(s),
his/their true reference number(s), drawing or item Part number(s) and
applicable data in addition to any Part or reference number(s) allocated by
the Contractor, plus draft item identification(s) if required by the Codification
Authority.

32.8   The Contractor shall provide the Technical Data required for codification of
those items ordered with this Contract and also for the pertaining support
items ordered with future contracts, including updating information regarding
all agreed modifications, design or drawing changes made to the equipment
or detailed Parts.

32.9   If the Contractor has previously supplied Technical Data (for the purpose
stated in Clause 31.2), the Contractor is to state this fact and indicate to
whom they were supplied and the Contractor shall not under normal
circumstances be required to make a further supply of the Technical Data
already provided. The Technical Data furnished by the Contractor and Sub-
contractor(s)/supplier(s) are to be presented in accordance with the
requirements for the preparation of item identification(s) as outlined in the
Guide for Industry provided by the Codification Authority.

32.10   The Contractor should contact the Codification Authority for any information
concerning the NATO codification system. This information is to be found at:
"http://www.nato.int/structur/ac/135/ncs_guide/e_guide.htm"

32.11 Markings

32.11.1   All Deliverables under this Contract will identify the owner of the
Deliverable and,if applicable, will prominently include notice of
the existence of its warranty, its substance, its duration, and
instructions to notify the Purchaser promptly if the Software is
found to be defective. The markings should also be included in
the operating and/or maintenance manuals or instructions
accompanying such Software.

32.11.2   All Deliverables regardless of the media they are delivered onto

43

The Contract General Provisions

and which are subject to export control restrictions shall be clearly marked indicating the type and nature of restriction as well as the national law imposing such restrictions. Nothing in this provision is intended to invalidate, void, or otherwise limit the rights of the Purchaser under this Contract.

33.   RELEASE FROM CLAIMS

33.1   Prior to final payment under this Contract, the Contractor and each assignee under this Contract shall execute and deliver a release discharging the Purchaser, its officers, agents and employees from all liabilities, obligations and claims arising out of or under this Contract subject only to the following exceptions:

33.1.1   specified claims in stated amounts or in estimated amounts where the amounts are not susceptible to exact statement by the Contractor;

33.1.2   claims for reimbursement of costs (other than expenses of the Contractor by reason of his indemnification of the Purchaser against patent liability) including reasonable expenses incidental thereto, incurred by the Contractor under the provisions of this Contract relating to patents.

33.1.3   a patent infringement resulting from specific written instructions from the Purchaser under this Contract.

33.1.4   a patent infringement resulting from changes or additions to the goods and services subsequent to final delivery and acceptance under this Contract.

34.   ASSIGNMENT OF CONTRACT

34.1   The Purchaser reserves the right to assign this Contract, in whole or in part, to another NATO body, agency or representative within NATO or NATO Nations. In such a case, the Purchaser shall notify the Contractor accordingly in writing.

34.2   NATO shall remain responsible for its obligations under the Contract and for the actions of the body, agency or representative to which this Contract may be assigned.

35.   TRANSFER AND SUB-LETTING

35.1   The Contractor shall not give, bargain, sell, assign, sub-let or otherwise dispose of the Contract or any part thereof or the benefit or advantage of the

Contract or any part thereof without the prior written consent of the Purchaser.

36. PURCHASER DELAY OF WORK

36.1 If the performance of all or any part of the Work is delayed or interrupted by an act of the Purchaser in the administration of this Contract, which act is not expressly or implicitly authorised by this Contract, or by the Purchaser's failure to act within the time specified in this Contract (or within a reasonable time if no time is specified), an adjustment shall be made for any increase in the cost of performance of this Contract caused by such delay or interruption and the Contract modified in writing accordingly.

36.2 Adjustment shall be made also in the delivery or performance dates and any other contractual provision affected by such delay or interruption. However, no adjustment shall be made under this Clause for any delay or interruption:

36.2.1 to the extent that performance would have been delayed or interrupted by any other cause, including the fault or negligence of the Contractor; or

36.2.2 for which an adjustment is provided or excluded under any other provision of this Contract.

36.3 No claim under this Clause shall be allowed:

36.3.1 if the Contractor has failed to notify the Purchaser in writing of the act or failure to act, indicating that this act or failure to act will result in a delay or increased costs;

36.3.2 for any costs incurred more than twenty (20) Days before the Contractor shall have notified the Purchaser in writing of the act or failure to act involved; and

36.3.3 unless the monetary claim, in an amount stated, is asserted in writing as soon as practicable after the termination of such delay or interruption, but not later than the date of final payment under the Contract.

37. CONTRACTOR NOTICE OF DELAY

37.1 In the event that the Contractor encounters difficulty in complying with the Contract schedule date(s) for whatever reason, including actual or potential labour disputes, the Contractor shall immediately notify the Contracting Authority in writing, giving pertinent details. This data shall be deemed to be informational in character and shall not be construed as a waiver by the Purchaser of any schedule or date, or of any rights or remedies provided by law or under this Contract.

The Contract General Provisions

37.2   Notwithstanding the above the Contractor shall be deemed to be in delay without notice from the Purchaser and only by simple expiry of the due date.

38.   LIQUIDATED DAMAGES

38.1   If the Contractor:

38.1.1   fails to meet the delivery schedule of the Work or any performance milestones specified in the Schedule of Work to this Contract, or any extension thereof, or

38.1.2   fails to obtain acceptance of the delivered Work as specified in the Contract, or, if no time for acceptance is specified in the contract within a reasonable time after work is delivered.

the actual damage to the Purchaser for the delay will be difficult or impossible to determine. Therefore, in lieu of actual damages the Contractor shall pay to the Purchaser, for each day of delinquency in achieving the deadline or milestone, fixed and agreed liquidated damages of .1% (one tenth of per cent) per day of the associated payment set forth in the Schedule of Payments provided in the Contract Special Provisions. If no Schedule of Payments is specifically set forth in the Contract Special Provisions, the liquidated damages will be assessed against the price of the applicable contract line item (CLIN) of the Schedule of Supplies, Services and Prices.

38.2   In addition to the liquidated damages referred to above, the Purchaser shall have the possibility of terminating this Contract in whole or in part, as provided in Clause 39 (Termination for Default). In the event of such termination, the Contractor shall be liable to pay the excess costs provided in Clause 38.5.

38.3   The Contractor shall not be charged with liquidated damages when the delay arises out of causes beyond the control and without the fault or negligence of the Contractor as defined in Clause 39.6 (Termination for Default). In such event, subject to the provisions of Clause 41 (Disputes), the Purchaser shall ascertain the facts and extent of the delay and shall extend the time for performance of the Contract when in his judgement the findings of the fact justify an extension.

38.4   Liquidated damages shall be payable to the Purchaser from the first day of delinquency and shall accrue at the rate specified in Clause 38.1 to 20% of the value of each line item individually not to exceed 15% of the value of the total Contract. These liquidated damages shall accrue automatically and without any further notice being required.

38.5   The rights and remedies of the Purchaser under this clause are in addition to any other rights and remedies provided by law or under this Contract.

39.   TERMINATION FOR DEFAULT

NATO UNCLASSIFIED

The Contract General Provisions

39.1 The Purchaser may, subject to Clause 39.6 below, by written notice of default to the Contractor, terminate the whole or any part of this Contract if the Contractor, inclusive but not limited to:

39.1.1 fails to make delivery of all or part of the Work within the time specified in the contract or any agreed extension thereof;

39.1.2 fails to make progress as to endanger performance of this Contract in accordance with its terms;

39.1.3 fails to meet the technical requirements or the Specifications of the Contract;

39.1.4 fails to comply with Clause 11 (Security);

39.1.5 transfer this Contract without the Purchaser's prior written consent;

39.1.6 breaches any provision of this Contract; or

39.2 In the case of any of the circumstances set forth in Clause 39.1 above, the Purchaser shall issue a letter to the Contractor stating that an actual or potential default exists and requiring a response from the Contractor within ten (10) Days that identifies:

39.2.1 in the case of late delivery of Work, when the Contractor shall deliver the Work and what circumstances exist which may be considered excusable delays under Clause 39.6.

39.2.2 in the case of the other circumstances identified in Clause 39.1 above, what steps the Contractor is taking to cure such failure(s) within a period of ten Days (or such longer period as the Purchaser may authorise in writing) after receipt of notice in writing from the Purchaser specifying such failure and identifying any circumstances which exist which may be considered excusable under Clause 39.6.

39.3 The Purchaser shall evaluate the response provided by the Contractor or, in the absence of a reply within the time period mentioned in Clause 39.2, all relevant elements of the case, and make a written determination within a reasonable period of time that:

39.3.1 sufficient grounds exist to terminate the Contract in whole or in part in accordance with this Clause and that the Contract is so terminated;

NATO UNCLASSIFIED

The Contract General Provisions

39.3.2   there are mitigating circumstances and the Contract should be amended accordingly; or

39.3.3   the Purchaser will enter a period of forbearance in which the Contractor must show progress, make deliveries, or comply with the Contract provisions as specified by the Purchaser. The Purchaser may apply other remedial actions as provided by this Contract during such period of forbearance. This period of forbearance shall in no event constitute a waiver of Purchaser's rights to terminate the Contract for default.

39.4   At the end of the period of forbearance, which may be extended at the Purchaser's discretion, the Purchaser may terminate this Contract in whole or in part as provided in Clause 39.1 if the Contractor has not made adequate progress, deliveries or compliance with the Contract provisions which were the terms of the period of forbearance.

39.5   In the event the Purchaser terminates this Contract in whole or in part, as provided in Clause 39.1, the Purchaser may procure, upon such terms and in such manner as the Purchaser may deem appropriate, Work similar to those so terminated, and the Contractor shall be liable to the Purchaser for any excess costs for such similar Work; however, the Contractor shall continue the performance of this Contract to the extent not terminated under the provisions of this clause.

39.6   Except with respect to the default of Sub-contractors, the Contractor shall not be held liable for a termination of the Contract for default if the failure to perform the Contract arises out of causes beyond the control and without the fault or negligence of the Contractor.

39.6.1   Such causes may include, but are not restricted to, acts of God, acts of the public enemy, acts of the Purchaser in its contractual capacity, acts of sovereign governments which the Contractor could not reasonably have anticipated, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes, and unusually severe weather; but in every case the failure to perform must be beyond the control and without the fault or negligence of the Contractor.

39.6.2   If the failure to perform is caused by the default of a Sub-contractor, and if such default arises out of causes beyond the control of both the Contractor and Sub-contractor, without the fault or negligence of either of them, the Contractor shall not be held liable for a termination for default for failure to perform unless the Work to be furnished by the Sub-contractor were obtainable from other sources in sufficient time to permit

The Contract General Provisions

the Contractor to meet the required delivery schedule.

39.7 If this Contract is terminated as provided in Clause 39.1, the Purchaser, in addition to any other rights provided in this Clause and the Contract, may require the Contractor to transfer title and deliver to the Purchaser, in the manner and to the extent directed by the Purchaser:

39.7.1 any completed Work with associated rights ;

39.7.2 such partially completed Work, materials, Parts, tools, dies, jigs, fixtures, plans, drawings, information, and Contract rights (hereinafter called "Manufacturing materials") with associated rights as the Contractor has specifically produced or specifically acquired for the performance of such part of this Contract as has been terminated;

39.8 In addition to Clause 39.7, the Contractor shall, upon direction of the Purchaser, protect and preserve property in the possession of the Contractor in which the Purchaser has an interest.

39.9 Payment for completed Work delivered to and accepted by the Purchaser shall be at the Contract price.

39.10 Payment for manufacturing materials delivered to and accepted by the Purchaser and for the protection and preservation of property shall be in an amount agreed upon by the Contractor and Purchaser, failure to agree to such amount shall be a dispute within the meaning of Clause 41 (Disputes).

39.11 The Purchaser may withhold from amounts otherwise due to the Contractor for such completed Work or manufacturing materials such sum as the Purchaser determines to be necessary to protect the Purchaser against loss because of outstanding liens or claims of former lien holders.

39.12 If, after notice of termination of this Contract under the provisions of this Clause, it is determined for any reason that the Contractor was not in default under the provisions of this Clause, or that the default was excusable under the provisions of this Clause, the rights and obligations of the Parties shall be the same as if the notice of termination had been issued pursuant to Clause 40 (Termination for the Convenience of the Purchaser).

39.13 If after such notice of termination of this Contract under the provisions of this Clause, it is determined for any reason that the Contractor was not in default under the provisions of this Clause and that the Parties agree that the Contract should be continued, the Contract shall be equitably adjusted to compensate for such termination and the Contract modified accordingly. Failure to agree to any such adjustment shall be a dispute within the meaning of Clause 41 (Disputes).

39.14 The rights and remedies of the Purchaser provided in this Clause shall not be

49

exclusive and are in addition to any other rights and remedies provided by law or under this Contract.

40. TERMINATION FOR THE CONVENIENCE OF THE PURCHASER

40.1 The performance of Work under this Contract may be terminated by the Purchaser in accordance with this Clause in whole, or from time to time in part, whenever the Purchaser shall determine that such termination is in the best interest of the Purchaser.

40.2 Any such termination shall be effected by delivery to the Contractor of a written notice of termination, signed by the Contracting Authority, specifying the extent to which performance of Work under the Contract is terminated, and the date upon which such termination becomes effective.

40.3 After receipt of a Notice of Termination and except as otherwise directed by the Contracting Authority, the Contractor shall:

40.3.1 stop the Work on the date and to the extent specified in the notice of termination;

40.3.2 place no further orders or Sub-contracts for Work, Parts, materials, services or facilities, except as may be necessary for completion of such portion of the Work under the Contract as is not terminated;

40.3.3 terminate all orders and Sub-contracts to the extent that they relate to the performance of Work terminated by the Notice of Termination;

40.3.4 assign to the Purchaser, in the manner, at the times and to the extent directed by the Purchaser, all of the right, title and interest of the Contractor under the orders and Sub-contracts so terminated, in which case the Purchaser shall have the right, in its discretion, to settle or pay any or all claims arising out of the termination of such orders and Sub-contracts;

40.3.5 settle all outstanding liabilities and all claims arising out of such termination of orders and Sub-contracts, with the approval or ratification of the Purchaser to the extent he may require, which approval or ratification shall be final for all the purposes of this Clause;

40.3.6 transfer title and deliver to the Purchaser in the manner, at the times, and to the extent, if any, directed by the Contracting Authority of:

The Contract General Provisions

40.3.6.1 the fabricated parts, work in process, completed work, Work, and other material produced as a part of, or acquired in connection with the performance of the Work terminated by the notice of termination, and

40.3.6.2 the completed or partially completed plans, drawings, information, and other property which, if the Contract had been completed, would have been required to be furnished to the Purchaser;

40.3.7 use his best efforts to sell, in the manner, at the times, to the extent, and at the price or prices directed or authorised by the Contracting Authority, any property of the types referred to in Clause 40.3.6 above. However, the Contractor:

40.3.7.1 shall not be required to extend credit to any Buyer; and

40.3.7.2 may acquire any such property under the conditions prescribed by and at a price or prices approved by the Purchaser; and provided further that the proceeds of any such transfer or disposition shall be applied in reduction of any payments to be made by the Purchaser to the Contractor under this Contract or shall otherwise be credited to the price or cost of the Work or paid in such manner as the Contracting Authority may direct;

40.3.8 complete performance of such part of the Work as shall not have been terminated by the Notice of Termination; and

40.3.9 take such action as may be necessary, or as the Purchaser may direct, for the protection and preservation of the property related to this Contract which is in the possession of the Contractor and in which the Purchaser has or may acquire an interest.

40.4 The Contractor may submit to the Purchaser a list, certified as to quantity and quality, of any or all items of termination inventory not previously disposed of, exclusive of items the disposition of which has been directed or authorised by the Purchaser, and may request the Purchaser to remove such items or enter into a storage agreement covering the same; provided that the list submitted

51

The Contract General Provisions

shall be subject to verification by the Purchaser upon removal of the items, or if the items are stored, within forty-five (45) Days from the date of submission of the list, and any necessary adjustment to correct the list as submitted shall be made prior to final settlement.

40.5   After receipt of a notice of termination, the Contractor shall submit to the Purchaser his termination Claim for the Work covered by the notice of termination, in the form and with certification prescribed by the Purchaser. Such claim shall be submitted promptly but in no event later than six (6) months from the effective date of termination, unless one or more extensions are granted in writing by the Purchaser, upon request of the Contractor made in writing within such six-month period or authorised extension thereof. However, if the Purchaser determines that the facts justify such action, the Purchaser may receive and act upon any such termination claim at any time after such six-month period or any extension thereof. Upon failure of the Contractor to submit his termination claim within the time allowed, the Purchaser may determine on the basis of information available to him, the amount, if any, due to the Contractor by reason of the termination and shall thereupon pay to the Contractor the amount so determined.

40.6   Subject to the provisions of Clause 40.5, the Contractor and the Purchaser may agree upon the whole or any part of the amount or amounts to be paid to the Contractor by reason of the total or partial termination of Work pursuant to this Clause, which amount or amounts may include a reasonable allowance for profit on work done; provided that such agreed amount or amounts exclusive of settlement costs shall not exceed total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of the Work not terminated. The Contract shall be amended accordingly and the Contractor shall be paid the amount agreed.

40.7   In the event of the failure of the Contractor and the Purchaser to agree as provided in Clause 40.6 upon the whole amount to be paid to the Contractor by reason of the termination of Work pursuant to Clause 40, the Purchaser shall pay to the Contractor the amounts determined by the Purchaser as follows, but without duplication of any amounts agreed upon in accordance with Clause 40.6 the total of:

    40.7.1   for completed Work accepted by the Purchaser (or sold or acquired as provided in Clause 40.3 above) and not therefore paid for, a sum equivalent to the aggregate price for such Work computed in accordance with the price or prices specified in the Contract, appropriately adjusted for any saving of freight or other charges;

    40.7.2   the costs incurred in the performance of the Work terminated including initial costs and preparatory expense allocable thereto, but exclusive of any costs attributable

The Contract General Provisions

to Work paid or to be paid for under Clause 40.7.1;

40.7.3 the cost of settling and paying claims arising out of the termination of work under Sub-contracts or orders, as provided in Clause 40.3.5, which are properly chargeable to the terminated portion of the Contract, exclusive of amounts paid or payable on account of Work or materials delivered or services furnished by Sub-contractors or vendors prior to the effective date of the notice of termination, which amounts shall be included in the costs payable under Clause 40.7.2; and

40.7.4 a sum, as profit on Clause 40.7.1 above, determined by the Purchaser to be fair and reasonable; provided, however, that if it appears that the Contractor would have sustained a loss on the entire Contract, had it been completed, no profit shall be included or allowed and an appropriate adjustment shall be made reducing the amount of the settlement to reflect the indicated rate of loss; and

40.7.5 the reasonable costs of settlement, including accounting, legal, clerical and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination and settlement of Sub-contracts there under, together with reasonable storage, transportation, and other costs incurred in connection with the protection, or disposition of property allocable to this Contract.

40.8 The total sum to be paid to the Contractor under Clause 40.7 shall not exceed the total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of Work not terminated.

40.9 Except for normal spoilage, and except to the extent that the Purchaser shall have otherwise expressly assumed the risk of loss, there shall be excluded from the amounts payable to the Contractor, as provided in Clause 40.7 above, the fair value, as determined by the Purchaser, of property which is destroyed, lost, stolen, or damaged so as to become undeliverable to the Purchaser, or to a buyer pursuant to Clause 40.3.7 above.

40.10 The Contractor shall have the right to dispute, under the Clause 41 (Disputes), any determination made by the Purchaser under Clauses 40.5 and 40.7, except that if the Contractor has failed to submit his claim within the time provided in Clause 40.5 and has failed to request extension of such time, the Contractor shall be foreclosed from his right to dispute said determination. In

The Contract General Provisions

any case where the Purchaser has made a determination of the amount due under Clauses 40.5 and 40.7, the Purchaser shall pay the Contractor the following:

40.10.1 if there is no right of appeal hereunder or if no timely appeal has been taken, the amount so determined by the Purchaser, or

40.10.2 if an appeal has been taken, the amount finally determined on such appeal.

40.11 In arriving at the amount due to the Contractor under this Clause there shall be deducted:

40.11.1 all unliquidated advance or other payments on account theretofore made to the Contractor, applicable to the terminated portion of this Contract;

40.11.2 any claim which the Purchaser may have against the Contractor in connection with this Contract; and

40.11.3 the agreed price for, or the proceeds of the sale of, any materials, Work, or other things acquired by the Contractor or sold, pursuant to the provisions of this Clause, and not otherwise recovered by or credited to the Purchaser.

40.12 If the termination hereunder is partial, prior to the settlement of the terminated portion of this Contract, the Contractor may file with the Purchaser, in accordance with Clause 16 (Changes), a request in writing for an equitable adjustment of the price or prices relating to the continued portion of the Contract (the portion not terminated by the notice of termination), and such equitable adjustment as may be agreed upon shall be made in such price or prices.

40.13 The Purchaser may from time to time, under such terms and conditions as it may prescribe, make partial payments and payments on account against costs incurred by the Contractor in connection with the terminated portion of this Contract whenever in the opinion of the Purchaser the aggregate of such payments shall be within the amount to which the Contractor will be entitled hereunder. If the total of such payment is in excess of the amount finally agreed or determined to be due under this Clause, such excess shall be payable by the Contractor to the Purchaser upon demand, together with interest calculated using the average of the official base rate(s) per annum of the deposit facility rate as notified by the European Central Bank or such other official source as may be determined by the Purchaser, for the period from the date the excess is received by the Contractor to the date such excess is repaid to the Purchaser, provided, however, that no interest shall be charged with respect to any such excess payment attributed to a reduction in the

The Contract General Provisions

Contractor's claim by reason of retention or other disposition of termination inventory until ten days after the date of such retention or disposition or such later date as determined by the Purchaser by reason of the circumstances.

40.14 Unless otherwise provided for in this Contract, the Contractor, from the effective date of termination and for a period of three years after final settlement under this Contract, shall preserve and make available to the Purchaser at all reasonable times at the office of the Contractor, but without direct charge to the Purchaser, all his books, records, documents, computer files and other evidence bearing on the costs and expenses of the Contractor under this Contract and relating to the work terminated hereunder, or, to the extent approved by the Purchaser, photographs, micro-photographs, or other authentic reproductions thereof.

41.   DISPUTES

41.1   Except to the extent to which special provision is made elsewhere in the Contract, all disputes, differences or questions which are not disposed of by agreement between the Parties to the Contract with respect to any matter arising out of or relating to the Contract, other than a matter as to which the decision of the Contracting Authority under the Contract is said to be final and conclusive, shall be decided by the Contracting Authority. The Contracting Authority shall reduce his decision to writing and mail or otherwise furnish a copy thereof to the Contractor.

41.2   The Contracting Authority shall not proceed with the evaluation and decision in respect of any claim until and unless the Contractor has submitted the attestation as foreseen in Clause 18 (Claims), as well as the complete proof and evidence of the claim (either by submission or by identification of the relevant documentation).

41.3   The Contracting Authority's decision shall be final and conclusive unless, within 30 Days from the date of receipt of such copy, the Contractor mails or otherwise furnishes to the Contracting Authority his decision to open arbitration proceedings in accordance with the Clause 42 (Arbitration). The burden of proof for both receipt and delivery of such documentation shall be by signed and dated registered mail receipt or by hand receipt as acknowledged and signed by the Contracting Authority.

41.4   Pending final decision of a dispute, the Contractor shall proceed diligently with the performance of the Contract, unless otherwise instructed by the Contracting Authority.

42.   ARBITRATION

42.1   Within a period of thirty days from the date of receipt of the notification referred to in Clause 41.3 above, the Parties shall jointly appoint an arbitrator. In the event of failure to appoint an arbitrator, the dispute or disputes shall be

The Contract General Provisions

submitted to an Arbitration Tribunal consisting of three arbitrators, one being appointed by the Purchaser, another by the other contracting party and the third, who shall act as President of the Tribunal, by these two arbitrators. Should one of the Parties fail to appoint an arbitrator during the fifteen days following the expiration of the first period of thirty days, or should the two arbitrators be unable to agree on the choice of the third member of the Arbitration Tribunal within thirty days following the expiration of the said first period, the appointment shall be made, within twenty-one days, at the request of the Party instituting the proceedings, by the Secretary General of the Permanent Court of Arbitration at The Hague.

42.2   Regardless of the procedure concerning the appointment of this Arbitration Tribunal, the third arbitrator will have to be of a nationality different from the nationality of the other two members of the Tribunal.

42.3   Any arbitrator must be of the nationality of any one of the member states of NATO and shall be bound by the rules of security in force within NATO.

42.4   Any person appearing before the Arbitration Tribunal in the capacity of an expert witness shall, if he is of the nationality of one of the member states of NATO, be bound by the rules of security in force within NATO. If he is of another nationality, no NATO classified documents or information shall be communicated to him.

42.5   An arbitrator, who, for any reason whatsoever, ceases to act as an arbitrator, shall be replaced under the procedure laid down in Clause 42.1 above.

42.6   The Contractor agrees to submit to the Arbitration Tribunal only such issues, facts, evidence and proof which the Contractor had beforehand identified and submitted to the Contracting Authority for decision in accordance with Clause 41 (Disputes). The jurisdictional authority of the Arbitration Tribunal shall be restricted to consider only those identical issues, facts, evidence and proof so identified and submitted to the Contracting Authority.

42.7   The Purchaser likewise agrees to restrict its submissions only to the information on which the Contracting Authority based its decision and not to introduce new information and arguments which cannot reasonably be deduced or inferred from the written decision of the Contracting Authority in response to the original dispute.

42.8   The Arbitration Tribunal will take its decisions by a majority vote. It shall decide where it will meet and, unless it decides otherwise, shall follow the arbitration procedures of the International Chamber of Commerce in force at the date of signature of the present Contract.

42.9   The awards of the arbitrator or of the Arbitration Tribunal shall be final and there shall be no right of appeal or recourse of any kind. These awards shall

determine the apportionment of the arbitration expenses.

42.10 Pending final decision of a dispute, the Contractor shall proceed diligently with the performance of the Contract, unless otherwise instructed by the Contracting Authority.

43.   **SEVERABILITY**

43.1   If one or more of the provisions of this Contract is declared to be invalid, illegal or unenforceable in any respect under any applicable law, the validity, legality and enforceability of the remaining provisions shall not be affected. Each of the Parties shall use its best efforts to immediately and in good faith negotiate a legally valid replacement provision.

44.   **APPLICABLE LAW**

44.1   This Contract shall be governed, interpreted and construed in accordance with the private contract law of the Kingdom of Belgium.

*   *

ANNEX 1 TO GENERAL PROVISONS: PURCHASER'S PRICING PRINCIPLES

A.   General

1. With regard to all actions included in Clause 19," Pricing of Changes, Amendments and Claims", the Parties agree that the Purchaser's Pricing Principles contained herein shall govern.

2. As may be requested by the Purchaser, the Contractor shall provide documentation. that the standards or principles employed in the submission of cost or pricing data are in conformance with governing national policies and regulation. The Contractor, when submitting a price proposal based upon national standards and regulations, shall provide a point of contact within the national body governing such standards and regulations in order to allow Purchaser verification and audit.

3. Where such conformance cannot be demonstrated to the satisfaction of the Purchaser, the Purchaser's Pricing Principles will govern.

4. The Contractor shall clearly state whether national standards and rules or the Purchaser's Pricing Principles and formats are the basis for the price proposal.

5. Whether national standards or Purchaser pricing principles are applied, all cost and pricing data shall be verifiable, factual and include information reasonably required to explain the estimating process.

6. The Contractor shall also incorporate provisions corresponding to those mentioned herein in all sub-contracts, and shall require price and cost analysis provisions be included therein.

B.   Purchaser's Pricing Principles

1.   Allowable cost

A cost is allowable for consideration by the Purchaser if the following conditions are fulfilled:

(a) it is incurred specifically for the Contract or benefits both the Contract and other work or is necessary to the overall operation of the business although a direct relationship to any particular product or service cannot be established and is allocated to them in respective proportion according to the benefit received;

   i. Direct Costs
   A direct cost is any cost which can be identified specifically with a particular cost objective as generally accepted. Direct costs are not limited to items which are incorporated in the end product as material or labour.

   ii.   Indirect Costs

NATO UNCLASSIFIED

IFB-CO-14176-SOA-IDM

Book II - The Prospective Contract

Part II - The General Provisions

The Contract General Provisions
Annex 1: Purchaser's Pricing Principles

An indirect cost is one which is not readily subject to treatment as a direct cost. When presented these costs shall be accumulated in logical cost groupings in accordance with sound accounting principles and the Contractor's established practices. An indirect cost may be allocated to more than one final cost objective. An indirect cost shall not be allocated to a final cost objective if other costs incurred for the same purpose, in like circumstances, have been included as a direct cost of that or any other final cost objective. Such costs shall be presented as overhead rates and be applied to each related direct cost grouping.

(b) The Contractor shall specify the allocation of costs to either of the cost groupings. The method by which costs are accumulated and distributed as part of direct or indirect costs cannot be modified during the duration of the Contract.

(c) it is reasonable and expedient in its nature and amount and does not exceed that which would be incurred by an ordinary prudent person in the conduct of competitive business;

(d) it is not liable to any limitations or exclusion as to types or amounts of cost items as set forth herein.

(e) The Purchaser will review other costs presented against the contract and will determine if they would be allowable.

2.   Unallowable Costs

In general all costs which cannot be shown by the contractor to be directly or indirectly of benefit to the Contract are totally unallowable. =Examples of such costs are, among others:

(a) Advertising costs

(b) Costs of remuneration, having the nature of profit sharing.

(c) Costs of maintaining, repairing and housing idle and excess facilities.

(d) Fines and penalties as well as legal and administrative expenses resulting from a violation of laws and regulations.

(e) Losses on other contracts or on expected follow-on contracts

(f) Costs incurred for the creation of reserves for general contingencies or other reserves (e.g. for bad debts, including losses).

(g) Losses on bad debts, including legal expenses and collection costs in connection with bad debts.

NATO UNCLASSIFIED

IFB-CO-14176-SOA-IDM

Book II - The Prospective Contract

Part II - The General Provisions

The Contract General Provisions
Annex 1: Purchaser's Pricing Principles

(h)   Costs incurred to raise capital.

(i)   Gains and losses of any nature arising from the sale or exchange of capital assets other than depreciable property.

(j)   Taxes on profits.

(k)   Contractual penalties incurred.

(l)   Commissions and gratuities.

(m)   Interest on borrowings.

3.   <u>Rates and Factors</u>

   (a) The Contractor shall inform the Purchaser of his rates and factors the basis upon which they were computed.

   (b) If the Contractor's rates and factors for similar contracts placed with national or international public services have not been established or approved by a government agency or an agency accepted by his government, the Contractor shall provide the necessary data to support the proposed rates.

   (c) The term "provisional " used in the title of a rate or factor means a tentative rate established for interim billing purposes pending negotiation and agreement to the final rate or factor.

   (d) A rate or factor is pre-determined if it is fixed before or during a certain period and based on (estimated) costs to be incurred during this period. An rate or factor is post-determined if it is fixed after a certain period and based on costs actually incurred during this period. Pre-determined rates or factors shall be agreed upon as final rates whenever possible; otherwise the provisions of paragraph 3c above shall apply pending agreement to post-determined rates or factors.

   (e) Such rates or factors shall be determined on the basis of Contractor's properly supported actual cost experience.

   (f)   If the rates or factors of the Contractor for similar contracts placed by national or international public services have been established or approved by a government agency or an agency accepted by his government and the Contractor proposes the application of these rates, he shall state the name and address of the agency which has accepted or approved the rates and the period for which they were established. If he proposes rates which vary from the rates mentioned above, he shall furthermore provide a justification for the difference.

A1-3

NATO UNCLASSIFIED

IFB-CO-14176-SOA-IDM

Book II - The Prospective Contract

Part II - The General Provisions

The Contract General Provisions
Annex 1: Purchaser's Pricing Principles

4. <u>Profit/Benefit</u>

(a) Over the entire life cycle of a given acquisition, Profit and/or Benefit may be subject to negotiation.

(b) Subcontracting profit/benefit amounts are dependent upon the size, nature and oversight needs of the subcontract(s) the prime contractor will use for work performance period.

(c) Profit/benefit is considered by the Purchaser to be directly related to the anticipated risk of the Contractor during the performance of the Contract.

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

BOOK II – PART IV

STATEMENT OF WORK (SOW)

DOCUMENT CONTROL PAGE

VERSION HISTORY

Version	Author	Date	Reason for Change	Superseded Document

TABLE OF CONTENTS

Tables

Figures

SECTION 1: INTRODUCTION

1.1. Scope of the Statement of Work

> [SOW-1]   *The Contractor SHALL be responsible for the totality of the implementation of the solution, which meets the requirements set forth in this Statement of Work (SoW), including but not limited to: overall design, integration, security accreditation and system engineering of the Service Oriented Architecture (SOA) & Identity Management (IdM) Platform throughout the Contract's Period of Performance.*

1.1.1.   The scope of this Statement of Work (SoW) describes requirements, development, delivery and implementation of the SOA & IdM Platform and is included in two Waves as described below in Table 1: Waves and Packages.

Wave 1	Wave 2
Work Package 2.1-2.7 – Basic SOA Platform	Work Package 2.8-2.14 – Extended SOA Platform
Work Package 4.1-4.7 – Basic IdM Platform	Work Package 4.8-4.14 – Extended IdM Platform
Work Package 6.1-6.2 – Support pilot Integration cases	Work Package 6.3-6.4 – Support pilot Integration cases
Work Package 7 – Support Integration of other projects	

Table 1: Waves and Packages

1.2. Project Vision

1.2.1.   Historically, NATO capabilities have been delivered as a collection of self-contained, individual systems. Separate projects procured all the necessary hardware, software and services required to implement a required capability, which operated within its own system and information silo. These systems rarely shared information between themselves, and certain features and functionality were recreated time and again. These characteristics of systems do not take advantage of economies of scale or the rationalisation of Information Technology (IT) infrastructure that NATO is capable of leveraging.

1.2.2.   Now NATO is changing the way it delivers its Information Technology and Communications infrastructure and applications. Under the banner of "IT Modernisation" (ITM), it is shifting from an independent, stove-piped approach to a more granular set of loosely coupled services that can be quickly and easily composed to deliver agile and cost-effective support to operations.

1.2.3.   Future systems within NATO will adapt to the architectural paradigms adopted in modern Cloud Computing solutions, as originally outlined in the NATO Network Enabled Capability (NNEC) Feasibility Study and which have been broadly and successfully implemented in militaries and industries across the NATO Nations.

1.2.4.   The IT infrastructure of the future will be consolidated into a limited number of data centres, based on a common hardware platform with a centralised Operations & Maintenance environment. All of this will be delivered as a service (known in Cloud Computing terms as "Infrastructure-as-a-Service", or IaaS).

1.2.5.   At the applications/systems level, the IT platform of the future will provide the environment to enable systems developers rapidly implement and deploy new capabilities – and reuse existing capabilities – into the NATO functional landscape. In Cloud Computing terms this is known as "Platform-as-a-Service" (PaaS).

1.2.6.   PaaS is a category of Cloud Computing services that provides a platform allowing for the development, execution, and management of applications without the cost and complexity of building and maintaining the underlying common services necessary for almost all applications.

1.2.7.   Providing the NATO Enterprise with a robust, secure PaaS environment is the primary role of the SOA & IdM Platform.
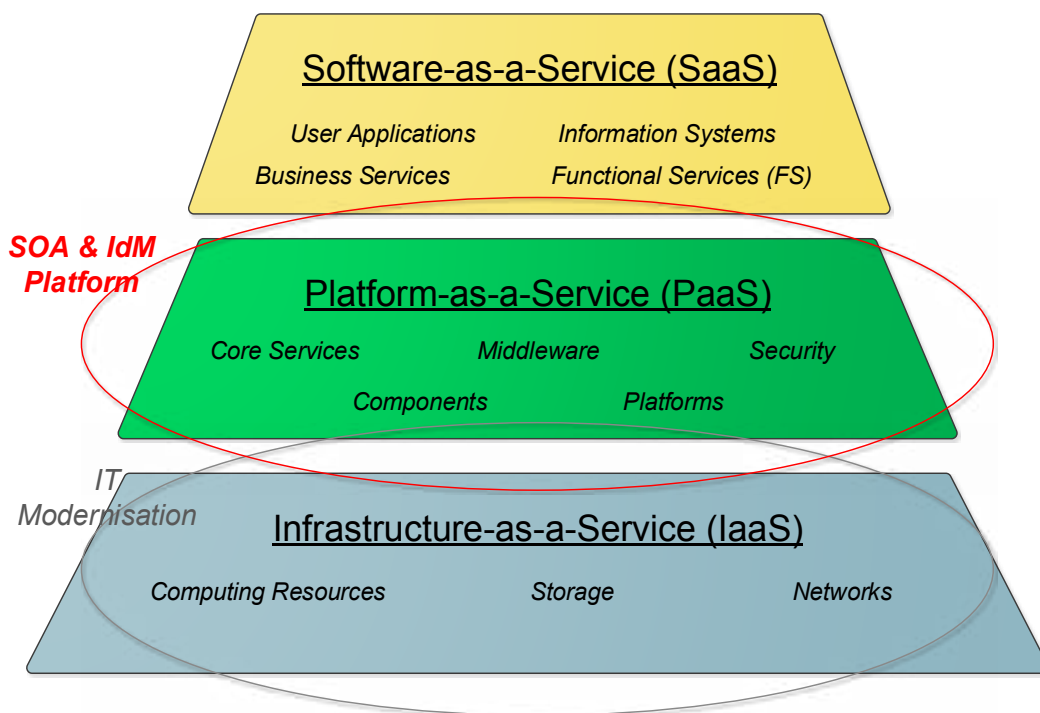
Figure 1: Cloud Computing stack and the Role of the SOA & IdM Platform

[SOW-2]   Through his responses to the requirements in this Statement of Work (SoW), the Contractor SHALL at all times ensure the integrity of the SOA & IdM Vision and strive to effect its achievement.

1.3.   Capability Vision

1.3.1.   The SOA & IdM Platform provides a flexible framework to support the delivery of dynamic Functional Services (FS) that can be rapidly reconfigured and deployed to support a broad range of missions.

1.3.2.   This will transform the next generation of Functional Services, and enable the shift to the more agile and rapid development of more granular functionality for operations. Information can freely flow between different actors, both within the Alliance and broader coalitions to improve both human and machine decision making. Even as the information is more widely available, access to the information will be more tightly and dynamically controlled, ensuring secure information superiority.

1.3.2.1.   Capability Goal 1: The Platform is available across every network in NATO. It allows FS to be rapidly deployed and / or reconfigured in response to the current Mission environment and requirements. It is integrated with the Infrastructure as a Service (IaaS) provided by ITM to ensure that different capabilities can be rapidly and flexibly scaled to meet operational needs. New services are quickly introduced and incorporated into the overall environment in order to ensure consistent and ongoing enhancements of capabilities.

1.3.2.2.   Capability Goal 2: Information will be available to the widest possible audience, thus supporting the "responsibility to share". Information flows are supported between different systems, and are agnostic of data formats. The information arrives at the consuming system in the format that is required, ensuring that not every system needs to understand every data format. New information sources are brought online dynamically, and occasionally only temporarily, in order to support the ambition for Information Superiority.

1.3.2.3.   Capability Goal 3: The Responsibility to Share is tempered by the "Need to Know". Information can be identified with comprehensive metadata, which makes the information easier both to find and control. A consistent Identity ecosystem is delivered to ensure that the identity of each and every information consumer can be resolved and audited from end to end. Access to information is managed according to formally defined Security Policies, meaning that only those who are authorised to consume information are allowed to do so. The Policies can be updated dynamically, in response to changing operational conditions, and can also incorporate heuristics to help mitigate the insider threat. Information flows securely both within and between networks of different classifications.

1.3.2.4.   Capability Goal 4: Operational Capabilities need to adapt the way that they are developed and procured to take advantage of the new operating paradigm. The developers of FS do not have to consider many of the fundamentals of system development, such as security and interoperability, and so are able to focus on delivering capabilities that meet the needs of the users in the operational community. They deliver a user experience that is much more consistent and integrated across different operating environments.
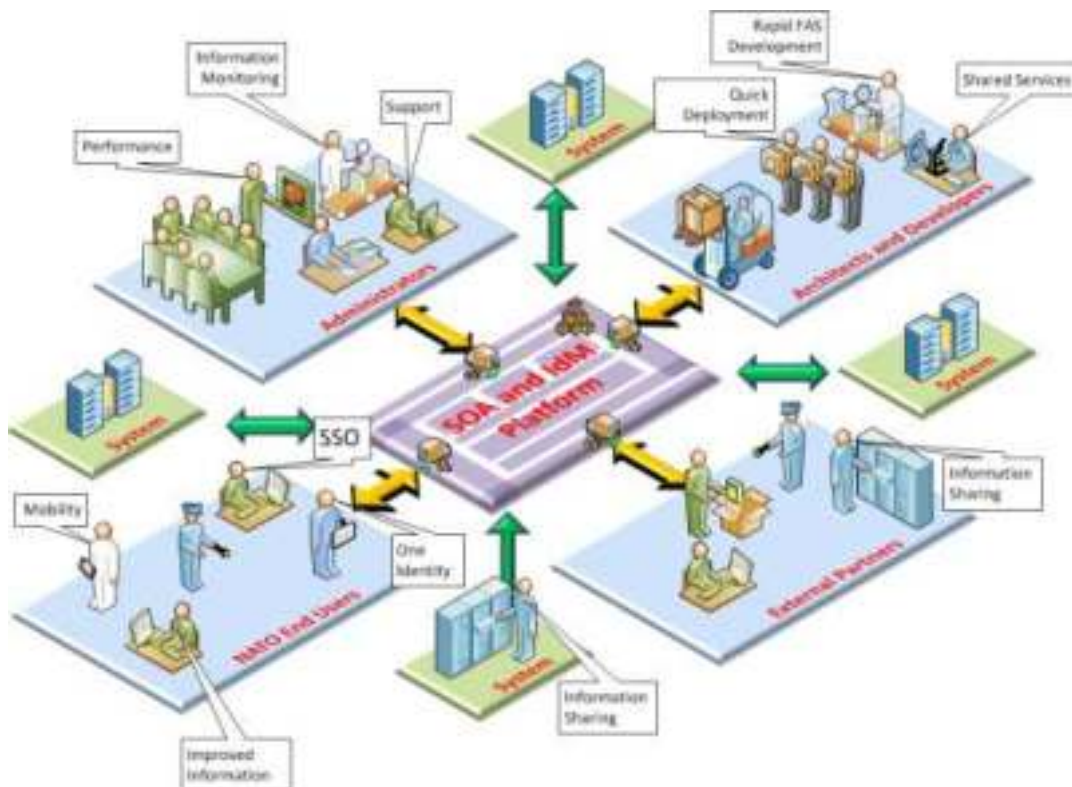
Figure 2: High-Level Operational Concept Description

1.4. Background

1.4.1. Platform Purpose

1.4.1.1. The SOA & IdM Platform delivers a foundational set of core services and components that can be easily reused within new applications.

1.4.1.2. The purpose of the SOA & IdM Platform is to support the development, operation and evolution of NATO capabilities; it is not an end in itself. Rather than having to consistently "reinvent the wheel", Functional Service providers or other systems are able to reach into an existing toolkit for common building blocks such as Messaging, Service Discovery and Identity and Access Management (IAM).

1.4.1.3. The components provided offer proven, clear and well-documented interfaces that can be easily integrated. This leaves the FS providers free to concentrate on their subject matter expertise, which is to understand, articulate and manifest the business logic that supports the operational requirements of their Communities of Interest (CoI).

1.4.1.4. As well as delivering the functional components themselves, the Platform comes with a clear set of guidelines, tools, best practices and process definitions that support the whole lifecycle of a FS. The integration components also support the integration of legacy systems into the broader, service-oriented ecosystem, thus ensuring continuing Return on Investment (ROI) and wider information sharing.

1.4.2. Platform Functionality

1.4.2.1. The key functionality of the SOA & IdM Platform is two-fold.

1.4.2.2.   First, it provides a common environment, with common services already implemented, which enables NATO and the Bi-Strategic Command (Bi-SC) Automated Information System (AIS) to rapidly deliver integrated information systems. To achieve this purpose, the Platform:

1.4.2.2.1.   Offers re-usable building blocks for the implementation of service-oriented systems and provide a foundation to support the management and improved information exchange of Functional Services (FS) and user applications.

1.4.2.2.2.   Provides the common "back end" services for the NATO Enterprise which other projects will depend on for the adoption of the SOA paradigm.

1.4.2.2.3.   Designs and implements an initial enterprise-wide capability to enable the management of core data, SOA and web services.

1.4.2.2.4.   Supports the move away from individual point-to-point connections, towards data sharing with unanticipated users in a loosely-coupled, network-enabled environment, thus delivering more flexible and agile services.

1.4.2.2.5.   Allows for reuse and/or decomposition of existing monolithic stove-piped systems, by providing the capability to "service enable" functions of currently operational capability.

1.4.2.2.6.   Supports implementation of cross-domain solutions by enabling federation for certain services (e.g. Messaging).

1.4.2.3.   Second, the Platform implements for the NATO Enterprise a set of common IAM services. In this context, the Platform:

1.4.2.3.1.   Provides a set of IdM services, including all necessary underlying hardware and software components, in support of FS and other NATO information systems.

1.4.2.3.2.   Provides additional security services and control mechanisms (i.e. IAM) in support of FS and other NATO information systems.

1.4.2.3.3.   Integrates with NATO Public Key Infrastructure (NPKI) to support strong authentication.

1.4.2.3.4.   Extends the scope of the NATO Enterprise Directory Service (NEDS) to cover the Protected Business Network (PBN) and the exchange of identity information across domains (e.g. NATO ←→ National) in support of federated solutions.

1.4.2.3.5.   Interfaces with IdM-related systems as required, such as the Automated Personnel Management System (APMS), Allied Command Operations (ACO)/Allied Command Transformation (ACT) and Missions Identification System (AMIS) and physical access control systems.

1.4.2.4.   Together with the underlying IaaS infrastructure, this PaaS Platform changes the way NATO builds and procures FS and other user applications.

1.4.2.5. The Platform enables other projects to use consistent, coherent and proven solutions to common problems, allowing them to focus on delivering real business value to NATO.

1.4.2.6. The reuse of existing services and components ensures that NATO achieves a greater return on investment on information systems. At the same time, the ability of different Communities of Interest to share and distribute information in a controlled way to a broader range of partners ensures that the Alliance meets its "Responsibility to Share". Figure 3 illustrates this concept.

1.4.2.7. In addition, the Platform-provided IAM services ensures coherent identity management and the common implementation of application-level security policies and practices across all NATO systems and Functional Services which leverage the Platform.
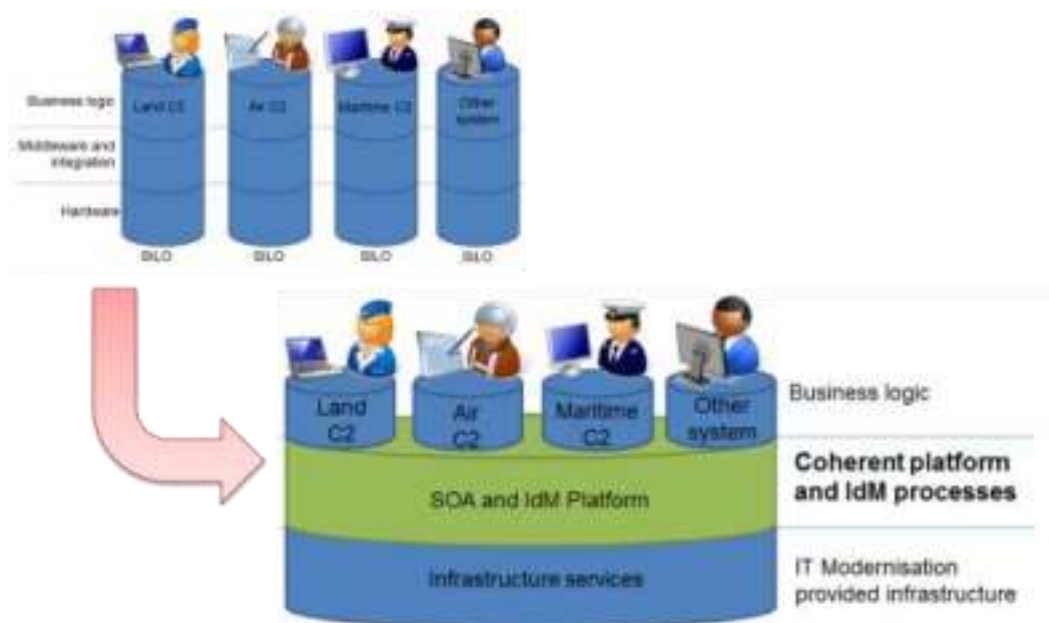
Figure 3: Changes introduced by this Platform to the way NATO builds software

[SOW-3]   *The Contractor SHALL ensure during the execution of the contract that the purpose and functionality described in this SoW are completely addressed in the products and services provided.*

1.4.3. Platform Audience

1.4.3.1. The SOA & IdM Platform provides services to the NATO Enterprise (i.e. NATO Command Structure, NATO HQ, and Agencies belonging to the NATO Enterprise) as needed. Services may also be offered to NATO partners and/or other organisations, as requirements and policies allow. The users/systems from both the Alliance Enterprise and the Coalition Enterprise benefit from the services via network connectivity, in accordance with NATO security policies.

1.4.3.2.   The SOA & IdM Platform addresses both the Operational Network (ON) and the PBN.

1.4.3.3.   The SOA & IdM Platform provides an ecosystem to support integration of existing NATO SOA and non-SOA systems, and integration of NATO systems with federated national and non-NATO systems.

1.4.3.4.   The SOA & IdM Platform provides a web hosting platform in order to support the development of new NATO systems following the SOA approach.

1.4.3.5.   The SOA & IdM Platform provides the necessary tools to manage the full lifecycle of identity provisioning within the NATO Enterprise. This is completed with the definition of a clear set of business processes (such as "new staff member joining the organisation" process) which streamlines and simplifies IdM across Functional Services (FS) and sites.

1.4.3.6.   The SOA & IdM Platform integrates with Enterprise NATO Public Key Infrastructure (E-NPKI) to support strong authentication to NATO Communication and Information Systems (CIS).

1.4.3.7.   The SOA & IdM Platform provides NATO Enterprise wide capabilities to manage metadata (e.g. schemas) and service definitions (e.g. interfaces, service contracts) in an NNEC environment.

1.4.4.   Mode of Operation

1.4.4.1.   The SOA & IdM Platform services are interoperable with similar services in the deployed and federated domains – for example, allowing information sharing with equivalent core services in the Nations or between the ON and Deployable Computer Information System (DCIS) networks, or federating Messaging services across networks – via clearly defined interfaces based on agreed open standards.

1.4.4.2.   The SOA & IdM Platform services are consistent with the requirements of DCIS, in order to allow instance(s) of the Platform to be implemented on the DCIS infrastructure without modification.

1.4.4.3.   The Platform leverages existing border protection and cross domain services where these offer mechanisms for information exchange across security domains (both with NATO and external domains). The Platform also implements additional components into existing cross-domain solutions if required.

1.4.4.4.   The SOA & IdM Platform supports the integration of FS and user applications through the integration of a number of commercially available connectors for common specifications and protocols, ensuring that CIS Security is maintained; e.g. web services, e-mail, directory services. Development of custom connectors and integration cases is outside the scope of the SOA & IdM Platform, although it is technically possible through the extensibility mechanisms of the platform.

1.4.4.5.   The technical solution for the SOA & IdM Platform is able to support modes of operation including peacetime, crisis, and exercise – as well as for training purposes – from the static locations through network connectivity.

1.4.4.6.   The technical solution for SOA & IdM Platform is sized for peacetime with the ability to scale up to support other modes of operation.

1.4.4.7.   The SOA & IdM Platform provides interfaces with NATO Nations for Directory Services (upgrade of the existing synchronisation mechanism between NATO and NATO Nations).

1.4.4.8.   The SOA & IdM Platform may interface with NATO Nations for user access to NATO CIS (i.e. federation scenario), provided cross-domain connections are in place.

1.4.4.9.   Mission Network provisioning is not within the scope of the Platform implementation, nor is installation on the Deployable CIS provided by Capability Package (CP) 0A0149. However, the Platform is compatible with the deployed environment and therefore complies with the relevant requirements.

1.5. Priorities

1.5.1.   The top priority in the execution of this contract is the achievement of the project milestones described in SECTION 4: Milestones of this Statement of Work. In particular Wave 1 must be completed within 17 months of the Effective Date of Contract (EDC).

> [SOW-4]   *The Contractor SHALL observe the Project's priorities in their planning and execution of the work.*

SECTION 2: APPLICABLE DOCUMENTS

[SOW-5]   *The Contractor SHALL be aware and comply with the documents as referenced in ANNEX F and ANNEX G throughout the Contract.*

SECTION 3: SCOPE

3.1. Overview

3.1.1. This Statement of Work (SoW) describes the responsibilities of and activities to be conducted by the Contractor to meet the requirements of the SOA & IdM Platform project.

> [SOW-6] *The Contractor SHALL provide all necessary resources to include services, personnel, materials, components, equipment, data and documentation needed to accomplish all the tasks described in the SoW, to meet all the requirements of the SoW (including annexes) and to fulfil all other Contract's provisions.*

> [SOW-7] *The documents listed in SECTION 2: Applicable Documents may be revised over time. The Contractor SHALL always use the current version of each document.*

> [SOW-8] *The Contractor SHALL be aware and comply with the above-mentioned documents throughout the duration of this Contract.*

3.1.2. Except as otherwise stated, the delivery dates of the associated deliverables are provided in the Schedule of Supplies and Services (SSS).

> [SOW-9] *The Contractor SHALL provide project management services.*

> [SOW-10] *The Contractor SHALL provide systems engineering services to cover: requirements review, system design and system integration.*

> [SOW-11] *The Contractor SHALL provide test services to prove the system Product Baseline (PBL) as meeting its requirements.*

> [SOW-12] *The Contractor SHALL fully document the design, operation and maintenance of SOA & IdM Platform by providing the required manuals, operational procedures, supporting technical data, computer software and drawings required by the Contract.*

> [SOW-13] *The Contractor SHALL conduct all necessary activities to support the Purchaser in achieving Security Accreditation at the Operational Network up to NATO SECRET (NS) and Protected Business Network (PBN - NATO RESTRICTED and PBN - NATO UNCLASSIFIED) levels.*

> [SOW-14] *The Contractor SHALL co-ordinate with the Purchaser to ensure that the Site preparation activities are completed in accordance with the installation requirements of the delivered system.*

> [SOW-15] *The Contractor SHALL procure and prepare the system components for delivery to the Sites specified in this Contract.*

> [SOW-16] *The Contractor SHALL deliver the required software to the prepared Sites, and execute installation/deployment, on-site testing, training and activation.*

> [SOW-17] *The Contractor SHALL provide support to application and service management integration and to pilot cases.*

[SOW-18] *The Contractor SHALL provide Integrated Logistics Support (ILS) services (see SECTION 14), including Training Services.*

[SOW-19] *The Contractor SHALL provide Operation and Maintenance (O&M) support with appropriate service management interfaces both at information (monitoring / reporting) and process (request / incident) level (see ANNEX B).*

[SOW-20] *The Contractor SHALL comply with all overarching requirements as described in the SoW (Testing process, Site Survey process, Quality Assurance and Control, Configuration Management).*

3.2. Scope

3.2.1. The scope of the NATO Enterprise for C3 capabilities and the provision of Information and Communication Technology (ICT) services is defined in [AC/322-D(2015)0014-REV3-AS1, 2015].

3.2.2. Functional Scope

The purpose of the SOA & IdM Platform is described in System Requirement Specifications (SRS).

3.2.3. Work Packages

3.2.3.1. Waves and Work Packages are described in Table 1: Waves and Packages in para 1.1.1.

3.2.4. Project Phasing

3.2.4.1. Project phasing is described in SECTION 4: Milestones and in SECTION 6: System Implementation , more specifically SECTIONS 6.8 - 6.12).

3.3. Overall project schedule

3.3.1. A detailed project schedule is provided in SECTION.4.2: Overall project and key milestones schedule.

3.4. Relationships with other Programmes and Systems

3.4.1. Relationships with other Programmes and Systems

3.4.1.1. The SOA & IdM Platform is part of the Bi-Strategic Command Automated Information System (Bi-SC AIS), as defined in the Bi-SC AIS Reference Architecture [NAC AC/322-D(2005)0037, 2005].

3.4.1.2. The Bi-SC AIS is NATO's Command and Control Information System used throughout the NATO Command Structure, in NATO Command Deployments and in NATO Exercises. The Bi-SC AIS is in turn one element of NATO's overall CIS Capability, which includes a number of strategic sub-systems such as the NATO Core Communications Network, Planning, Intelligence, Theatre Missile Defence, and Deployable CIS and so on.

3.4.1.3. The SOA & IdM Platform capability to be acquired under the CP 9C0150 is to be a fully integrated element of the Bi-SC AIS.

3.4.1.3.1. In this context, the SOA & IdM Platform co-exists and eventually integrates with (by providing a future common platform for) Intelligence Functional Services (Intel-FS), Logistics Functional Services (LOG FS), Maritime Functional Services (MCCIS), Land Functional Services (LC2IS), Air Functional Services (AirC2IS), Planning Functional Services (TOPFAS) and other functional services such as the NATO Common Operational Picture (NCOP), as they become available.

3.4.1.3.2. The SOA & IdM Platform takes advantage of the Bi-SC AIS core services (directory, registry, e-mail, etc.) to the extent possible.

3.4.1.4. The Platform provides its services and interfaces to external systems.

3.4.1.4.1. Different Authoritative Identity Data Sources exchange information with the Platform's NEDS (NATO Enterprise Directory Services) component. The E-NPKI is one of these sources, but is also acting in another role in underpinning trust for the Security Services.

3.4.1.4.2. External information sources provide the Information Platform access to data that can be integrated and exposed in a single, standards-based format together with descriptive metadata to aid the understanding of the information, facilitate information security, and enable automated processing.

3.4.1.4.3. The Integration Services enable information sharing between heterogeneous and decoupled External systems, such as FS and other NATO applications.

3.4.1.4.4. Specific information is pushed between SOA & IdM Platform elements (e.g. NEDS) from PBN to ON through data diodes that are already available NATO networks.

3.4.1.4.5. Several services can also be made available to external partners, provided that cross-domain solutions are in place. These include the Messaging Services, the Registry and Repository Services, the directory services via the Allied Replication Hub, and the Security Token Services.

3.4.2. Existing Capabilities

3.4.2.1. The SOA & IdM Platform has interdependencies with a large number of projects that either have been fielded or are in the process of being delivered. Some examples of these include the current Active Directory Federation Services (ADFS) implementations and the extant NATO Metadata Registry and Repository (NMRR), which provides a subset of the Metadata Registry services that the Platform implements.

3.4.2.2. The following sections describe projects that the SOA & IdM Platform relies on, build upon, or provide an essential service to. The nature of these dependencies is mostly technical, and it is self-evident that they therefore introduce constraints on the timing of the different Platform delivery activities.

3.4.2.3. Related Projects and Systems

3.4.2.3.1.   NATO Enterprise Directory Services (NEDS)

3.4.2.3.1.1   The NATO Enterprise Directory Services provides Directory synchronisation between the various NATO directory and data repositories.The SOA and IdM Platform project is intended to further integrate the NEDS system with additional data sources (e.g. NPKI and Physical Access Control Systems).

3.4.2.3.2.   IT Modernisation (ITM)

3.4.2.3.2.1   The ITM project transforms the way IT services are provided to users across the NATO enterprise, including the NCS, the NATO Headquarters (NHQ) and NATO agencies. It provides Infrastructure as a Service (IaaS) and an Enterprise Service Management and Control Service as wellas user services and user devices. ITM is the amalgamation of the three CP 9C0150 Projects: OIS03091; OIS03092, and OIS03101.

3.4.2.3.2.2   The SOA & IdM Platform is primarily deployed in the Data Centres delivered by the ITM project. This means that the SOA & IdM Platform is able to take advantage of the ITM infrastructure (IaaS), thus reducing the amount of Hardware that is specifically procured.

3.4.2.3.2.3   The SOA & IdM Platform relies on the timely delivery of the IT infrastructure by the ITM project.

3.4.2.3.2.4   The SOA & IdM Platform also needs to integrate its Service Management tooling with the Service Management and Control (SMC) framework as provided by ITM.

3.4.2.3.3.   Enterprise NATO Public Key Infrastructure (E-NPKI)

3.4.2.3.3.1   The E-NPKI project will deploy a PKI environment for NATO that fully complies with the NPKI Certificate Policy [NAC AC/322-D(2004)0024-REV2, 2008].

3.4.2.3.3.2   The SOA & IdM Platform implements a number of services, including its authentication and authorisation services, which depend on the implementation of a PKI capability across the NATO Enterprise.

3.4.2.3.3.3   NEDS is the repository for E-NPKI information; e.g. Certification Revocation List (CRL), public certificates. The SOA & IdM Platform proliferates and improves this function.

3.4.2.3.3.4   Due to their mutual dependence, the delivery of the SOA & IdM Platform is closely coordinated with that of E-NPKI.

3.4.2.3.4.   Functional Service (FS) implementation projects

3.4.2.3.4.1   It is expected that the majority of FSs take advantage of the services offered by the SOA & IdM Platform. This means that all FS have an interdependency with the Platform. The components and services that are provided are an integral part of new FS.

3.4.2.3.4.2   The fact that the implementations of different FS that could make use of SOA services have already started challenges the delivery of the SOA & IdM Platform. This issue is addressed in several ways:

3.4.2.3.4.2.1   Projects that are supposed to be implemented in several increments can postpone usage and integration with SOA services until future increments.

3.4.2.3.4.2.2   Projects can implement FS compatible with standards and interfaces identified for the SOA & IdM Platform [NAC AC/322-N(2011)0205, 2011], but postpone their use until the availability of SOA & IdM Platform. When services provided by the SOA & IdM Platform become available, the FS are reconfigured and/or updated to make use of them. Because of use of the same standards and well defined interfaces, additional implementation effort for the FS is reduced. Detailed descriptions of selected interfaces to be provided by the SOA & IdM Platform are available in form of Service Interface Profiles (SIP) [NAC ADatP-34(G)-REV1, 2013].

3.4.2.3.4.2.3   Projects can implement their own intermediate SOA services, compatible with the available SIPs, with the intention of replacing them with the enterprise SOA & IdM Platform services, when they become available.

3.4.2.3.4.2.4   In limited cases, projects do not wait for the SOA & IdM Platform but implement their own alternative solutions, often using different technology or based on point-to-point connections with other systems.

3.4.2.3.5.   Deployable CIS (DCIS)

3.4.2.3.5.1   The SOA & IdM Platform services will need to be consistent with the requirements of DCIS, in order to allow instance(s) of the Platform to be implemented on the DCIS infrastructure without modification.

3.4.2.3.6.   Provide Information Exchange Services

3.4.2.3.6.1   The SOA & IdM Platform leverages existing Information Exchange Gateways (IEG) and other border protection and cross-domain services where these offer mechanisms for information exchange across security domains (both with NATO and external domains).

3.4.2.3.6.2   The SOA & IdM Platform coordinates in that respect with the CP 9C0150 Project 2012/0IS03102, which will implement additional cross-domain solutions.

3.4.2.3.7.   NATO Computer Incident Response Capability (NCIRC)

3.4.2.3.7.1   The NCIRC performs security monitoring and security management of NATO's CIS infrastructure throughout the NATO Enterprise.

3.4.2.3.8.   NATO Communications Infrastructure (NCI)

3.4.2.3.8.1 The NCI project will upgrade the NATO General Purpose Communication System (NGCS) to a modern IP networking architecture. It will provide high performance and resilient NATO-wide NATO Unclassified (NU), NATO Restricted (NR) and NATO Secret (NS) Internet Protocol (IP) services.

3.4.2.3.9. Service Management and Control (SMC) Capability Package (CP 102) and SMC Target Architecture

3.4.2.3.9.1 The nature of the future Enterprise SMC capability will be largely determined by the SMC Target Architecture. The SOA & IdM Platform will ultimately rely upon the Enterprise SMC capability when it is available. In the meantime, the Platform will need to anticipate the necessary Application Programming Interfaces (API) and/or data interfaces to operate with compatible data models and vocabularies that will prevail in the Enterprise SMC capability.

[SOW-21] *The Contractor SHALL deliver the analysis for Service Management interfaces between their Domain Service Management (the Contractor's) and the Enterprise Service Management (the Purchaser's), including but not limited to: Service Asset and Configuration Management, Event Management, Incident and Request escalation and delegation, raw or pre-processed data feed for service dashboarding and Service Level Agreement (SLA)/ Operational Level Agreement (OLA) reporting purposes.*

[SOW-22] *The Contractor SHALL actively contribute to the convergence between their Domain Service Management and the Enterprise Service Management and SHALL keep track of the SMC Target Architecture [NCIA SMC TA, 2018] development.*

3.4.3. Dependency Assumptions

3.4.3.1. It is assumed that the following projects have delivered, or at least are available for integration to the SOA & IdM Platform:

a. ITM;

b. E-NPKI (Enterprise NATO Public Key Infrastructure);

c. IEG or other cross-domain services for federation capabilities.

3.4.3.2. It is assumed that future NATO FS and other information systems integrated by the SOA & IdM Platform are centralised in the Data Centres provided by the ITM project.

3.4.3.3. In exceptional cases, systems not installed in the Data Centres – such as via DCIS – will have sufficient network connectivity (bandwidth and latency) to integrate through the SOA & IdM Platform. The Platform will have sufficient robustness (e.g. guaranteed message delivery) to deal with the potential intermittent connectivity and latency issues that are part of this environment.

3.4.3.4. It is assumed that in parallel with the implementation of the SOA & IdM Platform, the Purchaser staff transformation currently taking place provides the competencies and skill sets, at the locations needed, to support the new Platform.

3.4.3.5.   The modifications of any other systems (beyond those covered by the pilots) are out of scope of the implementation of this Platform.

[SOW-23]   *As part of the project management activities, the Contractor SHALL maintain the necessary relationships with the above-mentioned projects, including other Purchaser's systems to be interfaced with SOA & IdM Platform and associated Contractors, as applicable:*

a. *the Contractor SHALL attend, organise and conduct meetings as necessary;*

b. *the Contractor SHALL be proactive in order to ensure the SOA & IdM Platform effectiveness when delivering services to the relying systems, including systems already implemented as well as ones planned for deployment;*

c. *per Purchaser's request, the Contractor SHALL identify any documents, meeting minutes or any other information from these projects required to maintain an effective coordination process.*

SECTION 4: MILESTONES

4.1. Introduction

4.1.1. This section provides a notional view of the project logical schedule as well as the list of key project milestones and criteria to be met by the Contractor to achieve them.

4.1.2. Key project milestones are defined as:

    a. Milestone 0: Effective Date of Contract (EDC)

    b. Milestone 1: System Design Review (SDR) for Wave 1 consisting of Preliminary Design Review (PDR) and Critical Design Review (CDR)

    c. Milestone 2: Provisional System Acceptance (PSA) for Wave 1

    d. Milestone 3: Final System Acceptance (FSA) for Wave 1

    e. Milestone 4: System Design Review (SDR) for Wave 2 consisting of Preliminary Design Review (PDR) and Critical Design Review (CDR)

    f. Milestone 5: Provisional System Acceptance (PSA) for Wave 2

    g. Milestone 6: Final System Acceptance (FSA) for Wave 2

    h. Milestone 7: Operation and Maintenance (O&M).

4.2. Overall project and key milestones schedule

4.2.1. Figure 4 provides the Overall Project Schedule with expected timeline for each Work Package. Each Work Package scope is defined in SECTION 6: System Implementation.

4.2.2. Figure 4 below provides Key milestones suggested schedule and delivery approach.

4.2.3. Project will be split up in two Waves (see Table 2 below):

    a. Work Packages of Wave 1 will last no longer than 18 months and will be completed upon reaching its FSA milestone;

    b. Work Packages of Wave 2 will last no longer than 15 months and will be completed upon reaching its FSA milestone;

    c. Work Packages 6 and 7 (for both Waves) will start during Work Packages 2 and 4 respectively (in regards to Waves), no earlier then PBL and last for a period of 24 (twenty four) months and will be completed upon reaching its FSA milestone.

[SOW-24] *The Contractor SHALL adhere to the Overall Project Schedule and split of Work Packages into two separate Waves.*

[SOW-25] *The Contractor SHALL reflect the Overall Project Schedule and split of Work Packages in all relevant Project Management Documentation (SECTION 5.4: Project Management Documentation).*

IFB_CO-14176-SOA-IDM
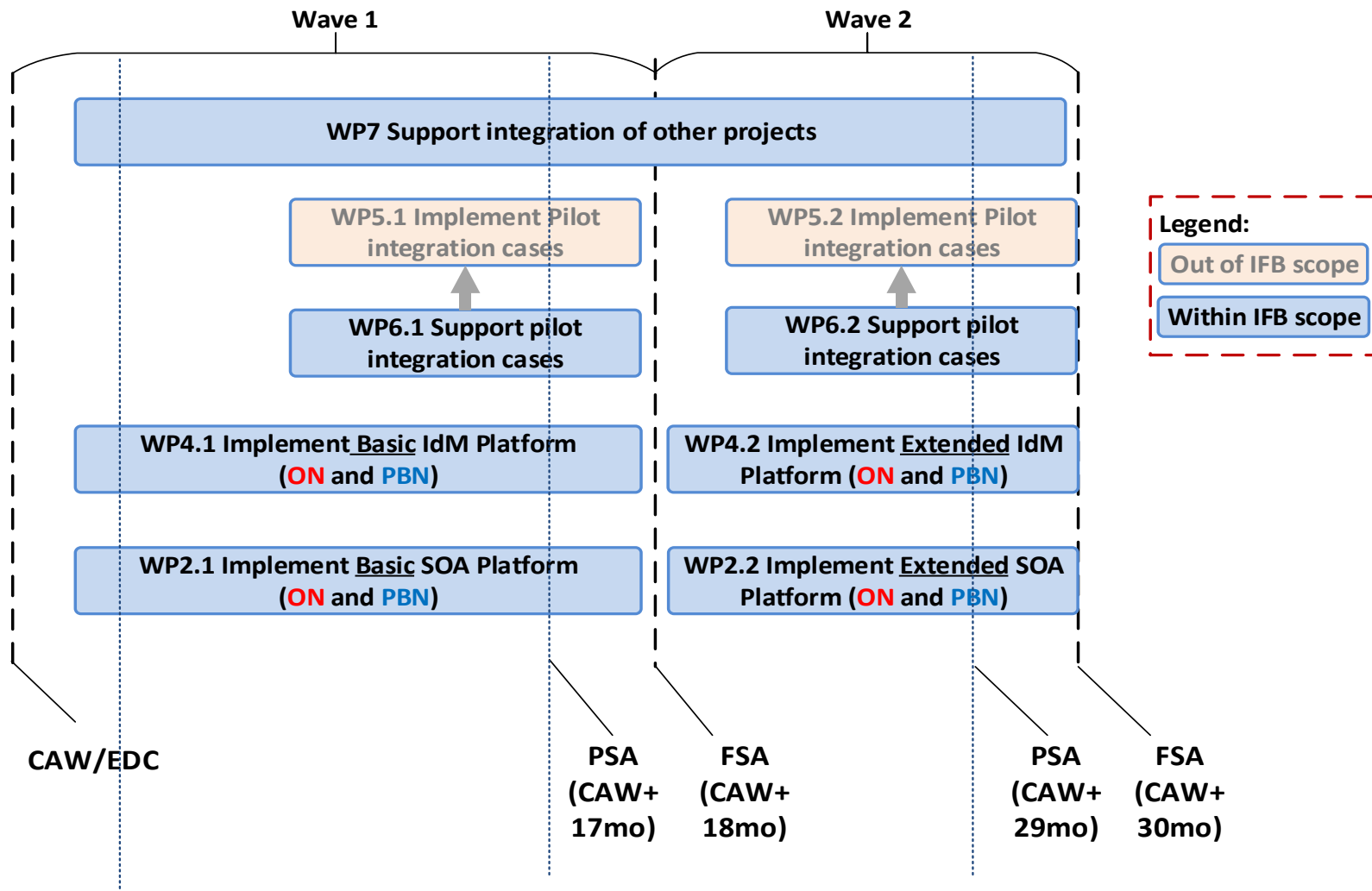
Figure 4: Overall Project Schedule

IFB_CO-14176-SOA-IDM

Work Packages & Milestones		Wave 1																	
Timeline	Months after EDC	+1	+2	+3	+4	+5	+6	+7	+8	+9	+10	+11	+12	+13	+14	+15	+16	+17	+18	+19-41
WP 2.1 Implement basic SOA Platform	SOA	SRR	SDR (PDR & CDR)	Sprint	Sprint	Sprint	IRCv1 alpha	PBL (IRCv1.1)	PBL (IRCv1.2)	PBL (IRCv1.3)	IRCv2 beta	PBL (IRCv2.1)	PBL (IRCv2.2)	PBL (IRCv2.3)	RCv3 external	OBL (RCv3.1)	DA	PSA/ OBL Wave 1	FSA Wave 1	
WP 4.1 Implement basic IdM Platform	IdM																			
Sprints/Flow		R&D Review					Release				Release				Release		Release	Acceptance		
Payment'$ schedule WP 2.1 and WP 4.1			After CDR approval $				IRC released to PMIC $								RC released to IV&V $			$	Final $	
WP 6.1 Support Pilot Cases																		Support pilot cases 24months		

Work Packages & Milestones		Wave 2																
Timeline	Months after EDC	+19	+20	+21	+22	+23	+24	+25	+26	+27	+28	+29	+30	+31	+32	+33	+34-56	Legend:
WP 2.8 Implement extended SOA Platform	SOA	PDR	CDR	Sprint	Sprint	IRCv4 alpha	PBL (IRCv4.1)	PBL (IRCv4.2)	IRCv5 beta	PBL (IRCv5.1)	PBL (IRCv5.2)	RCv6 external	OBL (RCv6.1)	DA	PSA/ OBL Wave 2	FSA Wave 2		$ = acceptance required
WP 4.8 Implement extended IdM Platform	IdM																	
Sprints/Flow		R&D Review				Release			Release			Release		Release	Acceptance			
Payment'$ schedule WP 2.8 and WP 4.8			After CDR approval $			IRC released to PMIC $						RC released to IV&V $			$	Final $		
WP 6.3 Support Cases		Support pilot cases 24months (continued)																

Table 2: Key milestones suggested schedule and delivery approach

[SOW-26]   The Contractor SHALL integrate the Key milestones suggested schedule and delivery approach (see Table 2) in its Project Master Schedule, at a minimum by committing to deliver:

a. System Requirement Review (SRR) at the beginning of each Wave;

b. System Design Review (SDR) milestone at the beginning of Wave 1 and updated (delta) SDR at the beginning of Wave 2;

c. monthly System Baseline (SBL) for WP2 and WP4;

d. quarterly IRC (Internal Release Candidate) and RC (Release Candidate) for Wave 1 for WP2 and WP4;

e. bi-monthly IRC and RC for Wave 2 for WP2 and WP4;

f. final RC for the DA for WP2 and WP4;

g. PSA and FSA milestone at the end of Wave 1 and Wave 2;

[SOW-27]   The Contractor SHALL meet or exceed the dates mentioned in the above schedule. "Exceed" is understood as a situation where the Contractor has delivered earlier than the dates (i.e. EDC + 'x' months) mentioned in the above schedule, and the Purchaser has accepted the milestone accordingly.

[SOW-28]   The Contractor SHALL implement SOA & IdM Platform at the following sites and networks described below in Table 3:

Site	Purpose	Networks	
		ON	PBN
Datacentres			
Supreme Headquarters Allied Powers Europe (SHAPE), Mons, BE	Datacentre	Y	Y
Lago Patria, Joint Force Command (JFC) Naples, IT	Datacentre	Y	Y
New NATO Headquarter (NNHQ), Brussels, BE (September 2020)	Datacentre	Y	Y
Development, Testing & Verification			
NCIA (The Hague)	PMIC Lab, deployment needed for achieving IRC and RC milestone	N	Y
NCIA (Mons)	Reference Environment, deployment needed for achieving DA milestone	Y	Y
Special Purpose Networks			
JWC (hosted by Datacentre, separate network)	JWC Exercise 1	Y	N

JWC (hosted by Datacentre, separate network)	JWC Exercise 2	Y	N
JFTC (hosted by Datacentre, separate network)	JFTC Exercise	Y	N
JFTC (hosted by Datacentre, separate network)	JFTC Exercise	Y	N
SHAPE (hosted by Datacentre, separate network)	Mission Preparation 1	Y	N
SHAPE (hosted by Datacentre, separate network)	Mission Preparation 2	Y	N

Table 3: Deployment Locations and Networks

[SOW-29]   The Contractor SHALL propose the implementation sequence of the sites in Project Implementation Plan in order to match the Purchaser's milestones.

4.3. Effective Date of Contract (EDC)

4.3.1.   The EDC will be established at the time of Contract Award (CAW).

4.4. System Requirements Review (SRR)

[SOW-30]   The Contractor SHALL host and conduct a System Design Review (SDR), as defined in SECTION 7: System Engineering and Integration, and the associated documentation SHALL be approved by the Purchaser.

4.4.1.   The achievement of the successful SRR is subject to the Purchaser's approval.

4.5. System Design Review (SDR)

[SOW-31]   The Contractor SHALL host and conduct a System Design Review (SDR), as defined in SECTION 7: System Engineering and Integration, and the associated documentation SHALL be approved by the Purchaser.

4.5.1.   The achievement of the SDR milestone is subject to the Purchaser approval.

4.6. System Baseline (SBL)

[SOW-32]   The Contractor SHALL achieve SBL every time the Contractor updates the Software Version and conducts a Sprint Test of this new Software Version.

[SOW-33]   The Contractor SHALL perform necessary activities to satisfy criteria for meeting SBL as defined in SECTION 8.1 and SHALL submit the associated documentation for Purchaser approval.

4.6.1.   Baselines definitions are described in Figure 12: Configuration Baseline.

4.7. Internal Release Candidate (IRC) and Release Candidate (RC)

[SOW-34]   The Contractor SHALL achieve IRC and RC by successfully completing the Integration Test at Purchaser's Program Management and Integration Capability (PMIC) environment for the release.

[SOW-35]   The Contractor SHALL have performed necessary activities and satisfied the criteria for meeting IRC and RC milestone as defined in SECTION 8: Testing and Acceptance, and the associated documentation SHALL have been approved by the Purchaser.

[SOW-36]   Once IRC or RC is accepted and a Release is planned, the Contractor SHALL generate an updated Baseline as a result of IRC or RC, and SHALL install the updated SBL (System Baseline IRC/RCv.x) on the SOA & IdM Platform Reference System and integrate it within the appropriate IV&V Reference Environment.

[SOW-37]   The achievement of the IRC and RC is subject to the Purchaser's approval. In particular, the Contractor SHALL note that any implementation activities on the IV&V environment MUST NOT start until the RC milestone is approved by the Purchaser.

4.8. Deployment Authorisation (DA)

[SOW-38]   The Contractor SHALL have performed necessary activities and satisfied criteria for meeting DA as defined in SECTION 8: Testing and Acceptance and Request For Change (RFC) testing and the associated documentation SHALL have been approved by the Purchaser.

4.9. Provisional System Acceptance (PSA)

[SOW-39]   The Contractor SHALL demonstrate that for the applicable Wave:

a. all implementation activities have been executed at all the sites to be implemented under this contract, including; installation, testing and activation of all the SOA & IdM Platform components as described and defined in:

   i. SECTION 4: Milestones;

   ii. SECTION 6: System Implementation;

   iii. SECTION 7: System Engineering and Integration;

   iv. SECTION 8: Testing and Acceptance;

   v. SECTION 11: Quality Assurance and Control;

   vi. SECTION 14: Integrated Logistics Support (ILS).

b. all SOA & IdM Platform functionality specified in this SoW has been successfully implemented;

c. the Site Survey process has been completed as defined in SECTION 9: Site Surveys and the associated reports have been delivered for all the sites that form part of PSA scope (SECTIONs 8.2, 8.5 and 12.2.5).

d. all agreed test cases have been executed, and all tests have a status "PASS" (see SECTION 8.3.5).

e. *all documentation has been deliverd as described in this SOW and in accordance to the templates provided in ANNEX G where applicable.*

f. *the Configuration Management Database (CMDB) pertaining to this site has been delivered to the Purchaser.*

g. *applicable Operational Acceptance Criteria (OAC) are met (see 8.5);*

h. *centralised management and control of the SOA & IdM Platform has been fully implemented according to the requirements specified in this SoW.*

i. *all required personnel has been trained according to SECTION 14.7: Training.*

j. *the security requirements are satisfied in accordance to SECTION 10: Security.*

k. *all activities have been executed required to have all SOA & IdM Platform software components on the AFPL, in accordance to SECTION 8.*

l. *the OBL has been updated as described in 0 to reflect the actual PSA configuration (as built).*

[SOW-40] *The Contractor SHALL record any any discrepancies discovered in achieving PSA on observation sheet(s) with a statement on their required resolution.*

4.9.1.1. All discrepancies will be categorised by the Purchaser as either:

  a. requirements (required to be solved prior to PSA Wave Acceptance);
  b. deferments (to be resolved after PSA fixed timeframe);
  c. omissions.

4.9.1.2. Depending on the severity of the discrepancy discovered, the Purchaser may withheld the PSA until satisfactory resolution. However, some of the discrepancies may be deferred to the the FSA.

4.9.1.3. The achievement of PSA is subject to the Purchaser approval, in writing.

4.9.1.4. Upon successful PSA the system is handed over for operations.

4.10. Final System Acceptance (FSA)

4.10.1. FSA is the act by which the Purchaser has evaluated and determined that the implemented SOA & IdM Platform System meets the requirements of the Contract, and that the Contractor has fully delivered all requirements.

[SOW-41] *All PSA milestone requirements (see Sect. 4.9), Site Activation and Site Acceptance milestone requirements (see Sect. 6.6.5), as well as Security Accreditation (Sect. 10.1) SHALL be met by the Contractor for all the sites to be implemented under this contract.*

[SOW-42] *The Contractor SHALL demonstrate that:*

a. all the identified deficiencies are either fixed or waived by the Purchaser;

b. SOA & IdM Platform has been fully implemented across the entire NATO Enterprise and all requirements of this SoW are fully met.

[SOW-43]   The Contractor SHALL deliver all deliverables and conducted all activities, as specified in this Contract.

[SOW-44]   The Contractor SHALL close to the satisfaction of the Purchaser all outstanding issues, failures, and deficiencies.

4.10.2. The achievement of FSA is subject to the Purchaser approval, in writing.

SECTION 5: PROJECT MANAGEMENT

5.1. Introduction

5.1.1. This section outlines the Project Management requirements for this Contract.

5.1.2. The Contractor's Project Management activity is viewed as a critical factor in the successful execution of the SOA & IdM Platform project.

> [SOW-45] *The Contractor SHALL at all times ensure that:*
>
> a. *adequate resources are applied to all activities undertaken under this Contract;*
>
> b. *the timely achievement of milestones is identified and met;*
>
> c. *the project status information is comprehensively reported to the Purchaser in a timely manner;*
>
> d. *Configuration Management baselines are established and maintained throughout the project lifecycle;*
>
> e. *all risks (Purchaser's and Contractor's risks) to project's achievement are identified and managed;*
>
> f. *professional standards of project activities and deliverables through the application of Quality Assurance techniques are applied;*
>
> g. *due account is taken of Purchaser Furnished Information (PFI), including Process Management Directives.*

5.1.3. The success of the SOA & IdM Platform project depends upon a sound project management approach. Full and open communication between the Contractor and the Purchaser is an essential element of this approach.

5.1.4. To facilitate the efficient way of communication email is considered as an official communication channel, unless stated otherwise.

> [SOW-46] *The Contractor SHALL acknowledge email delivery and also answer to email communication received from NATO project team members (see SECTION 5.3) no later then the next business day.*

5.2. Methodology

> [SOW-47] *The Contractor SHOULD use a blended approach for Project Management as shown below in Figure 5.*

Figure 5: Blended approach for Project Management

[SOW-48]   *The Contractor SHOULD use PRINCE2 or an equivalent Project Management standard for the direction, governance and management activities for the entire project. If an equivalent Project Management standard is used, the Contractor SHALL prove that it at minimum meets all requirements stated in this section.*

[SOW-49]   *The Contractor SHOULD follow Agile approach as preferred by the Purchaser or propose any other IT industry approach (e.g. for testing procedures) and provide results to the Purchaser as required.*

5.2.1.   The Agile Process

5.2.1.1.   Agile development is a method for product creation based on iterative and incremental development. Although Agile is born as a software development methodology, it is related to Lean management and has been proven to have applicability for other types of activities, including manufacturing and testing.

5.2.1.2.   The original "Manifesto for Agile Development" specified four main tenets for Agile development:

5.2.1.3.   Individuals and interactions over processes and tools;

5.2.1.4.   Working software over comprehensive documentation;

5.2.1.5.   Customer collaboration over contract negotiation;

5.2.1.6.   Responding to change over following a plan.

5.2.1.7.   While there are different specific approaches to implementing Agile, they all share the same fundamental elements which will be used for the SOA & IdM Platform project:

5.2.1.8.   A time-boxed iterative delivery approach

5.2.1.9.   Adaptive, continual (re-)planning and (re-)prioritisation

5.2.1.10.   Deep involvement of customers and other stakeholders throughout the development process

5.2.1.11.   Evolutionary (incremental) development and delivery, with prototyping and frequent demonstration of product features

5.2.1.12.   A test-driven approach, with frequent and comprehensive testing activities using testing automation to the greatest possible extent

5.2.1.13.   Team collaboration, rich communication and transparency.

5.2.1.14.   Agile and the SOA & IdM Platform

5.2.1.14.1.   The delivery of the SOA & IdM Platform is a major project and will need to be managed as such. This brings the requirement, as stated elsewhere in this Statement of Work, for traditional project management elements such as work breakdown structures, financial management and linear planning timelines and milestones (e.g. Gantt charts).

5.2.1.14.2. However, blending the phased implementation approach of a large-scale fixed-price project at the "macro" level with the iterative approach of the Agile development and testing process at the short-term or "micro" level is not only possible, it is highly advantageous because of the benefits as noted above of short-term deliverables, continuous planning and prioritisation, and deep customer (Purchaser) involvement.

5.2.1.14.3. Therefore, regardless of what project management methodology (e.g. PRINCE2) the Contractor chooses to implement the SOA & IdM Platform, he is expected to implement an Agile approach specifically for the Product Creation and Testing Processes of certain Work Packages, following the method described in the next section.

5.2.1.15. Product Creation Process

5.2.1.15.1. The Agile process is executed via a series of short-term, time-boxed iterations, or "sprints", in which work is completed. Each sprint covers a small time period, typically no longer than four weeks (and potentially as short as 1-2 weeks).

5.2.1.15.2. Although the scope of the overall SOA & IdM Platform project will span multiple sprints, it is important to remember that each individual sprint is its own (mini) product development cycle, which results in concrete deliverables at the end of the iteration.

5.2.1.15.3. At the beginning of each sprint, a set of deliverables (the "backlog") is identified to be worked on, along with criteria for establishing whether or not each has been successfully done. At the end of each sprint, the work on each deliverable for that iteration is reviewed and accepted (or not) by the customer (Purchaser). The backlog is then re-evaluated and re-prioritised – a process involving both the development team and the customers – in order to identify and plan the work for the next sprint.

5.2.1.15.4. Plan the Agile approach:

5.2.1.15.4.1 create a Work Breakdown Structure (WBS) from the broader project plan and its Work Packages, and ensure that all requirements are covered;

5.2.1.15.4.2 define the time-box for each sprint; four (4) weeks is recommended.

5.2.1.15.5. Execute the Agile approach:

    a.   Create/update a set of "user stories", each of which is a high-level definition of a requirement, containing just enough information so that the developers can produce a reasonable estimate of the effort to implement it

    b.   Create/update the "backlog" of user stories, which together represent the products (or "features") necessary to implement the system and which address all aspects of the WBS:

        i.   Each user story should be testable, with a clearly stated test plan and expected results

        ii.   Each user story has a clear definition of "done", i.e. what acceptance criteria must be met to consider the user story completed

    iii.   Each user story should generally be discrete enough to be able to complete it during the course of one sprint

    iv.   Each user story is broken down into tasks which comprise the total feature

c.   Prioritise the user stories in the backlog, in coordination with the Purchaser's "Product Owner", who is the focal point for the project

d.   Estimate the effort involved in developing and testing each user story (or at least the most highly prioritised ones), and identify which will be achieved in the next sprint

e.   During the course of the sprint, develop and test the products identified for that sprint

f.   During the course of the sprint, meet frequently (preferably a daily "stand up") with both the development team and the Product Owner to discuss progress and issues

g.   At the end of the sprint, demonstrate the completed product(s) for the Purchaser – along with the successfully executed test cases –at which time the Purchaser accepts (or not) the products developed during the sprint; these are then considered done

h.   At the end of the sprint, conduct a full set of tests on the system developed to date, including:

    i.   Unit and Component Test(s)

    ii.   Component Integration Test(s)

    iii.   System Test

    iv.   Update the planning for the next sprint based on lessons learned from the just-completed sprint (for example, estimates of effort for backlog tasks)

i.   Update the broader (PRINCE2-based) project plan as necessary, including timelines, risk logs and issue logs

j.   Repeat steps (a) to (j) until the project is complete.

5.2.1.15.6.   This process is geared toward software development, so it is expected to be used during the development of the Services identified in the System Requirements Specification (SRS), as planned for Work Packages 2.1, 2.2, 4.1 and 4.2 (see SECTION 6.8). It may also be applicable for Work Packages 5.1 and 5.2 (Pilot Integration Cases - see SECTION 6.8.1.4); this will be determined by the Purchaser when required.

5.2.1.15.7.   Testing also lends itself naturally to an Agile approach, so it is expected that the Contractor will implement this process for major testing activities – such as the System Integration Test (SIT) and the Site Acceptance Test (SAT) – as well (tailored as needed).

> [SOW-50]   *The Contractor SHOULD implement the Agile approach as described in this section for:*
>
>   a.   *the Product Creation process in Work Packages 2.1, 2.2, 4.1 and 4.2.*
>
>   b.   *the major testing activities, to include the System Integration Test and SAT.*

[SOW-51]   The Contractor SHALL define and describe its implementation of the required blended Project Management approach so that at minimum it shows a clear and consistent exchange of information between the Project team and minimal duplication of information and project management activities. For example:

   a. Project Master Schedule (Gantt chart) SHALL be used for higher level project planning (including all milestones for all Work Packages) tracking and SHALL be regularly fed by information from Product Delivery Reviews;

   b. Project Status Report (PSR) SHALL include inputs about delivery progress, issues and risks taken from Product Delivery Reviews and meeting.

[SOW-52]   Although the Agile approach offers certain flexibility for the product delivery (e.g. prioritisation of features) within a a Work Package it MUST NOT by default tolerate deviations in the defined time, scope and cost within each authorised and initiated Work Package. If such deviations are forecasted, they SHALL be reviewed and approved according to the Configuration Management (CM) process (see SECTION 11: Quality Assurance and Control).

IFB_CO-14176-SOA-IDM
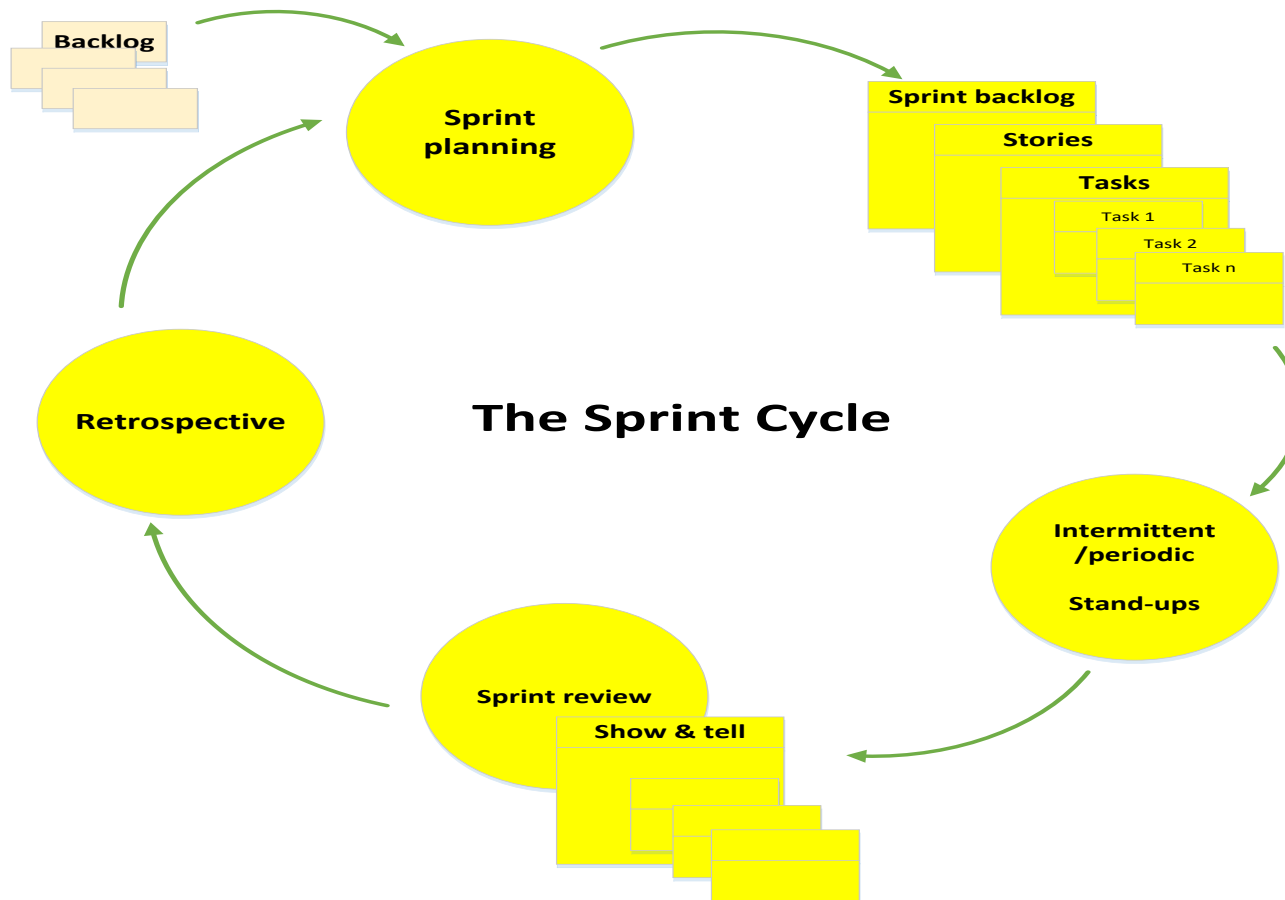
Figure 6: Agile Sprint Cycle

5.3. Project Management Organisation

5.3.1. Overall Project Organisation

[SOW-53] *The Contractor SHALL at minimum implement and conform to the Overall Project Organisation as structured in Figure 7: Project .*
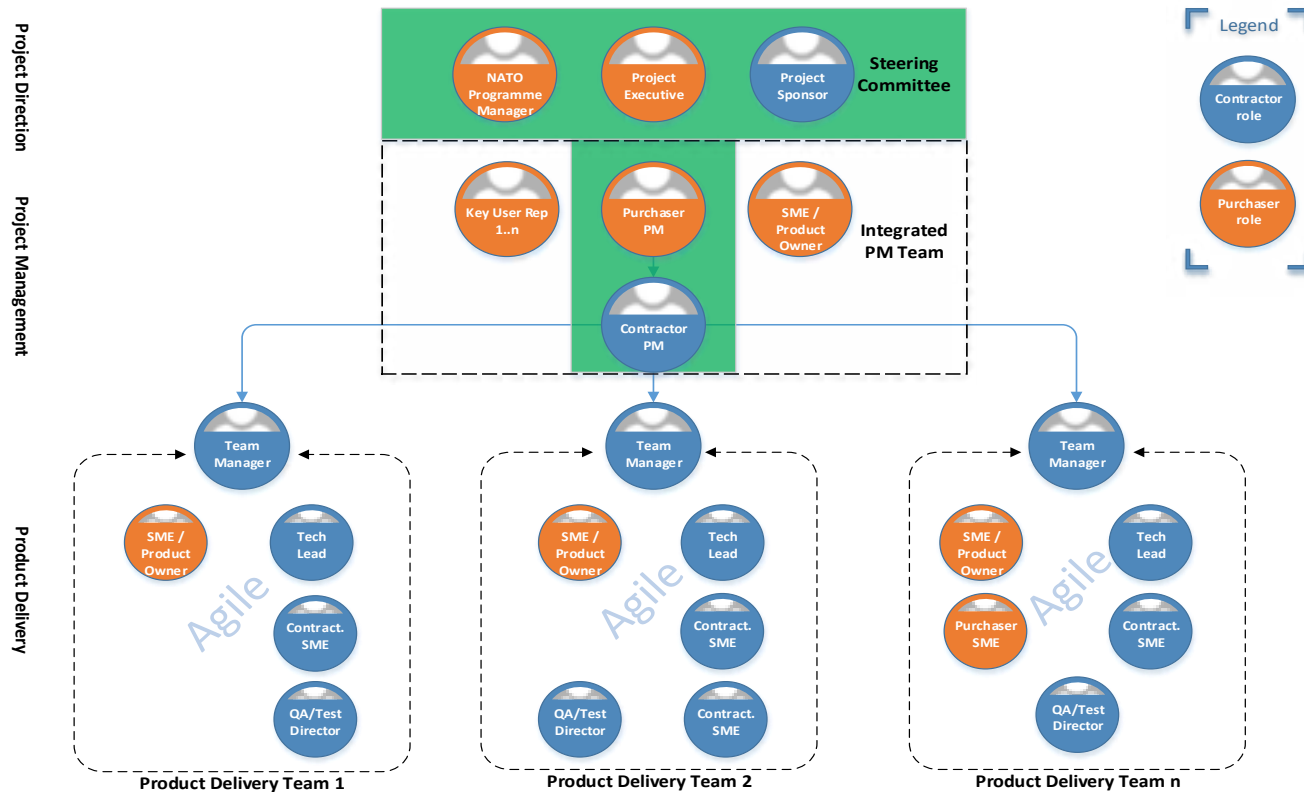
Figure 7: Project Organisation

5.3.1.1. The Steering Committee is accountable for the project success and has the authority to direct the project by making key decisions and exercising overall control. The Steering Committee manages by exception via reports provided by Project Managers.

5.3.1.2. Integrated Project Management Team is in charge for the day-to-day management of the project and its responsibilities are described in SECTION 5.3.2.

5.3.1.3. Product Delivery Teams are in charge for the development of required products. The number of needed Product Delivery Teams in each project phase as well as the number of resources in each Product Delivery Team will be agreed upon between the Contractor's and Purchasers' Project Managers.

> [SOW-54] *The Contractor SHALL establish Product Delivery Teams which at least consist of the following roles: Team Manager, Technical Leader, Product Owner (Purchaser provided) and Test Director/QA Manager. One person can be a member of more than 1 Product Delivery Teams.*
>
> [SOW-55] *The Contractor's Project Manager (CPM) SHALL frequently (at least once a week) liaise with Team Manager(s) to receive inputs from the Product Delivery and with the Purchaser Project Manager to provide inputs for overall Project Management and Direction, all of which SHALL be defined in the Project Communication plan (part of the Project Management Plan).*

5.3.2. Purchaser Project Organisation and Responsibilities

5.3.2.1. The Purchaser's Project Manager (PPM) will act as the Purchaser's representative and will be the primary interface between the Contractor and Purchaser after the EDC.

5.3.2.2. The Purchaser's Project Manager will be supported by Subject Matter Experts (SME) in certain areas who may, from time to time, be delegated to act on the Purchaser's Project Manager's behalf in their area of expertise.

5.3.2.3. The Purchaser's Project Manager, the specialists, other team members, or any other NATO personnel are not allowed to make changes to the Terms and Conditions (T&C) of the Contract. They may only provide the Purchaser's interpretation of technical matters.

5.3.2.4. All changes to the Contract will be made through the Purchaser's Contracting Office only.

5.3.2.5. The Purchaser's and Contractor's Project Managers, the specialists, and the key Stakeholders' representatives collectively form the SOA & IdM Platform's Integrated Project Management Team (IPMT).

5.3.2.6. The Purchaser's Project Manager chairs the SOA & IdM Platform's IPMT meetings. The other voting members are the designated representatives of the stakeholders (Key User representatives). All other members serve as advisory members.

5.3.2.7.   The IPMT serves as the primary mechanism for monitoring project status, resolving issues or conflicts within the project and advising the Purchaser Project Manager.

5.3.2.8.   The IPMT also serves as the Purchaser's Change Control Board (CCB), to which the following items may be submitted for baselining decision as required by the Purchaser:

a. Project Management Plan:
   a. The Purchaser's Project Manager can, at his/her own discretion and without consulting the other SOA & IdM Platform CCB members, approve changes to the PMS that do not affect other baselined documents, and/or do not incur additional costs, and/or do not bring the project beyond time tolerance available to him/her
b. Project Master Schedule (see 5.4.4), for the first version and for all changes beyond tolerance available to the Purchaser Project Manager ;
c. Project Implementation Plan (PIP) (see SECTION 6.4); and Annex G.3.1
d. Integrated Logistics Support Plan (ILS; see SECTION 14.2);
e. Functional Baseline (FBL; see SECTION 12.2.2);
f. Allocated Baseline (ABL; see SECTION 12.2.3);
g. Product Baseline (PBL; see SECTION 12.2.4);
h. Operational Baseline (OBL; see SECTION 12.2.5)
i. Configuration Management Plan (see 12.3);
j. Quality Assurance Plan(SAP; see 11.6).

[SOW-56]   The Purchaser is the official Product Owner (PO); however, the Contractor SHALL also ensure its SMEs are available to temporarily engage in the role of PO as needed. The Contractor's representative engaged in the role of PO will represent the Purchaser's interests within Product Delivery Teams and will work to enable:

a. detailed product requirements are well-defined, understood and prioritised for development;

b. Product Deliverables are reviewed, fitting the purpose and have been tested by the Contractor according to the agreed upon Test Plan;

c. communication, collaboration and feedback from other Purchaser representatives such as end user representatives and other subject matter experts.

5.3.3.   Contractor Organisation and Responsibilities

[SOW-57]   The Contractor SHALL identify all major Contractor's Organisational Units (OU) and any Sub-Contractors involved in the implementation of the SOA & IdM Platform and SHALL provide a description of the portion of the overall effort or list deliverable items for which they are responsible.

[SOW-58]   The Contractor SHALL establish and maintain a Project Management Office (PMO) in Mons, Belgium area, to perform and

manage all efforts necessary to discharge all his responsibilities under this Contract.

[SOW-59]   *The Contractor SHALL ensure the continuity of personnel assigned to work on this project.*

[SOW-60]   *The Contractor's staff SHALL be identified as a key personnel, as listed in SECTION 13: Labour Categories*

[SOW-61]   *The Contractor SHALL also provide all necessary manpower and resources to conduct and support the management and administration of operations in order to meet the objectives of the project, including taking all reasonable steps to ensure continuity of personnel assigned to work on this project.*

5.3.3.1.   The following members of the Contractor Project Management Office are Key Personnel for this project:

[SOW-62]   *All Contractors' Key Personnel SHALL be available throughout the performace of the Contract until the project's completion.*

[SOW-63]   *The Contractor SHALL designate a Contractor's Project Manager (CPM), who will direct and co-ordinate the activities of the Contractor's project team.*

[SOW-64]   *The Contractor's Project Manager SHALL be the Contractor's primary contact for the Purchaser's Project Manager and SHALL conduct all major project design, test and review meetings. See SECTION 13 for Labour Categories requirements.*

[SOW-65]   *The Contractor SHALL designate a Senior Test Engineer to serve as a Test Director for all test activities conducted under this Contract. See SECTION 13 for Labour Categories requirements.*

[SOW-66]   *The Contractor SHALL designate an Engineer to serve as a Quality Assurance Manager throughout the performance of the Contract.*

[SOW-67]   *The Contractor's Quality Assurance (QA) Manager SHALL report to a separate manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.*

[SOW-68]   *ILS, Change and Configuration Manager: The Contractor SHALL designate a Senior Engineer to serve as an ILS Manager throughout the performance of the Contract, including the O&M Phase (see SECTION 14: Integrated Logistics Support).*

[SOW-69]   *The Contractor's team SHALL be available during Central European Time (CET) zone in business working hours: 8:30 - 17:30 Monday-Friday..*

5.4. Project Management Documentation

[SOW-70]   *The Contractor SHALL deliver all Project Mananagement documentations as described in ANNEX G.*

5.4.1.   For the purpose of this Contract, Deliverables are split into two categories:

a.   Management products are all Contract Deliverables covered under the Project Management activities as described in this section.

b. Specialist products are all other Deliverables in this Contract.

5.4.2. Project Management Plan (PMP)

[SOW-71] *The Contractor SHALL establish and maintain a PMP which describes how the Contractor will implement the totality of the Project as specified in this SoW.*

[SOW-72] *The Contractor's PMP SHALL cover all aspects of the project implementation including its management structure and project management processes, personnel roles and responsibilities, external dependencies necessary to provide the capability as required by this Contract.*

[SOW-73] *The Contractor's PMP SHALL be sufficiently detailed to ensure that the Purchaser is able to assess the Contractor's plans with insight into the Contractor's plans, capabilities and ability to satisfactorily implement the entire Project in conformance with the requirements as specified in this SoW.*

[SOW-74] *The Contractor SHALL propose PMP according to Annex G.2.1: Project Management Plan (PMP).*

[SOW-75] *The Contractor SHALL ensure that the PMP comprises at minimum of the following sections, as described in Annex G.2.1: Project Management Plan (PMP):*

a. *an "Organisation" section describing the Contractor's organisation for this project according to the requirements in this SECTION 5. This section SHALL include:*

i. *an organisational chart showing the members of the Contractor's Project Team (including the members of the Contractor PMO);*

ii. *showing their respective responsibilities and authority;*

iii. *proposed Project Communication Plan;*

b. *a "Project Planning" section describing the Contractor's processes supporting the development and maintenance of the Product Breakdown Structure (PBS), Product Flow Diagram (PFD) and Project Master Schedule (PMS) according to the requirements of:*

i. *SECTION 5: Project Management; and*

ii. *SECTION 11: Quality Assurance and Control;*

c. *a "Risk management" section describing the Contractor's processes supporting Risk Management by the Contractor, according to the requirements of SECTION 5: Project Management;*

d. *a "System Engineering" section describing the Contractor approach to these activities according to the requirements in SECTION 7: System Engineering and Integration;*

e. *a ": System Implementation" section describing the Contractor approach to these activities according to the requirements in SECTION 6: System Implementation;*

f. an "Operation and Maintenance" section describing the Contractor approach to these activities according to the requirements in SECTION 14.3 Maintenance and Support concept;

g. a "Testing" section describing the Contractor approach to these activities according to the requirements in SECTION 8: Testing and Acceptance.

[SOW-76]   The Contractor's SOA & IdM Platform SDS (System Design Specification) SHALL be developed as per the detailed contents indicated in Annex G.2.1.

[SOW-77]   The Contractor's PMP SHALL align with the SoW, but it MUST NOT be a simple 'cut & paste' from the relevant SoW sections. It SHALL demonstrate that the Contractor understands the work to be performed, applying industry best practices.

[SOW-78]   The Contractor's PMP SHALL be provided to the Purchaser for acceptance.

5.4.2.1.   The acceptance of the Contractor's PMP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

[SOW-79]   Acceptance of any deliverable provided by the Contractor to the Purchaser MUST NOT imply any waiver or any uni-sided interpretation of the original requirements as stated in the Contract. It remains the sole responsibility of the Contractor to unabridged fulfil all Contractual requirements and provide evidence of this to the Purchaser.

5.4.3.   Product Breakdown Structure (PBS) and Product Flow Diagram (PFD)

[SOW-80]   The Contractor SHALL establish and maintain a PBS and a PFD.

[SOW-81]   The Contractor's PBS SHALL identify the start and finish dates, duration, predecessors, successors and resource requirements for each task.

[SOW-82]   The Contractor's PBS SHALL decompose all SOA & IdM Platform tasks to a level that exposes all project's risk factors and allows accurate estimation of each task's duration, resource requirements, inputs and outputs, and predecessors and successors.

[SOW-83]   The Contractor's PBS SHALL identify all products and it SHALL distinguish between management products and specialist products.

[SOW-84]   The Contractor's PBS SHALL include a hierarchical diagram of all the products (management products and specialist products), having at its topmost product the final product of the overall project, i.e. the SOA & IdM Platform System.

[SOW-85]   The Contractor's PBS SHALL describe each product (management products and specialist products) including its quality requirements. The product descriptions SHALL address sufficient detail to permit management assessment of progress.

[SOW-86]   *The Contractor's PFD SHALL sequence all products in their logical order of creation.*

[SOW-87]   *The Contractor's initial version of the PBS and PFD SHALL be provided to the Purchaser for acceptance.*

5.4.3.1.   The acceptance of the PBS and of the PFD by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

5.4.4.   Project Master Schedule (PMS)

[SOW-88]   *The Contractor's PMS SHALL correlate with the products defined in the PBS and sequentially ordered in the PFD.*

[SOW-89]   *The Contractor's PMS SHALL:*

   a.   *be provided in Microsoft Project format;*

   b.   *identify the critical path for the overall project;*

   c.   *identify the start and finish dates, duration, predecessors, constraints (as necessary) and the total slack of each task;*

   d.   *identify key resources needed for each task completion;*

   e.   *identify the main project milestones (see SECTION 4: Milestones) and intermediate milestones as required;*

   f.   *identify the "physical" progress for each task;*

   g.   *identify the applicable baseline and SHALL show progress against the baseline;*

   h.   *minimise the use of constraints and absolute dates;*

   i.   *provide network, milestone, Gantt and Tracking Gantt views;*

   j.   *identify the main deliverables.*

[SOW-90]   *The Contractor's PMS SHALL be provided to the Purchaser for acceptance.*

[SOW-91]   *The Contractor's PBS, the PFD and the PMS SHALL be used as the primary framework for Contract planning and reporting to the Purchaser.*

5.4.5.   Agile Product Backlog

[SOW-92]   *The Contractor SHALL create and maintain a Product Backlog (PB) derived from the main PBS.*

[SOW-93]   *The Contractor's PB SHALL contain a prioritised list of all required product features and SHOULD be used for planning and progress tracking of development activities within each time-boxed project effort.*

[SOW-94]   *The Contractor's PB SHOULD also be used for the planning of iterative deployment of product features (releases) into test and production environments.*

5.4.6.   Risk Management Plan (RMP)

[SOW-95]   *The Contractor SHALL establish and maintain an RMP according to Annex G.2.2 Risk Management Plan (RMP), which*

SHALL describe how the Contractor will implement the Risk Management process.

[SOW-96]   *The Contractor's RMP SHALL at least describe:*

    a. *overall Risk Management approach;*

    b. *Key Risk Management processes;*

    c. *Key Risk Categories;*

    d. *Risk Prioritisation Matrix;*

    e. *Risk Management roles and responsibilities;*

    f. *Risk Log.*

5.4.7.   Risk ManagementRisk Management

[SOW-97]   *The Contractor SHALL establish and maintain a Risk Management process for the project, and described it in the Risk Management Plan according to Annex G.2.2.*

[SOW-98]   *The Contractor's Risk Management process SHALL at minimum enable and define identification of all types of risks, evaluation and prioritisation of each risk, definition of proposed response strategy, owner and actions and suggested monitor and control mechanisms.*

[SOW-99]   *The Contractor SHALL rate risk based on its probability of occurrence and impact.*

[SOW-100]   *The Contractor SHALL propose an appropriate response for each risk.*

[SOW-101]   *If the Contractor and the Purchaser agree that the response to a risk is other than to accept it, the Contractor SHALL plan risk response tasks (having: start, finish, work required, resources to be used, result expected).*

[SOW-102]   *The Contractor SHALL include in the Project Status Report (PSR) a chart that lists all active risks rated high on any factor and note any significant forecasted changes in these risks.*

5.4.7.1.   Risk Log (Register)

[SOW-103]   *The Contractor SHALL document, update and maintain status of all risks in the Risk Log where he SHALL record and track all project risks regardless of their status at every Project Review Meeting (PRM) and Design Review Meeting.*

[SOW-104]   *The Contractor SHALL provide the Risk Log listing the risks, and indicating for each one the following information (but not limited to):*

    a. *Risk identifier: unique code to allow grouping of all information on this risk;*

    b. *Description: brief description of the risk;*

    c. *Risk category (e.g. management, technical, schedule, quality and cost risks);*

    d. *Impact: effect on the project if this risk were to occur;*

 e. *Probability: estimate of the likelihood of the risk occurring;*

 f. *Risk rating (High, Medium, Low);*

 g. *Proximity: how close in time is the risk likely to occur;*

 h. *Response strategy: avoidance, mitigation, acceptance, transference*

 i. *Response plan(s): what actions have been taken/will be taken to counter this risk;*

 j. *Owner: who has been appointed to keep an eye on this risk;*

 k. *Author: who submitted the risk;*

 l. *Date identified: when was the risk first identified;*

 m. *Date of last update: when was the status of this risk last checked;*

 n. *Status: e.g. closed, reducing, increasing, no change.*

[SOW-105] *The Contractor SHALL update Risk Log at minimum on a monthly basis as an input for the PSR (see SECTION 5.5.1) and provide to the Purchaser in an agreed format (e.g. Microsoft Excel).*

[SOW-106] *The Contractor SHALL add to the Risk Log additional risks identified by the Purchaser.*

[SOW-107] *The Contractor SHALL deliver the Risk Log to the Purchaser, throughout the duration of the Contract, and keep it up to date on the project portal.*

5.4.7.2.   Issue management

5.4.7.3.   A Project Issue is anything that affects the Project, either detrimental or beneficial (e.g. problem, error, anomaly, risk occurring, query, change in the project environment, change request, off-specification). An issue is defined as, in accordance with PRINCE2 2009 ed.: "*a relevant event that has happened, that was not planned, and requires management action. It can be any concern, query, request for change, suggestion or off-specification raised during a project. Project issues can be about anything to do with the project*".

[SOW-108] *The Contractor SHALL establish and maintain a process for identifying, tracking, reviewing, reporting and resolving all project issues.*

[SOW-109] *The Contractor SHALL describe the Issue Management Process in the Configuration Management Plan (see SECTION 12.3).*

5.4.7.4.   Issue Log (Register)

[SOW-110] *The Contractor SHALL develop and maintain an Issue Log where it SHALL record and track all project issues regardless of their status.*

[SOW-111] *The Contractor SHALL ensure that the Issue Log comprises the following information (but not limited to):*

 a. *Project Issue Number;*

    b. *Project Issue Type (Request for change, Off-specification, general issue such as a question or a statement of concern);*

    c. *Author;*

    d. *Date identified;*

    e. *Date of last update;*

    f. *Description;*

    g. *Action item/Decision;*

    h. *Responsible person (individual in charge of the action item);*

    i. *Suspense date (Suspense date for the action item);*

    j. *Priority;*

    k. *Status.*

[SOW-112] *The Contractor SHALL include the Issue Log in the configuration management process and keep it under configuration control and in the CMDB.*

[SOW-113] *The Contractor SHALL update Issue Log at minimum on a monthly basis as an input for the PSR (see section 5.5.1).*

[SOW-114] *The Contractor SHALL add to the Issue Log additional issues identified by the Purchaser.*

[SOW-115] *The Contractor SHALL deliver the Issue Log to the Purchaser, throughout the duration of the Contract, and keep it up to date on the project portal.*

5.4.7.4.1.   Issue Management Plan (IMP)

5.4.7.4.2.   The IMP is derived from the definition of the Issue and change control procedure under the Configuration Management Strategy as defined in the PRINCE2 ed. 2009.

    [SOW-116] *The Contractor's Issue Management Plan SHALL at least contain items described in Annex G.2.5.*

5.4.7.4.3.   The Contractor is free to propose the format of the Issue Management Plan providing that all requirements for content and the provisions are met.

5.4.8.   Decision Log

    [SOW-117] *All decisions taken during the project implementation lifecycle SHALL be tracked by the Contractor per project phase, together with evidence of options analysis when apply.*

    [SOW-118] *First decisions SHALL be already available at CaW stage covering the Contractor's:*

        a. *design decisions,*

        b. *development decisions,*

        c. *tools and environment covered by the proposal;*

        d. *any possible proposed change before starting the project implementation.*

[SOW-119]   The Contractor's workflow SHALL allow for NCI Agency PM agreement with the decisions when proposed decisions are based on NCI Agency SME and stakeholders inputs.

[SOW-120]   The Contractor's log SHALL also record design rationale, i.e. information capturing the reasoning of the designer that led to the system as designed; including design options, trade-offs considered, decision made and the justification of those decisions.

[SOW-121]   The Contractor's log SHALL also record "architectural and implementation rationale", i.e. information capturing the reasoning of the developer that led to the system as build, including implementation options, trade-offs considered, decision made and the justification of those decisions.

[SOW-122]   A decision CANNOT and SHALL NOT overrule or modify:

    a. the Contract;

    b. the Statement of Work;

    c. the Product Scope as specified in the Contract;

    d. any part of an already accepted or baselined Workproduct.

[SOW-123]   Any decision in a meeting to change any of the above artefacts SHALL be formalised by a Project Change through the Project Change Process.

[SOW-124]   The Contractor SHALL ensure that requirements traceability to requirements changes, user histories, use cases, low level design - down to the application level (classes, packages and application) -, verification methods, test cases, test phases and test results are recorded and ready to be reported in the form of bi-directional requirements traceability matrixes and requirements verification matrix.

[SOW-125]   A requirements baseline SHALL be created after each product release.

[SOW-126]   The requirements baseline SHALL be provided to the purchaser as an export in DOORS format, for both of the SRS and the SoW.

[SOW-127]   The Contractor SHALL keep the purchasers requirements ID for traceabiliy.

5.4.9.   Configuration management (CM)

[SOW-128]   The Contractor SHALL implement a CM process as referred to in NATO STANAG 4427, 2014 and [NATO ACMP-2000, 2017],[NATO ACMP 2009, 2017],[NATO ACMP-2100, 2017]to carry out the Configuration Management functions as described in this SoW (Configuration Item identification, configuration control, configuration status accounting, and configuration verification) and to perform Quality Assurance and Control.

5.5. Project Management Communications

5.5.1.   Project Status Report (PSR)

[SOW-129] *The Contractor SHALL provide, no later than the third working day of each month, a PSR.*

[SOW-130] *The Contractor's PSR SHALL at minimum summarise completed, ongoing, and upcoming activities, as well as attached updated PMS, and the status of any dependencies which affects or may affect the project.*

[SOW-131] *The Contractor SHALL ensure that the PSR summarises activities, including (but not limited to):*

    a. *Changes in key Contractor personnel;*

    b. *Summary of Contract activities during the preceding month, including the status of current and pending activities;*

    c. *Progress of work and schedule status, highlighting any changes since the preceding report;*

    d. *CSA report addressing all products in the Project Breakdown Structure;*

    e. *Issue Log;*

    f. *Change Requests status;*

    g. *Off-Specifications status;*

    h. *Risk Log;*

    i. *Test(s) conducted and results;*

    j. *Summary of any site surveys conducted;*

    k. *Plans for activities during the following reporting period;*

    l. *Provisional financial status and predicted expenditures.*

5.5.1.1.   The Purchaser will issue comments to The Contractor's PSR (being a monthly document) no later than 2 (two) weeks after receipt of the document.

[SOW-132] *The Contractor SHALL issue answers to those comments within 1 week after their receipt. No comment received within that timeframe means that the Contractor agrees to the comments issued by the Purchaser.*

5.5.2. Meetings

5.5.2.1.   General

5.5.2.2.   Except otherwise stated in the Contract, the following provisions SHALL apply to all meetings (including "attendance in person" meetings, video or tele conference meetings, reviews…) to be held under the Contract.

[SOW-133] *The Contractor SHALL schedule project meetings in the PIP.*

[SOW-134] *The Contractor SHALL produce a draft agenda for the Purchaser's approval at least one week before the meeting.*

[SOW-135] *The Contractor SHALL take meeting minutes, submit them in draft version to the Purchaser for approval within 2 (two) working*

days of the meeting. The minutes SHALL be submitted to an accelerated review cycle at Purchaser's discretion.

[SOW-136] The participants and mainly the Contractor's representatives SHALL NOT regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract nor as a vehicle to alter the design or configuration of equipment or systems. Any such changes SHALL only be made by authorised mechanisms as set forth in the Contract.

[SOW-137] All relevant documentation (even in draft format) SHALL be provided by the Contractor to the Purchaser no later than 2 (two) working days before the meeting.

5.5.2.3. Formal meetings

[SOW-138] The Contractor's PM or his designated representative SHALL participate in all formal project meetings (kick-off meeting, PRMs and Design Review meetings).

[SOW-139] The Contractor SHALL participate in a project kick-off meeting that shall be held at the Purchaser's facility.

[SOW-140] The following provisions SHALL apply to Contractor, to all formal meetings to be held under the contract:

a. the Contractor SHALL take meeting notes (capturing main points, decisions and action items) and submit them in draft version to the Purchaser for approval within three (3) working days after the meeting;

b. the final version of the meeting notes SHALL be posted by the Contractor on the Project Website (see SECTION 5.5.3 below) within 3 (three) working days of receipt of Purchaser approval;

c. the participants shall not regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract or as a vehicle to alter the design or configuration of equipment or systems. Any such changes shall only be made by agreement, amendment or by authorised mechanisms as set forth in the Contract;

d. any documentation, even in draft format, that may be useful to the Purchaser in preparing for Design Review Meetings or PRMs and ensuring efficient discussions during the meetings shall be provided to the Purchaser no later than 10 (ten) working days before the meeting.

5.5.2.4. Project Review Meetings

[SOW-141] The Contractor SHALL coordinate and hold PRMs with the Purchaser at least once a month throughout the Contract period of performance.

[SOW-142] The Contractor SHALL provide updated PSR not older than 5 (five) working days as a base document for the PRM as sent to all PRM participants at least 2 (two) business days in advance.

[SOW-143] At each PRM, the Contractor SHALL provide the status of all on-going tasks, the status of the Contract deliverables, identify any changes to the PMP, PMS, PIP, Integtated Logistics Support Plan

(ILSP), Quality Assurance Plan (QAP), Issue Log, Change Requests document, Off-specifications document, baselines and Risk Log, and identify any problems.

[SOW-144]   The Contractor SHALL address and discuss key project issues, risks and events with the Purchaser Project Manager promptly, and SHALL not postpone it until PRMs.

[SOW-145]   The location of PRMs will vary and, when possible, and SHALL be scheduled by the Contractor in coordination with the Purchaser with other project meetings. Attendance in person is preferred but via video or telephone conference is acceptable when it can be arranged.

5.5.2.5.   Product Delivery Meetings

[SOW-146]   The Contractor SHALL organize Product Delivery Meetings (PDM) in accordance with the chosen Agile framework.

[SOW-147]   Contractor's PDMs SHALL at minimum cover the following activities:

    a. Product Delivery Planning meeting with frequency of minimum 1 (one) per month;

    b. Product Delivery Review meeting with frequency of minimum 1 (one) per month;

    c. Product Delivery Progress Meeting with frequency of minimum every 2 (two) working days.

[SOW-148]   All Product Delivery Meetings SHALL be organized and run by the CPM, Team Manager or Tech Lead appointed by the Contractor.

5.5.2.6.   Purchaser representative (Product Owner and/or Project Manager) will attend Product Delivery Planning and Review meetings and per need also Product Delivery Progress Meetings.

[SOW-149]   The Contractor SHALL record all outputs from all Product Delivery Meetings in a product delivery toolset chosen, implemented and hosted by the Contractor.

[SOW-150]   The Contractor SHALL ensure Purchasers access to the abovementioned product delivery toolset.

[SOW-151]   The Contractor SHALL report key outputs from PDMs such as delivery progress information (e.g. product backlog status, key test results, burndown / burnup charts) as well as key changes, issues and risks to the Contractor Project Manager who SHALL integrate that information in the PSR.

5.5.2.7.   Informal meetings

[SOW-152]   The Contractor SHALL carry out ad-hoc project-level communication activities as needed to clarify project issues.

[SOW-153]   The Purchaser and Contractor PM SHALL hold fortnightly contact from the Kick off meeting through the remaining contractual period. When unforeseen meetings are required the Contractor

SHALL provide attendance within 3 (three) working days of the Purchaser request.

5.5.2.7.1. The parties will agree on a day (e.g. specific days of the week) and time for the regular conference calls.

[SOW-154] *The Purchaser and Contractor SHALL exchange contact telephone numbers and agree on conference call requirements (day and time) during the project kick-off meeting. The Contractor SHALL provide responses to Purchaser Emails on any subject within 1 (one) working day.*

[SOW-155] *Action Items from the conference calls SHALL be drafted by the Contractor and added to the SOA & IdM Platform Action Item List by the Contractor within 2 (two) days of the conference call.*

5.5.2.8. Integrated Project Management Team (IPMT) Meetings

5.5.2.9. Upon award of this Contract, the Contractor's Project Manager shall become an advisory member of the SOA & IdM Platform IPMT.

[SOW-156] *The Contractor's Project Manager SHALL provide inputs to and attend IPMT meetings as requested by the Purchaser Project Manager.*

5.5.2.9.1. All IPMT meetings of the SOA & IdM Platform will take place at the Purchaser premises (Brussels or Mons (Belgium) and/or The Hague – Netherlands).

5.5.2.10. Other Meetings

5.5.2.10.1. The Purchaser will host all other meetings agreed by both parties unless there is a specifically agreed need to review material, witness technical demonstrations, or perform any other activity outside of the Purchaser's premises as part of the meeting.

5.5.3. Project Website

[SOW-157] *The Contractor SHALL use the project website provided by the Purchaser to maintain all NATO UNCLASSIFIED (NU) documents.*

5.5.3.1. The Purchaser will provide the necessary access rights to the Contractor.

[SOW-158] *The Contractor SHALL maintain on this website all unclassified documents, as soon as they are submitted in draft version to the Purchaser. This includes all project deliverables, presentation materials from all meetings, as well as the Contract SoW and SRS, and all applicable documents. More generally, the website SHALL include any document as deemed necessary by the Purchaser.*

[SOW-159] *The Project Website SHALL identify all relevant classified documents by title, unless a title itself is classified and SHALL state from where the classified document can be obtained.*

5.5.3.2. The Purchaser may be able to provide the Contractor with a capability (named "REACH") to exchange NATO RESTRICTED information over the Internet with the Purchaser. If the Purchaser is not in position to

provide such a capability, other means shall be defined on a case by case basis.

5.5.4. Documentation Delivery and Review

[SOW-160]   *The Contractor SHALL submit all documentation in electronic format to the Purchaser for review and comments as applicable.*

[SOW-161]   *The Contractor SHALL not provide any Contractual documentation in a partial or gradual manner.*

[SOW-162]   *The Contractor SHALL ensure that any documentation delivered to the Purchaser has been properly reviewed according to Contractor's quality management process.*

5.5.4.1.   Except otherwise stated for specific documents, the following provisions shall apply for any documentation to be provided by the Contractor under this Contract.

[SOW-163]   *The Contractor SHALL provide a first version of each deliverable for Purchaser review.*

5.5.4.2.   The Purchaser will provide questions, comments, corrections, and suggested changes to the Contractor within 4 (four) weeks of receipt. The Purchaser reserves the right to return without review a document that has significant deficiencies (e.g. a document only including a table of contents).

[SOW-164]   *The Contractor SHALL not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.*

[SOW-165]   *The Contractor SHALL resubmit the document as a revised version (version 0.2) incorporating the Purchaser's comments within 2 (two) weeks after receipt.*

5.5.4.3.   The Purchaser will provide comments, corrections, and suggested changes to the Contractor within 3 (three) weeks of receipt.

[SOW-166]   *The Contractor SHALL provide an updated version of the document within two weeks of receipt of the Purchaser's comments on the revised version.*

[SOW-167]   *The above cycle SHALL continue until the document reach a quality level acceptable by the Purchaser.*

[SOW-168]   *If the document is included as part of the FBL, ABL or PBL, the Contractor SHALL remain responsible for updating the document as required in the course of the project (to correct errors, inconsistencies, omissions, etc. and to reflect changes in the system design, system implementation, support arrangements) as part of its Configuration Management tasks.*

5.5.5. Co-ordination with other NATO projects

5.5.5.1.   The NATO CIS environment will be under continual development by other NATO projects that are being implemented in parallel with the SOA & IdM Platform project.

5.5.5.2. The Purchaser will inform the Contractor and provide information concerning the operational environment that may emerge as a result of these projects.

[SOW-169] *The Contractor SHALL be able adapt the SOA & IdM Platform to accommodate abovementioned additional information.*

[SOW-170] *The Contractor per Purchaser request SHALL identify any documents, meeting minutes, or other information from these projects required to maintain an effective coordination process.*

[SOW-171] *The Contractor SHALL include into Project Communication Plan (part of PMP) activities clearly identifying his proactive approach with regards to the coordination with other related NATO projects.*

5.5.6. Project-level communication

[SOW-172] *As a Project-level communication activity, the Contractor SHALL provide an SOA & IdM Platform Information Sheet of maximum 2 (two) pages providing an overview of the SOA & IdM Platform system, its functions, external interfaces and major components, and its projected installation schedule.*

SECTION 6: SYSTEM IMPLEMENTATION

6.1. General

6.1.1. In addition to the requirements related to what is to be implemented, the Purchaser also has requirements about how the implementation is to be undertaken. Those requirements are the subject of this part of the section.

6.1.2. Further requirements related to test and acceptance appears in SECTION 8: Testing and Acceptance; requirements related to logistics and training appears in SECTION 14: Integrated Logistics Support.

> [SOW-173]   The Contractor SHALL ensure that overall implementation at the sites of Technical Services respects the achievement of Milestones as described in SECTION 4.

> [SOW-174]   In accordance with this Statement of Work, during the implementation phase the Contractor SHALL implement at the capacity to support Wave 1 and Wave 2 as described in SECTION 4: Milestones and below in SECTION 6.8 - 6-12:
>
> a. all of the functionality required;
>
> b. the performance levels required;
>
> c. all of the interfaces required;
>
> d. all of the services required.

> [SOW-175]   The Contractor SHALL implement System in two steps as described in para 3.2 Scope.

6.2. Implementation Constraints

6.2.1. Throughout the whole system implementation activities the Purchaser will retain all administrator privileges on existing systems (e.g. Enterprise Administrator, Domain Administrator) which will therefore not be granted to the Contractor.

6.2.2. The Purchaser reserves the right to suspend the Contractor's installation and/or or activation work for up to 10 (ten) working days to avoid interfering with or disrupting a critical operational event at no cost for the Purchaser.

6.2.3. The Purchaser's acceptance of the Contractor's design does not in any way relieve the Contractor of his responsibility to achieve an implementation which meets all of the requirements of this Statement of Work.

> [SOW-176]   The Contractor SHALL ensure that the Purchaser's requirements for functionality, performance, interfaces and services are traceable from this SoW to the delivered product via the Contractor's accepted design.

> [SOW-177]   The Contractor SHALL maintain traceability from the implemented baseline to all of the requirements of this SoW and SRS through the Traceability Matrix and the Configuration Management Database.

> [SOW-178]   The Contractor SHALL ensure that the implementation activities are executed in the following steps:
>
> a. update and deliver the Project Implementation Plan (PIP) described below in Section 6.4;

b. conduct Preparations for Installation activities described below in Section 6.5;

c. conduct Site Installation and Activation described below in Section 6.6.

6.3. Site surveys

6.3.1. The SOA & IdM Platform will be hosted in the NATO data centres on the virtualised infrastructure provided by the ITM project. It will not provide its own infrastructure or data centre.

6.3.2. As such, the concept of a "site survey" is slightly different than it is normally understood. The activity referred to as "site survey" will still occur, and will result in the production of the documents listed below. However, the site survey for the SOA & IdM Platform will not necessarily involve physical visit(s) to site(s), but instead will be composed of meeting(s) with the Purchaser-provided ITM Point of Contact (POC) to ensure the Contractor understands all relevant details about the data centre and IaaS environment in which the Platform will be hosted.

[SOW-179] The Contractor SHALL conduct site surveys, as described above, for all the sites related to the Site Activation and FSA milestones, and which are part of the contract (i.e. basic sites, and optional sites which have been activated under the contract).

[SOW-180] The Contractor SHALL follow the Site Surveys process for the target installation sites, as described in SECTION 9: Site Surveys.

[SOW-181] Before implementation begins at the sites designated in the contract the Contractor SHALL complete Site Surveys:

a. for the target installation sites;

b. for each site surveyed the Contractor SHALL present and provide to the Purchaser the Site Survey Report;

c. the Site Survey Reports SHALL include a completed Site Survey Template.

[SOW-182] The provided Site Survey Template is an initial template. The Contractor SHALL be responsible to tailor the template to ensure all relevant information is captured to complete the implementation of the SOA & IdM Platform at the site.

[SOW-183] During the Site Survey the Contractor SHALL:

a. identify and document Installation and migration schedules and constraints;

b. identify and document any elements relevant to the implementation but not covered in this SoW.

[SOW-184] At the beginning of the Site Survey the Contractor SHALL provide a presentation to the local site personnel on the objectives and conduct of the site visit in the context of the overall SOA & IdM Platform project.

[SOW-185] At the end of the Site Survey the Contractor SHALL provide an out brief on the outcome of the site survey and identify actions and follow-on activities.

[SOW-186] *The Contractor SHALL adjust the activities and deliverables to the results of the Site Surveys.*

6.4. Project Implementation Plan (PIP)

The key document in the planning and execution of implementation activities is the Contractor's PIP.

[SOW-187] *The Contractor SHALL deliver the PIP that fully describes their PIP plan and activities.*

[SOW-188] *The Contractor SHALL include in the PIP a clear rationale for the logic and sequencing of all implementation activity which demonstrates how new capabilities and services will be introduced in an efficient and controlled manner with optimal use of resources and no loss of service to users.*

6.4.1. Subject to the constraints in this SoW, the Contractor is free to propose the order and timing of all implementation activity providing that at the time of site acceptance the centralised management services and tools SHALL be operational.

6.4.1.1. The Contractor SHALL note that Platform Implementation activities are not to start before the Deployment Authorisation (DA) milestone milestone is fully accepted by the Purchaser.

[SOW-189] *The Contractor SHALL submit to the Purchaser the Project Implementation Plan with the following information:*

a. *the Contractor's approach to all system implementation tasks (including the sequence of activation of the sites to be implemented);*

b. *the Contractor organisation and key personnel involved in system implementation;*

c. *the overall schedule for implementation activities including site survey, site preparation, site installation and activation;*

d. *the schedule of all planned outages of any kind in the sites;*

e. *the detailed implementation sequence of Technical Services and User services considering and adapting to the ITM implementation sequence in order to minimise the impacts on both projects;*

f. *the installation plan addressing:*

i. *a general installation plan showing how the gradual installation and activation of the SOA & IdM Platform will be carried out by the Contractor;*

ii. *the installation procedures, showing that those procedures will cause no or minimal disruption to the sites and to the User desktop applications;*

iii. *a site-specific design for each site;*

iv. *a detailed installation plan for each site;*

v. *site and system installation checklist;*

vi. *Site Activation checklist;*

NATO UNCLASSIFIED

  vii. an Allocation Matrix showing the allocation of each system CIs (nature and quantities) to each site, and the number of users and support staff for each site;

  viii. any specific tools the Contractor intends to furnish and use during the site installation.

 g. the activation plan addressing:

  i. the Site Activation activities;

  ii. any post-activation tasks;

  iii. the "back-out" procedures enabling deactivation and/or removal of all installed SOA & IdM Platform components and restoration of existing services without disruption of those services.

 h. the potential disruption/outage that the implementation activities might generate ensuring potential outages will be kept short (less than 3 hours in duration), planned (approved by the Purchaser at 48 hours in advance based on a Contractor-provided plan to restore functionality within 30 minutes), localised (limited to areas agreed to by the Purchaser) and, if possible, carried out during week-ends.

[SOW-190] The Contractor SHALL structure the PIP so that general implementation information is maintained in the body of the plan and site-specific details are kept as annexes.

[SOW-191] The Contractor SHALL provide the PIP for the Purchaser acceptance.

6.4.2. Provisioning of System/Application

[SOW-192] In accordance to NATO policy [AC/317-D/71 (revised), 1996] the Contractor SHALL use Commercial-Off-The-Shelf (COTS) software in preference to the development of new software unless it evidently contains major disadvantages (e.g. cost effectiveness, negative impact on existing IT infrastructure, security, market stability, etc.) indicated by the Contractor.

[SOW-193] The Contractor SHALL integrate the system/application delivery and provisioning mechanism with Datacentre provided solution as specified in SRS.

6.4.3. Backup, Archive and Disaster Recovery for SOA & IdM Platform

[SOW-194] The Contractor SHALL include backup and restore testing (using ITM capability) as part of the test plans to confirm the functionality and performance.

[SOW-195] The Contractor SHALL include Remediation Plan section in the PIP.

[SOW-196] If the installation of any component of the SOA & IdM Platform is found to be interfering with the operation of other Purchaser's systems the Contractor's back-out plan SHALL be implemented by the Contractor.

[SOW-197] The Contrator's implementation of the back-out plan SHALL ensure no loss or corruption of data in any of the existing systems.

6.4.4. The acceptance of the PIP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relives the contractor from its responsibility to meet the requirements stated in this Contract.

> [SOW-198] *The installation and activation dates reflected in the PIP SHALL be co-ordinated by the Contractor with the Purchaser and the Site POCs to accommodate site-specific requirements, exercises, holiday periods, and other considerations. Any such dates and any revision of these dates SHALL be coordinated with the Purchaser and the relevant sites at least 4 (four) weeks before the start of the relevant activities.*

6.5. Preparations for Installation

> [SOW-199] *The Contractor SHALL provide each site POC, with a copy to the Purchaser Project Manager, with a draft list of software to be shipped, and a list of Contractor's personnel together with a copy of each person's personnel Security Clearance for those who will be involved in site installation and activation work.*

> [SOW-200] *The Contractor SHALL monitor the progress of any required Site facilities preparations, and the progress of any required provision of input by the Purchaser and the Site, to ensure timeliness and quality of the preparatory work required from the Purchaser.*

> [SOW-201] *The Contractor SHALL ensure that anything that may delay installation is brought to the attention of the Purchaser Project Manager promptly.*

> [SOW-202] *The Contractor SHALL prepare and conduct a Site Verification Survey (see SECTION 9) no later than 2 months prior to installation activities at the site. The purpose of this Site Verification Survey is to verify that the information provided by the site is still valid, and to perform any necessary updates to the system implementation documentation. The actual visit of the sites subject to the Site Verification Survey is left to Contractor's appreciation.*

> [SOW-203] *The Contractor SHALL submit the updated PIP for the Purchaser's acceptance immediately after the Site Verification Survey and no later than 2 weeks before the Site installation and obtain the Purchaser approval of the PIP before planned start date.*

6.6. Site Installation and Activation

6.6.1. The Site should be considered as a virtual site, as SOA & IdM Platform will be installed on the existing ITM provided platform. All sites are described in SECTION 4.2.3 and SECTION 7.4.1.

> [SOW-204] *The Contractor SHALL perform site installation of any SOA & IdM Platform elements, including establishment of network connectivity between all required components.*

> [SOW-205] *The Contractor SHALL perform site activation.*

> [SOW-206] *The Contractor SHALL execute all activities related to security accreditation.*

> [SOW-207] *The Contractor SHALL execute system configuration audit.*

[SOW-208] *The Contractor SHALL deliver all documentation associated to site installation and activation.*

[SOW-209] *The Contractor SHALL produce a Site Activation Plan in coordination with the Purchaser.*

6.6.2. Reference System Installation

6.6.2.1. The Reference system installation is pre-requisite for any site installation. The main objective is to ensure that IV&V SL has a representative environment, in which to perform testing, verification and validation activities.

6.6.2.2. The Reference system will also need to allow for development and testing of new future services. Therefore these environments will need to be equipped with a set of tools to help create, modify, test and deploy services.

[SOW-210] *The Contractor SHALL deliver the SOA & IdM Platform Reference system to the Purchaser before the Reference Test.*

[SOW-211] *The Contractor SHALL provide the toolset to the reference environments to allow future Services to be designed, built, unit tested, integrated and approved.*

[SOW-212] *The Contractor SHALL provide pre-configured templates including required tools, services, processes and repositories to the reference environments.*

[SOW-213] *The Contractor SHALL provide the toolset for the reference environment to support different development and testing methodologies, in particular for remote (non-NATO staff) development:*

    a. *external remote connection to the NATO dev/test environment*

    b. *NATO dev/test environment connection to external environment (i.e.: Contractor premises)*

    c. *downloading of a copy of the environment as a virtual machine (VM).*

[SOW-214] *The Contractor SHALL provide the toolset to the reference environments to support:*

    a. *Functional Service testing*

    b. *Data driven service testing*

    c. *Performance testing*

    d. *Service load testing*

6.6.3. Site Installation

[SOW-215] *The Contractor SHALL coordinate the start date of the planned installation no later than 3 (three) weeks before that start date.*

[SOW-216] *Throughout all Site installation activities the Contractor SHALL hold a daily meeting with the site POC to agree on the work to be conducted during the day.*

[SOW-217]   *Although the Purchaser will provide the facilities in which the SOA & IdM Platform will be installed and the external systems to which it will be interfaced, the Contractor SHALL be responsible for timely and complete delivery and installation of all relevant supplies.*

[SOW-218]   *If required for the Implementation, the Contractor SHALL solve all integration and interface problems that may occur during the SOA & IdM Platform installation.*

[SOW-219]   *The Contractor SHALL provide and install all miscellaneous equipment (for example shelves, mounting brackets, power filters, signal filters, cables, installation kits) to enable the connection of SOA & IdM Platform elements to the existing infrastructure at a site.*

[SOW-220]   *The Contractor SHALL ensure that all the necessary miscellaneous equipment come out from the site survey so it could be quantified and monitored.*

[SOW-221]   *The Contractor SHALL deliver the SOA & IdM Platform in accordance with:*

>   a. *the agreed PIP;*

>   b. *the agreed design and SRS;*

>   c. *site specific implementation details.*

[SOW-222]   *The Contractor SHALL deliver the SOA & IdM Platform to sites in line with details in SECTION 14: Integrated Logistics Support.*

6.6.4.   Integrate Service Management and Control capability

6.6.4.1.   The successful implementation of the SMC capability is a critical success factor for this project. The SMC functionality will enable the Purchaser to manage, maintain and support the provision of services to its users.

6.6.4.2.   The SMC capability of the SOA & IdM Platform is a "domain" SMC, which interfaces with the existing Enterprise SMC at the IaaS level.

6.6.5.   Site Acceptance

6.6.5.1.   The purpose of site acceptance is to ensure that all SOA & IdM Platform components installed at that site are ready for operational use and meet with the SRS requirements.

[SOW-223]   *The Contractor SHALL perform site acceptance activities locally at the site.*

[SOW-224]   *The Contractor SHALL ensure that none of the site activation activities have any impact on any operational elements of the SOA & IdM Platform, nor on the NATO Staff Users' desktop applications, except for some authorised potential and limited outages.*

6.6.5.2.   Site Acceptance Tests (SAT)

[SOW-225]   *The Contractor SHALL conduct the SAT as per the process detailed in SECTION 8: Testing and Acceptance.*

6.6.5.2.1. The Purchaser reserves the right to observe the SATs and to have the Contractor perform additional tests in order to demonstrate that the system is meeting the contractual requirements.

6.6.5.2.2. The completion of SAT SHALL be subject to the Purchaser's confirmation that all SATs at a site have been completed successfully. For that purpose:

[SOW-226] *The Contractor SHALL produce a test report after the successful completion of SAT. SAT Test Report for each site is subject to the Purchaser approval.*

6.6.5.2.3. Site Acceptance Tests (SAT) on operational sites

[SOW-227] *The Contractor SHALL ensure that SAT on the operational sites demonstrate that the system installed provides the Contractual functionality and performance level, including all interfaces with all internal and external systems, including administration requirements, and is ready for operational use.*

[SOW-228] *The Contractor SHALL carry out the SAT for a maximum of one week at each site, exclusive of any preparation time.*

6.6.6. Local Security Accreditation activities

6.6.6.1. As part of the local security accreditation, some security documents need to be modified to align with the local security requirements and environment. Additionally, any security tests are to be performed on the local SOA & IdM Platform component.

[SOW-229] *The Contractor SHALL support the Purchaser in obtaining Security Accreditation with the activities and deliverables as specified in SECTION 10: Security.*

6.6.6.2. Security Operations Procedures (SecOPs)

[SOW-230] *For each of the sites where a component of the SOA & IdM Platform system is to be installed, the Contractor SHALL modify the approved generic Security Operating Procedures (SecOPs) to meet the requirements of the local site.*

[SOW-231] *The Contractor SHALL deliver and present the localised version of the SOA & IdM Platform SecOPs to the local Security Accreditation Authority for approval.*

[SOW-232] *The Contractor SHALL take into account any comments from the reviewers and Local Security Accreditation Authority and SHALL update the document as many times as necessary in order to gain Local Security Accreditation Authority approval of the SOA & IdM Platform localised SecOPs for the site.*

6.6.6.3. Security Test and Verification Plan (STVP)

[SOW-233] *For each of the sites where a component of the SOA & IdM Platform system is to be installed, the Contractor SHALL modify the approved generic STVP to meet the requirements of the local site.*

[SOW-234] *The Contractor SHALL deliver and present the localised version of the STVP to the Local Security Accreditation authority for approval.*

[SOW-235]   The Contractor SHALL take into account any comments from the reviewers and Local Security Accreditation Authority and SHALL update the document as many times as necessary in order to gain Local Security Accreditation Authority approval of the SOA & IdM Platform localised STVP for the site.

[SOW-236]   The Contractor SHALL support the NCI Agency in the execution of the STVP.

6.6.7.   Documentation

[SOW-237]   The Contractor SHALL update the documentation delivered at the sites to accommodate any site-specific changes and/or configurations.

[SOW-238]   Upon completion of site implementation work, the Contractor SHALL provide the Purchaser with a copy of the site installation and activation checklist and resolve any discrepancies identified.

[SOW-239]   The Contractor SHALL keep the documentation under configuration control, as per SECTION 12.11:   Configuration Identification and Documentation.

[SOW-240]   The Contractor SHALL deliver training documentation and execute the required training, as described in SECTION 14.7: Training.

6.7. Services

[SOW-241]   The Contractor SHALL design and document all the required Support Service as required in the SECTION 14: Integrated Logistics Support, and in compliance with the support concept depicted in ANNEX B: Maintenance and Support Concept (After PSA).

6.8. Work Packages Introduction for Wave 1 and Wave 2

6.8.1.   This section provides a notional view of the Work Packages (WP) that shall be executed during Wave 1 and 2 of the bundled project.

   6.8.1.1.   WP 2: Implement SOA platform

      a. Implement Basic SOA Platform (Wave 1)
      b. Implement Extended SOA Platform (Wave 2)

   6.8.1.2.   WP 3: Proliferate NEDS on both ON and PBN (during both Waves).

   6.8.1.3.   WP 4: Implement Basic IdM Platform

      a. Implement Basic IdM Platform (Wave 1)
      b. Implement Extended IdM Platform (Wave 2)

   6.8.1.4.   WP 5: Pilot integration cases (during both Waves)

   6.8.1.5.   WP 6: Support pilot integration cases (during both Waves)

   6.8.1.6.   WP 7: Support other FASes integration

6.8.1.7. WP 8 and WP 9: Hardware and Software Acquisition (during both Waves)

6.8.1.8. WP 10: Independent Verification and Validation (during both Waves)

6.8.1.9. WP 11: Standardisation

6.8.2. Work Packages relationships is described below in Figure 8.
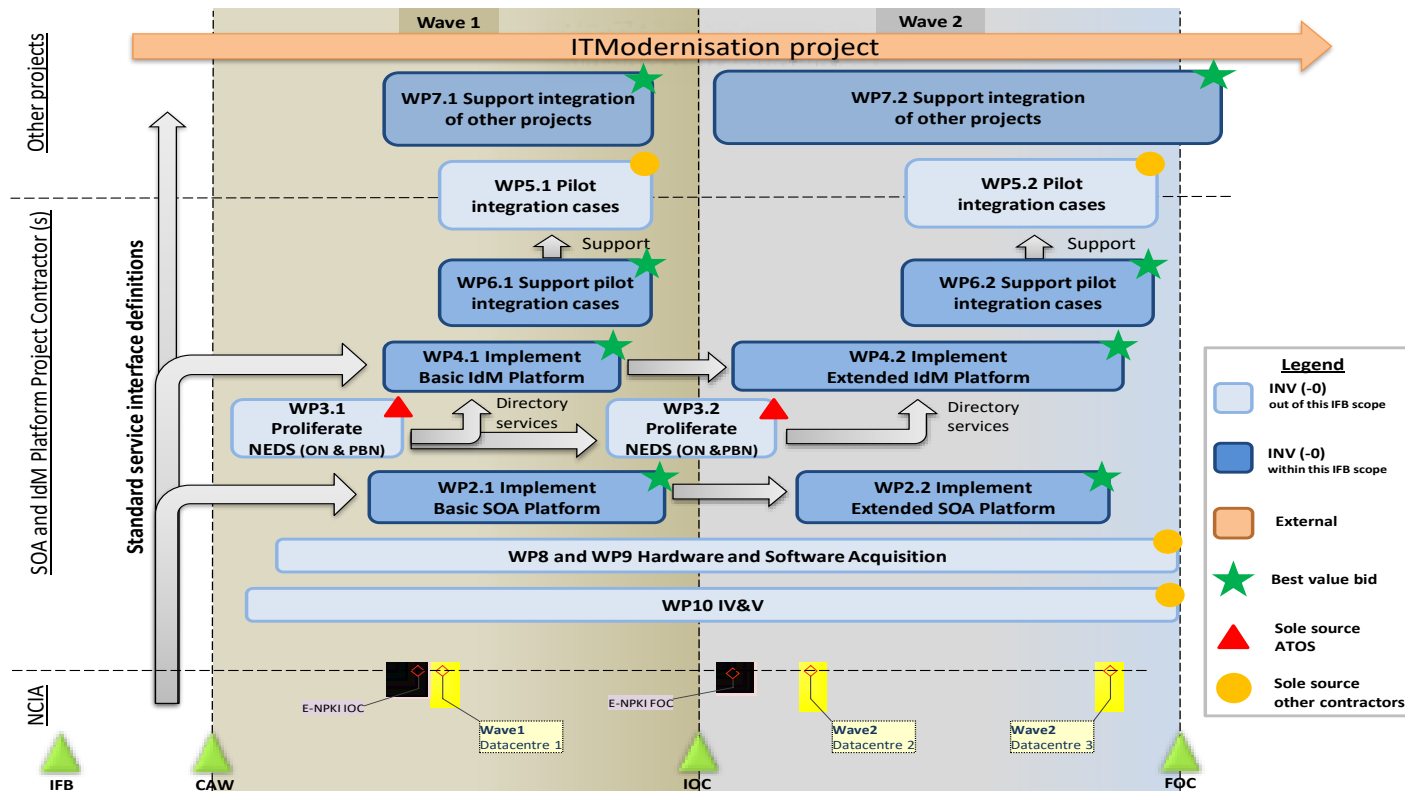
Figure 8: Work Packages relationship (not time scaled)

6.8.3. The Contractor shall note that only Work Packages WP 2, WP 2, WP 4, WP 4.2, WP 6. WP 6, WP 7 are part of this Information for Bid (IFB): see Figure 4: Overall Project Schedule in SECTION 4: Milestones; more specifically SECTION 4.2.1.

6.8.4. The Contractor shall note that the above milestones have been defined in a chronological order. The start of activities leading to a milestone requires the acceptance of the previous milestone (for example, the start of SECTION 6: System Implementation requires the prior acceptance of the Baseline milestone (SECTION 4: Milestones)).

6.9. Work Package 2: Implement SOA Platform: Basic - Wave 1; and Extended - Wave 2

6.9.1. This WP will provide a common platform to existing and new systems to enable the migration towards a Service Oriented Architecture (SOA), on both: ON and PBN.

6.9.2. The scope of this Work Package will be delivered in two subsequent Work Packages corresponding to the implementation Waves.

> [SOW-242] *The Contractor SHALL provide following components of WP 2 during Wave 1:*
>
>   a. *Integration Services:*
>
>   i. *Messaging Infrastructure;*
>
>   ii. *Mediation;*
>
>   b. *SMC Services;*
>
>   c. *Platform Hosting Services.*
>
> [SOW-243] *The Contractor SHALL provide following components of WP 2 during Wave 2:*
>
>   a. *Integration Services:*
>
>   i. *Composition;*
>
>   b. *Registry and Repository Services;*
>
>   c. *Information Services;*
>
>   d. *SMC Services (in support of Wave 2).*

6.10. Work Package 4: Implement Identity Management (IdM) Platform: Basic - Wave 1; and Extended - Wave 2

6.10.1. This WP will provide a common IdM Platform to existing and new systems.

6.10.2. The scope of this Work Package will be delivered in two subsequent Work Packages corresponding to the implementation Waves.

> [SOW-244] *The Contractor under Wave 1 (Basic IdM Platform Implementation) SHALL provide following components on both ON and PBN environment (including Enhanced nodes if required) in corresponding reference facilities and in the integration and testing facility, enabling the following capabilities:*
>
>   a. *Identities Management;*
>
>   b. *Credential Management;*

   c. *Authentication Management:*

     i. Authentication;

     ii. Security Token Services;

   d. *Access Management.*

[SOW-245] *The Contractor under Wave 2 (Extended IdM Platform Implementation) SHALL provide following components on both ON and PBN environment (and also on Enhanced nodes if required) in corresponding reference facilities and in the integration and testing facility:*

   a. *Identity Federation;*

   b. *Allied Replication Hub;*

   c. *Federated Authentication.*

6.11. Work Package 6: Support pilot integration cases during both Waves

6.11.1. Introduction

   6.11.1.1. It is essential that the technical services delivered by the SOA & IdM Platform provide value to other projects and are sufficiently documented to enable their use by 3rd party solution architects and developers. This will be ensured by implementing pilot integration cases with other projects by the end of Basic Platform Service Capabilities (Wave 1) and extended Platform Service Capabilities (Wave 2).

6.11.2. Description

   6.11.2.1. Thise Work Package is to provide consultancy and on-demand support to a 3rd party contractor and developers working under on implementing the pilot integration cases with the SOA & IdM Platform.

[SOW-246] *The Contrator SHALL provide:*

   a. *Project management Plan;*

   b. *Project Status Report;*

   c. *PMO.*

[SOW-247] *The Contractor SHALL provide Training according to Section 14.7 and SHALL deliver:*

   a. *Training Requirements Analysis and Report (TRA/TRR);*

   b. *Training Needs Amalysis (TNA);*

   c. *Training Program/Plan;*

   d. *Training Materials.*

[SOW-248] *The Contractor SHALL provide the Implementation Plan for Work Packages 6 (as described below).*

[SOW-249] *The Contractor SHALL provide support to the Functional Service 3rd party contractor, in:*

   a. *consultancy (for support of other Sole Source Contractor);*

NATO UNCLASSIFIED

b. integration.

[SOW-250]   The Contractor SHALL deliver:

    a. requirements for installation of other FSs on SOA platform and integration and connection to the IdM Platform;

    b. documentation for connection and integration of other FSs as described above;

    c. lessons learned.

[SOW-251]   The Contractor SHALL provide a not-to-exceed level of effort of 625 (six hundred twenty five) man-days over a 2 (two) years period. This support will be provided to a number of projects, with:

    a. approximately 4 (four) man-days/week for the SOA platform;

    b. approximately 2 (two) man-day/week for the IdM platform.

6.11.2.2.   Organisation

[SOW-252]   The Contractor SHALL start Work Packages 6 during Work Packages 5 and propose to the Purchaser the exact start date, including the following:

    a. the Contractor SHALL ensure, that Work Package 6 for Wave 1 is finished before or together with WP5 PSA;

    b. the Contractor SHALL ensure, that Work Package 6 for Wave 2 is finished before or together with WP5 FSA.

Integration Services

Messaging Services
- Message Broker
- Message Queue
- Message Router
- Message Proxy
- Message Cache

Mediation Services
- Data Transformation
- Protocol Transformation

Information Services

Registry and Repository Services

Platform Hosting Services

Platform Environment

Identity and Security Services

Identities Management

Credentials Management

Authentication Management — Security Token Services

Access Management
- Privilege Management
- Policy Decision Point
- Policy Enforcement Point
- Policy Administration Point

Service Management and Control Services

Configuration Management

Process Automation

Event Management
- Logging
- Alerting
- Reporting

Performance and Capacity Management
- Monitoring
- Metering
- Message Tracking

Figure 9: Services for Wave 1
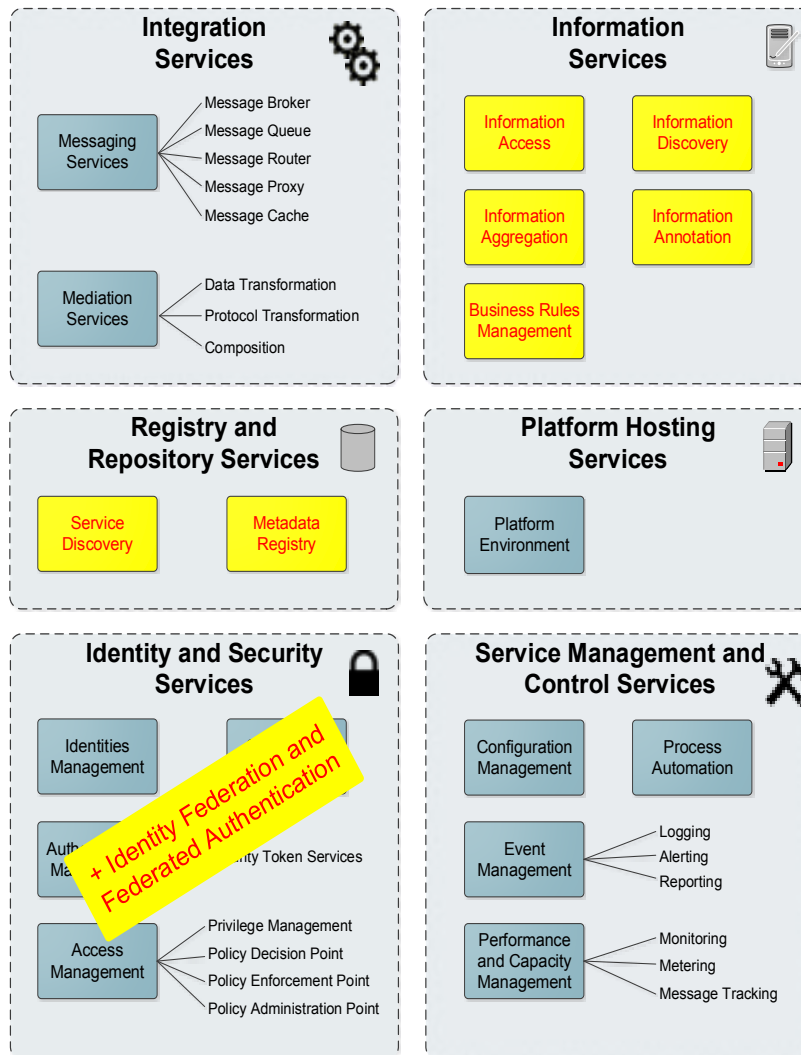
Figure 10: Services for Wave 2

6.12. Work Package 7: Support Integration to other Projects

6.12.1. This Work Package is to provide on-demand support (including post-implementation support) for 3rd party contractors working for other projects that will integrate their systems with the SOA & IdM Platform.

[SOW-253]   The Contrator SHALL provide:

  a. Project Management Plan;

  b. Project Status Report;

  c. PMO.

[SOW-254]   The Contractor SHALL provide a not-to-exceed level of effort of 300 (three hundred) man-days over a 2 (two) years period. This support will be provided to a number of projects, with:

  a. approximately 2 (two) man-days/week for the SOA platform;

  b. approximately 1 (one) man-day/week for the IdM platform.

6.12.2. Performance Start Date is not earlier than PSA date of Wave 1.

6.13. Project Management

> [SOW-255] *The Contractor SHALL meet the requirements listed in SECTION 5: Project Management.*

6.14. Engineering, Integration and Tests

> [SOW-256] *The Contractor SHALL meet the Engineering requirements listed in SECTION 7: System Engineering and Integration.*

> [SOW-257] *The Contractor SHALL meet the requirements listed in SECTION 8: Testing and Acceptance.*

6.15. Implementation

> [SOW-258] *The Contractor SHALL meet the requirements listed in SECTION 6: System Implementation.*

6.16. Integrated Logistics Support

> [SOW-259] *The Contractor SHALL meet the requirements listed in SECTION 14: Integrated Logistics Support.*

6.17. System Operation and Maintenance – Warranty

> [SOW-260] *The Contractor SHALL meet the requirements listed in SECTION 14.3 Maintenance and Support concept and ANNEX B: Maintenance and Support Concept (After PSA).*

SECTION 7: SYSTEM ENGINEERING AND INTEGRATION

7.1. General

7.1.1. This section outlines the System Engineering and Integration of SOA & IdM Platform project.

[SOW-261] The Contractor SHALL develop the SOA & IdM Platform System Design Specification based on an analysis of the Purchaser's requirements.

[SOW-262] The Contractor SHALL integrate all necessary components to establish the SOA & IdM Platform SBL, and plan and execute a series of tests to confirm that this baseline meets its requirements.

[SOW-263] The Contractor SHALL perform the activities described in this section considering that the SOA & IdM Platform will support a wide variety of NATO activities and systems (e.g. Core Services, Functional Services (FS)).

[SOW-264] The Contractor SHALL be responsible for integration of the SOA & IdM Platform System. This means both the integration of the various hardware and software products that constitute the SOA & IdM Platform System and the integration of the SOA & IdM Platform System with other NATO systems.

[SOW-265] The Contractor SHALL make use of "testbeds" to perform this integration and more generally to conduct tests, in particular:

   a. tests related to "Software Approval" SHALL be conducted on the SOA & IdM Platform Reference System, at the Purchaser premises, (see SECTION [SOW-330]);

   b. the baseline tests SHALL be conducted on the SOA & IdM Platform Reference System, at Purchaser premises.

[SOW-266] The Contractor SHALL deliver and activate the SOA & IdM Platform Reference System as required in this section for the Reference System.

[SOW-267] The Contractor SHALL integrate the SOA & IdM Platform Reference System with the appropriate IV&V Reference Environment.

7.2. Orientation Workshop

[SOW-268] The Contractor SHALL conduct a workshop (at a Purchaser-provided facility) to orient the SOA & IdM Platform Administrators and other stakeholders (Contractor proposes Purchaser decision) on the overall system design and capabilities (not eralier than SRR). As part of this workshop, the Contractor SHALL:

   a. deliver overview briefings on the anticipated SOA & IdM Platform system, and lead question and answer sessions with the attendees;

> b. *provide information about the anticipated SOA & IdM Platform System Implementation;*
>
> c. *provide information about how the System Design fully meets the requirements specified in this SoW and SRS;*
>
> d. *provide an overall description of the external interfaces;*
>
> e. *provide an overall description of the ILS concept and strategy;*
>
> f. *provide an overall description of Configuration Management and Quality concept and strategy.*

7.2.1.   This workshop is a key meeting in the course of the Project. As any other meeting outcomes of such WILL be subject to the Purchaser Acceptance.

7.3.   System Requirements Analysis and Review

7.3.1.   Review of the requirements

> [SOW-269]   *The Contractor SHALL review the SRS (see ANNEX A) and all applicable documents, meet and communicate with NATO SMEs as necessary, and present its findings in terms of proposed changes to the SRS based on system cost, schedule, or performance impacts.*
>
> [SOW-270]   *The Contractor SHALL also identify any inconsistencies within the requirements. Any inconsistencies not identified by the requirements review will not be accepted later as the basis for a change with cost impact.*
>
> [SOW-271]   *The Contractor SHALL host and conduct a SRR to present and discuss its findings and proposed changes to the requirement baseline for the design and integration of the SOA & IdM Platform. The purpose of this review is to agree upon the requirement baseline for the design and integration of the SOA & IdM Platform system.*

7.3.2.   Change Requests

> [SOW-272]   *Upon completion of the SRR, the Contractor SHALL identify any proposed changes to SRS in the form of one or more Change Requests. These Change Requests SHALL be addressed according to the processes implemented by the Contractor to meet the requirements of SECTION 12.6: Engineering Change Proposals.*
>
> [SOW-273]   *The Contractor SHALL ensure that Change Request documentation includes:*
>
> > a. *list of all Change Requests processed since the start of the project, in a tabular form, indicating for each of them the date it was created and the current status;*
> >
> > b. *all Change Requests processed since the start of the project.*

7.3.2.1.   The Purchaser will update and provide an updated FBL (in SECTION 12.2.2) as necessary to reflect the decision of the SOA & IdM Platform CCB on these Change Requests.

[SOW-274] *The Contractor SHALL use the updated FBL as the basis for the SOA & IdM Platform system design and subsequent activities.*

7.3.3. Off-specification Report

[SOW-275] *The Contractor SHALL provide the following information with each off-specification report:*

    a. *off-specification identification;*

    b. *date identified;*

    c. *description of the Off-specification;*

    d. *related requirement;*

    e. *related test (if the Off-specification was raised further to a test failure);*

    f. *severity (Major or Minor):*

        i. *Major: an off-specification categorised as Major SHALL be corrected by the Contractor (at no cost to the Purchaser) before the deployment;*

        ii. *Minor: an off-specification categorised as Minor SHALL be corrected by the Contractor (at no cost to the Purchaser) as soon as practicable and as part of this Contract;*

    g. *Configuration Items (CIs) affected;*

    h. *action taken;*

    i. *Fault Resolution status:*

        i. *Conceded = the Purchaser's decision is to leave the off-specification not resolved;*

        ii. *Open = the Off-specification is identified and work is in progress to resolve it;*

        iii. *Resolved = remedial action has been taken by the Contractor and demonstrated through tests conducted by the Contractor without official witnessing by the Purchaser;*

        iv. *Closed = the resolution was formally demonstrated to the Purchaser.*

    j. *comments.*

7.3.3.1. Off-specifications Document

[SOW-276] *The Contractor SHALL submit to the Purchaser off-specification document which includes:*

a. *list of all Off-specification Reports processed since the start of the project, in tabular form, indicating for each of them the date it was created and the current status;*

b. *all Off-specification Reports processed since the start of the project.*

7.4. System Design

7.4.1. Design activities

7.4.1.1. The Contractor should review the Purchaser-provided SOA & IdM Platform Target Architecture (TA; [NCIA SOA & IdM TA, 2017]) and should consider this TA as a document for information which should be helpful to conduct its design activities. Therefore, the Contractor SHALL NOT consider the Target Architecture as a binding document.

[SOW-277] *The Contractor SHALL consider two-steps architecture:*

a. *in first step design the Architecture for two datacenters working in asynchronous mode: Lago Patria (JFC Naples) and Mons (SHAPE);*

b. *in second step design the Architecture for three datacentres: Brussels (NNHQ) and Mons (SHAPE) working in synchronous mode and Lago Patria (JFC Naples) working in asynchronous mode with Mons (SHAPE) and Brussels (NNHQ) with preliminary delivery date for datacenter in Brussels (NNHQ), in October of 2020.*

[SOW-278] *The Contractor SHALL conduct the necessary Design Activities and develop its own complete design of the SOA & IdM Platform at the Preliminary and Critical levels, including all interfaces to other systems to meet the SRS.*

[SOW-279] *The Contractor SHALL keep the system design documentation package (including security accreditation documentation) up to date throughout project execution, in particular as a result from the site surveys and/or in order to obtain the security accreditation.*

[SOW-280] *The Contractor's SOA & IdM Platform System Design SHALL cover all sites identified for this project.*

[SOW-281] *The Contractor's SOA & IdM Platform architecture SHALL be designed so that it can be reused for other security classification levels (in any case, the system will be installed and operated at System High mode of operation).*

[SOW-282] *The Contractor's SOA & IdM Platform system SHALL be built to a modular design that allows future extension and enhancements.*

7.4.2. System Design Documentation Package

[SOW-283] *The Contractor SHALL establish, deliver and maintain the SOA & IdM Platform System Design Documentation Package, comprising of:*

a. *the Project Implementation Plan (PIP);*

NATO UNCLASSIFIED

b. the System Design Specification, the Interface Control Document;

c. the Security Accreditation Documentation Package;

d. the Requirements Traceability Matrix (RTM);

e. Project Master Test Plan (PMTP);

f. Integrated Logistic Support (ILS) Plan;

g. Training Needs Analysis (TNA).

7.4.2.1.   System Design Specification (SDS)

[SOW-284]   The Contractor's SDS SHALL describe the SOA & IdM Platform System to a level of detail that is sufficient for the Purchaser to be able to understand how the requirements in the SRS and the security requirements (see ANNEX A) SHALL be implemented and Functional and non-Functional Requirements (see SRS) SHALL be addressed.

[SOW-285]   Based on the CDR, the Contractor SHALL provide the specification and quantity of the Virtual Machines required to operate the SOA & IdM Platform for each Wave.

[SOW-286]   Based on the CDR, the Contractor SHALL provide the specification and quantity of the Enterprise Software (Operating System, Database System) required to operate the SOA & IdM Platform for each Wave.

[SOW-287]   At CDR, the Contractor SHALL provide the Purchaser with the schedule clearly identifying when required Virtual Machines and Enterprise Software, to be provided by the Purchaser, are required.

7.4.2.2.   The Purchaser will provide the required Virtual Machines and Enterprise Software as per Contractor's specification as PFE (see ANNEX C C.2.1)

[SOW-288]   The Contractor SHALL include the following information in the SDS document (but not limited to):

a. System architecture

i.   The following Operational and Systems Views, as defined in the NATO Architecture Framework (NAF, [NAC AC/322-D92007)0048, 2017]):

1. NATO Operational View (NOV)-1 High-Level Operational Concept Diagram;

2. NATO System View (NSV)-1 Systems Interface Description (Composition);

3. NSV-1 System Interface Description (Intra System);

4. NSV-1 System Interface Description (Inter System);

5. NSV-2, Systems Communications Description – this includes: NSV-2a: System Port Specification;

6. NSV-4 System Functionality.

ii. The (minimum) information in the NAF views the Contractor SHALL supply is defined in the Table 4 below.

iii. The NAF views SHALL be produced and provided in the format of the NCI Agency approved architecture tools (Software AG Aris IT Architect, IBM System Architect or Troux Architect). If not, the Contractor SHALL ensure the exchange format SHALL be approved by the Purchaser upfront.

iv. Physical layout and operation principles of the SOA & IdM Platform in the deployment sites (including the site of the SOA & IdM Platform Reference System), including as a minimum:

7. identification of where the components will be installed, of how users (NATO Staff Users) will make use of the provided functionality, of how support staff (SOA & IdM Platform Administrators will operate the system. This SHALL cover in particular how the SOA & IdM Platform components SHALL integrate into the storage and backup solutions existing at the implementation sites.

i. Results of the network simulation, showing the integration with the underlying network infrastructure, the mitigation of potential impact of the available bandwidth and of any latency;

ii. Replication, synchronisation and browsing protocols and flows;

iii. Proposed topology for the system;

iv. Routing, Transport, and connectivity to SOA & IdM Platform components;

v. Administration model design (Administrative groups and permissions, administrative roles, trust relationships between separate domains);

vi. Schema;

vii. Attributes to which the NATO Staff Users have read-access.

b. System Functionalities;

c. Functional breakdown of the SOA & IdM Platform system;

d. APIs and libraries;

e. *System internal interfaces - description of the interworking of all components to meet the system requirements (e.g. physical interfaces between components, data flows)*

f. *Performance Requirements (defined in the SRS);*

g. *Equipment if applicable:*

   i. *Physical breakdown of the operational SOA & IdM Platform system, of the Reference Test Bed, into hardware/software CIs (including the number of licenses for each SW CI), with traceability to the functional breakdown;*

   ii. *Identification of all COTS included in the system;*

   iii. *CSA reports addressing all system CIs;*

   iv. *All configuration information (parameters, settings, etc.) for all of the SOA & IdM Platform components;*

h. *Security: description of how the system complies with all security requirements.*

NAF view (sub-view)	Purpose	NAF objects to be used	NAF relationships to be used
NSV-1 (composition)	To show the different components of the envisaged SOA & IdM Platform system	System	ResourceComposition (System->System)
NSV-1 (intra-system)	To identify the interactions between the different components of the SOA & IdM Platform system. For each interaction applicable standards/formats/protocols need to be identified	System, DataElement, Standard/Protocol	ResourceInteraction (System->System), ConveyedElement (ResourceInteraction->DataElement) ConformsTo (ResourceInteraction->Standard/Protocol)
NSV-1 (inter-system)	To identify the interaction of the SOA & IdM Platform system with other systems. This also incl. dependencies on hosting platforms. For each interaction applicable standards/formats/protocols need to be identified	System, DataElement, Standard/Protocol	ResourceInteraction (System->System), ConveyedElement (ResourceInteraction->DataElement) ConformsTo (ResourceInteraction->Standard/Protocol) ConformsTo (DataElement ->Standard/Protocol)
NSV-1 (deployment)	To show the deployment of components to locations (site-level). Note: this is a NAF extension	System, Location	RequiredLocation (System->Location)

NAF view (sub-view)	Purpose	NAF objects to be used	NAF relationships to be used
NSV-2a (System port description) aka Interface Specification	To identify and specify each internal (i.e. between system components) and external (i.e. between SOA & IdM Platform and other systems) interface.	System, System Port (aka interface), Protocol	Association (System->SystemPort), ImplementsProtocol (SystemPort->Protocol)
NSV-4 (system functionality)	To identify the functionality that each component provides. Each functional requirement must be traceable to a system function	System, SystemFunction, Requirement	FunctionProvision (System->SystemFunction), Satisfy (SystemFunction->Requirement)

Table 4: NAF Information Requirements

7.4.2.2.1.   Interface Control Document (ICD)

[SOW-289]   The Contractor SHALL ensure that:

    a. each direct interface between the SOA & IdM Platform and other systems (e.g. NEDS) is documented in a specific annex of the ICD;

    b. each interface between the SOA & IdM Platform and SOA & IdM Platform in another security domain is documented in a specific annex of the ICD;

    c. each interface between the SOA & IdM Platform and other systems is documented in a specific annex of the ICD;

    d. each interface between the SOA & IdM Platform subordinate or superior SOA & IdM Platform components is documented in a specific annex of the ICD;

    e. each interface between the SOA & IdM Platform and end-entity users and devices is documented in a specific annex of the ICD;

    f. the ICD includes detailed description of the interfaces between the SOA & IdM Platform and NEDS, including any "configuration settings" and agreements to enable synchronisation between SOA & IdM Platform and NEDS;

    g. where work was conducted by the Contractor under this Contract to document the design of any system to be interfaced to the SOA & IdM Platform, the results of that work is included in the relevant annex of the ICD.

[SOW-290]   The Contractor SHALL develop ICD in accordance with [NTEMP-1] and contain the following information:

    a. A list of the applicable technical standards

b. A catalogue of the services and interfaces exposed by the Platform

c. A detailed description of the interfaces, including diagrams, Data Elements, data formats, Performance values, communication protocols, security settings, etc.

d. Descriptions of Data Elements

e. units of measure required for the Data Element, such as seconds, meters, kilohertz, etc.

f. limit/range of values required for the data element (for constants provide the actual value)

g. accuracy required for the Data Element

h. precision or resolution required for the Data Element in terms of significant digits,

i. frequency at which the Data Element is calculated or refreshed, such as 10 KHz or 50 msec

j. legality checks performed on the Data Element

k. data type, such as integer, ASCII, fixed, real, enumerated, etc.

l. data representation/format

m. priority of the Data Element

n. Service Descriptors, identifying the services endpoints, a detailed description of the service operations and service parameters

o. All related Artefacts such as WSDL, schema files and descriptors

p. Message descriptions

q. Interface priority

r. Communications protocol

7.4.2.2.2.   Security Accreditation Documentation Package

[SOW-291]   The Contractor SHALL ensure that the Security Accreditation Documentation Package comprises all documentation mentioned in SECTION 10.1.3.

7.4.2.2.3.   Requirements Traceability Matrix (RTM)

[SOW-292]   The Contractor SHALL develop and maintain a RTM as required below.

[SOW-293]   The Contractor SHALL ensure that the RTM includes the following information (but is not limited to):

a. the requirements stated in the SRS and SSRS;

b. the detailed contents of the SDS in terms of SDS statements and lowest-level Cis;

c. for each requirement, two-way traceability between the requirement and the design feature that implements the requirement;

d. for each requirement, identification of any Off-specifications associated with the requirement;

e. for each requirement, identification of the verification method;

f. for each requirement already successfully verified or tested: identification of the test(s) or test waiver(s) on the basis of which the requirement was demonstrated;

g. for each requirement not yet successfully tested: identification of the test(s) or test waiver(s) that are intended to demonstrate the requirement; identification of the associated problem report;

h. the requirement coverage status by the RTM date with a clear identification of what is the requirement status (met, not met, not yet verified) and if the verification has been witnessed by NCI Agency as part of an acceptance test activity.

[SOW-294]   The Contractor SHALL ensure that RTM will maintain raceability to Use Histories/ Use cases, Change Requests and their approval status.

[SOW-295]   As part of the Configuration Management activities, and like any other management product or specialist product, the Contractor SHALL update the System Design Documentation Package to reflect changes, at least at each of the following major milestones: a new design review, the start of a test phase, the completion of each tests activities, the start of the deployment, PSA, FSA.

[SOW-296]   The Contractor's RTM SHALL provide the basis for scope and change management.

[SOW-297]   The Contractor SHALL ensure, that in the RTM maintains full traceability between the functional, the allocated and the product baselines, so that the Purchaser can verify their compliance throughout the Contract, including time and place of tested environment, test result and linked test cases and deficiencies.

[SOW-298]   The Contractor SHALL ensure that RTM is kept up to date in order to reflect any changes during the implementation of the project, in a timely manner (i.e., within one (1) week of change occurring).

[SOW-299]   The Contractor SHALL provide the RTM in a format compatible with the current version of Microsoft Excel.

[SOW-300]   The Contractor SHALL post RTM to the Project's Documentation portal.

[SOW-301]   The Contractor's RTM SHALL be generated automatically from information managed by means of requirements/test management tools.

[SOW-302]   The Contractor SHALL ensure that In order to maintain clear consistency throughout all documents in the System Design Documentation Package, any update of any of the documents comprised in the System Design Documentation Package SHALL

result in re-delivery of a new version of the complete System Design Documentation Package.

7.4.3. Disaster Recovery Plan

[SOW-303] *The Disaster Recovery Plan & Procedures and the Backup Plan & Procedures prepared by the Contractor SHALL address the best practices developed by the vendors of the system components (hardware and software), including security best practices and SHALL be coordinated with ITM design).*

[SOW-304] *The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL address all possible scenarios and corresponding actions, including security.*

[SOW-305] *The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL align with the site-specific Disaster Recovery Plan & Procedures.*

[SOW-306] *The Backup Plan & Procedures prepared by the Contractor SHALL align with the site-specific Backup Plan & Procedures.*

[SOW-307] *As a minimum, the Disaster Recovery Plan & Procedures prepared by the Contractor SHALL address the following scenarios:*

   a. *recovering the entire SOA & IdM Platform;*

   b. *transferring of a SOA & IdM Platform service from one platform to another.*

[SOW-308] *The Disaster Recovery Plans & Procedures prepared by the Contractor SHALL clearly distinguish between service restoration and data restoration, and SHALL include a disaster recovery kit.*

[SOW-309] *The Contractor SHALL deliver the disaster recovery kit which SHALL contain distribution media for all software (including versions, upgrades/updates, patches and hot-fixes) to restore an SOA & IdM Platform Element from "bare metal", in accordance with site-specific Disaster Recovery plans.*

[SOW-310] *The Contractor SHALL deliver the disaster recovery kit that includes a full, customised, installation plan that covers all steps (including OS installation) to build and configure each of the SOA & IdM Platform components.*

[SOW-311] *The Contractor SHALL deliver the disaster recovery kit that includes a list of all passwords, community strings, etc. required, with the exception of the information that is retained by the Purchaser as stipulated in the Contract.*

[SOW-312] *The Contractor SHALL ensure that Volume Shadow copy service is used to optimise the backup/recovery process where appropriate.*

[SOW-313] *The Contractor SHALL ensure that disaster recovery procedures are included in the Technical Manuals and SHALL be a dedicated section of it.*

[SOW-314] *The Contractor SHALL ensure that disaster recovery Kit is analysed in terms of ILS resources and all the necessary resources and support needed for disaster recovery is produced as required in the SECTION 14: Integrated Logistics Support of this document.*

7.4.4. System Requirements Review (SRR)

[SOW-315] The Contractor SHALL review the SOA & IdM Platform System Requirements Specification (SRS) and all other applicable documents:

    a. liaise with NATO subject matter experts as necessary;

    b. prepare its recommendations in terms of proposed changes to the SRS;

    c. The Contractor MAY propose changes to the SRS, in order to resolve inconsistencies and/or make improvements; such proposals SHALL be considered by the Purchaser through the Configuration Control Board (CCB) process after Systems Requirements Review (SRR) Meetings.

[SOW-316] The Contractor SHALL justify any proposed changes to the requirements together with the expected system cost, schedule, performance and supportability impacts.

[SOW-317] The Contractor SHALL identify any inconsistencies within the requirements or that which are in conflict (e.g., with design constraints). Any inconsistencies not identified by the requirements review WILL NOT be accepted later by the Purchaser as the basis for a change with cost impact.

[SOW-318] The Contractor's SRS SHALL be the Purchaser provided SRS with approved changes and, as required, extended with additional details supporting the approved scope.

[SOW-319] The Contractor's proposed changes to the SRS SHALL be delivered five (5) days prior to SRR.

[SOW-320] The Contractor SHALL use the DOORS (IBM) requirements management tool for management of the SRS and project requirements.

[SOW-321] The Contractor SHALL organise and conduct SRR to present its proposed changes for the design and integration of the SOA & IdM Platform.

[SOW-322] The Contractor SHALL provide items listed below in Table 27:

Serial	Requirement
1.	Proposed, updated SRS
2.	CIS Description
3.	Preliminary Security Risk Assessment (SRA) reports (separate for NU/NR and NS)
4.	Active Change Requests
5.	Updated RTM

Table 5: The SRR documents

[SOW-323] The Contractor's SRR SHALL be considered completed when the Purchaser and the Contractor have agreed to all necessary

changes to the SRS and when the changes will be implemented accordingly, such that the SRS is sufficient to begin or continue with the design and implementation work.

[SOW-324] The Contractor SHALL update the Change Proposal documentation, as defined in SECTION 12.6: Engineering Change Proposals.

7.4.5. System Design Reviews (SDR)

[SOW-325] The duration of the review cycle for the SOA & IdM Platform System Design Documentation Package SHALL not exceed 4 (four) weeks.

[SOW-326] Purchaser review and acceptance of the System Design Documentation Package SHALL not imply Purchaser acceptance of the SOA & IdM Platform Design. The Contractor SHALL prove the design through the regime of testing set forth in the Contract and the Contractor SHALL be responsible in the event that the system proves deficient in meeting the Contractual requirements.

[SOW-327] The Contractor SHALL conduct System Design Reviews (Preliminary Design Review (PDR) and Critical Design Review (CDR)) to present the SOA & IdM Platform Design Documentation Package and evidence that all other engineering documents and tools and data is ready to proceed with the development/customization and testing stage. The Contractor SHALL include the following areas in the Design Review:

    a. SOA & IdM Platform overall system architecture and interactions;

    b. system functionality, modularity and interfaces, breakdown into lowest-level Configuration Items (see SECTION 12.4 for Configuration Item Identification and Documentation);

    c. off-the-shelf products to be used in the system: the Contractor SHALL identify the intended product and version, and note if any additional elements (such as macros or plug-ins) are required;

    d. interfaces with other relevant systems (in particular with NEDS);

    e. system security design: Presentation of the Risk Assessment Methodology that the Contractor intends to use for the Project, Results of the Risk Analysis, Definition and implementation of the Security measures to counter the risks identified in the Security Risk Assessment. This presentation SHALL be done as a separate item;

    f. sequence and scope of system tests of the ABL and any requirements for Purchaser support and participation;

    g. any change request or off-specification;

    h. any changes to the PBS and PFD;

    i. any changes to the PMS;

  j. cost considerations;

  k. risk assessment of proposed changes and an update of the Risk Log and Issue Log;

  l. Requirements Traceability Matrix (RTM).

[SOW-328] *The Contractor SHALL provide a Design Review Report.*

[SOW-329] *The Contractor SHALL update the Design Documentation Package as per the result of the Design Review.*

[SOW-330] *The Contractor SHALL provide all the ILS engineering activities and analysis integrated in the System Design as requested in Section 14.3 and in Section 14.4 and as described in the Integrated Logistic Support Plan.*

7.5. Dvelopment (Software) Approval

[SOW-331] *The Contractor SHALL support the AFPL-associated process and tests as defined in SECTION 8: Testing and Acceptance.*

7.6. Site Surveys

[SOW-332] *As part of this work package, the Contractor SHALL conduct site surveys at all the sites related to the PSA milestone (see SECTION 3: Scope and SECTION 4: Milestones).*

[SOW-333] *The Contractor SHALL re-deliver any changed documentation.*

7.7. Support Services

[SOW-334] *The Contractor SHALL design and document all the Support, Operation and Maintenance services for SOA & IdM Platform in complete integration with the System platform, as required in the Integrated Logistics Support (SECTION 14) and ANNEX B: Maintenance and Support Concept (After PSA).*

SECTION 8: TESTING AND ACCEPTANCE

This section outlines the specific requirements to be applied by the Contractor to the testing & acceptance processes and activities, which are required for verification of the SOA & IdM Platform's compliance with the requirements set forth under this Contract by the Purchaser.

The main objectives of the Testing on the SOA & IdM Platform are:

   a. *to provide verifiable objective evidence that the system is fit for purpose;*

   b. *to provide verifiable objective evidence that the system satisfies all requirements in the requirements specification;*

   c. *to detect and eliminate all defects with critical, or major severity;*

   d. *to detect and eliminate all defects with minor, or trivial severity;*

   e. *to maximize test automation to increase the maintainability and repeatability of the tests.*

8.1. Testing Approach

[SOW-335]   *The Contractor SHALL perform all the testing & acceptance activities according to the best market practices, as identified and referred to by the Contractor, unless specific testing process requirements and/or definitions are given in this Contract. Should the Contractor deviate from the requirements set forth in this section, it is the Contractor's responsibility to demonstrate the benefit of such approach to the Purchaser.*

[SOW-336]   *The contractor SHALL define test automation strategy in PMTP.*

[SOW-337]   *The Contractor SHALL plan and undertake a comprehensive set of test steps which will be described in the Project Master Test Plan (PMTP).*

8.1.1. Quality-Based Testing

[SOW-338]   *The Contractor SHALL conduct Quality-Based Testing (QBT) for each Release prior to any deployment activity.*

[SOW-339]   *The Contractor SHALL ensure that QBT demonstrates compliance of the installed, configured and integrated environment based on criteria described in detail in ANNEX A, SRS, SECTION 4 Non-functional Requirements*

[SOW-340]   *The Contractor SHALL develop test cases for each type of quality criteria and ensure full test coverage.*

[SOW-341]   *The Contractor SHALL provide the following information for each Test Case:*

   a. *its objective, by clearly identifying the SRS, SRA, and SSRS requirements (subset of the Requirements Traceability Matrix) intended to be demonstrated by the test procedure;*

NATO UNCLASSIFIED

b. the SOA & IdM Platform CIs and facilities and test equipment involved;

c. any pre-conditions which SHALL be satisfied prior to application of the test;

d. any post-condition which SHALL be satisfied after execution of the test;

e. a block diagram showing the proposed method of meeting the test requirements;

f. the data to be collected;

g. the sequence of testing steps in the procedure, to a level of detail that enables full understanding by the Purchaser of the purpose and effect of each test step;

h. the expected outcome;

i. the means of measurement and/or assessment for the test.

8.1.1.1. The Purchaser (IV&V Team) shall have right to participate in Sprint tests and Alpha tests at Contractor Environment as observer.

[SOW-342] The Contractor SHALL obtain the Purchaser approval for test cases prior to their execution.

8.1.2. Service-Based Testing

8.1.2.1. The purpose of the Service-Based Testing (SBT) is to ensure that the SOA & IdM Platform toolset, processes and people can work effectively and efficiently together to deliver SOA & IdM Platform services, according to the requirements of this SoW.

[SOW-343] The contractor SHALL define test scenarios that will demonstrate that the SOA & IdM Platform can be used by the pilot application chosen under WP6.

[SOW-344] The Contractor's test scenarios SHALL include elements of the three pillars: people, processes and technology.

[SOW-345] All Contractor's test cases and scenarios SHALL be approved prior to their execution by the Purchaser.

[SOW-346] The Contractor SHALL demonstrate through testing the integration of the system (SMC toolset, as described in ANNEX A, ANNEX C and ANNEX F), with processes and with trained users.

8.1.3. Sequencing

[SOW-347] The Contractor's Testing approach SHALL comprise of test phases and milestones described in this section.

[SOW-348] The Contractor's Testing SHALL be performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.

8.1.3.1. The testing (functional and non-functional) sequencing is described below
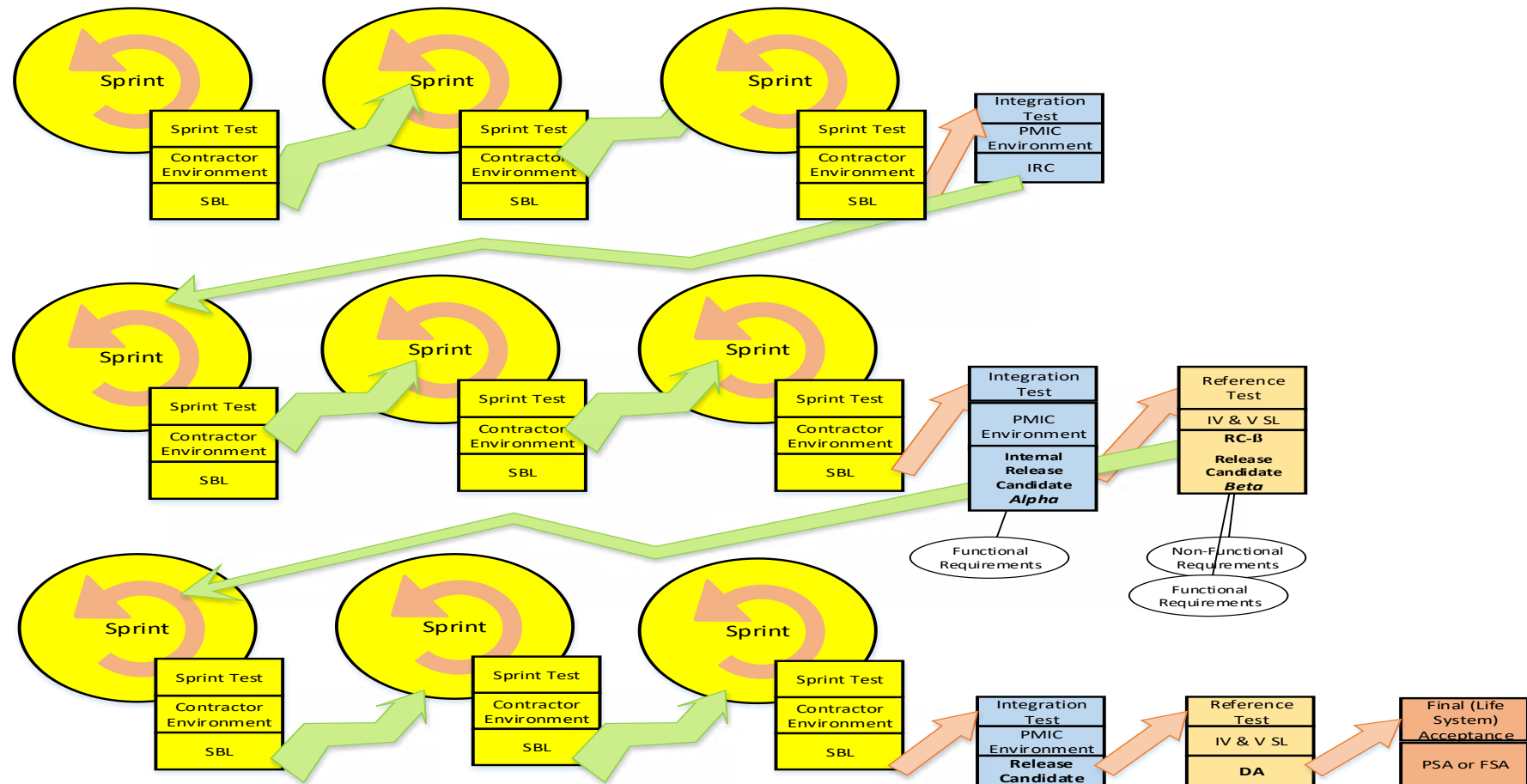
Figure 11: Agile Testing approach for the SOA & IdM Platform Project

8.1.3.2.

8.2. Testing phases

8.2.1. Engineering Tests

8.2.1.1. Overview

> [SOW-349] *The Contractor SHALL conduct engineering Tests during each sprint at the Contractor's environment, consisting of Unit and Component Test, Component Integration Test and system test.*
>
> [SOW-350] *During the Sprint Planning session, the Contractor SHALL:*
>> a. *identify functional and non-functional requirements of the system that will be develop during the sprint phase;*
>> b. *define testable User Stories;*
>> c. *create test cases for user stories;*
>> d. *participate in project risk analysis;*
>> e. *plan Test for the release;*
>> f. *estimate test effort;*
>> g. *support test automation.*
>
> [SOW-351] *During each Sprint the Contractor SHALL:*
>> a. *integrate and execute automated and manual tests;*
>> b. *report the test status to the project team;*
>> c. *update test cases when new scenarios arise.*

8.2.1.1.1. Unit testing is a software testing method by which individual units of source code, sets of one or more computer program modules together with associated control data, usage procedures, and operating procedures, are tested to determine whether they are fit for use.

8.2.1.1.2. Component Integration Testing is performed to verify that the interfaces and interaction between integrated components meets specified requirements.

8.2.1.1.3. A System Base Line (see also SECTION 4.6) will be the result of a successful Sprint Test.

8.2.1.2. Exit criteria

> [SOW-352] *The Contractor SHALL deliver Test Reports according to paragraph 8.4.2.*

8.2.1.3. Systems Integration Tests (SIT) Overview

> [SOW-353] *After three sprints, the Contractor SHALL perform a set of System Integration Tests and code quality check on the Purchaser's environment.*

8.2.1.3.1. Systems Integration Tests exercise a system's coexistence and interoperability with other systems. It exercises a system's compatibility with the target implementation environment and its interfaces with other systems in that environment. It also assesses a system's use of resources

in the target implementation environment to identify any undesirable effects on other systems.

8.2.1.3.2. For the code quality check the Purchaser has the following tools available.

a. SonarQube 6.3 to analyse the code for quality issues
b. HP Fortify 17.10 to analyse the code for security vulnerabilities.

8.2.1.3.2.1 A different set of tools may be used by the Contractor in the integrated development tools; the reference will the the policies that are available to be activated in the tools.

[SOW-354] Per the Purchaser request the Contractor SHALL submit code for inspection.

8.2.1.3.3. An Internal Release Candidate or Release Candidate will be the result of a successful Integration Test.

8.2.1.4. Exit Criteria

[SOW-355] To achieve the IRC and RC milestone, the Contractor SHALL:

  a. execute all agreed test cases;

  b. correct and re-tested all failures with severity "Critical" or "Major"

  c. create an agreed action plan for failures with severity "Moderate", "Minor" and "Cosmetic".

[SOW-356] The Contractor SHALL show that the plan is suitable and effective in ensuring a smooth activation and avoiding any loss of existing SOA & IdM Platform functionality while maintaining service availability and performance as stated in the Contractual requirements;

[SOW-357] The Contractor SHALL deliver the following documentation:

  a. Installation and activation plans (see SECTION 6).

  b. SHALL show that the plan is suitable and effective in ensuring a smooth activation and avoiding any loss of existing SOA & IdM Platform functionality while maintaining service availability and performance as stated in the Contractual requirements;

  c. updated documentation, including the ILSP;

  d. Original Equipment Manufacturer (OEM) Manuals, the Custom Manuals, and the System Tests Documentation Package in support of the Release Acceptance Tests;

  e. Disaster Recovery Plan & Procedures;

  f. Backup Plan & Procedures.

[SOW-358] The Contractor SHALL make sure that the SOA & IdM Platform Reference System environment used to conduct Release Acceptance Tests and Software Approval Tests is representative of the actual operational environment, including (but not limited to):

a. *design and configuration;*

b. *performance;*

c. *security settings;*

d. *software versions.*

8.2.2.   Dry-run on the Reference Environment

8.2.2.1.　The Contractor can perform a dry-run before submitting the final Release Package on the Agency Reference Environment.

8.2.2.2.　The purpose of the dry-run is to allow the contractor to verify that the SOA & IdM Platform will function correctly when installed in its operational environment. This testing is conducted in configured Purchaser Reference Environments that provide representations of the target network/security domain, including security settings, patches, network configurations and interfacing systems and services as necessary to represent the live environment as viewed from the perspective of the product, system or service being tested.

> [SOW-359]　*The Contractor SHALL schedule a period of 6 weeks for the Reference Test phase in the PMTP.*
>
> [SOW-360]　*The Contractor SHALL identify any limitations due to the Reference environment regarding its representatively of the actual operational environment, including (but not limited to):*
>
> > a. *design and configuration;*
> >
> > b. *performance;*
> >
> > c. *security settings;*
> >
> > d. *software versions.*
>
> [SOW-361]　*For each version, the Contractor SHALL verify and validate any new features of the SOA & IdM Platform or Reference Environment that requires a configuration alignment with the Production Environment.*
>
> [SOW-362]　*The Contractor SHALL execute any regression tests as required by the Purchaser.*

8.2.2.3.　Deployable Computer Information System (DCIS) Testing

8.2.2.3.1.　To validate whether the Platform can also operate in a deployed environment, a set of tests will be conducted on the DCIS Reference Environment, where a number of scenarios will be conducted to demonstrate operation under degraded and/or disrupted network connectivity.

> [SOW-363]　*The Contractor SHALL provide a DCIS Test Plan for Purchaser's review and approval.*
>
> [SOW-364]　*The Contractor SHALL prepare the DCIS Test Cases, Test Procedures and Test Steps based on Purchaser provided scenarios and submitted these to the Purchaser for their review and approval.*
>
> [SOW-365]　*The Contractor SHALL carry out the DCIS test at the Contractor's facility on a test environment that is representative for the deployed environment.*
>
> [SOW-366]　*The Contractor SHALL execute the DCIS Test, which will be witnessed by the Purchaser and Purchaser designated Quality Representative(s).*
>
> [SOW-367]　*The Contractor SHALL reference the DCIS test case and steps to a requirement with a pass and fail.*

[SOW-368]   The Contractor SHALL record all DCIS test cases and test step results based on the agreed pass/fail criteria and incident categorization, and in case of a fail document the reason of failure.

[SOW-369]   For successful completion of the DCIS Test, the Contractor SHALL:

    a. Execute all the agreed test cases;

    b. Correct and re-test all failures with severity "Critical" or "Major"

    c. Create an agreed action plan for failures with severity "Minor" and "Cosmetic".

8.2.3.   Request For Change (RFC)

[SOW-370]   The Contractor SHALL support the Purchaser's RFC test, which consists of a:

    a. Independent Verification and Validation;

    b. preliminary User Acceptance Test (UAT);

    c. cybersecurity testing.

[SOW-371]   The Contractor SHALL provide fifteen days (15 days) of support to the Purchaser in preparing a RFC to meet the requirements of the Purchaser's Change Evaluation process.

[SOW-372]   The Contractor's RFC Evaluation SHALL include security testing.

[SOW-373]   The Contractor SHALL support the Functional Configuration Audit (FCA) as described in SECTION 12.9.

[SOW-374]   The Contractor SHALL execute any regression tests on the updated PBL as required by the Purchaser.

[SOW-375]   The Contractor SHALL support any Software Approval tests on the updated PBL as required by the Purchaser, in order to achieve the incorporation of SOA & IdM Platform on the AFPL.

8.2.3.1.   The Purchaser reserves the right to observe the tests and to have the Contractor perform additional tests in order to demonstrate that the system meets the contract requirements.

[SOW-376]   These potential additional tests SHALL be performed by the Contractor to the Purchaser's satisfaction before DA milestone can be accepted by the Purchaser.

[SOW-377]   DA and Software Approval Tests SHALL NOT start before the Design Documentation Package is accepted by the Purchaser.

[SOW-378]   The Contractor SHALL complete the Software Approval process for all the software products part of the solution provided by the Contractor, and obtain the Change Advisory Board approval.

[SOW-379]   The Contractor SHALL obtain Purchaser approval for ILSP as defined in SECTION 14.

8.2.3.2.   Independent Verification and Validation (IV&V).

8.2.3.2.1. The purpose of RFC testing is to provide confidence that the SOA & IdM Platform will function correctly when installed in its operational environment. IV&V and cyber-security testing are conducted in configured Purchaser Reference Environments that provide representations of the target network/security domain, including security settings, patches, network configurations and interfacing systems and services as necessary to represent the live environment as viewed from perspective the of the product, system or service being tested.

> [SOW-380] *The Contractor SHALL provide a tool and a procedure to ensure that the Reference Environment is kept up to date and in line with the Production Environment.*

8.2.3.2.2. Successful completion of this activity is a prerequisite for adding the SOA & IdM Platform Release Package to the AFPL for the target domain (each security domain has its own AFPL), which is itself a pre-requisite for authorisation to deploy the SOA & IdM Platform on to NATO networks.

> [SOW-381] *The Contractor SHALL support Independent Verification and Validation (IV&V) conducted by the NCI Agency.*

8.2.3.2.3. Release Package

> [SOW-382] *The Contractor SHALL supply the items listed in (see: 12.2.5 Operational Baseline (OBL)) for inclusion in the NCI Agency Release Package*

Serial	Item
1	System Media (system installation executables)
2	System Installation Instructions
3	System User Manual (or equivalent User Documentation)
4	Version Release Description/System Release Notes
5	Deployment Plan describing when and where application(s) will be deployed, and in which security domain.
6	End User Licence Agreement (EULA) for embedded Open Source Software (OSS)
7	Architecture Document - High-Level Operational Concept Description (NOV-1)
8	Architecture Document - Operational Node Connectivity Description (NOV-2)
9	Architecture Document - System Interface Description (NSV 1)
10	Support Plan as described in SECTION 14
11	Component Test Phase Report(s)
12	System Integration Test Phase Reports
13	Security Test and Evaluation Report
14	System Integration Test Report
15	User Acceptance Test Report
16	Requirements Traceability Matrix

Table 6: Items to be supplied for inclusion in the NCI Agency Release Package

8.2.4. Security Test and Verification

8.2.4.1. Security testing, including verification of compliance with NATO CIS security regulations, shall be planned as an integral part of the test process.

8.2.4.2. The Contractor will provide an maintain a Security Test & Verification Plan (STVP) as further described in section 10.1.3.7.

8.2.4.3. Security Implementation and Verification Procedures (SIVP)

[SOW-383] *The Contractor SHALL provide and maintain SIVP, if required, or if requested by the Purchaser. The SIVP shall consist of a set of software scripts and/or security tests (in addition to the STVP) to confirm the correct installation and configuration of the system and/or components, in compliance with the Security Documentation Package.*

8.2.5. User Acceptance Test (UAT)

8.2.5.1. The UAT consists of formal testing to determine whether or not a system satisfies user needs, requirements, and business processes and to enable the user, purchasers or other authorised entity to determine whether or not to accept the system.

8.2.5.2. UAT can be conducted in 2 phases:

a. the preliminary UAT that needs to performed before or during the Reference Test;
b. and the final UAT which is performed on the live system during Final System Acceptance Tests.

8.2.5.2.1. The responsibility assignment matrix applies to UAT, as described in Table 7: User Acceptance Test Responsibilities.

Activity	Task/work product	Purchaser	Contractor(s)	
			Test Manager	**QA Manager**
Creating test phase plan	User Acceptance Test (UAT) Plan	C	A/R	C/I
Creating test specifications	Test cases in repository	C	A/R	C/I
Creating test data	Test case	C	A/R	C/I
Implementing test environment	Test Environment	C	A/R	C/I
Reviewing test readiness	Test Readiness Review Report (TRR)	R	A/R	C
Executing test cases	Test Log, Test Defect Report	R	A/R	C/I
Creating monthly test progress report	Monthly Test Progress Report	I	A/R	I
Defect removal and reporting	Test Defect Report	I	I	I
Delivering software and instructions	Complete Build, Build/Version Number and Release/Deployment/installation Instructions	I	R/C	C
Updating Requirements Traceability Matrix	Requirements Traceability Matrix (RTM)	I	A/R	C/I
Creating test phase report	User Acceptance Test (UAT) Report	C/I	A/R	C/I

Table 7: User Acceptance Test Responsibilities

8.2.5.2.2.   Entry Criteria (User Acceptance Test Phase)

[SOW-384]   *The Contractor SHALL use test cases automation to the maximum extent.*

[SOW-385]   *The Contractor SHALL start the UAT phase after the Purchaser has reviewed, approved and signed-off the PSA and Project Test Plan.*

[SOW-386]   *The Contractor SHALL prepare the UAT Plan and UAT Specification in accordance with the Project Test Plan.*

[SOW-387]   *The Contractor SHALL plan to perform regression testing at the end of the User Tests.*

[SOW-388]   *The Contractor's regression tests SHALL be conducted using 100% automated test cases.*

[SOW-389]   *The Contractor SHALL specify sufficient test cases at the UAT phase to enable the Purchaser and users designated by the Purchaser to determine whether the SOA & IdM Platform satisfies user needs, requirements, and business processes.*

[SOW-390]   *The Contractor SHALL specify use cases, user scenarios and business processes to exercise all user roles for SOA & IdM Platform.*

[SOW-391]   *The Contractor SHALL specify test cases to exercise the functions of SOA & IdM Platform by means of use cases, user scenarios and business processes in a representative test environment.*

[SOW-392]   *The Contractor SHALL specify test cases to exercise the interactions of SOA & IdM Platform with other systems by means of use cases, user scenarios and business processes.*

[SOW-393]   *The Contractor SHALL provide the UAT Plan to the Purchaser at least three weeks before the Test Readiness Review (TRR) meeting.*

[SOW-394]   *The Contractor SHALL provide the UAT Specification to the Purchaser at least two weeks before the TRR meeting.*

[SOW-395]   *The Contractor SHALL prepare the test data and test environment in accordance with the UAT Plan and UAT Specification.*

[SOW-396]   *The Contractor SHALL review test readiness prior to execution of User Acceptance tests. The review of test readiness SHALL confirm, as a minimum, that:*

     a. *the conditions for exit from the System Test and Integration Test have been met;*

     b. *the UAT Plan and UAT Specification are completed and have been approved by the Purchaser;*

     c. *the test environment and test data are ready;*

     d. *the UAT Specification has been validated;*

     e. *the Contractor has provided sufficient training in the use of SOA & IdM Platform to Purchaser and users designated by the Purchaser;*

NATO UNCLASSIFIED

f. the Purchaser and users designated by the Purchaser are available to attend the UATs.

[SOW-397]   After successful completion of the review of test readiness, the Contractor SHALL execute User Acceptance tests in accordance with the UAT Specification and record the test execution in Test Logs and Test Defect Reports.

[SOW-398]   The Contractor's QA Manager SHALL review and sign-off all completed User Acceptance test cases and submit for the Purchaser approval.

[SOW-399]   The Contractor SHALL prepare periodic (preferably monthly) test reports of UATs.

[SOW-400]   The Contractor SHALL update the Requirements Traceability Matrix to provide traceability from tests completed to contracted requirements and provide the updated Matrix to the Purchaser in soft copy format.

[SOW-401]   The Contractor SHALL facilitate and support fifteen (15) days of user testing by the Purchaser and users designated by the Purchaser.

[SOW-402]   The Contractor SHALL record and assess any anomalies identified during user testing, and include it in UAT Report.

[SOW-403]   The Contractor SHALL prepare a complete build including source and object code, version description document (including issues and workarounds), including deployment and installation instructions.

[SOW-404]   The Contractor SHALL prepare a UAT Report on completion of User Acceptance testing.

[SOW-405]   The Contractor SHALL ensure that security testing, including verification of compliance with NATO CIS security regulations, is planned as an integral part of the test process.

8.2.5.2.3.   Exit Criteria

[SOW-406]   The Contractor SHALL exit the UAT phase after it has met the following conditions:

a. all UATs have been completed;

b. user testing by Purchaser personnel has been completed;

c. regression testing has been completed;

d. there are no uncorrected system defects with Critical or Major severity;

e. actions to resolve all open items have been agreed;

f. the UAT Report has been reviewed and signed off by the Contractor and the Purchaser;

g. a complete SOA & IdM Platform build (Release Package) is available.

[SOW-407]   The Contractor SHALL execute all agreed test cases (including security test cases) and all failures with severity "Critical",

"Major" or "Moderate" SHALL be corrected and re-tested OK, and an action plan SHALL be agreed for failures with severity "Minor" and "Cosmetic".

8.2.5.2.4. A DA (see SECTION 4.8) Milestone will be the result of a successful Request For Change approved by Change Advisory Board (CAB).

8.2.5.2.4.1 The achievement of the DA milestone is subject to the Purchaser approval. In particular, the Contractor SHALL note that:

[SOW-408] *The Contractor's System implementation activities in operational environment SHALL not start until the DA milestone is approved by the Purchaser.*

8.2.6. Provisional System Acceptance (PSA)

8.2.6.1. The acceptance by the Purchaser will signify that the Service Operation Center (SOC) is ready to provide support for the SOA & IdM Platform.

[SOW-409] *The Contractor SHALL perform for each Release that will be published in operational environment a SAT on the Purchaser's operational environment at a limited number of sites, where Release will be implemented. This typically will be after completion of an SOA and IdM Platform Wave (see also SECTION 6.8: Work Packages Introduction for Wave 1 and Wave 2 and ANNEX C).*

[SOW-410] *The Contractor's System Acceptance Test SHALL enable checking compliance with relevant SRS requirements, System Design Documentation Package (including Security Accreditation Documentation Package), and all applicable documents.*

[SOW-411] *As part of Preliminary System Acceptance Test the Contractor SHALL:*

    a. *demonstrate that all components of the SOA & IdM Platform have been integrated (including other systems, like NEDS) to meet all the SOA & IdM Platform requirements of the SRS as well as all security requirements specified in the SOA & IdM Platform Security Accreditation Documentation;*

    b. *demonstrate that the SOA & IdM Platform meets all of the interface requirements of the SOA & IdM Platform SRS and the SOA & IdM Platform Security Accreditation Documentation package;*

    c. *demonstrate the STVP for the SOA & IdM Platform.*

[SOW-412] *The Contractor SHALL support any Software Approval tests on the updated product baseline as required by the Purchaser, tests in order to achieve the listing of SOA & IdM Platform on the AFPL.*

8.2.6.2. The Purchaser reserves the right to observe the tests and to have the Contractor perform additional tests in order to demonstrate that the system meets the contract requirements.

[SOW-413] *Above mentioned potential additional tests SHALL be performed by the Contractor to the Purchaser's satisfaction before DA milestone can be accepted by the Purchaser.*

[SOW-414] *The Contractor SHALL NOT start DA and Software Approval Tests before the Design Documentation Package is accepted by the Purchaser.*

[SOW-415] *The Contractor SHALL conduct the DA, and in compliance with the overall System Testing Process (see SECTION 8: Testing and Acceptance).*

[SOW-416] *The Contractor SHALL successfully conduct Software Approval Tests as defined in SECTION 8.2, and in compliance with the overall System Testing Process detailed in SECTION 10.*

[SOW-417] *The Contractor SHALL successfully implement the SOA & IdM Platform Reference System with all its components as defined in SECTION 6.6.2, in compliance with the processes described in SECTION 7: System Engineering and Integration.*

[SOW-418] *The Contractor SHALL complete the Software Approval process for all the software products part of the solution provided by the Contractor and the CAB has given its approval.*

[SOW-419] *The Contractor SHALL deliver the ILSP as defined in SECTION 14: ILS, and the ILSP SHALL have been approved by the Purchaser.*

[SOW-420] *The Contractor SHALL complete the delivery of Allocated and Product Baselines (ABL and PBL) as defined in SECTION 12: Configuration Management.*

8.2.7. Site Acceptance Test (SAT)

[SOW-421] *The Contractor SHALL develop a SAT Plan, which SHALL be approved by the Purchaser.*

[SOW-422] *After getting the authorisation to deploy the Contractor SHALL execute SAT at every Site (if required) during the implementation.*

[SOW-423] *The Contractor's SAT SHALL be arranged, so that the Purchaser can witness Test at each deployment location.*

8.2.7.1. PSA and FSA (see: Milestones SECTION 4.9 and 4.10) respectively will be the result of a successful System Acceptance Test.

8.2.8. Final System Acceptance (FSA)

8.2.8.1. FSA will be reached when all the sites will have been accepted.

[SOW-424] *The Contractor SHALL conduct the DA, and in compliance with the overall Testing Process.*

[SOW-425] *The Contractor SHALL successfully conduct Software Approval Tests as defined in SECTION 8: Testing and Acceptance, and in compliance with the overall System Testing Process.*

[SOW-426] *The Contractor SHALL successfully implement the SOA & IdM Platform with all its components as defined in SECTION 6.6.2 Reference System Installation and SECTION 7: System Engineering and Integration, in compliance with the processes described in SECTION 7: System Engineering and Integration.*

8.3. System Test Documentation Package (STDP)

[SOW-427] The Contractor SHALL develop and deliver the STDP and keep it up to date, as the supporting documentation for each test session.

[SOW-428] The Contractor SHALL ensure that STDP comprises the following documents:

    a. the Test and Acceptance Plan (TAP);

    b. the STVP;

    c. SIVP;

    d. any submitted test Waivers (together with supporting material);

    e. the System Version Definition Document (SVDD);

    f. the description of the Test Bed with complete list of Configuration Items (CI):

        i. hardware and software documentation;

        ii. services installed;

        iii. all configuration information;

    g. the test procedures;

    h. the test reports (with issues);

    i. the RTM updated with test related information;

    j. the results of any dry-runs performed by the Contractor as a preparation for the upcoming test session.

The Purchaser will review the Contractor's STDP for correctness, completeness and acceptance. Specifically, the Purchaser reserves the right to reject any test Waiver.

[SOW-429] The Contractor MAY propose to combine any complementary (i.e. non-overlapping) test documentation package (e.g., the STDP might be complementary to the SAT Packages).

8.3.1.   System Build Description

8.3.1.1.   The build contains the standalone SOA & IdM Platform software artefact(s) that can be run on a computer. The complete build contains all the SOA & IdM Platform software artefacts and the Release/Deployment/Installation Instructions. The build/version number assigns either a unique name or a unique number to a unique state of the SOA & IdM Platform computer software.

8.3.2.   Test Specifications

[SOW-430] The Contractor SHALL design, develop, execute and maintain the SOA & IdM Platform test cases. The test cases SHALL be described and/or referenced in each Sprint Test phase.

[SOW-431] The Contractor SHALL format the test cases such that these can be handed over to the Purchaser in a format that is compatible with the Purchasers Tools (TestRail).

[SOW-432]   The Contractor SHALL use a Test Management System accessible by the Purchaser.

[SOW-433]   The Contractor SHALL propose which test should be automated with automated verification conditions. If the automated test will not be performed, the Contractor SHALL justify to the Purchaser lack of automation and obtain its approval.

8.3.3.   Test and Acceptance Plan (TAP)

[SOW-434]   The Contractor SHALL provide and maintain the TAP.

[SOW-435]   Within the TAP, the Contractor SHALL define his overall concept of testing and accepting of the SOA & IdM Platform deliverables, and SHALL ensure that above is in line with SAT, SBT, QBT and other testing requirements.

[SOW-436]   The Contractor SHALL propose a testing process which should use automated testing to the maximum applicable extent.

[SOW-437]   The Contract SHALL estimate the target automation level and provide explanation on what and why cannot be automated.

[SOW-438]   In the TAP, the Contractor SHALL define a set of test activities to verify each deliverable's compliance with the contractual requirements, to demonstrate its operational suitability and to evaluate its performance to establish benchmarks for future enhancements and capture above in RTM.

[SOW-439]   In the TAP, the Contractor SHALL provide the schedule for the provision of the TAP deliverables and detail the conduct of testing (test suites, test scripts, conduct of tests, test reports, etc.).

[SOW-440]   In the TAP, the Contractor SHALL indicate which requirements from the RTM are being addressed in each test to be executed.

[SOW-441]   In the TAP, the Contractor SHALL detail which tests are to be conducted during the specific test stage.

8.3.4.   System Version Definition Document (SVDD)

[SOW-442]   The Contractor SHALL ensure that the SVDD includes the following:

    a. list of differences between this and the previous System version including documentation;

    b. list of capabilities of this System version;

    c. guidelines on how to install this System version;

    d. breakdown of the system into CIs and provision of accurate identification information for every CI, in accordance to the CMDB (see SECTION 12.4).

8.3.5.   Test Acceptance Criteria

[SOW-443]   The Contractor SHALL ensure that the TAP is issued to the Purchaser at least one (1) month before the delivery of the Test Suites and Test Scripts.

[SOW-444]   The Contractor SHALL provide Test Suites and Test Scripts to the Purchaser at least one (1) month before the planned start of testing.

[SOW-445]   The Contractor SHALL ensure that Test Acceptance Criteria provide clear evidence that the SoW requirements are fully met.

[SOW-446]   The Contractor SHALL take Purchaser's comments into account as part of the update of the Test Suites prior to their execution.

[SOW-447]   The Contractor SHALL formally organise testing once the Test Suites and Test Scripts have been approved by the Purchaser.

[SOW-448]   The Contractor SHALL ensure that Testing Process verifies that the quality parameters listed in SRS section 4 Non-functional Requirements.

[SOW-449]   The Contractor SHALL have the overall responsibility for meeting the SOA & IdM Platform testing requirements and conducting all related activities (except for the tests executed by NCI Agency staff and/or other Purchaser's Contractors). This includes the development of all tests and associated documentation required under this Contract, the conduct of all testing and the evaluation and documentation of the tests results.

8.3.5.1.   The Purchaser reserves the right to monitor and inspect the Contractor's test activities to verify their compliance with the requirements set forth in this Contract.

8.3.5.2.   Each test will only be declared 'PASSED' if the entirety of the expected results were obtained when running the test.

[SOW-450]   The Contractor SHALL use a common and verified Test Management System in coordination with the Purchaser, create TAP and SHALL provide the outputs of the Test Management System as required.

[SOW-451]   The Contractor SHALL ensure that Testing is performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.

8.4.   Management of test activities

8.4.1.   Requirements Traceability Matrix (RTM)

[SOW-452]   The Contractor's RTM SHALL demonstrate that the RTM is implemented as requested in Section 7.4.2.2.3 Requirements Traceability Matrix (RTM).

8.4.2.   Test Reports

[SOW-453]   The Contractor SHALL record the results for each test called for in the Test Plan in a Test Log (also known as Test Execution Log).

[SOW-454]   The Contractor SHALL summarise the evaluation process in the Test Report and submit for acceptance by the Purchaser.

[SOW-455]   The Contractor's Test Report SHALL indicate the result of the Test Cases execution.

[SOW-456]   The Contractor SHALL provide the following information with test report:

    a. reference to Test Case/Suite;

    b. date when the test was run;

    c. test result ("Pass", "Fail", "Not run"); if "Fail", identification of the associated problem report;

    d. any annotations by the Purchaser's representative;

    e. comments;

    f. contractor representative signature (Test Suite);

    g. purchaser representative signature;

    h. identification of the PBL under test;

    i. identification of the data set used to conduct the test session;

    j. description of the system under test and of the configuration of the testbed.

[SOW-457]   The Contractor SHALL submit Test Report cover sheet which clearly shows how many tests passed, failed, or were not run.

[SOW-458]   Where the Purchaser or his representative has witnessed the testing, the Contractor SHALL make appropriate annotations on each page of the test results to ensure that the test report is a true record of test activities and results as witnessed by the Purchaser, and the whole test report SHALL be signed by the Contractor representative and by the Purchaser representative on completion of that testing.

[SOW-459]   Each original Contractor's test report plus one copy SHALL be distributed to the Purchaser for acceptance within 10 (ten) working days after the completion of the test.

8.4.2.1.   Test Session Report

[SOW-460]   Upon completion of the test session, the Contractor SHALL provide the updated version of the STDP and a System Test Session Report.

8.4.3.   Test Progress Report

[SOW-461]   The Contractor SHALL provide a Test Progress Report.

8.4.4.   Test Reviews

[SOW-462]   The start of any test session SHALL be subject to the Purchaser approval. All entry criteria SHALL be reviewed during a TRR meeting to be held before the test session starts.

[SOW-463]   The end of any test session SHALL be subject to the Purchaser approval. All exit criteria SHALL be reviewed during a Status Test Review (STR) meeting to be held after the execution of a test session.

8.4.5. Test Defect Categorisation

[SOW-464] *Should a failure occur during testing, a failure report SHALL be raised by the Contractor and a preliminary investigation SHALL be immediately carried out in order to classify the failure according to its severity and its priority following the definitions in Table 8: Definitions for Defect .*

Category	Definition
Severity	*The severity of a failure is the degree of impact that the failure has on the development or operation of a component or system.* *The severity of the failure shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached the Purchaser's PM will set the severity.*
Priority	*The priority of a defect defines the order in which defects SHALL be resolved.* *The priority of the defect shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached the Purchaser's PM will set the priority.*

Table 8: Definitions for Defect Categorisation

8.4.5.1.　　Severity

[SOW-465]　*According to their severity, failures SHALL be classified as one of the following in Table 9: Classification of defects based on severity:*

Severity Class	Description
Critical	A major failure for which a work around does not exist. The defect totally prevents the system from performing operational processes and/or causes unrecoverable data loss. Applies to conditions under which one or more components are totally inoperative and jeopardize the ability to continue using the system. This condition generally is characterized by a complete or catastrophic system failure and requires immediate restoration or correction.
Major	Test executed during this situation would likely require retesting when the blocking defect is fixed. The test execution schedule is likely to be compromised. A significant failure that causes severely impaired functions but does not prevent operational processing. Applies to conditions under which one or more components are partially inoperative, but are still usable by the users. A workaround might be available but it may require manual intervention.
Minor	A functional failure that causes a specific aspect of the system to fail. There is a reasonably satisfactory work around which can be used during normal operations for a limited period of time. The system may be released provided the defect and work around is documented. Applies to conditions under which one or more components are usable with limited functions, but creates a manageable situation with respect to the normal operations. A work around is available and does not require any manual intervention.
Cosmetic	A functional failure, which causes only slight impairment and for which a work around exists. Applies to conditions under which one or more components are usable and the conditions do not adversely affect overall system operation. These problems are those resulting in a minor failure that minimally impacts the process.

Table 9: Classification of defects based on severity

8.4.5.2.   Priority

[SOW-466]   *The Contractor SHALL ensure, that according to their priority, failures are classified as one of the following in Table 10: Priority Classes for Defect Classification:*

Priority Class	Description
Urgent	*The defect shall be resolved as soon as possible.*
Medium	*The defect shall be resolved in the normal course of development activities. It can wait until a new build or version is created.*
Low	*The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.*

Table 10: Priority Classes for Defect Classification

8.4.6.   Tests status meetings

[SOW-467]   *Throughout any test session the Contractor SHALL organise and conduct Tests Status Meetings with the Purchaser as listed in Table 11: Test Status Meetings below:*

Test Status Meeting	Description
Daily	*At the beginning of the working day as an introduction to the testing activities of the day and at the end of each working day to wrap-up the day activities.*
Weekly	*The results of the tests run to date;* *Any new issues or off-specifications raised;* *Any adjustments to the schedule of test activities within the test session.*

Table 11: Test Status Meetings

8.4.7.   Test Waivers

[SOW-468]   *The Contractor MAY request a Test Waiver, if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts.*

[SOW-469]   *The Contractor SHALL request a Waiver on any subset of the above principles by providing sufficient arguments, which state the benefits for the Purchaser. If the Purchaser grants the waiver, the Contractor SHALL execute the Testing in accordance with the Waiver.*

[SOW-470]   *The Contractor SHALL certify that the Test Environment to be implemented is identical to that which was originally used for testing of components being in scope of a Waiver, or advise the Purchaser of design changes which affect form, fit or function.*

8.4.7.1.   The Purchaser, after review of such changes and their impact, reserves the right to require test and certification of the modified equipment at no additional cost to the Purchaser.

[SOW-471] *The Contractor SHALL record and log all Waiver requests along with their resolution.*

8.5. Operational Acceptance Criteria (OAC)

8.5.1. Operational Acceptance Criteria (OAC) have been defined to support the handover of the SOA and IdM Platform for operation & maintenance [SHAPE SH/CCD J6/SM FCIS/163/17-317951, 2017]. Whereas a number of criteria are not an immediate Contractor responsibility, awareness is beneficial to the project as a whole. In some cases criteria will need to be demonstrated through certain deliverables and at different stages of testing.

[SOW-472] *The Contractor SHALL take the following actions into account in their activities and deliverables to meet the criteria identified in the OAC:*

IFB_CO-14176-SOA-IDM

OAC ID	Source	Reference	Action
T1-T2	SOW	SECTION 14.7.2	Training Need Assessment SHALL fulfil criteria
T3	SOW	SECTION 14.7.4	Training Materials SHALL fulfil criteria
T4	SOW	SECTION 14.7.3	Training Plan SHALL fulfil criteria
MP01-MP06, MP09	SRS	SECTION 3	Functionality SHALL be demonstrated through SAT
MP07	SOW	SECTION 4.2	Implementation SHALL be demonstrated through final SAT
MP08	SOW	SECTION 8 and SECTION 10	Covered through testing and security accreditation. Contractor SHALL support Purchaser.
MP10, MF01	SRS	SECTION 2	Key SOA & IdM Platform (design) principle, but will also need to be demonstrated through support to pilot cases (WP 6.1 and WP 6.2)
MP11	SOW	SECTION 8	Resolution of open issues SHALL be demonstrated through final SAT
MC02	SRS	SECTION 4.9	Compliance to standards SHALL be demonstrated through SAT
MC03	SOW	SECTION 14.4	Criteria SHALL be addressed in the Total Cost of Ownership Analysis
MQ02	SRS	SECTION 4 (Non-functional requirements)	ITM service levels SHALL be taken into account in demonstrating availability
MQ04	SOW/SRS	SOW SECTION 8 and SRS NATO Bi-SC AIS Deployable CIS requirements	Special test cases SHALL be developed to demonstrate correct operation on Deployable CIS
MQ05	SOW	SECTION 4	Disaster Recovery Plan SHALL fulfil criteria
MF02	SRS	SECTION 4 (Non-functional requirements)	Special test cases SHALL be developed to demonstrate scalability and capacity requirements
MF03	SOW	SECTION 4 (Scope)	Will be achieved by deployment according to scope, and meeting related non-functional requirements.

MS01	SOW	SECTION 14.7.5	To achieve PSA (Waver 1 and Wave 2) required personnel SHALL have been trained
MU01	SOW	SECTION 14.7.5	Training Assessment and Evaluation SHALL fulfill criteria
MU02	SOW	SECTION 8.2.5	The UAT SHALL demonstrate criteria
MU03	SOW/SRS	SOW SECTION 7.4 and SRS	Criteria SHALL be addredded in SDS
MU04	SOW	SECTION 7	Deploying the capability SHALL have mimimal impact to operation or business continuity
MS01-MS03	SoW	SECTION 10	Contractor to support accreditation process
I1-I4	SRS	SECTION 4 (Non-functional requirements)	Meeting interoperability criteria is demonstrated through SAT

Table 12: Activities and deliverables to fulfil the OAC

SECTION 9: SITE SURVEYS

9.1. Introduction

9.1.1. The purpose of the Site Survey is to gather all information of interest in view of the preparation, installation, configuration, on-site testing and support. This section outlines the requirements applicable for site surveys.

9.1.2. The *Site* should be considered as a virtual site, as SOA & IdM Platform will be installed on existing system: IaaS. All sites are described in SECTION 4.2.3/ [SOW-28] and SECTION 7.4.1: Design activities/ [SOW-277].

> [SOW-473]   *The Contractor SHALL respect below requirements for every site survey.*

> [SOW-474]   *For each site survey, the Contractor SHALL conduct site survey preparatory work, visit each site subject to site survey, survey relevant facilities, interview site personnel, and collect data to support project activities.*

> [SOW-475]   *The Contractor SHALL ensure coherence between site survey results and project documentation (e.g. System Design Documentation Package, PIP) at any time. The Contractor SHALL update project documentation accordingly.*

9.2. Site Survey Preparatory work

9.2.1. Site Survey Workbook (SSWB)

> [SOW-476]   *The Contractor SHALL prepare a SSWB of checklists, fill-in forms, installation sketches, contact information, installation specifications, and site data to be collected by the Contractor during the site survey, and any other documentation required to perform site surveys.*

> [SOW-477]   *The Contractor's SSWB SHALL be available for Purchaser review and comment before the first site survey, and SHALL be maintained and updated as necessary during the site survey process.*

> [SOW-478]   *Upon acceptance of the SSWB by the Purchaser, the Contractor SHALL distribute the Site Survey Workbook to the Site(s) for preparation of the Site Surveys. This approach will enable a better preparation by the sites.*

9.2.2. Agenda

> [SOW-479]   *The Contractor's site survey(s) and installation sequence and dates reflected in the Project Implementation Plan SHALL be co-ordinated by the Contractor with the Purchaser and the Site POCs to accommodate site-specific requirements, exercises, holiday periods, and other considerations.*

9.2.3. Introductory Briefing:

> [SOW-480]   *The Contractor's Introductory Briefing SHALL be an introduction to the SOA & IdM Platform project outlining the system requirements, describing the system functionalities, the sites to be implemented, the project timelines, the goals and objectives and agenda of the Site Survey process, and the notional implementation*

identified for the surveyed site and to be refined through the Site Surveys activities.

[SOW-481]   *The Contractor's Introductory Briefing SHALL NOT assume other than basic knowledge of the project by the site personnel.*

9.3.   Survey of the site facilities

[SOW-482]   *During the Site Surveys activities the Contractor SHALL determine the necessary installation preparations and support arrangements and collect all system implementation-relevant information. This SHALL include:*

a.   *identification of the relevant for SOA & IdM Platform Administrators, Operators, and more generally all POCs;*

b.   *identification of existing business processes (for both physical access control and logical access control), and how those processes will integrate with SOA & IdM Platform.*

c.   *analysis of the training needs (see also para 14.7 Training);*

d.   *identification of any input (item of equipment, documentation, information) or work required from the Purchaser and from the Site with indication of suspense date;*

e.   *identification of the facilities where the SOA & IdM Platform will have to be installed, together with each facility's zone level (see [NAC AC/322-N(2014)0158-ADD3, 2015]);*

f.   *identification of any potential TEMPEST-related requirement for the SOA & IdM Platform equipment (see [NAC AC/322-N(2014)0158-ADD3, 2015]);*

g.   *list of all system CIs (nature and quantities) to be installed in the site;*

h.   *update of the user list;*

i.   *identification of the tools, policies and procedures in use at Purchaser facilities, in order to determine the integration requirements with the ITSM tools.*

9.4.   Site specific-requirements

9.4.1.   Notwithstanding the requirements related to storage and backup solutions, some Purchaser locations have site-specific equipment (e.g. specific brand names for servers), which may differ from the project baselines at a site, to reduce operations and maintenance costs or to use existing facilities in the most efficient manner.

[SOW-483]   *The Contractor SHALL determine if site-specific equipment is required at a location as part of any Site Survey performed under this Contract.*

[SOW-484]   If site-specific equipment is required, the Contractor SHALL issue an Engineering Change Proposal (ECP).

[SOW-485]   In the ECP, the Contractor SHALL identify any requirements of the SOA & IdM Platform System Design Specification it believes will not be met due to differences between the site-specific equipment and the standard baseline.

[SOW-486]   If these exceptions to the SOA & IdM Platform System Design Specification are accepted by the Purchaser and incorporated into the Contract as formal amendments, the Contractor is not required to demonstrate, as part of its Site Activation work, that the associated System Design Specification requirement has been met. In such a case, the Contractor SHALL update the System Design Specification to reflect site-specific situations.

[SOW-487]   The Contractor SHALL identify all facilities support, including modifications or additions, required. After coordination with the Purchaser, this notification SHALL be in the form of a letter to the site POC, with a copy to the Purchaser, accompanied by engineering drawings, checklists, or any other supporting information. Facilities support issues that represent Medium or High risk items SHALL be reflected in the Risk Log.

9.5. Outcomes

[SOW-488]   The Contractor SHALL produce and deliver a Site Survey Report for each site, detailing its findings from the site survey, identifying all required Purchaser and Contractor actions and follow-on activities, to prepare for, conduct, or support SOA & IdM Platform installation and activation, and identifying the type of training courses required and the number of Purchaser staff to be trained for each course.

[SOW-489]   The Contractor's Site Survey Reports SHALL be provided within one week after the respective Site Survey is completed.

[SOW-490]   At minimum, the Site Survey Report SHALL include:

   a. Installation & Activation:

      i.   Stakeholders communication;

      ii. System installation requirements;

      iii. Schedule of installation activities;

   b. Training requirements;

   c. Logistics:

      i.   available system location & and space;

      ii. technical infrastructure;

      iii. delivery details;

   d. Local Security Accreditation Authority documentation:

      i.   Contact Details of security responsibilities;

> ii. *Interconnection details;*
>
> iii. *Network diagrams;*
>
> e. *Register for all findings that require modification of the site infrastructure or change of the agreed implementation scope. For each of the changes the Contractor SHALL produce a formal change proposal;*
>
> f. *For each out of scope item that requires either technical support or procurement activity, the Contractor SHALL offer a proposal to the Purchaser with his recommended solution;*
>
> g. *Site diagram that SHALL be used as the basis for the "As Built" Documentation and used in the installation of the site.*
>
> [SOW-491] *After all site survey the Contractor SHALL organise whole sites survey out-brief.*

9.5.1. The Purchaser will provide the Contractor with the exact shipment addresses and NATO POC.

SECTION 10: SECURITY

10.1. Security Accreditation

10.1.1. Introduction

10.1.1.1. The SOA & IdM Platform must achieve security accreditation in order to be granted the authority to go live. To achieve this, the system will need to go through a Security Accreditation process and obtain the approval from Security Accreditation Authorities to use SOA & IdM Platform on all NATO networks/security domains in scope of this contract. The SOA & IdM Platform will need to demonstrate compliance with the NATO relevant Security Policy and supporting directives.

[SOW-492] The Contractor SHALL be responsible to follow, implement and conform to the Pre-Accreditation Activities, and the Accreditation Process as defined and documented in [NAC AC/35-D/2005-REV3, 2015] and in SOA and IdM Platform SAP [NCIA NSAP SOA & IdM, 2017]in order to obtain the required security accreditation statement(s) for the SOA & IdM Platform during each phase of the SOA & IdM Platform project.

[SOW-493] The Contractor SHALL be required to carry out and meet the terms of the Security Accreditation Authority to perform any Post-Accreditation activities, such as periodic re-assessments of the security risks and periodic inspections up to the time of handover of the SOA & IdM Platform to the CIS Provider.

[SOW-494] The Contractor SHALL obtain Approval for Testing (AfT) and (Interim) Security Accreditation ((I)SA) statements which are necessary during the stages of the implementation, tests and trials of the SOA & IdM Platform project. Achieving ISA does not diminish the requirement for the Contractor to obtain the full Security Accreditation statement.

10.1.2. Security Accreditation Authority (SAA)

10.1.2.1. The overall SAA for the SOA & IdM Platform is the NATO CIS Security Accreditation Board (NSAB). Local SAA's will be involved in accreditation of the sites of SOA & IdM Platform. Their role will be to ensure the NSAB recommendations are implemented and ensure that any agreed local (site specific) configurations are applied and/or implemented.

10.1.2.2. Coordination with the SAAs will be conducted by the Purchaser. The Contractor may be invited to provide briefings for the meetings with the SAAs.

[SOW-495]   *The Contractor SHALL carry out the necessary work as well as to implement the advice, instructions and changes provided by the Security Accreditation Authority and local Security Accreditation Authorities.*

10.1.3. Security Accreditation Documentation

10.1.3.1. The achievement of the SOA & IdM Platform security accreditation will require a prescribed set of security documentation to be produced, using security accreditation documentation templates. The templates will be made available to the Contractor after the CAW.

[SOW-496]   *The Contractor SHALL produce security accreditation documentation and/or provide inputs to documents in support of the SOA & IdM Platform security accreditation, as detailed in Table 13, below.*

[SOW-497]   *The Contractor SHALL produce all security accreditation documentation or inputs to documents using security document templates and/or generic documents provided by the Purchaser. These will be provided after the CAW.*

[SOW-498]   *The documentation to be developed to support the SOA & IdM Platform security accreditation process is listed below. The following subsections describe these documents in detail. The documentation set is described in SOA and IdM Platform SAP [NCIA NSAP SOA & IdM, 2017] and includes:*

    a. *Communication Information System (CIS) description that includes the Security Mechanisms (SMs)*

    b. *Security Accreditation Plan (SAP);*

    c. *Security Risk Assessment (SRA) Reports (separate for ON and PBN);*

    d. *Delta System-specific Security Requirement Statement (SSRS) (dSSRS) (separate for ON and PBN);*

    e. *Security Operating Procedures (SecOPs); generic SecOPs will be providedby the Purchaser after CAW;*

    f. *Security Test and Verification Plans (STVP) (separate for ON and PBN);*

    g. *Security Test and Verification Report (STVR) template;*

h. *Site-specific documentation:*

i. *Annex to delta SSRS (if required by the Local Security Accreditation Authority);*

ii. *System Interconnection Security Requirements Statement (SISRS; if required by the Local Security Accreditation Authority);*

iii. *Local SecOPs (if required by the Local Security Accreditation Authority);*

iv. *Local STVP (if required by the Local Security Accreditation Authority); and*

v. *Test Report (mandated for each site).*

10.1.3.2. A SAP has been developed by the Purchaser and approved by the SAA. This document will be made available to the Contractor after the CAW. The SAP will be maintained by the Purchaser during the project life-cycle. Any SAP update will be presented to the SAA for its approval. Further security accreditation activities will be dependent on the decisions of the NSAB regarding the SAP.

[SOW-499] *The Contractor SHALL be responsible to implement the activities described in the SAP as approved by the Security Accreditation Authority.*

10.1.3.3. An initial System Description for the SOA & IdM Platform has been developed by the Purchaser and endorsed by the SAA. This document will be made available to the Contractor after the CAW, together with the CIS description template [NTEMP-3]. The System Description is the first document related to security accreditation to be updated after the CAW. It will contain all relevant information taken from the System Design Documentation Package and adapted to SAA needs.

[SOW-500] *The Contractor SHALL update the initial CIS description document based on the CIS description [NTEMP-3] provided by the Purchaser, maintain the CIS description during the project, including all relevant information taken from the System Design Documentation Package as required to understand the content of the CIS description document.*

[SOW-501] *The Contractor SHALL conduct SRA, separate for ON and PBN, and develop the SRA Reports in accordance with Guidelines for Security Risk Risk Management of Communication and Information Systems (CIS) [NAC AC/35-D/1017 –REV3, 2017]. These Reports SHALL address risks specific for SOA and IdM Platform not covered in the formal SRAs for ITM (conducted by the Purchaser) and risks related to modern CIS technologies.*

[SOW-502] *The Contractor SHALL use the NATO template "SRA Report (PILAR) Template" [NTEMP-4] to document the results of the SRAs.*

[SOW-503] *The Contractor SHALL identify areas of the SOA & IdM Platform requiring safeguards and countermeasures to comply with NATO Security Policy and supporting directives. The decision on specific security mechanisms will be based on evidence and results produced by the Security Risk Assessment.*

[SOW-504]   *The Contractor SHALL consider any change to be within the technical and financial scope of this Contract whenever the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components; no ECP shall be generated.*

[SOW-505]   *The Contractor SHALL raise an ECP whenever the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand.*

10.1.3.4.   dSSRSs, separate for ON and PBN, will be developed, as directed by the SAA, in form of "delta" to the Community Security Requirement Statement (CSRS) for NATO SECRET, NATO RESTRICTED Automated Information System provided by IT Modernization [ITM NS AIS CSRS, 2017]/[ITM NR AIS CSRS, 2017]. The dSSRS template [NTEMP-5] and the applicable CSRSs will be provided by the Purchaser after the CAW.

[SOW-506]   *The Contractor SHALL produce a dSSRS to include the minimum levels of security deemed necessary in addition to the security measures in Automated Information Systems for the NATO SECRET, NATO RESTRICTED and NATO UNCLASSIFIED environments, provided by IT Modernization, in order to counter the risks identified in the SOA & IdM Platform SRAs.*

[SOW-507]   *The Contractor SHALL produce the SOA & IdM Platform dSSRS using the NATO dSSRS Template [NTEMP-5] and following the guidance on SRS development [Ref. NAC AC/35-D/1015-REV3, 2012].*

[SOW-508]   *The Contractor SHALL ensure that each security requirement in the dSSRS has a unique identifier which is cross-referenced to the security mechanism addressing the requirement.*

[SOW-509]   *The Contractor SHALL determine whether each security mechanism is mandatory or recommended. Note: final decision which security mechanisms is mandatory belongs to the CIS Operational Authority (CISOA) and the SAA.*

10.1.3.5.   The Security Architecture needs to adhere to the NATO Security Architecture Methodology (NSAM) mainly as to:

a. Crosscheck with and show adherence to the NATO CIS Security Reference Baseline, whereas relevant

b. Develop the Security Mechanisms in scope, whether implemented by the project or received by the Purchaser, by identifying the pertinent security countermeasures

c. Anchor the identified Security Mechanisms to the business requirements/objectives of the project as to justify scope and cost of the security measures

d. Assign Security Mechanisms to systems in scope and link them with services in scope, either enabled by the project or received from the Purchaser

e. Maintain traceability of the use of Security Mechanisms throughout the security architecture and design development,

implementation, testing, operation and maintenance and decommissioning

f. Reflect the use of the Security Mechanisms in the Security Accreditation Documentation as directed by the NATO CIS Security Accreditation Board and other NATO security-related governing body

[SOW-510] *The Contractor SHALL produce the Security Architecture according to the guidelines stated in the appropriate CIS Security Reference Baselines (NATO SECRET CIS Security Reference Baseline [NS CIS Security Reference Baseline, 2017] for ON; NR Reference Baseline for PBN provided in the [ITM NR AIS CSRS]) and per the guidance received by the NATO IT and Security Architect.*

10.1.3.6. Security Operating Procedures (SecOPs) will be developed for the centrally managed the SOA & IdM Platform. Either, if available, the ITM SecOPs, or otherwise the Generic NS AIS SecOPs [2014] will be made available to the Contractor after the CAW.

[SOW-511] *The Contractor SHALL produce the Security Operating Procedures (SecOPs) for the SOA & IdM Platform system according to the guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for CIS [NAC AC/35-D/1014 –REV3, 2012], using either, if available, the ITM SecOPs or otherwise the Generic NS AIS SecOPs [2014].*

10.1.3.7. The STVP defines a complete sequence of steps to be followed to prove that the security mechanisms designed into the SOA & IdM Platform enforce the security requirements identified in the SOA & IdM Platform SRAs. It will be developed by Contractor. The Security Test and Verification Plan template for either, if available, ITM or otherwise the NS AIS [NTEMP-8] will be made available to the Contractor after the CAW.

[SOW-512] *The Contractor SHALL produce the STVPs for the SOA & IdM Platform, separate for ON and PBN, using the NATO template for either, if available, ITM or otherwise the NS AIS [NTEMP-8], defining the complete sequence of steps to be followed to prove that the security mechanisms designed into the SOA & IdM Platform enforce the security requirements identified in the SOA & IdM Platform SRAs.*

[SOW-513] *The Contractor SHALL ensure every security test is cross-referenced to the corresponding security requirement from dSSRSs as well as to the tested security mechanisms.*

[SOW-514] *The Contractor SHALL ensure all security mechanisms of the SOA & IdM Platform are planned for testing.*

10.1.3.8. The STVR provides results of all security tests specified in the STVP. Security Test and Verification Report will be generated by Contractor. The Security Test and Verification Report template [NTEMP-6] will be made available to the Contractor after the CAW.

[SOW-515] *The Contractor SHALL generate a Security Test and Verification Report, containing results of all security tests specified in the STVP, using the Security Test and Verification Report template [NTEMP-6].*

[SOW-516] *The Contractor SHALL ensure security test identifiers are preserved in the Report as defined in the STVP.*

10.1.3.9. The SISRS is required for each of the interconnections between security domains served by SOA & IdM Platform. This includes for example NATO RESTRICTED to NATO UNCLASSIFIED. The SISRS template [NTEMP-7] will be made available to the Contractor after the CAW.

[SOW-517] *The Contractor SHALL produce SOA & IdM Platform SISRS for each of the interconnections between security domains served by SOA & IdM Platform, using the NATO SISRS template [NTEMP-7].*

10.1.4. Other initial security documentation provided by Purchaser

10.1.4.1. Existing security documentation for the NS AIS will be made available to the Contractor after the CAW.

10.1.4.2. Existing security documentation for ITM will be made available to the Contractor after the CAW.

10.1.5. Security Documentation Review

10.1.5.1. All documents for security accreditation will be subject to Purchaser and SAA review and approval.

10.1.5.2. The Contractor should expect a number of review rounds per document before it will be approved, which makes security accreditation an iterative and sometimes lengthy process.

[SOW-518] *The Contractor SHALL ensure documents or inputs are delivered within 1 month of Design acceptance.*

[SOW-519] *The Contractor SHALL ensure implementation plans are flexible to take account of the time required for accreditation.*

[SOW-520] *The Contractor SHALL produce Security Documentation under the close supervision and guidance of Purchaser's specialists.*

[SOW-521] *The Contractor SHALL submit Security Documentation to the Purchaser for review before submission to Security Accreditation Authority for approval.*

[SOW-522] *The Contractor SHALL take into account any comments from the reviewers and Security Accreditation Authority and shall update Security Documentation as many times as necessary in order to gain Security Accreditation Authority approval.*

10.1.6. Responsibilities

10.1.6.1. Table below summarises responsibilities related development of each document required for security accreditation process.

10.1.6.2. Column "Baseline/Guidance" lists available templates, relevant NATO Security Directives and Guidance, and similar documentation existing NATO CIS which can be used as an example or initial input.

[SOW-523]   *The Contractor SHALL undertake the work identified in the column 'Contractor Responsibility' in Table 13 below:*

Document	Baseline/Guidance	Contractor Responsibility (*The Contractor SHALL*:)	Purchaser Responsibility
Generic documentation			
SAP	The SAP needs to be updated to the latest approved SAP template	None	Update SAP Coordination with the Security Accreditation Authority
CIS description	CIS description template	Provide update to the system design described in initial CIS description, based on the Contractor's design and adjust it to the template	Provide template and guidance to the Contractor Review Coordination with the Security Accreditation Authority
SRAs (for ON and PBN)	SRA for ITM (ON part) SRA for ITM (PBN part) [AC/35-D/1015] [AC/35-D/1017] [NTEMP-4] Tool for formal SRA:NATO PILAR NATO PILAR User Guide NR CIS Security Reference Baseline in [ITM NR AIS CSRS, 2017] [NS CIS Security Reference Baseline, 2017]	Conduct and maintain SRAs Address additional technical security requirements from the SRAs (if not already included in system design)	Provide guidance to the Contractor Provide SRA Report (PILAR) Template Provide the relevant NATO CIS Security Reference Baselines Review SRA Report provided by the Contractor Coordination with the Security Accreditation Authority

Document	Baseline/Guidance	Contractor Responsibility (*The Contractor SHALL*:)	Purchaser Responsibility
dSSRSs (for ON and PBN)	[AC/35-D/1015] [ITM NS AIS CSRS] [ITM NR AIS CSRS, 2017] [NTEMP-5]	Provide dSSRSs, separate for ON and PNB.	Provide template and guidance to the Contractor Review dSSRSs provided by the Contractor Coordination with the Security Accreditation Authority
Security Architecture	AC/35-D/2004-REV3 [NS CIS Security Reference Baseline, 2017] NR CIS Security Reference Baseline in [ITM NR AIS CSRS, 2017]	Provide the Security Architecture Demonstrate adherence to the NATO CIS Security Reference Baseline Ensure the Security Mechanisms enable traceability throughout the project lifecycle and to provide assurance that security is rightly sized to the project scope	Provide guidance on the NATO Security Architecture Methodology and relevant templates Provide guidance on provision of NATO IA Products, whether in scope for the project or received from the Purchaser.
SecOPs	[AC/35-D/1014] [NS AIS SecOPS, 2014], [NR AIS Adm SecOPs, 2017] or ITM equivalent if available	Develop SecOPs for centralised management of the SOA & IdM Platform.	Provide generic SecOPs Review SecOPs provided by the Contractor Coordination with the Security Accreditation Authority

Document	Baseline/Guidance	Contractor Responsibility (*The Contractor SHALL*:)	Purchaser Responsibility
STVPs for ON and PBN	[AC/35-D/2005] [NTEMP-8] or ITM equivalent if available	Develop STVPs Specific tests for ON/PBN part can be addressed in annexes. The STVP shall refer to dSSRSs	Provide template and guidance to the Contractor Review Coordination with the Security Accreditation Authority

Table 13: Security Accreditation Documentation and Contractor Responsibility

10.2. Security Mechanisms to be implemented by the SOA & IdM Platform

10.2.1. Identification of Security Mechanisms for implementation by the SOA & IdM Platform.

> [SOW-524]   *The Contractor SHALL identify Security Mechanism (SM) to be implemented by the SOA & IdM Platform, based on:*
>
> > a. *the outcome of the SRA; and*
> >
> > b. *the Purchaser-developed SM Baselines for the PBN and ON networks (Ref. [NS CIS Security Reference Baseline, 2017], [ITM NR AIS CSRS, 2017]). The NATO CIS Security Reference Baseline(s) will be provided to the Contractor after the CAW.*
>
> [SOW-525]   *During design stage the Contractor SHALL apply SRA-recommended security measures in the design, utilizing the NATO CIS Security Reference Baselines ([ITM NR AIS CSRS, 2013], [NS CIS Security Reference Baseline, 2017]).*
>
> [SOW-526]   *The Contractor, in the SOA & IdM Platform design, SHALL include implementation of the required Security Mechanisms and provide full traceability of high level security measures requirements down to the implementation level, testing phases, and project lifecycle, utilizing the following documents.*
>
> > a. *NATO SECRET CIS Security Reference Baseline [NS CIS Security Reference Baseline, 2017] for NATO SECRET environment;*
> >
> > b. *Community Security Requirement Statement (CSRS) for NATO RESTRICTED Automated Information System provided by IT Modernization [ITM NR AIS CSRS, 2013];*
> >
> > c. *Community Security Requirement Statement (CSRS) for NATO RESTRICTED Automated Information System provided by IT Modernization [ITM NR AIS CSRS, 2013];*
> >
> > d. *System Description template [NTEMP-3];*
> >
> > e. *Delta System Security Requirements Statement (dSSRS) template [NTEMP-5];*
> >
> > f. *Security Test and Verification Plan (STVP) template Secure AIS STVP Template [NTEMP-8], ; and*
> >
> > g. *Security Test and Verification Report template.*
>
> [SOW-527]   *The Contractor SHALL maintain an end-to-end traceability of the required security measures throughout the project, in order to provide assurance that security does support the business requirements and objectives and it is rightly sized to the scope of the project and the solution(s) developed and implemented.*
>
> [SOW-528]   *The Contractor SHALL include any additional security measures resulting from the follow-on risk assessments as part of the end-to-end traceability.*

10.2.2. The SOA & IdM Platform security relation with other systems.

10.2.2.1. The SOA & IdM Platform will operate in a multi-layered security environment, with a number of security mechanisms implemented by other systems in addition to ones to be delivered with the SOA & IdM Platform.

10.2.2.2. The SOA & IdM Platform-specific security mechanisms, identified at the SRA, are required to integrate with the existing NATO wide IA Services capability as to foster the reuse and standardisation of enterprise class of security services. The other systems for consideration when analysing security mechanisms include:

a. The NATO Computer Incident Response Capability (NCIRC);

b. The NATO PKI certificate Authority and Registration Authority;

c. The enterprise systems management operated by NCI Agency and other system management controls operated either directly by NATO or under NATO supervision;

d. The NATO Enterprise Directory Seviced (NEDS) project, as described in Section 3.4.2.3.1.;

e. The IaaS delivered by the ITM program, as described in Section 3.4.2.3.2. See ANNEX H: ITM Security MechAnisms;

f. The Bi-Strategic Command Automated Information System (Bi-SC AIS), as defined in the Bi-SC AIS Reference Architecture [NAC AC/322-D(2005)0037, 2005] (see SECTION 3.4.1), including security requirements as specified in the NS AIS CSRS [2013],

[SOW-529] *The Contractor SHALL design the SOA & IdM Platform security mechanisms to integrate with the existing NATO wide IA Services capability as defined in SRS.*

10.2.3. Implementation of the SOA & IdM Security Mechanisms.

[SOW-530] *The Contractor SHALL implement the security mechanisms, approved by the Purchaser after coordination with the Security Accreditation Authority, as a part of the SOA & IdM Platform design and security accreditation work and SHALL produce the associated documentation.*

SECTION 11: QUALITY ASSURANCE AND CONTROL

11.1. General definition

11.1.1. Quality Control (QC) is a procedure or set of procedures intended to ensure that a manufactured product or performed service adheres to a defined set of quality criteria or meets the requirements of the client or customer.

11.1.2. Quality Assurance (QA) is as a procedure or set of procedures intended to ensure that a product or service under development meets specified requirements.

11.1.3. Under this contract the Quality Assurance process is intended as Quality Assurance and Control Process. The term Quality Assurance will include also the Quality Control definition.

11.1.4. Certificate of Conformity is a document, signed by the Supplier, which states that the product conforms with contractual requirements and regulations

11.1.5. The Certificate of Conformity, verifies the process quality-enabled items produced or shipped comply with test procedures and quality specifications prescribed by the customer. It presents data derived from quality management information.

11.2. Quality Assurance and Control System

> [SOW-531] The Contractor SHALL establish, execute, and maintain an effective Quality Management process throughout the Contract lifetime. It SHALL be based on [AQAP-2110, 2016], which incorporates by reference ISO 9001 directive.

11.3. Quality Assurance Process

> [SOW-532] The Quality Assurance (QA) implemented by the Contractor SHALL apply to all hardware, software (including firmware) and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract. This includes non-deliverable test and support hardware and software.

> [SOW-533] The Contractor SHALL be responsible for the control of quality of all deliverables and associated Contractual products throughout the life-cycle of the Contract.

> [SOW-534] The Contractor's QA Process SHALL ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.

> [SOW-535] The Contractor's QA Process SHALL be described in the QA Plan as outlined below. The process is subject to approval by the Purchaser, or its delegated representative(s), whenever it does not meet the Quality Assurance requirements.

> [SOW-536] The Contractor's overall QA Process SHALL adhere to the provisions of [AQAP-2110, 2016].

> [SOW-537] The Contractor SHALL use its own Quality Manual as a reference in the Quality Assurance Process.

[SOW-538]   The Contractor's Quality Manual SHALL outline the quality focus and the objectives in the Contractor's organisation.

[SOW-539]   The Contractor SHALL demonstrate, with the Quality Assurance process, that the processes set up for design, develop, produce and maintain the product will assure the product will meet all the requirements.

[SOW-540]   If sub-contracted quality resources are used, the Contractor's Quality Management Process SHALL describe the controls and processes in place for monitoring the sub-Contractor's work against agreed timelines and levels of quality.

[SOW-541]   The Contractor SHALL assure that all the test and procedure used to demonstrate the requirements will be monitored and controlled under the QA process.

[SOW-542]   Unless when invoked in this contract, the Contractor (or his Supplier) SHALL determine the test methods required and perform the tests to demonstrate conformity with the corresponding requirements at appropriate stages up to and including the final product

[SOW-543]   The Contractor SHALL on request provide the Purchaser with a copy of any subcontracts or orders for products related to the contract.

[SOW-544]   The Contractor SHALL notify Purchaser if a subcontract or order has been identified as constituting or involving risk.

[SOW-545]   The Contractor SHALL documented all the identified risks in accordance with SECTION 5.4.6: Risk Management Plan (RMP) and [AQAP-2110, 2016].

[SOW-546]   The Contractor SHALL flow down the applicable contractual requirements to Sub-suppliers by referencing the stated contractual requirement, including relevant AQAP(s).

[SOW-547]   The Contractor SHALL be responsible of ensure that the procedures and processes required to fulfil contract requirements are fully implemented at the Sub-supplier's facilities.

[SOW-548]   The Contractor SHALL periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser POC.

[SOW-549]   The Contractor SHALL ensure that all contractual requirements, including NATO supplements, are included in internal audits.

[SOW-550]   The Contractor SHALL inform the Government Quality Assurance Representative (GQAR) and/or Purchaser of deficiencies identified during internal audit unless otherwise agreed between the GQAR and/or the Purchaser and the Contractor.

11.4. Corrective Actions

[SOW-551]   The Contractor and Sub-contractor SHALL provide objective evidence, that risks are considered during planning, including but not limited to Risk Identification, Risk analysis, Risk Control and Risk Mitigation.

[SOW-552] The Contractor SHALL start planning with risk identification during contract review and updated thereafter in a timely manner. The Purchaser reserve the right to reject QPs, Risk Plans and their revisions.

[SOW-553] The Contractor SHALL implement a quality/product assurance risk log/action track system, which identifies all the major/minor non conformity raised during the life cycle of the product.

[SOW-554] The contractor SHALL demonstrate that all the non-conformities are solved before the product acceptance.

[SOW-555] The Contractor SHALL establish and implement a Corrective Action System to ensure prompt detection, documentation and correction of problems and deficiencies (non-conformities).

[SOW-556] The Corrective Action System SHALL track all reported and recorded problems and deficiencies until their closure and clearance.

[SOW-557] The Contractor SHALL notify the Purchaser of proposed action, resulting from Review Output that will affect compliance with contractual requirements.

[SOW-558] The Contractor's Review outputs SHALL, where action item(s) are identified, specify the responsible person/function and due date of the action item(s).

[SOW-559] The Contractor SHALL issue and implement documented procedures which identify, control and segregate all non-conforming products. Documented procedures for the disposition of non-conforming product are subject to approval by the Purchaser when it can be shown that they do not provide the necessary controls.

[SOW-560] The Contractor SHALL notify the Purchaser of non-conformities and corrective actions required, unless otherwise agreed with the Purchaser.

[SOW-561] When the Contractor establishes that a subcontractor or a Government Furnished Equipment (GFE) product is unsuitable for its intended use, he SHALL immediately report to and coordinate with the Purchaser the remedial actions to be taken.

[SOW-562] The Contractor SHALL ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.

[SOW-563] The Contractor SHALL document the Corrective Action System in the QA Plan.

11.5. Certificate of Conformity

11.5.1. The Contractor is solely responsible for the conformance to requirements, of products provided to the Purchaser.

[SOW-564] The Contractor SHALL deliver all the Certificate of Conformity (CoC) for products, COTS SW (including firmware) and hardware released by the COTS Vendors unless otherwise instructed.

[SOW-565] The CoCs delivered by the Contractor SHALL be part of the acceptance data package of the product.

11.6. Quality Assurance Plan (QAP)

[SOW-566]   The Contractor SHALL provide a QAP to the Purchaser in accordance with the requirements of AQAP-2105, Edition 2 and the above mentioned AQAPs, and as amended herein.

[SOW-567]   The Contractor's QAP SHALL be submitted to the Purchaser for review.

[SOW-568]   The Contractor's QAP SHALL distinguish between the Quality Assurance process and Quality Control Process and plan, manage and resource both.

[SOW-569]   The Contractor's QAP SHALL be structured as a living document subject to revision/update, as required.

[SOW-570]   The Contractor's QAP SHALL reference or document and explain the Contractor's QA procedures for analysis, software support, development, design, production, installation, configuration management, control of Purchaser furnished property, documentation, records, programming standards and coding conventions, library controls, reviews and audits, testing, corrective action and certification as specifically related to this project.

[SOW-571]   The Contractor's QAP SHALL be compatible and consistent with all other plans, specifications, standards, documents and schedules, which are utilised under this Contract.

[SOW-572]   All Contractor procedures referenced in the QA Plan SHALL either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.

[SOW-573]   The QA Plan and all related QA procedures shall be subject to Purchaser QAR approval.

11.7. Organisation

[SOW-574]   The Contractor's personnel comprising the QA organisation SHALL have sufficient responsibility, authority, organisational freedom and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective action.

[SOW-575]   The Contractor's Personnel performing Quality Assurance functions SHALL have specific documented definitions of their assigned duties.

[SOW-576]   The Contractor's QA personnel performing QA functions MUST NOT be the same personnel responsible for performing other tasks that are reviewed by QA.

[SOW-577]   The Contractor's QA Manager Role SHALL provide the Purchaser with all required by this SoW documentation and technical data.

[SOW-578]   The Contractor's QA personnel SHALL participate in the early planning and development stages to ensure that attributes of good quality for life-cycle procurement are specified in plans, standards, specifications and documentation.

[SOW-579]   After establishment of attributes, controls and procedures, Contractor QA personnel SHALL ensure that all elements of the QA

Process are properly executed, including inspections, tests, analysis, reviews and audits.

[SOW-580] *The Contractor's QA personnel SHALL be designated as the Contractor's QA Management Representative and point of contact for interface with and resolution of quality matters raised by the NCI Agency or his delegated National Quality Assurance Representative (NQAR) and identified in the Quality Assurance Plan.*

[SOW-581] *The Contractor SHALL ensure that Quality Management personnel have the required qualifications, knowledge, skills, ability, practical experience and training for working with, and in accordance with the applicable NATO AQAP's and ISO standards.*

[SOW-582] *The Contractor SHALL ensure that Quality Management Personnel are of sufficient number and have sufficient resources to adequately and effectively monitor and control the QA Process.*

11.8. Contractor (and subcontractors) Control and Audit

11.8.1. The Purchaser reserves the right to perform Reviews and Quality audits at any of the Contractor (or Sub-Contractor(s)) facilities. Audit activities at Sub-supplier's facilities do not relieve the Contractor and Subcontractors from any contractual quality responsibilities.

[SOW-583] *The Contractor SHALL notify the Purchaser if a sub-supplied product is rejected or repaired which has been identified as involving risk or supplied by a Sub-contractor whose selection or subsequent performance has been identified as involving risk.*

SECTION 12: CONFIGURATION MANAGEMENT

12.1. General

[SOW-584]   *The Contractor's Configuration Management (CM) process SHALL enable the baselining of Configuration Items (CIs) into the FBL, ABL, PBL and OBL as defined in this section of the SoW and the maintenance of these baselines throughout the duration of the Contract.*

[SOW-585]   *The Contractor SHALL ensure that an effective CM organisation is established to implement and manage the Configuration Management processes throughout the duration of this Contract.*

[SOW-586]   *The Contractor SHALL create and maintain 4 (four) Configuration Baselines, as follows (see Figure 12).*

  a. *Functional Baseline (FBL or "as-required");*

  b. *Allocated Baseline (ABL, or "as-designed");*

  c. *Product Baseline (PBL, or "as-built");*

  d. *Operational Baseline (OBL, or "as-delivered", or "as-deployed").*

Figure 12: Configuration Baseline

1. **SRR →** produces **FBL (baseline as-required)**

2. **SDR + SBR(s) →** produces **ABL (baseline as-designed)**

3. **IRC + DA Review(s) →** produces **PBL (baseline as-built)**

4. **PSA + FSA Reviews →** produces **OBL (baseline as-delivered/deployed)**

Legend:

SoW – Statement of Work
SRS – System Requirements Specification
SRR – System Requirements Review
FBL – Functional Baseline
SDR – System Design Review
ABL – Allocated Baseline
SBR – System Baseline Review
IRC – Internal Release Candidate
DA – Deployment Authorization
PBL – Product Baseline Acceptance
PSA – Partial System Acceptance
OBL – Operational Baseline
FSA – Final System Acceptance

[SOW-587] *Under the CM process the Contractor SHALL maintain and update all project CIs as requested by changes within the project or external to the project throughout the duration of the Contract;*

12.2. Baselines

12.2.1. Traceability

[SOW-588] *The Contractor SHALL ensure that there is full traceability through all baselines back to the functional baseline.*

[SOW-589] *The Contractor's developed baselines SHALL be encapsulated and maintained by the Contractor in a database established by the Contractor as specified under Configuration Management Tools.*

12.2.2. Functional Baseline (FBL)

12.2.2.1. The Contractor's developed Functional Baseline is a set of documents that specifies the functional and non-functional requirements of a service or product and that is used as the approved basis for comparison.

[SOW-590] *The Contractor's developed FBL SHALL be derived from the SOA & IdM Platform SRS and SHALL be established at the successful completion of the SRR with the approved updated SRS.*

12.2.3. Allocated Baseline (ABL)

12.2.3.1. The ABL is a set of documents that specifies the design of a service or product and is used as the approved basis for comparison.

[SOW-591] *The Contractor's design in the ABL SHALL meet the functional and non-functional requirements allocated in the FBL.*

[SOW-592] *The Contractor's ABL set of documents and Artefacts SHALL contain (but is not limited to) the following documents:*

    a. *Software Design Specification;*

    b. *the Test Specification;*

    c. *Requirment Traceability Matrix (RTM).*

[SOW-593] *The Contractor's ABL SHALL be established at the successful completion of the SDR.*

12.2.4. Product Baseline (PBL)

12.2.4.1. The PBL is a set of products and/or services, including supporting documents, which is used as the approved basis for comparison.

[SOW-594] *The Contractor's PBL SHALL meet the functional and non-functional requirements allocated in the FBL and the design of the ABL.*

[SOW-595] *The Contractor's developed PBL for SOA & IdM Platform SHALL be established after successful completion of the RC and DA Review(s). It reflects the "as-built" configuration of the system.*

[SOW-596] *The Contractor's PBL products SHALL be distinguished in documentation, software, hardware/equipment and services.*

[SOW-597] The Contractor's software products of the PBL SHALL contain the following: (off-the-shelf) software media, (off-the-self) software license(s).

[SOW-598] The Contractor's (supporting) documentation products of the PBL SHALL contain:

    a. PBL (as-built) drawings,

    b. off-the-shelf OEM manuals,

    c. FBL (as-required) documentation,

    d. ABL (as-designed) documentation,

    e. Operations and Maintenance support documentation,

    f. Inventory documentation,

    g. Training documentation,

    h. Quality assurance documentation,

    i. Security documentation,

    j. Configuration Management documentation,

    k. Warranty documentation and Traceability Matrix.

[SOW-599] The Contractor SHALL include the System Design Specifications (SDS including the Requirements Traceability Matrix), the Test Plan, and any other documentation deemed appropriate by the Contractor, in accordance with provisions of IEEE 12207, to ensure that requirements are reflected in the system during development and integration can be demonstrated through a comprehensive set of tests and can be delivered in the form of the PBL.

12.2.5. Operational Baseline (OBL)

[SOW-600] The Contractor's developed OBL SHALL be initially established after successful completion of the PSA and then finally established after successful completion of FSA. It reflects the "as-deployed" ("as-delivered") configuration of the system

[SOW-601] The Contractor's OBL SHALL contain:

    a. all delivered Software Configuration Item (SWCI), including COTS;

    b. all delivered Hardware Configuration Item (HWCI), if any;

    c. Computer Software Configuration Item (CSCI);

    d. all the Documentation that comprise the system and any subsequent releases and SHALL reflects the "as-deployed" configuration of the system.

[SOW-602] SOA-IdM Platform baselines SHALL be given by a Contractor a major release number and a minor release number comprising an X.X notation. Some of the releases will be defined beforehand and numbering system can be summarised as per following example:

    a. SOA-IDM RCv3.0.0 is the OBL at First PSA;

b. *SOA-IDM RCv3.0.1 is 3.0.0 with minor modifications as applied until Next PSA;*

c. *SOA-IDM RCv3.1.0 is the OBL at Next PSA;*

d. *SOA-IDM RCv3.1.1 is 3.1.0 with minor modifications as applied until Next PSA (or last – FSA);*

e. *for Wave 2 – similar: SOA-IDM RCv7.0.0 is the OBL at First PSA.*

12.2.5.1.   Intermediate baselines, whether they are FBL, ABL, PBL or OBL SHALL be labelled logically within this scheme.

[SOW-603]   *The Contractor SHALL include in the PBL and/or OBL release package the following elements, as a minimum all items described below in Table 14:*

Serial	Requirement
1	All required CSCI
2	The source code of elements categorised as foreground knowledge, script, and configuration setting baseline, including the documentation for these items.
3	The script and configuration setting baseline, including documentation for these items, for non-development software items (e.g. Microsoft Office).
4	Release notes, which include a description of what is new or changed in each software module.
5	List of open known problems and faults.
6	The SRS and SDS versions against which the baseline has been developed.
7	Interface Control Documents for the various interfaces
8	All design artefacts provided as part of the SDS, updated to reflect the PBL.
9	Conversion programs and instructions.
10	Plug-ins/add-ins, glue-code and interfaces.
11	Parameter definitions.
12	Initial data sets.
13	Online help files.
14	Test stub, along with test scenario and sample data to support the integration of SOA & IdM Platform with other services.
15	Test procedures and scripts for any automated tests, along with all source data for the manual and automated tests and including the documentation for these items.
16	Copyright and license information.
17	Instructions for system administration staff to follow to save the previously installed SBL, to install the new baseline, and to recover the old baseline if the new baseline installation must be interrupted or aborted.
18	Installation scripts.
19	Instructions on how to identify and report problems after acceptance.
20	Instructions for the generation of new PBLs, distribution and installation of new software versions, and any test procedures and test cases necessary to verify the generated baseline before distribution.
21	Additional documentation artefacts identified in the SRS.

Table 14: Content for Project Baseline Release Package

12.3. Configuration Management Plan (CMP)

[SOW-604]   The Contractor SHALL provide a CMP tailored to the requirements of the proposed technical solution.

[SOW-605]   The Contractor's CMP SHALL be structured as a living document subject to revisions and updates, as required.

[SOW-606]   The Contractor SHALL place the CMP under configuration control prior to its implementation and for the life of the Contract.

12.3.1. The Contractor's CMP is a Product Lifecycle document that will survive the project post-FSA. As such, this documents are not to be submitted as part of the PMP, but will be part of the Technical Proposal.

[SOW-607] In producing the Contractor's CMP, the Contractor SHALL define the organisation and procedures used to configuration manage the functional and physical characteristics of CIs, including interfaces and configuration identification documents.

[SOW-608] The Contractor SHALL ensure that all required elements of CM are applied in such a manner as to provide a comprehensive CM process.

[SOW-609] The Contractor's CMP SHALL be compatible and consistent with all other plans, specifications, standards, documents and schedules.

[SOW-610] The Contractor SHALL propose in the CMP detailed configuration control procedures.

[SOW-611] All Contractor and Purchaser activities and milestones related to CM SHALL be identified and included in the PMS of the PMP.

[SOW-612] The CMP SHALL address all disciplines within this section and SHALL as a minimum include the following sections:

  a. Introduction;

  b. Organisation;

  c. Configuration Identification and Documentation;

  d. Configuration Control;

  e. Configuration Status accounting;

  f. Configuration Audits;

  g. Configuration Management tools/Interface management.

12.4. Configuration Item Identification and Documentation

[SOW-613] The Contractor SHALL divide the products and specialist products into CIs (Configuration Items).

[SOW-614] The Contractor's CI structure SHALL show the relationships between the lower level baselines and CIs.

[SOW-615] The Contractor SHALL propose appropriate CIs in the CMP including an explanation of the rational and criteria used in the selection process, based on the criteria for selection of CIs as detailed in [NATO ACMP 2009, 2017].

[SOW-616] The Contractor's CIs SHALL be chosen in a way to assure visibility and ease of management throughout the development effort and the support to the OBL after acceptance.

[SOW-617] All Contractor's COTS, adapted, and developed software SHALL be designated as CIs.

[SOW-618] Where Contractor's COTS product can be installed in a modular fashion, the description of the CI, the Contractor SHALL unambiguously identify the complete list of installed components.

[SOW-619] The Contractor SHALL designate all complete hardware elements as CIs (if any).

12.4.1. Additional guidance about CI selection can be found in STANAG 4427, 2014 and in STANAG 4159.

[SOW-620]   The Contractor SHALL create or use a COTS software to maintain the CMDB that persists the Configuration Items (CIs) attributes, (inter-) relationships and Configuration Baselines.

[SOW-621]   The Contractor SHALL ensure that the Configuration Baselines and CIs are persistently stored, maintained and managed in the CMDB.

[SOW-622]   The Contractor SHALL keep the CMDB consistent and updated.

[SOW-623]   The Contractor's CMDB SHALL be compliant with the Purchaser's ITSM Tools.

[SOW-624]   The Contractor's CMDB SHALL provide the ability to trace higher and subordinate CIs using CI identifiers or other CI attributes.

12.4.2. The Purchaser reserves the right to modify the CI structure and attributes.

[SOW-625]   The level of granularity for the Contractor's Configuration Item selection SHALL reach at minimum:

a. Line Replaceable Units (LRUs) - Hardware CIs,(if any);

b. Software Assets and/or Firmware/Software CIs;

c. Documentation delivered under this Contract - Documentation CIs;

d. The Hardware CI attributes SHALL include, but is not limited to, the Material Datasheet information,(Optional);

e. The Software CI attributes SHALL include, but is not limited to, the STANAG 4427, 2014 definitions;

f. Any Documentation CI that is not linked to a Software CI or Hardware CI (optional) SHALL include, but is not limited to, the Contract SSS attributes.

12.5. Configuration Control

[SOW-626]   The Contractor SHALL be responsible for issuing in a timely manner, as required by this SoW, all approved changes and revisions to the functional, development and product baseline documents included in the Contract. This includes changes originated both by the Contractor and the Purchaser.

[SOW-627]   Where a change affects more than one document, or affects documents previously approved and delivered, the Contractor SHALL ensure that the change is properly reflected in all baseline documents affected by that change.

[SOW-628]   All design changes SHALL be appropriately reflected in the technical documentation by the issue of appropriate changes or revisions and SHALL be provided to the Purchaser.

[SOW-629]   The Contractor SHALL be fully responsible for the Configuration Control of all baselines and CIs in accordance with [NATO ACMP 2009, 2017].

[SOW-630]   The Contractor SHALL define the responsibilities and procedures used within the Contractor's organisation for configuration control of established CI, and for processing changes to these CI.

[SOW-631]   The Contractor SHALL define the Configuration Baseline Change procedures and SHALL submit Notice of Revision or Request for Deviations and Wavers when required and approved by the Purchaser.

12.6. Engineering Change Proposals (ECP)

[SOW-632]   Changes to the Contractor's developed baselined CIs SHALL be processed as either Class I or Class II ECPs as defined in [NATO ACMP 2009, 2017] and the change request requirements specified in SECTION 7.3.2.

[SOW-633]   The Contractor SHALL use the configuration control procedures specified in the CMP for the preparation, submission for approval implementation and handling of ECPs to baselined CIs.

[SOW-634]   When submitting ECPs, the Contractor SHALL assign a priority rating of Emergency, Urgent or Routine Extensions to the target times for processing.

[SOW-635]   Class I ECPs SHALL have to be mutually agreed upon by the Contractor and Purchaser.

[SOW-636]   The Contractor SHALL propose in the CMP an ECP format based on the requirements in [NATO ACMP 2009, 2017].

[SOW-637]   The Contractor SHALL use the configuration control procedures specified in the CMP for the preparation, submission for approval implementation and handling of ECPs to baseline CIs.

[SOW-638]   Extensions to the target times for processing Class I ECPs SHALL be mutually agreed upon by the Contractor and Purchaser.

[SOW-639]   Prior to implementation, all Class II ECPs SHALL be submitted by the Contractor to the Purchaser for review and classification concurrence.

[SOW-640]   If the Purchaser's representative does not concur in the classification, Class I ECP procedures SHALL be applied by the Contractor and the ECP and then formally submitted to the Purchaser for approval or rejection.

[SOW-641]   The Contractor SHALL appropriately reflect in the technical documentation all design changes by the issue of appropriate changes or revisions.

[SOW-642]   Any Engineering Change Proposal SHALL include, as a minimum, the following information:

   a. Reference Number;

   b. requirement affected (using the outline numbering of the core SoW, or of Annex A and B);

   c. nature of change;

   d. rationale for the change;

   e. impact of change;

f. description of how the change will be reflected in the delivered system's cost, schedule, and/or performance. This description SHALL include any trade-offs that SHALL be considered;

g. status;

h. priority.

12.7. Requests for Deviation (RFD) and Requests for Waiver (RFW)

[SOW-643]   If required, the Contractor SHALL prepare, handle, and submit for Purchaser's approval, RFDs and RFWs as defined in [NATO ACMP 2009, 2017]

[SOW-644]   The Contractor SHALL propose in the CMP a RFD/RFW format based on the requirements in [NATO ACMP 2009, 2017]

[SOW-645]   The Contractor SHALL be aware that permanent departures from a baseline SHALL be accomplished by ECP action rather than by RFD.

12.8. Configuration Status Accounting (CSA)

[SOW-646]   The Contractor SHALL be fully responsible for the CSA for all CIs in accordance with [NATO ACMP 2009, 2017]

[SOW-647]   The Contractor SHALL propose the format of CSA report his CMP for Purchaser's approval.

[SOW-648]   The Contractor SHALL deliver CSA reports to the Purchaser both as part of management and specialist products in this contract and also as standalone documents at the Purchaser's request.

[SOW-649]   At the end of the Contract, the Contractor SHALL deliver a set of final CSA reports for each CI or set of CI's in both hard copy and in electronic media.

12.9. Configuration Verification and Audits

[SOW-650]   Upon request from the Purchaser, the Contractor SHALL support configuration audits to demonstrate that the actual status of all CIs matches the authorised state of CIs as registered in the CSA reports.

[SOW-651]   The Contractor SHALL support the FCA and Physical Configuration Audit (PCA) by providing the required Baseline Documentation and answering questions from the Purchaser's Auditor.

[SOW-652]   The Contractor SHALL draft a Configuration Audit Report for the FCA and PCA that summarises the results for the Purchaser's approval.

[SOW-653]   The Contractor SHALL solve any deficiencies found during the Configuration Management Audits within the agreed timeframe and update the baseline accordingly.

[SOW-654]   *The initial version of the Contractor's ABL, and PBL SHALL be provided to the Purchaser for acceptance.*

[SOW-655]   *Upon Purchaser Acceptance, ABL and PBL SHALL be placed by the Contractor under the control of the CCB.*

12.9.1. The acceptance of the ABL and PBL by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements.

[SOW-656]   *The Contractor SHALL keep the contents of the ABL and PBL under Configuration Control to reflect the progress of the project activities.*

12.10.   Configuration Management and Software versioning Tool

[SOW-657]   *The Contractor's version control/configuration management automated tool SHALL include the capabilities for baselines management, source code control versioning, configuration item identification, change request management, deficiency reporting management, and configuration status accounting.*

[SOW-658]   *The Contractor SHALL provide the Purchaser read-only access to the version control/configuration management automated tool, including source code of the baseline.*

[SOW-659]   *The Contractor SHALL provide these tools as part of the SOA & IdM Platform Reference System to enable life-cycle configuration management.*

12.11.   Configuration Identification and Documentation

[SOW-660]   *The Contractor SHALL establish a Configuration Identification System.*

[SOW-661]   *The Contractor's configuration Identification System SHALL identify all documents necessary to provide a full technical description of the characteristics of the Hardware and Software Configuration Items (CIs) that require control at the time each baseline is established.*

[SOW-662]   *The Contractor's configuration Identification System SHALL include the relevant deliverables in the contract.*

[SOW-663]   *The Contractor's CI structure SHALL be a tree structure with the system being the top level CI.*

12.11.1. Documentation

[SOW-664]   *Detailed proposals for the documents that will comprise the above baselines SHALL be included in the CMP for approval by the Purchaser.*

[SOW-665]   *At the end of the contract, the Contractor SHALL deliver the baseline documentation in a format which complies with section 14.6.12: Publication Criteria*

[SOW-666]   *As part of the CMDB, as specified under Configuration Management Tools, the Contractor SHALL transfer to CMDB a copy of the current version of all baselines to the Purchaser at contract completion.*

SECTION 13: LABOUR CATEGORIES

13.1. General

13.1.1. This section outlines minimum educational qualifications, experience qualifications, and responsibilities for Contractor's key personnel assigned to this Contract.

> [SOW-667] All Contractor's SOA & IdM Platform project key personnel SHALL demonstrate spoken and written fluency in English language, at a minimum of 4343 as defined in [STANAG 6001, 2014].

> [SOW-668] All Contractor's SOA & IdM Platform project key personnel SHALL have a current NATO SECRET security clearance and maintain it throughout the lifecycle of the Contract.

> [SOW-669] All Contractor's SOA & IdM Platform personnel who need System Administrator privileges or access when working on NATO SECRET systems SHALL hold NATO CTS (Cosmic Top Secret) clearance and maintain it throughout the lifecycle of the Contract.

> [SOW-670] All Contractor's SOA & IdM Platform project key personnel SHALL present references of successful project delivery and description of roles, responsibilities, activities executed, and SHALL include reachable points of contact for above.

13.1.2. Substitution of experience or education is allowed as outlined in Table 15: Experience / Education substitution below:

Education	Equivalent Education + Experience	Equivalent Experience
Associates degree		4 years of relevant experience
Bachelor's degree	Associates + 4 years of relevant experience	8 years of relevant experience
Master's degree	Bachelor's + 6 years of experience	10 years of relevant experience

Table 15: Experience / Education substitution

13.2. SOA & IdM Platform Project Manager (PM)

13.2.1. PM Education

> [SOW-671] The Contractor's SOA & IdM Platform PM SHALL meet educational requirements:

> a. have an university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, equivalent to a Master's, supported by relevant certificates/diplomas; exceptionally, extensive relevant experience may be considered if the above qualifications are not met;

> b. have current Project Management certification (Information Technology Infrastructure Library (ITIL) Foundation, Prince2 Practitioner or Project

Management Institute (PMI) Project Management Professional (PMP), or equivalent);

c. SHOULD HOLD relevant Agile Practitioner Certificate.

13.2.2. PM experience

[SOW-672] The Contractor's SOA & IdM Platform PM SHALL meet experience requirements:

a. have at least ten (10) years of experience as an Information and Communication Technology (ICT) project manager;

b. have at least five (5) years of experience as the project manager for an effort of similar scope to the SOA & IdM Platform project;

c. have preferably including the application of a formal project management methodology such as PRINCE2 or Agile.

d. experience SHALL include, as the project manager, the successful delivery of at least one similar project involving PaaS implementation, migration of applications, integration of the capabilities under one centralised service management and control system in an environment where security was a significant concern. The experience SHALL be supported by project references, points of contact, and description of role/responsibilities/activities executed.

13.2.3. PM responsibilities

[SOW-673] The Contractor's SOA & IdM Platform PM SHALL:

a. be responsible for:

    i. project management;

    ii. performance and completion of tasks and deliveries;

b. establish and monitor project plans and schedules and has full authority to allocate resources to insure that the established and agreed upon plans and schedules are met;

c. manage costs, technical work, project risks, quality, and corporate performance;

d. manage the development of designs and prototypes, test and acceptance criteria, and implementation plans;

e. establish and maintain contact with Purchaser, subcontractors, and project team members;

f. provide administrative oversight, handles Contractual matters and serves as a liaison between the Purchaser and corporate management;

g. ensure that all activities conform to the terms and conditions of the Contract.

NATO UNCLASSIFIED

13.3. SOA & IdM Platform Technical Lead (TL) and/or Senior Systems Engineer (SSE)

13.3.1. Senior Systems Engineer and Technical Lead duties may be performed by the same person.

13.3.2. TL/SSE education

> [SOW-674]   The Contractor's SOA & IdM Platform TL/SSE SHALL have university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/diplomas.

> [SOW-675]   The Contractor's SOA & IdM Platform TL/SSE SHALL have current ITIL Foundation and Service Design certificates.

13.3.3. TL/SSE experience

> [SOW-676]   The Contractor's SOA & IdM Platform TL/SSE SHALL meet experience requirements:
>
> a. have at least seven (7) years in engineering positions associated with the review, design, development, evaluation, planning and operation PaaS components, subsystems, or systems for government or commercial use (e.g., middleware, Service Oriented Architecture, Network Access/Admission Control, IdM);
>
> b. have at least 5 years of the experience which SHALL be related to the architecture, design and implementation of system/platform similar to SOA & IdM Platform project;
>
> c. have a minimum of one (1) years' experience in undertaking ICT QA activities;
>
> d. have knowledge and experience with QA standards (either AQAP or ISO), processes for integration and testing;
>
> e. have a minimum of three (3) years of experience as a team leader or project manager to ensure the technical management oversight of a: SOA platform designer, IdM Platform designer, Infosec/Compusec designer, communications engineer and systems integrator; which SHALL be supported by project references, points of contact, and technical description of the role, responsibilities and activities;
>
> f. have an ITILv3 Intermediate certification (ITIL Service Operation and/or ITIL Service Transition).

13.3.4. TL/SSE responsibilities

> [SOW-677]   The Contractor's SOA & IdM Platform TL/SSE SHALL:
>
> a. plan and co-ordinate engineering activities to meet SRS requirements;
>
> b. perform complex engineering tasks and multiple tasks simultaneously;

c. direct and co-ordinate all activities necessary to complete a major, complex engineering program or multiple smaller tasks or programs;

d. perform advanced engineering research, hardware or software development;

e. supervise the work of a design, integration, test, and implementation team;

f. analyse architectural options for performance and manageability;

g. recommend design changes/enhancements for improved system performance;

h. provide comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance;

i. be competent in technical disciplines as applied to government and commercial information and communications systems.

13.4. SOA & IdM Platform Test Director and/or Test Engineer

[SOW-678] The Contractor's SOA & IdM Platform Test Director and/or Test Engineer SHALL NOT perform any other duties within the SOA & IdM Platform project.

13.4.1. Test Director (TD) and Test Engineer (TE) duties may be performed by the same person.

13.4.2. TD/TE education

[SOW-679] The Contractor's SOA & IdM Platform TD/TE SHALL have university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/diplomas.

13.4.3. TD/TE experience

[SOW-680] The Contractor's SOA & IdM Platform TD/TE SHALL meet experience requirements:

a. have integration and testing engineering skills with five (5) years of experience as part of projects at least equivalent to SOA & IdM Platform, supported by project reference and description of role, responsibilities and activities;

b. have demonstration of practical experience in planning, conducting and assessing integration and testing activities in support of projects for at least equivalent to SOA & IdM Platform for at least two (2) years, supported by project references and description of role, responsibilities and activities;

c. have at least ten (10) years of experience in the planning and execution of testing information systems, defence systems, and large scale C2 systems.

13.4.4. TD/TE responsibilities

[SOW-681] *The Contractor's SOA & IdM Platform TD/TE SHALL:*

a. *be responsible for directing test planning, design and tools selection;*

b. *establish guidelines for test procedures and reports;*

c. *co-ordinate with Purchaser on test support requirements and manage Contractor test resources.*

13.5. SOA & IdM Platform Quality Assurance (QA) Manager

[SOW-682] *The Contractor's SOA & IdM Platform QA Manager SHALL NOT perform any other duties within the SOA & IdM Platform project.*

13.5.1. QA Manager education

[SOW-683] *The Contractor's SOA & IdM Platform QA Manager SHALL have university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/diplomas.*

13.5.2. QA Manager experience

[SOW-684] *The Contractor's SOA & IdM Platform QA Manager SHALL meet experience requirements:*

a. *have at least seven (7) years working with quality control methods and tools,*

b. *have at least four (4) years supporting system development and test projects.*

13.5.3. QA Manager Responsibilities

[SOW-685] *The Contractor's SOA & IdM Platform QA Manager SHALL:*

a. *establish and maintain process for evaluating software, hardware, and associated documentation;*

b. *determine the resources required for Quality Control;*

c. *maintain the level of quality throughout the system life cycle;*

d. *prepare and guide the development of system Quality Assurance plans;*

e. *develop project Quality Assurance plan;*

f. *guide development and implement quality standards;*

g. *review hardware, software, and documentation;*

h. *prepare and guide formal and informal reviews to determine quality;*

i. *examine and evaluate design, integration, and test processes and recommend enhancements and modifications;*

j. *conduct formal and informal reviews at predetermined points throughout the system life cycle;*

k. audit subcontractors, suppliers and outsource companies to ensure that appropriate standard practices are applied;

l. be competent in technical disciplines as applied to government and commercial information and communications systems.

SECTION 14: INTEGRATED LOGISTICS SUPPORT (ILS)

14.1. General

14.1.1. This section outlines the supportability requirements of the project. It addresses the ILS elements requirements.

14.1.2. Requirements for the inclusion of all Contractor's identified activities and milestones are described in 4.2: Overall project and key milestones schedule.

> [SOW-686] *The Contractor SHALL use the [AIA/ASD SX000i, 2016] specification as guidance when establishing and conducting the ILS Process, in accordance with the requirements of the contract.*

14.2. Integrated Logistics Support Plan (ILSP)

> [SOW-687] *The Contractor SHALL provide and maintain an Integrated Logistic Support Plan, tailored to the Project Program phases.*

> [SOW-688] *The Contractor SHALL develop the ILSP in accordance with the requirements described in this section.*

14.2.1. The ILSP is a standalone Product Lifecycle documents that will survive the project post-FSA. As such, these documents are not to be submitted as part of the PMP, but will be part of the Technical Proposal.

> [SOW-689] *The Contractor SHALL ensure compatibility between the ILS management documentation and the System Management Plan by providing the ILS relevant inputs for the System Management Plan*

> [SOW-690] *The Contractor SHALL detail in the ILSP how Integrated Logistics Support will be designed, managed, procured and provided throughout the system lifetime.*

> [SOW-691] *The Contractor's initial version of the ILSP SHALL be provided to the Purchaser for acceptance.*

14.2.2. The acceptance of the ILSP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

> [SOW-692] *The Contractor SHALL maintain and update the ILSP as required to reflect changes in the PBLs, in the SoW, or in support arrangements for any SOA & IdM Platform CIs.*

14.3. Maintenance and Support concept

> [SOW-693] *As an Annex of the ILSP and in accordance with ANNEX B, the Contractor SHALL develop and maintain the SOA & IdM Platform Maintenance and Support Concept that defines the maintenance and support environment, constraints, locations, procedures, artefacts, organisation and personnel skills to maintain the Delivered Baselines of the platform.*

> [SOW-694] *The Contractor's Maintenance and Support Concept SHALL refer to the functional and non-functional Requirements of the SOA & IdM Platform.*

[SOW-695]   The Contractor's Maintenance and Support Concept SHALL define the Maintenance and Support tasks at any level of support and at any level of maintenance.

[SOW-696]   The Contractor's Maintenance and Support Concept SHALL define the Delivered Baselines maintenance and supply flow amongst the various NATO locations, organisations, groups, and people.

[SOW-697]   The Contractor's Maintenance and Support Concept SHALL define and describe the Maintenance and Support process interfaces to the other processes.

[SOW-698]   The Contractor SHALL define the 2nd and 3rd Level Support process interfaces to the other processes, including the existing NCI Agency's Service Desk (1st Level of Support).

[SOW-699]   The Contractor's Support process interface definition SHALL include the input and output information, its structure, the communication path, POCs, the time constraints for sending and receiving information, and quality criteria to evaluate the integrity of the interface.

[SOW-700]   At each Support and Maintenance Level, the Contractor's Support Concept SHALL describe the support environment, constraints, locations, procedures, artefacts, organisation and personnel.

[SOW-701]   The Contractor's procedural description SHALL include objective(s), triggering event(s), input(s), output(s), task(s), roles and responsibilities using a Responsible, Accountable, Consulted, Informed (RACI) matrix, constraints, exceptional case(s), and tool(s) support.

[SOW-702]   The Contractor's SOA & IdM Platform ILSP SHALL be based on the established Support Concept, approved by the Purchaser.

14.3.1.   Support Plan

[SOW-703]   As part of the Maintenance and Support Concept, the Contractor SHALL implement the Supply Support Plan.

[SOW-704]   The Contractor's Supply Support Plan SHALL:

    a. define the Supply Support requirements;

    b. describe the procedures for the provisioning, procurement, and acquiring of spare/repair parts, inventories, and consumable material for PBL and the OBL during the system lifetime.

14.4. Logistic Support Analysis

[SOW-705]   The Contractor SHALL conduct a Logistics Support Analysis (LSA) Process, tailored to support the specific scope of the System operation activities.

[SOW-706]   The Contractor's LSA SHALL include, as a minimum:

    a. Reliability, Availability, Maintainability and Testability (RAMT) responsibility, analysis and procedure :

NATO UNCLASSIFIED

    i.   *the RAMT analysis SHALL clearly capture and display the RAMT characteristics of each main platform component, aggregated up to the level of sub-system, and subsequently the entire system;*

    ii.   *the RAMT analysis SHALL be used to calculate and predict intrinsic availability and operational availability, as defined in SRS, for each type of subsystem, each type of node and each type of end-to-end connection;*

    iii.   *the Contractor SHALL ensure that the first issue of RAMT analysis is performed and delivered before SDR and accepted at SDR.*

b.   *planning of the identification of operation and Service Management and Control (SM&C) tasks;*

c.   *planning of a Task Analysis for operation tasks, SM&C tasks, corrective maintenance tasks and preventive maintenance tasks;*

d.   *Allocation of each Operational and Maintenance task to the correct Level of Support/Maintenance (Level of Repair Analysis (LoRA));*

e.   *Planning and execution of the Operation and Maintenance Procedures Verification Test;*

f.   *Total Cost of Ownership Analysis, which SHALL include the warranty cost and all the operational costs and all the maintenance cost for ALL the support and Maintenance levels for at least 5 years after FSA;*

g.   *Warranty Management and Obsolescence Analysis and Management.*

[SOW-707]   *The Contractor SHALL develop and maintain the necessary Support Cases in which all LSA activities SHALL be documented. The Support Case SHALL include:*

a.   *Reliability, Availability, Maintainability and Testability (RAMT)results and calculation;*

b.   *the complete data set of the Task Analysis, including listings of all operation tasks, SM&C tasks, corrective maintenance tasks and preventive maintenance tasks;*

c.   *The results of the Disaster Recovery Logistic Analysis;*

d.   *The results from the Operation and Maintenance Procedures Verification Test;*

e.   *The Total Cost of Ownership Analysis results;*

f.   *The Obsolescence Analysis results.*

[SOW-708]   *The Contractor's Support Case SHALL demonstrate that all LSA and RAMT requirements have been met, with correct data used and results achieved in all calculations and models.*

[SOW-709] *The Support Case SHALL provide rationale and justifications for all data and formulas used in any of the calculations and models.*

14.5. Reliability, Availability, Maintainability and Testability (RAMT) Requirements

14.5.1. Specific system level RAMT requirements and definition are included in the SRS.

[SOW-710] *The Contractor's design of the system SHALL include sufficient redundancy and other RAMT measures to ensure the requirements in this Contract are achieved and attained at an optimal TCO, minimising preventive maintenance, manpower requirement and usage of special-to-type tools and test equipment.*

[SOW-711] *Such measures taken to ensure fulfilment of RAMT requirements and optimisation of TCO SHALL be documented by the Contractor in the Support Case.*

14.5.2. Safety Assurance

14.5.2.1. Hazard definition: a Hazard is a real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (*MIL-STD 882E*).

[SOW-712] *The Contractor SHALL use the MIL-STD-882E as guideline to eliminate or mitigate risks associated with both Functional Safety and Health & Safety hazards*

[SOW-713] *The Contractor SHALL perform a System Hazard Analysis, ensure that any potential hazards to people or the environment will be identified and that associated risks are clearly documented and mitigated and/or eliminated.*

[SOW-714] *The Contractor SHALL document the result of the hazard analysis as an annex of the ILSP.*

14.5.3. Operation and Maintenance Task analysis

[SOW-715] *The Contractor SHALL develop and maintain the list of all operation tasks, SM&C (Service Management and Control) tasks, administrative tasks, corrective maintenance tasks and preventive maintenance tasks, to be used as a starting point for the task analysis.*

[SOW-716] *The Contractor SHALL perform and deliver the first issue of Operation and Maintenance Task Analysis before SDR and accepted at SDR.*

[SOW-717] *The Contractor's analysis SHALL contain also the list of procedures needed to configure the platform for mission and/or exercise environment.*

[SOW-718] *The Contractor's operation tasks SHALL be identified through analysis of the functional and no functional requirements of the new system taking into account mission scenarios and conditions under which the system will be operated.*

[SOW-719] *The Contractor's analysis SHALL examine each system function allocated to personnel and determine what operator tasks are involved in the performance of each system function*

[SOW-720]   *The Contractor's SM&C tasks SHALL be identified through analysis of all functions related to customer support and service management and control and analysis SHALL examine each customer support function and service management and control function allocated to personnel and determine what SM&C tasks are involved in the operation and maintenance of the system.*

[SOW-721]   *For each task, the Contractor SHALL determine the properties and physical resources required to execute the task. For that purpose, each task SHALL be analysed to identify and capture:*

  a. *the support level to be assigned;*

  b. *location/ facility involved;*

  c. *personnel skills required;*

  d. *task duration and frequency, reusing Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) data available;*

  e. *manpower required.*

[SOW-722]   *For each task, the Contractor SHALL perform a cost calculation based on the properties and physical resource requirements of each task.*

[SOW-723]   *The Contractor's cost calculation SHALL provide an estimated annual cost for each task.*

[SOW-724]   *The Contractor's data and results of the Task Analysis SHALL be used as input to the development of technical publication (all manuals at any level of maintenance) and the development of training material to the maximum extent possible*

14.6. Technical Documentation

14.6.1.   General

14.6.1.1.   All the requirements describing the "on-line" technical documentation are covered in the SRS, section 4.7.

[SOW-725]   *All the technical Documentation SHALL be kept updated by the Contractor and under configuration control for the entire life cycle of the system.*

[SOW-726]   *The above information contained in each technical documentation SHALL be coherent with the operational configuration (i.e. OBL) deployed.*

[SOW-727]   *The Contractor's technical documentation SHALL be developed as follows:*

  a. *on line technical publication SHALL be accessible using the platform;*

  b. *off line technical publication SHALL be accessible without using the platform.*

[SOW-728]   *Technical documentation SHALL consist (as a minimum) of:*

  a. *Technical Manuals:*

      i.   *training documentation (off line documentation);*

      ii.   *Operation and User Manuals (off line documentation);*

      iii.   *Maintenance Manual (including administration manuals) (off line documentation);*

      iv.   *OEM (for COTS product) (Off line documentation);*

      v.   *Quick user guide (on line documentation);*

      vi.   *Release Notes (On line documentation);*

      vii.   *Read me file (On line documentation);*

      viii.   *On line Help (On line documentation);*

      ix.   *Frequently Asked Question (FAQ; On line documentation);*

   b. *other project documentation as required in this SoW.*

[SOW-729] *All the activities, milestones and actors associated with the development of technical documentation SHALL be described in the Contractor's ILSP.*

[SOW-730] *All the off line technical documentation SHALL be provided by the Contractor in electronic form.*

[SOW-731] *The Platform developed by the Contractor SHALL make all relevant documentation accessible on line.*

[SOW-732] *The Contractor SHALL provide all the technical documentation in British English language.*

[SOW-733] *The Contractor SHALL maintain lowest level possible for Classification of the Technical documentation. The security classification of any on line Contractor's documentation SHALL not be higher than NATO UNCLASSIFIED.*

[SOW-734] *All Contractor's documents, however short, SHALL identify the complete name and version identifier of the software they refer to, originator, date of production, the type of document, and configuration management information of the document itself.*

[SOW-735] *All Contractor's documents SHALL contain a list of those CIs (title and version identifier) that the document or parts thereof refers to.*

[SOW-736] *The Contractor SHALL submit all final and accepted versions of documentation deliverables in Portable Document Format (PDF), with an Object Character Recognition (OCR) capability format or in Microsoft Office Professional (MsWord) compatible format.*

[SOW-737]   The Contractor SHALL submit documentation, intended for review by the Purchaser, with each modification identified through the change tracking feature or otherwise marked

[SOW-738]   The Contractor's developed manuals SHALL supplement the off-the-shelf OEM documentation the Contactor SHALL provide with the SOA & IdM Platform system

[SOW-739]   The Contractor SHALL capture and document lessons learned during the System development and the System Installation.

14.6.2. Training Documentation

14.6.2.1.   All the Training Documentation Requirements are in SECTION 14.7: Training

14.6.3. Operation and user Manuals

[SOW-740]   The Contractor SHALL develop, provide and maintain the System Operation Manual (SOM)

[SOW-741]   The Contractor's developed Operation Manual SHALL describe the complete system by the explanation of functional blocks and Configuration Items

[SOW-742]   The Contractor's developed Operation Manual SHALL define the in-depth, step-by-step procedure how to operate the system and how to perform Level 1 maintenance tasks

[SOW-743]   The Contractor's developed SOM SHALL include all the Standard Procedures in order to safely operate and use the platform.

[SOW-744]   The operation described in the Contractor's developed Manual SHALL be an outcome of the Operation and maintenance Task Analysis as described in SECTION 14.5.2

[SOW-745]   The Contractor SHALL include each and any procedure as a minimum the following information:

> a. location/ facility involved (if the operation is performed remotely, it has to be specified);
>
> b. personnel skills required;
>
> c. task duration and frequency, reusing MTBF and MTTR data available;
>
> d. manpower required;
>
> e. tools and special tools required (if any);
>
> f. the steps needed to perform the operation.

14.6.4. Maintenance and Administration Manuals (which includes all the Admin and Platform Manuals)

[SOW-746]   The Contractor SHALL develop, provide and maintain the System Maintenance and Administration Manual.

[SOW-747]   The Contractor's Maintenance Manual SHALL:

> a. contain all the possible Scheduled and Unscheduled Maintenance Procedure and all the possible Administration Procedures as requested in SECTION 14.5.2; the Contractor SHALL ensure that all

Configuration Items and all items required for maintenance are included in this full product breakdown list;

b. *define the in-depth, step-by-step procedure how to perform the 1st, 2nd and 3rd level corrective and preventive maintenance tasks and SM&C tasks;*

c. *contain a full product breakdown list.*

14.6.4.1. Requirements for the manuals are described in SECTION 14.5.2 Safety Assurance, and 14.5.3 Operation and Maintenance Task analysis.

[SOW-748] *The Contractor's manual SHALL include an annex with troubleshooting information. The troubleshooting annex SHALL provide a break-down on actions to solve a full range of (potential) problems or provide workarounds (Problem Management).*

[SOW-749] *The Contractor's manual SHALL contain all the possible configuration information and settings.*

[SOW-750] *The Contractor's Maintenance Manual SHALL also include all information, illustrations, and procedures required for the installation, configuration, provisioning, testing, repairing, replacing and troubleshooting of an item CI.*

[SOW-751] *The Contractor's manual SHALL contain all the possible information on the use and the locations of the log files*

[SOW-752] *Each and any procedure in the Contractor's manual SHALL include as a minimum the following information:*

    a. *the support level to be assigned;*

    b. *location/ facility involved (if the operation is performed remotely, it has to be specified);*

    c. *personnel skills required;*

    d. *task duration and frequency (if applicable), reusing MTBF and MTTR data available;*

    e. *manpower required;*

    f. *tools and special tools required (if any);*

    g. *the steps needed to perform the procedure.*

[SOW-753] *The Contractor's Maintenance and Administration Manual SHALL include an annex with database management information.*

[SOW-754] *The Contractor's database management annex SHALL describe as minimum:*

    a. *a break-down from the user interface (fields and actions) down to the effected database tables, triggers and stored procedures;*

    b. *the Platform Logical Data Model in full detail;*

    c. *the Platform Physical Data Model, where the following items SHALL be described:*

        i. *triggers;*

> ii. *foreign keys;*
>
> iii. *tables and columns;*
>
> iv. *stored procedures and parameters.*

14.6.5. Original Equipment Manufacturer (OEM) Manuals for Commercial Off The Shelf (COTS) product

[SOW-755] *The Contractor SHALL be responsible to keep the OEM COTS manual under configuration control and to assure that all the O&M COTS Manuals will be always coherent with the Operation configuration (i.e. OBL) deployed.*

[SOW-756] *The Contractor SHALL assure that all the possible information needed to configure, operate, manage and maintain the COTS product will be in the User Manual and in the Maintenance Manual if they are no in the COTS O&M manuals.*

14.6.6. Quick user guide

[SOW-757] *The Contractor's Platform SHALL be equipped with a Quick User Guide.*

[SOW-758] *The Contractor's Quick User guide SHALL describe the frequently used user functions in a short format.*

[SOW-759] *The Contractor's Quick User guide SHALL be integrated in the "help on line" publication.*

14.6.7. Release Note

[SOW-760] *Each Contractor's Platform release SHALL be equipped with a Release Notes file which SHALL include:*

> a. *the change log describing the difference in functionality with the previous release;*
>
> b. *known issues of the current release.*

14.6.8. Read Me File

[SOW-761] *The Contractor's Platform SHALL be equipped with 'Read Me' files for specific components.*

[SOW-762] *The Contractor's Platform Read Me files SHALL at minimum contain:*

> a. *minimal system requirements necessary to run the specific Platform part;*
>
> b. *the functional changes since the latest release;*
>
> c. *the solved errors;*
>
> d. *known errors;*
>
> e. *contact information for problem reporting.*

14.6.9. On Line Help

The requirements applicable to on line help are in the SRS, section 4.8.

14.6.10. Frequently Asked Question (FAQ)

The requirements applicable to on line help are in the SRS, section 4.8.

14.6.11. Other Project Documentation

[SOW-763] *All the Other Project Documentation required SHALL respect the general requirement about publication in this SoW, and therefore SECTION 14.6.1, 14.6.12, and 14.6.13 as a minimum.*

14.6.12. Publication Criteria

[SOW-764] *The Contractor SHALL prepare and submit for approval a set of business rules which explain the harmonisation criteria of all the technical documentation in terms of fonts, numbering, bullet points and all the publication rules to be used for the complete set of documentation. The business rules will be applicable for both Paper and electronic publication.*

[SOW-765] *The Contractor's Manuals SHALL be printable if required and therefore the page format SHALL be A4, printable in loose-leaf form, and possible to be presented bound in stiff backed covers with 4-ringed binders which permit the removal and insertion of individual pages and drawings.*

[SOW-766] *The Contractor SHALL ensure that each page contains the appropriate NATO classification of the manual at the top and bottom of each page and at the top and bottom of each drawing.*

[SOW-767] *The Contractor SHALL ensure that each drawing contains the security classification in the identification block of the drawing.*

[SOW-768] *The Contractor SHALL ensure that all drawings and schematic diagrams are of the same length (not width) as other pages of the manuals.*

[SOW-769] *The Contractor SHALL ensure that electronic copies of the documentation composed and compiled by the Contractor if not delivered via Project Portal SHALL be delivered in PDF compatible or Microsoft compatible format (doc, .docx, .xls, .xlsx, .ppt, .pptx, .mpp, or other Microsoft compatible) on Universal Serial Bus (USB) memory stick.*

[SOW-770] *The Contractor SHALL ensure that OEM Manuals SHALL be delivered in the format specified above, if available. If not available in this format, one of the other common use formats will be accepted. If the commercial documentation is not available on USB memory sick, another form of electronic media is acceptable with the prior authorisation of the Purchaser PM.*

[SOW-771] *The Contractor SHALL ensure that the physical support of the electronic, optical, soft or hard copies SHALL display the highest level of the classification of its contents.*

[SOW-772] *The Contractor SHALL ensure that the Header and/or Title of the directory structure of the documentation provided in soft or hard copies SHALL bear a reminder of the highest classification level of its contents at the top and the bottom of every document page.*

[SOW-773] *The Contractor SHALL ensure that unclassified documentation is separated from classified documentation and provided on separate media (e.g. USB memory stick, Compact Disc (CD)-Read-Only-Memory (ROM) or Digital Versatile Disc (DVD)-ROM.*

14.6.13. Amendments to documentation

[SOW-774]   The Contractor SHALL be the responsible authority for the issue, control, and distribution of amendments to delivered documentation in the format provided for the associated equipment or system until expiration of the warranty period.

14.6.14. Manual Issuing Schedule

14.6.14.1.   Releases of manuals are described in SECTION 5.5.4 Documentation Delivery and Review.

[SOW-775]   The Contractor SHALL test and validate the procedures and resources described in the technical manuals.

[SOW-776]   Not later than two (2) months prior to the delivery of the SOA & IdM Platform fit at the first location, the Contractor SHALL submit a copy of the draft to the Purchaser for review.

[SOW-777]   Any resulting recommended changes, corrections and/or additions submitted by the Purchaser SHALL be incorporated by the Contractor in the final version.

[SOW-778]   The Contractor SHALL provide the final versions of each Technical Publication, in the requisite number of copies within four (4) weeks of FSA.

[SOW-779]   Until the expiration of the warranty, the Contractor SHALL remain responsible for any changes to the manuals required as a result of any omission or inaccuracy discovered in use or, whenever changes/modifications in equipment or spare parts are made under the Contractor's responsibility.

[SOW-780]   The Contractor SHALL deliver two copies on CD-ROM of the SOA & IdM Platform Operations Manuals for each of the sites, plus two copies for the NCI Agency.

[SOW-781]   In addition to the "Manual Issuing schedule", the Contractor SHALL update all Manuals as needed throughout this contract.

14.7. Training

14.7.1.   General Requirements:

[SOW-782]   The Contractor SHALL provide SOA & IdM Platform training, including both classroom and E-learning/ Computer Based Training (CBT), for the Purchaser and users designated by the Purchaser.

[SOW-783]   The Contractor SHALL provide training for the SOA & IdM Platform support staff through development and implementation of a Training Process.

[SOW-784]   All the activities, milestones and actors associated with the Training of the SOA & IdM platform SHALL be guided by the Contractor's Training Plan.

[SOW-785]   The Contractor SHALL be able to design, develop, deliver and perform the following type of training:

   a.   Classroom Training;

   b.   On-site Training (with E-Learning/CBT Capabilities, when applicable);

    c. On the Job Training (including self-study training);

    d. Train-the-trainer training.

[SOW-786]   As part of the system implementation the Contractor SHALL provide on-site training to all support staff designated by the Site POC and on all tasks required to operate and maintain and recover the SOA & IdM Platform system.

[SOW-787]   As part of the training process the Contractor SHALL provide "Train the Trainer" courses for a minimum of 10 instructors designated by the Purchaser.

14.7.1.1.   The Purchaser will provide the following basic facilities: room, power supply, tables, chairs, network connectivity.

[SOW-788]   The Contractor SHALL provide all other facilities, services and equipment (including servers and workstations for students and teachers, network equipment, all required SW, etc....) necessary to carry out the On-Site Training activities.

[SOW-789]   The Contractor SHALL identify the prerequisite of the personnel for training participation as part of the training needs analysis.

[SOW-790]   The Contractor's Reference and Testing Facility staff SHALL be trained to operate the Reference and Testing Facility, through attending a short, informal, on-site training course, prepared, organised and led by the Contractor.

[SOW-791]   The Contractor's training SHALL be provided for both Waves of the project.

[SOW-792]   The Contractor's Training Materials SHALL include training on the Transition from the Platform Wave 1 to the next Platform increment (Wave 2) (when it's realised) and how to install, configure and maintain the Modified or new Platform capability, including COTS components.

14.7.2. Training Needs Analysis (TNA)

[SOW-793]   The Training Process and Procedures SHALL be based on the results of the TNA to be performed by the Contractor.

[SOW-794]   The Contractor SHALL conduct a TNA in accordance with the [BiSC D-075-007, 2015]. The TNA SHALL include:

    a. a Target Audience Analysis;

    b. a Performance Gap Analysis;

    c. a Difficulty, Importance and Frequency (DIF) Analysis;

    d. a Training Delivery Options Analysis.

[SOW-795]   The Contractor's TNA SHALL be based on the tasks resulting from Task Analysis carried out as part of the LSA Process and on the possible gaps highlighted during the site surveys (so called Target Audience Analysis)

[SOW-796]   The Contractor's Training Needs Analysis SHALL consider all assigned staff roles involved in SOA & IdM Platform operation, administration, maintenance and support at all levels

[SOW-797]   The Contractor's TNA SHALL include the transition training requirement from the Wave 1 to Wave 2.

[SOW-798]   The Contractor SHALL deliver a TNA Report that captures the results of the TNA. The TNA report SHALL include the following:

  a. a description of the TNA approach and activities;

  b. an account of the operation, support, corrective and preventive maintenance tasks considered in the TNA;

  c. the results of the Target Audience Analysis, the Performance Gap Analysis the DIF Analysis and the Training Options Analysis;

  d. the final list of Performance Objectives in the form of Table 2 of Annex H of BiSCD 75-7, 2015;

  e. the final list of Learning Objectives in accordance with Annex G of BiSCD 75-7, 2015;

  f. one or more Course Control Document II – Course Proposals in accordance with Annex L of [BiSCD 75-7, 2015] as summaries of the proposed E&IT solutions.

14.7.3. Training Plan

[SOW-799]   The Contractor SHALL develop and provide SOA and IdM Platform Training Plan.

[SOW-800]   The Contractor's Training Plan SHALL describe how it will meet the Training requirements found after the TNA for initial and follow-on training.

[SOW-801]   The Contractor's training plan SHALL describe the quality management process for training.

[SOW-802]   The Contractor's Training Plan SHALL address all stages of training development, delivery, and support covered under this Contract.

[SOW-803]   The Contractor's Training Plan SHALL describe in a coherent way how training will be designed, developed, delivered, and maintained throughout the life of the SOA & IdM Platform.

[SOW-804]   The Contractor's Training Plan SHALL include training design documentation using the Course Control Document III – Programme of Classes template provided in [BiSC D 75-7 2015] Annex R-4.

[SOW-805]   The Contractor SHALL describe in this plan the approach to training, milestones, resource requirements, management structure, interrelationships and other tasks related for training development.

[SOW-806]   The Contractor's Training Plan SHALL describe the training documentation for each course including but not limited to the syllabuses, schedules, course prerequisites (both for attendees and physical resources), evaluations and instructors.

[SOW-807]   The Contractor SHALL recommend in this plan the mode(s) of training (e.g. formal classroom, individual computer-based, on-the-

job, commercial or a combination) and the rationale for those recommendations for each type of training (User , Administrator, etc.).

[SOW-808]   *The Contractor's training plan SHALL describe the transition training process to manage the change of training from the transition of the platform from Wave 1 to Wave 2.*

[SOW-809]   *The Training Plan SHALL describe the support to be provided (manpower, services and material).*

14.7.4.   Training Materials

[SOW-810]   *The Contractor SHALL provide all the appropriate training documentation to support the Purchaser Personnel to test, operate and maintain the SOA & IdM Platform System and its support equipment.*

[SOW-811]   *The following Platform Training Material SHALL be generated by the Contractor:*

> a. *Training Syllabus;*
>
> b. *Student Manual;*
>
> c. *Instructor Guide and Material;*
>
> d. *Learning Guide;*
>
> e. *Quick Reference card;*
>
> f. *upon completion - a Training Certificate;*
>
> g. *course evaluation feedback form.*

[SOW-812]   *The Contractor's Training documentation SHALL conform to the standards outlined in the training section of the SoW and SRS.*

[SOW-813]   *The Contractor's training materials for the SOA & IdM Platform-specific courses SHALL provide all the information required to conduct the courses and maintain the training materials.*

[SOW-814]   *The Contractor's materials SHALL follow an existing instructional methodology that links training objectives with course structure, instructional techniques, course content, and assessment tools*

[SOW-815]   *For the development of training material, the Contractor SHALL reuse existing COTS documentation and manuals to the maximum extent possible.*

[SOW-816]   *All course content SHALL be referenced by the Contractor to commercial or Contractor-developed documentation - preferably user or technical manuals - that describe the subject matter and that are available on-site to students after course completion.*

[SOW-817]   *The hands-on exercises included in the Contractor's Training Process SHALL incorporate all SOA & IdM Platform implementation activities at a site.*

[SOW-818]   *The Contractor SHALL ensure that the SOA & IdM Platform Training Materials are all provided in the UK English language. It can be assumed that all Purchasers personnel selected to attend the courses will meet the minimum Standardised Language Proficiency (SLP) of 3232 in English as specified in STANAG 6001.*

[SOW-819]   The Contractor's Training presentation materials SHALL include all slides or other information to be presented by the instructor during the course.

[SOW-820]   The Contractor's Platform Training Course (i.e., NATO End Users, Administrators, Solution Architects and Developers)) SHALL include a Training Syllabus containing the following elements:

　　　　a.　course title;

　　　　b.　course description;

　　　　c.　learning objectives, as identified in the Training Needs Analysis and confirmed in the Training Plan;

　　　　d.　entry profile;

　　　　e.　concepts, Functions and Features presented in the course;

　　　　f.　instructional methodologies to be employed in the delivery of the course;

　　　　g.　in-class assignments or laboratories;

　　　　h.　evaluation tools;

　　　　i.　performance standards.

[SOW-821]   The Contractor SHALL develop and provide a Student Handbook for each course, with necessary information on all lesson objectives and contents, guidance for all learning activities and cross-references to assist the students in achieving the course objectives.

[SOW-822]   The Contractor's Student Manuals SHALL take into account results from the DIF analysis and SHALL enable students to perform their major tasks.

[SOW-823]   The Contractor's System Administrator Training SHALL provide as a minimum the following training on the platform:

　　　　a.　how to install, configure and maintain the Platform capability, including COTS components;

　　　　b.　how to maintain the Platform and how to use the logging and performance counters provided by the Platform which, as minimum, SHALL include:

　　　　　　i.　all the configuration settings for the Platform modules, services and components;

　　　　　　ii.　how to configure the logging and uses of performance counters;

　　　　　　iii.　where to find the log files;

　　　　　　iv.　the different categories of logging;

　　　　　　v.　the different performance counter categories;

　　　　c.　how to trouble shooting the system, including actions to solve a full range of (potential) problems or provide workarounds;

　　　　d.　how to manage database information, including database tables, triggers and stored procedures;

e. *how perform back-up and restore procedures.*

[SOW-824] *The Contractor SHALL provide an Instructor's Guide for each training course.*

[SOW-825] *The Contractor's Instructor's Guide SHALL contain all necessary information to prepare and conduct lessons and to evaluate students, including exercises, quizzes, and examinations and their corresponding answer sheets and SHALL also provide notes to instructors to assist in conducting the lecture or exercise.*

[SOW-826] *Presentation materials SHALL be provided in Microsoft PowerPoint.*

[SOW-827] *The Contractor's Platform Instructor Guide SHALL detail the sequence of course instruction, providing references to the applicable training presentation materials, assignments and laboratories, evaluation tools and answer keys, Student Manual, and the Platform on-line help function. The Instructor Guide SHALL also include:*

 a. *materials for in-class assignments and laboratories;*

 b. *sample evaluation tools and answer keys;*

 c. *Training System installation and configuration procedures.*

14.7.5. Training Assessment and Evaluation

[SOW-828] *The Contractor SHALL propose student's assessment and evaluation methodology to the Purchaser as part of the Training Plan.*

[SOW-829] *The Contractor's Training Assessment methodology SHALL be based on [BiSC D 75-7 2015] sections 7-6 and 7-7 for assessment approaches and instruments and include:*

 a. *examination methodologies and certification;*

 b. *minimum score to achieve for successfully passing the course;*

 c. *course(s) to be done to get the certification for each role;*

 d. *description of Role's certification process.*

[SOW-830] *The Contractor SHALL ensure that each student is instructed at the end of each course (or use of a CBT) to complete and return the course evaluation feedback form, provided as part of the training course or CBT/E-Learning product.*

[SOW-831] *The Contractor SHALL consolidate and forward student feedback to the Purchaser following each training course in the form of a Training Evaluation Report. The report SHALL also recommend changes and improvements to the training plan based on the consolidated student feedback. The report SHALL also address student attendance, problems encountered and actions taken to resolve the problems.*

[SOW-832] *The Contractor SHALL revise/ refine and reissue course material and CBT/E-Learning products to reflect the consolidated*

student feedback and proposed improvements in the training evaluation report.

[SOW-833] *The Contractor SHALL produce Training Certificates for each training session and student.*

[SOW-834] *The certificates SHALL be delivered not later than two weeks following the completion of the training.*

14.7.6. E-Learning Training / Computer Based Training (CBT)

[SOW-835] *The Contractor SHALL provide all the appropriate training documentation to support the Purchaser Personnel to perform the trainings using the NCIA Learning management system*

[SOW-836] *All Contractor's e-learning training material SHALL be prepared in compliance with the Sharable Content Object Reference Model (SCORM) edition 2004. Preferably any e-learning material should be deliverable on the NATO Advanced Distributed Learning (ADL) platform.*

[SOW-837] *The Contractor's CBT/E-Learning material SHALL complement the SOA & IdM Platform classroom training and online help capabilities by defining and explaining key concepts and terminology of the operational processes incorporated into SOA & IdM Platform features and functions.*

[SOW-838] *The Contractor's CBT/E-Learning Package SHALL allow modifications by the Purchaser to reflect changes in the training concept and/or content without any additional cost to NATO.*

14.8. Supply Support

14.8.1. This section defines the general requirements that are applicable to all SOA & IdM Platform equipment Supply Support and Delivery

14.8.2. System Inventory

[SOW-839] *The Contractor SHALL provide the Purchaser's ILS POC with a System Inventory in electronic Microsoft Excel format at least ten (10) working days before the first delivery of equipment.*

[SOW-840] *The Contractor's System Inventory is site-specific and SHALL include, in separate chapters, all items furnished under this Contract, as follows:*

a. *all support equipment – i.e. all tools, test equipment, etc. (where applicable);*

b. *all Purchaser Furnished Equipment (PFE); (where applicable);*

c. *all documentation, such as manuals, handbooks and drawings;*

d. *all training materials.*

[SOW-841] *The Contractor SHALL deliver a complete Material Datasheet (MDS) per Site. The MDS template will be available to the contractor upon request.*

14.8.2.1. An inventory template together with a full content description for each data element will be provided to the Contractor after the CAW at the request of the Contractor.

14.8.3. Physical Labelling

[SOW-842] *All equipment delivered by the Contractor SHALL be labelled with the true manufacturer's name, part number and serial number to ensure proper and quick identification, as they are procured, stored, and issued. Nameplates in the English language with non-erasable letters/ numbers, giving the true manufacturer part number (including modification state), serial number (including revision level), NCI Agency contract number, date of manufacture, manufacturer's name and address and principal characteristics, where appropriate SHALL be provided by the Contractor.*

[SOW-843] *All equipment labels delivered by the Contractor SHALL contain a machine-readable code (e.g. barcode) compliant with [STANAG 4329] and [AAP-44(A)] and in accordance with the NATO coding schema, which will be provided by the Purchaser at the request of the Contractor.*

[SOW-844] *The Contractor's labels SHALL enable positive identification of assemblies and modules upon removal for maintenance purposes and to prevent loss of utilisation of items that have been separated from their original packages or containers.*

[SOW-845] *Whenever practicable, the Contractor label SHALL be located in such a manner as to allow it to be visible after installation.*

[SOW-846] *Marking SHALL be capable of withstanding the same environment tests required of the part and any other tests specified for the label itself.*

[SOW-847] *When possible, the Contractor SHALL ensure that letters, numerals, and other characters are of such a size as to be clearly legible.*

[SOW-848] *All the plates SHALL be properly attached by the Contractor in a prominent position on each major assembly to enable reading and control with easy access when installed.*

14.8.4. Software delivery

[SOW-849] *The Contractor SHALL provide a detailed Software Distribution List (SWDL), which SHALL detail comprehensively all CSCIs and associated software, firmware or feature/performance licenses provided under this Contract. The SWDL SHALL include, the following data elements:*

    a. *CSCI identification number;*

    b. *nomenclature;*

    c. *version number;*

    d. *license key (if applicable);*

    e. *license renewal date (if applicable);*

    f. *warranty expiration date;*

    g. *date of distribution;*

h. distribution location (geographically);

i. distribution target (server).

[SOW-850] *The Contractor SHALL make sure that all licenses are registered with the NCI Agency as end-user.*

14.8.5. Tools and Test Equipment

14.8.5.1. Tools and Test Equipment fall into two (2) categories:

a. "Special to Type" Tools and Test Equipment which are intrinsically related to SOA & IdM Platform

b. "Standard" Tools and Test Equipment which are common and are likely to be already available at NATO sites.

[SOW-851] *The Contractor SHALL deliver a fully detailed and priced Recommended Tools and Test equipment List (RTTL), covering the "Standard" Tools and Test Equipment.*

[SOW-852] *The Contractor SHALL provide "Special to Type" tools and/or test equipment if required, in particular on the Reference System and/or on the Testbed.*

14.9. Packaging, Handling, Storage, Transportation (PHST)

14.9.1. Packaging

[SOW-853] *The Contractor SHALL, for the purpose of transportation, package, crate, or otherwise prepare items in accordance with the best commercial practices for the types of supplies involved, giving due consideration to shipping and other hazards associated with the transportation of consignments overseas.*

[SOW-854] *Packing lists SHALL accompany each shipment, which SHALL include the following:*

a. *the Purchaser's Contract Number;*

b. *the NATO project number;*

c. *names and addresses of the Contractor and the Purchaser;*

d. *names and addresses of the Carrier, Consignor and Consignee (if different from Contractor or Purchaser);*

e. *final destination address and POC;*

f. *method of spriorhipment;*

g. *for each item shipped:*

   i. *CLIN number as per the SSS;*

   ii. *nomenclature;*

   iii. *part number;*

   iv. *serial number;*

   v. *quantity;*

h. *for each box, pallet and container:*

    i.   *box/pallet/container identification number;*

    ii.   *number of boxes/pallets/containers;*

    iii. *weight;*

    iv. *dimensions.*

[SOW-855]   *The Contractor SHALL fasten two copies of the packing lists in a weather-proof, sealed envelope on the outside of each box, palette and/ or container, and additionally one packing list SHALL be put inside each container/box.*

14.9.2. Handling and Storage

[SOW-856]   *The Contractor SHALL be responsible for all handling and storage of equipment, packages, boxes and containers during the project.*

[SOW-857]   *The Contractor SHALL also be responsible for organising and operating any handling equipment and storage facilities required.*

14.9.3. Transportation

[SOW-858]   *Unless clearly specified otherwise, the Contractor SHALL be responsible for transportation of all equipment furnished under this Contract from its site in a NATO nation to its respective implementation destination.*

[SOW-859]   *The Contractor SHALL be responsible for any insurance covering these shipments.*

14.9.3.1.   All packages, boxes will be inspected visually by the Purchaser's POC at final destination to ensure that no damage has occurred during transport and that all packages, boxes and containers detailed in the packing list have been accounted for. The Purchaser will in no case open any package.

14.9.4. Customs

[SOW-860]   *The Contractor SHALL be responsible for customs clearance of all shipments into the destination countries. It is the Contractor's responsibility to take into account delays at customs. He SHALL therefore consider eventual delays and arrange for shipment in time. Under no circumstances can the Purchaser be held responsible for delays incurred, even when utilising Purchaser provided Customs Form 302*

14.9.4.1.   Notice of Shipment

[SOW-861]   *Ten (10) working days before each shipment of supplies, the Contractor SHALL provide the Purchaser with a Notice of Shipment comprising the following details:*

    a. *Shipment Date;*

    b. *Purchaser Contract Number;*

    c. *CLIN;*

    d. *Consignor's and Consignee's name and address;*

    e. *Number of Packages/Containers;*

    f. *Gross weight;*

    g. *Final/Partial Shipment;*

    h. *Mode of Shipment (e.g. road…);*

    i. *Number of 302 Forms used.*

14.9.4.2.   Shipment

[SOW-862] *The Contractor SHALL ship all required software, documentation, and installation or testing tools to the locations designated by the Purchaser.*

[SOW-863] *The Contractor SHALL be responsible for resolving any loss incurred in shipping.*

14.10.   Warranty and Operation Support

14.10.1. Warranty

[SOW-864] *The Contractor SHALL warrant that all equipment and software furnished under this Contract and all installation work performed under this Contract conform to the requirements and is free of any defect in material, code or workmanship for a period starting at date of each Wave PSA to date of PSA plus one (1) year.*

[SOW-865] *The Contractor SHALL fix/repair/replace all items received as per his internal procedures with the highest priority allocated.*

[SOW-866] *If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any supplies, the Contractor SHALL coordinate with the Purchaser and promptly correct the defect.*

[SOW-867] *Defective magnetic, solid state and electronic media storage devices (e.g. USB memory sticks, CD-ROMs, DVD-ROM's, solid state storage drives, hard drives) SHALL remain NATO property, at no additional cost, and not be returned to the Contractor when being replaced.*

[SOW-868] *Any such defective storage devices SHALL be replaced by the Contractor with new storage devices at no additional cost to the Purchaser.*

[SOW-869] *The Contractor SHALL be responsible for the provision of any alternative or superseding items, should the original part be no longer available, ensuring compliance with the original design provided by this Contract.*

[SOW-870] *During the warranty period, the Contractor SHALL be responsible for supplying all COTS hardware and software upgrades and updates.*

[SOW-871] *The availability of COTS hardware and software upgrades and updates SHALL be made known to the Purchaser and, if proposed for introduction by the Contractor for whatever reason, including any corrective action for an identified fault, SHALL always be subject to Purchaser approval.*

[SOW-872] *The Contractor SHALL not be responsible for the correction of defects in Purchaser furnished property, except for defects in*

installation, unless the Contractor performs, or is obligated to perform, any modifications or other work on such property. In the event described above, the Contractor SHALL be responsible for correction of defects that result from the modifications or other work.

14.10.1.1.   As an option the Purchaser can request additional warranty under the same conditions on a yearly basis.

14.10.2. Operation Support (CLS)

14.10.2.1.   As an option the Purchaser can request a Contract for Logistic Support (CLS) which follows the requirements of this section [14.10.2].

> [SOW-873]   *The Contractor SHALL provide CLS services in accordance with the requirements of this section for a period of five (5) years.*

> [SOW-874]   *The contractor SHALL integrate the Wave 2 CLS with Wave 1 CLS if the purchaser will activate Wave 2 CLS.*

> [SOW-875]   *The CLS services for 3rd and 4th Support and Maintenance levels SHALL be provided off-site from the Contractor's premises.*

> [SOW-876]   *The Contractor SHALL integrate Warranty with the CLS services.*

> [SOW-877]   *The contractor SHALL provide a CLS Plan as part of the ILSP, which explains in detail how the contractor fulfils all the CLS requirements in the contract and how the CLS services will be integrated with the Purchaser Operations.*

14.10.2.2.   Hardware and Sofwtare support during CLS

> [SOW-878]   *During the CLS period, the Contractor SHALL provide software and hardware support at all levels of support and at all levels of maintenance as described in ANNEX B.*

> [SOW-879]   *During the CLS period, as part of obsolescence management, the Contractor SHALL be responsible for the management, provision and implementation of any alternative or superseding hardware and software items should the original item be no longer available or no longer supported, ensuring compliance with the original design provided by this Contract.*

> [SOW-880]   *The availability of and need for superseding items SHALL be made known to the Purchaser and, if proposed for introduction by the Contractor for whatever reason, including any corrective action for an identified fault, shall always be subject to Purchaser approval.*

> [SOW-881]   *Defect magnetic and electronic media storage devices (i.e. CD-ROM's, DVD's, USB sticks, solid state drives, hard drives) SHALL remain NATO property and shall not be returned to the Contractor when being replaced under CLS arrangements*

> [SOW-882]   *The Contractor SHALL ensure that all software procured under the Contract have software licenses valid for the duration of the contracted CLS.*

> [SOW-883]   *The contractor SHALL renew Software licenses when required and for a duration sufficient to cover the contracted CLS period.*

14.10.2.3. Performance Monitoring, Reporting and Improvements during CLS

[SOW-884] The Contractor SHALL implement and document processes to record all events relating to the security of the SOA&IdM Capability, in a form of audit logs.

[SOW-885] The Contractor SHALL implement and document an input for NCIRC in support on-line security monitoring and management of NATO's CIS infrastructure, off-line analysis of incidents, and incident handling. The SOA&IdM input for NCIRC SHALL include event logs related to the SOA internal operations as well as to the Identity and Access Management (IAM) processes where SOA&IdM platform capability is utilized.

[SOW-886] The Contractor SHALL provide a monthly CLS Performance Report during the contract CLS period which includes, as a minimum, the following:

    a. actual measurements of the performance and quality figures defined in the SRS;

    b. details of all failures and warranty cases that have occurred during the reporting period;

    c. applied changes to the product baseline; and

    d. expended resources.

[SOW-887] For the purpose of monitoring and reporting, the Contractor SHALL maintain a configuration management database (CMDB) and a known error database (KEDB) for the duration of the contracted CLS.

[SOW-888] If the actual achieved performance and quality figures of SOA & IdM Platform does not (or no longer) satisfy the Performance and Quality figures requirements in this Contract then the Contractor shall modify the design and implementation of the platform to fulfil the requirements in this Contract.

[SOW-889] The CMDB and KEDB SHALL be provided to the Purchaser at the end of the contracted CLS period in a non-proprietary, electronic format.

14.10.2.4. Documentation Support during CLS

[SOW-890] The Contractor SHALL update and re-issue any documentation (including training material) delivered under this Contract each time a change is implemented resulting from the CLS arrangements and requirements in this Contract.

14.10.2.5. Training support during CLS

[SOW-891] During the CLS period, the Contractor SHALL provide an Annual Recurrent Training Programme, which consist of:

    a. one SOA&IdM training course for NCIA designated staff (Operators, Maintainers, train the trainers);

    b. an updated Computer-Based Training package, in accordance with the requirements of Section 14.7

[SOW-892] *The Contractor's training courses SHALL accommodate a maximum number of five (5) students per course and take place at Purchaser specified NATO locations and at Purchaser specified dates.*

14.11. Engineering and Integration Support to other Projects during CLS

As an option the Purchaser can request an Engineering and Integration Support to other project during the CLS contract.

[SOW-893] *The Contractor SHALL provide dedicated Engineering and integration support to a purhcaser's selected projects to enable migration of the functional service to SOA and IdM platform delivered under this Contract.*

[SOW-894] *The contractor SHALL integrate the Engineering and Integration activities in the CLS 3rd level of support activities, if it is activated by the Purchaser.*

14.12. Disposal of Equipment

14.12.1. The disposal of any legacy equipment will be the responsibility of NATO, in compliance with applicable policy.

[SOW-895] *The Contractor SHALL be responsible for the removal of the items from the installation facilities as required, and SHALL work with local site personnel to ensure the controlled removal and disposal.*

ANNEX A : System Requirements Specification (SRS)

ANNEX B : Maintenance and Support Concept (After PSA)

B.1. Introduction

The Maintenance Process need to ensure the maintainability of the PBL and the OBL. The Baseline Maintenance Process implements modifications to be made either proactively or reactively to the PBL to correct faults and/or deficiencies, to improve performance or other PBL attributes, or adapt the PBL/OBL to a modified environment. The maintenance concept is based on the incident management concept and each and any maintenance and support level could be managed by a different organisation during the Life Cycle of the project. The responsibility of each level, in accordance to the life cycle of the project will be part of the Contract. The Baseline Maintenance process is decomposed into 1st, 2nd, 3rd and 4th Level Maintenance tasks.

The maintenance concept includes the following activities:

a. the Maintenance of all the Configuration Items and all related items,
b. the execution of all the required preventive and corrective maintenance activities for all the system and its subsystems for each level,
c. the allocation of the Maintenance tasks to the respective maintenance levels and the related organisation.

B.2. Definition

Level of Support: Level of support indicates a specific extent of technical assistance in the total range of assistance that is provided by an information technology product to its customer. The Service management is divided in three different level of service, which interface each other, in order to activate the proper level of maintenance in accordance with the event (incident) happened on the system.

Level of Maintenance: are various echelons at which maintenance tasks are performed on systems and equipment. The levels are distinguished by the relative sophistication of skills, facilities and equipment available at them. Thus, although typically associated with specific organisations and/or geographic locations, in their purest form, the individual maintenance levels denote differences in inherent complexity of maintenance capability.

B.3. Support Concept

The Support concept is the set of activities and processes in charge of managing the various level of maintenance and to escalate the problem to the appropriate level in accordance with the defined responsibilities.

It uses a systematic approach, to minimise the logistic delay and assure the maximum level of Service and Operation availability.

It is based on the Incident management process defined in ISO/IEC 20000 and ITIL framework or equivalent.

The Service management is divided in three different level of service, which interface each other, in order to activate the proper level of maintenance in accordance with the event happened on the system.

The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.

The process of Support & Maintenance and the escalation process between the various levels is shown in below
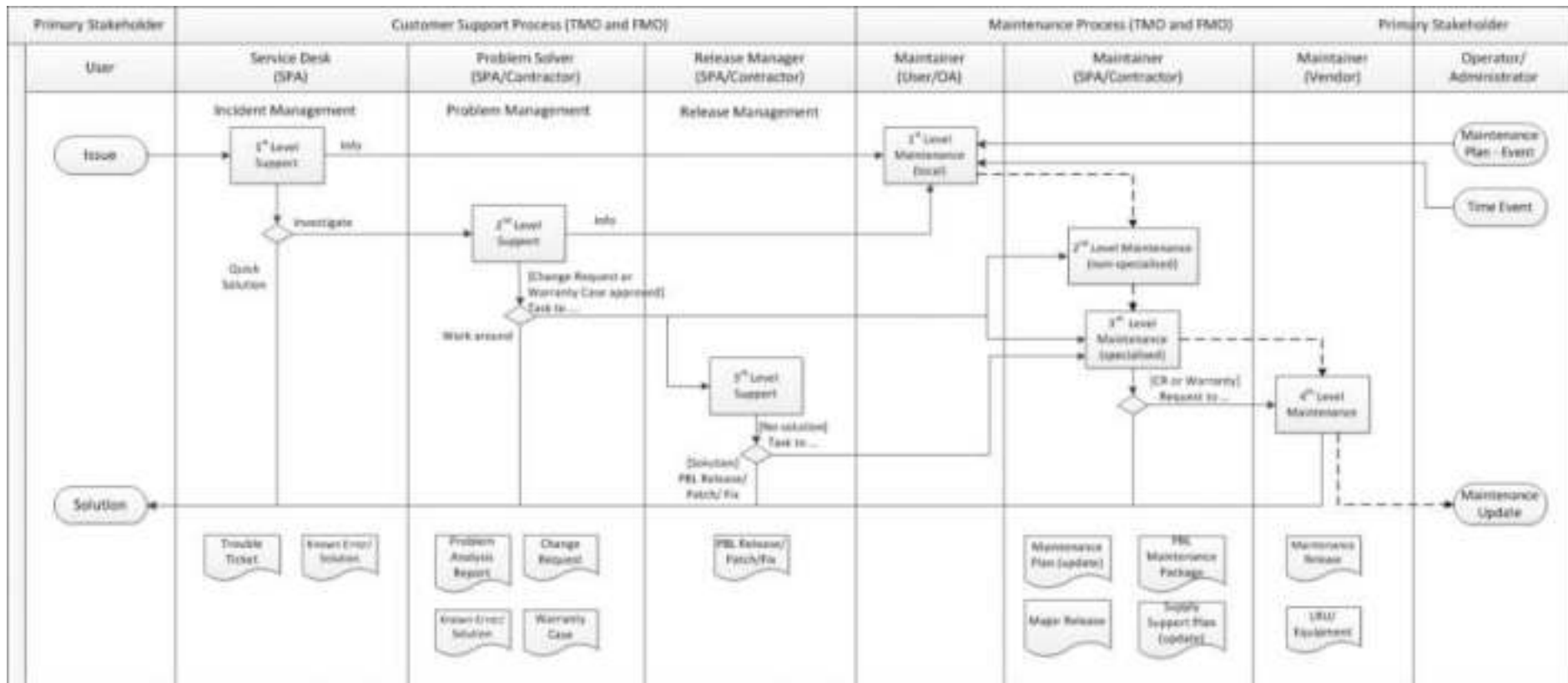
Figure 13: Support and Maintenance Concept Process

B.3.1. First Level Support Process

The 1st Level Support Process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket (TT)), performs an initial assessment and distributes it to the predefined actors to solve it

B.3.2. Second Level Support Process

The 2nd Level Support Process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

The Problem Management process receives the TT from the Service Desk and performs the following tasks (not limited to):

a. (Re-)evaluation of TT category, criticality and priority,
b. Identification of the root cause of the issue (e.g. by issue replication testing),
c. Identification of workarounds,
d. Identification and initial planning of possible short, medium and long-term solutions (e.g. workarounds, patches, or new baseline or CI releases),
e. Create Problem Analysis Report and Change Request incl. schedule of implementation, and synchronisation with the Baseline Maintenance process;
f. Presentation of the Problem Analysis Report and Change Request to the CCB for approval,
g. Monitor and Control the approved Change Request during implementation,
h. Trigger 3rd Level Support and/or 3rd Level Maintenance process to implement the Change Request, in case the incident cannot be solved at 2nd level;
i. Perform the post- Change Request implementation review.

B.3.3. Third Level Support Process

The 3rd Level Support Process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

The Deployment and Release Management process receives the approved Change Request from the 2nd Level Support and performs the following tasks (not limited to):

a. Release of the solution (release unit/record)
b. Development of the solution (e.g. new CI Fix, Repair, Replacement, Patch, or Release),
c. Testing of the solution (e.g. Regression testing, issue/deficiency replication testing),
d. Update of baseline content and status,
e. Delivery and deployment of the solution

B.4. Maintenance Concept

The Maintenance Concept is the set of activities and processes in charge of restoring the system functionality in the shortest time possible.

The Maintenance to be provided in a proactive and reactive manner by the Service Provider.

All proactive Maintenance tasks are defined in the Service/Capability and Site specific O&M Manuals (What) and corresponding Procedures (How) and scheduled in the Maintenance Plan.

Reactive Maintenance activities are triggered by Incident and Change Requests coming either from the Service Customer via the Customer Support Services or from the OEM/Vendor

B.4.1. Frist Level of Maintenance

It is responsible for the very basic maintenance activities. It is responsible to activate the second level of maintenance when it is needed.

It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding O&M Manual. All 1st Level Maintenance procedures do not require specialised tools and/or specialised personnel.

B.4.2. Second Level of Maintenance

It is responsible of isolation and resolution of system-level maintenance and management of deficiency reports and repair. It is responsible to activate the third level of maintenance when it is needed.

It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. All 2nd Level Maintenance procedures do not require specialised tools and/or specialised personnel.

B.4.3. Third Level of Maintenance

It is responsible of any support that involves a change to the system baseline, such as software patches or new releases. It is responsible of specialised hardware repair, if requested.

It implement the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. 3rd Level Maintenance procedures can require specialised tools and/or Personnel

B.4.4. Fourth Level of Maintenance

It is the hardware vendor or the software original developer. It is activated from the 3rd level of maintenance only when it is needed.

ANNEX C : Purchaser Furnished Information, Purchaser Furnished Equipment (PFE), Infrastructure & Services

C.1. Introduction

C.1.1. This section contains information describing Purchaser furnished information, PFE, Infrastructure and Services. This includes information regarding Purchaser Processes, Related Projects and Background Information on the way in which the current IT infrastructure is operated today. At various stages of the SOA and IdM Platform contract execution the Purchaser will provide to the Contractor further Information, Equipment, Services and Infrastructure for use by the Contractor during the execution of the contract

C.1.2. At EDC + 2 (two) weeks the Purchaser will deliver to the Contractor a package of Purchaser Furnished Information, if requested by the Contractor. That package will contain the following:

a. a copy of all government standards and regulations cited in the contract or a reference to where they may be obtained;
b. a set of Information Assurance Documentation and Policies including security settings for back end and user facing equipment currently in use;
c. an updated version of the Related Project Information.

C.2. Purchaser provided software

C.2.1. The Purchaser will provide the following licences/software:

a. Microsoft:
    i. Windows Server – Datacenter or Standard;
    ii. Structured Query Language (SQL) Enterprise Server;
b. Enterprise desktop license (in support of the desktop provisioning) containing:
    i. Windows desktop Operating System;
    ii. Office Professional Plus;
    iii. Enterprise Client Access licenses for Windows Server, Exchange, SharePoint, Lync, System Centre and SQL Server;
c. McAfee:
    i. McAfee Endpoint Protection;
    ii. McAfee Total Protection.

C.3. Purchaser Processes

C.3.1.

NCI Agency Business Processes are shown in Figure 14. The business processes are defined in a set of documents, including: Agency Directives and Process Definition and Execution Documents. A number of these, either in draft or final form are included in the documentation released to Bidders with the IFB. At CAW (EDC+2 (two) weeks) an update of these documents will be provided to the successful Contractor. These should be adhered to, to the extent possible, while still meeting the requirements of the SOA & IdM Platform project
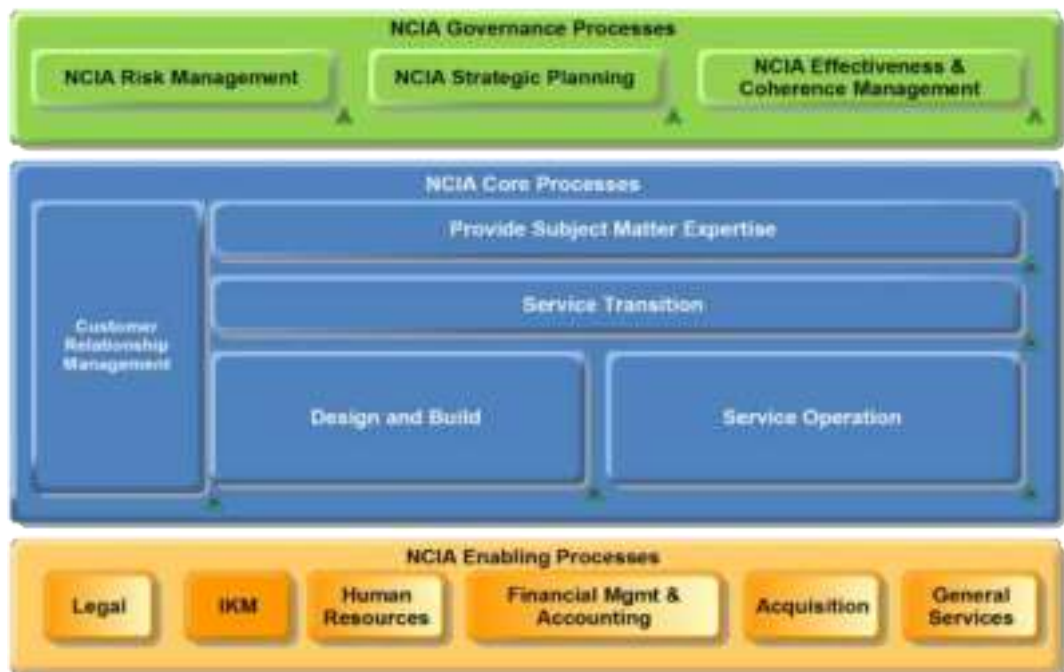
Figure 14: NCI Agency Level 0 Business Processe
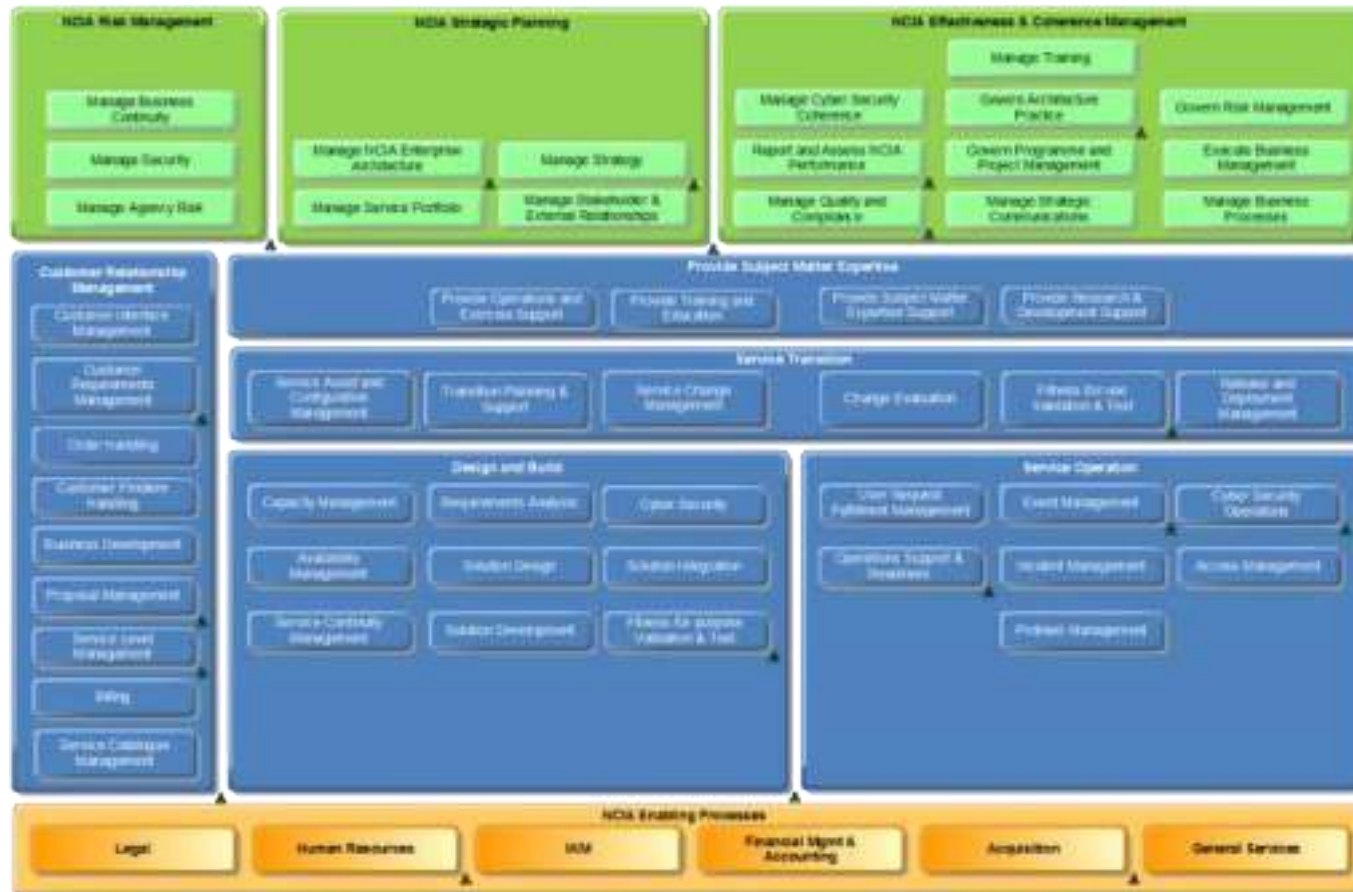
IFB_CO-14176-SOA-IDM

Figure 15: NCI Agency Level 1 Business Processes
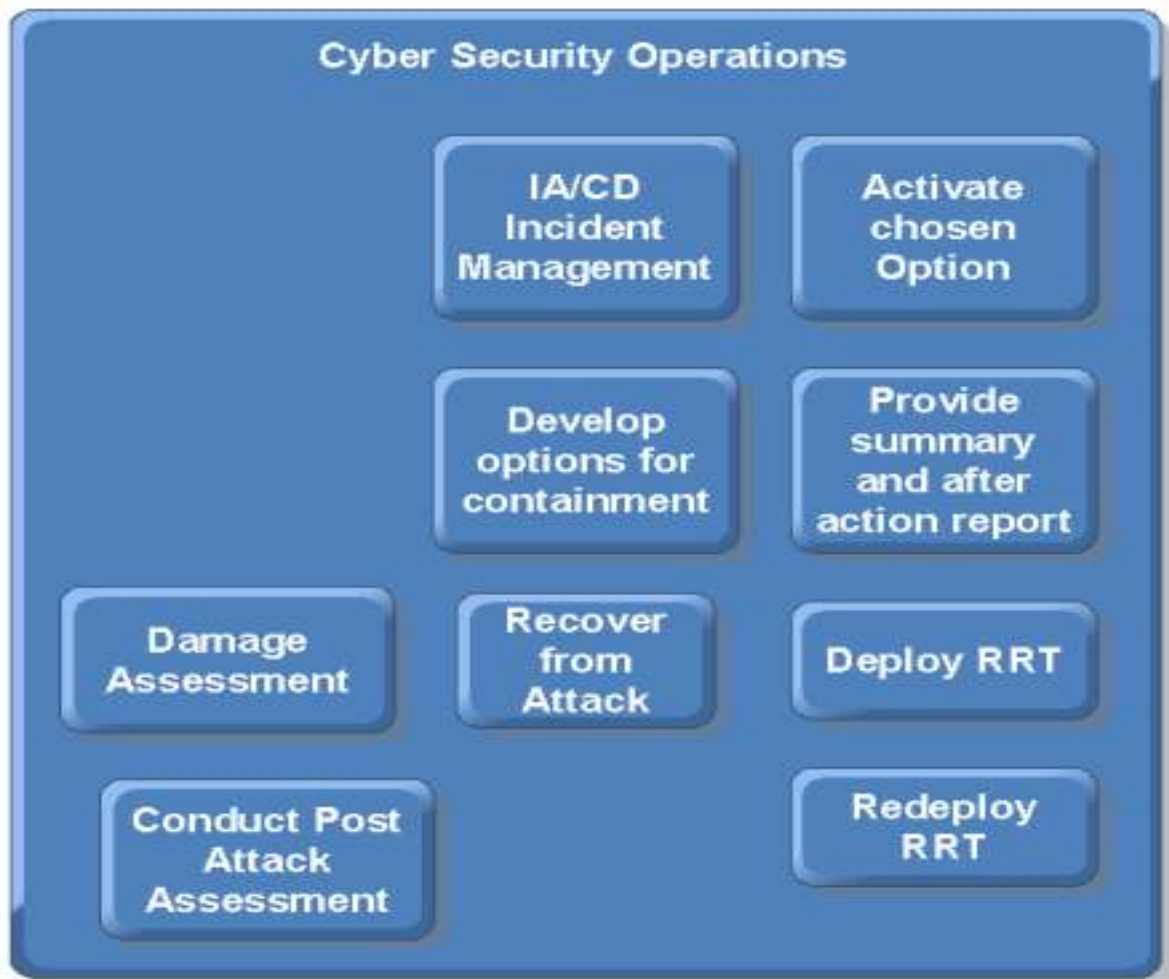
Figure 16: CIS Security Operations

C.3.2. The Purchaser Processes is described below in Table 16:

No.	Processes	Directive	Process Definition and Execution Document (PDED)	Process Ownership
1	Request Fulfilment		Approved	SMC SL
2	Incident Management		Approved	SMC SL
3	Problem management		Not started	SMC SL
4	Operational Change Management	Pending for approval	In progress	SMC SL
5	Service Change Management			Service Strategy
6	Release Management	Approved		SMC SL
7	Deployment Management	Approved		SMC SL
8	Event Management			SMC SL
9	Transition Planning & Support			Service Strategy
10	Service Continuity Management			Service Strategy
11	Service Asset & configuration Management			Service Strategy
12	Availability Management			Service Strategy
13	Capacity Management			Service Strategy
14	Service Level Management			Service Strategy

Table 16: Purchaser Processes

C.4. Background Information

C.4.1. Bi-SC AIS security domain overview

Figure 17 below shows the current security domain structure in NATO Networks.
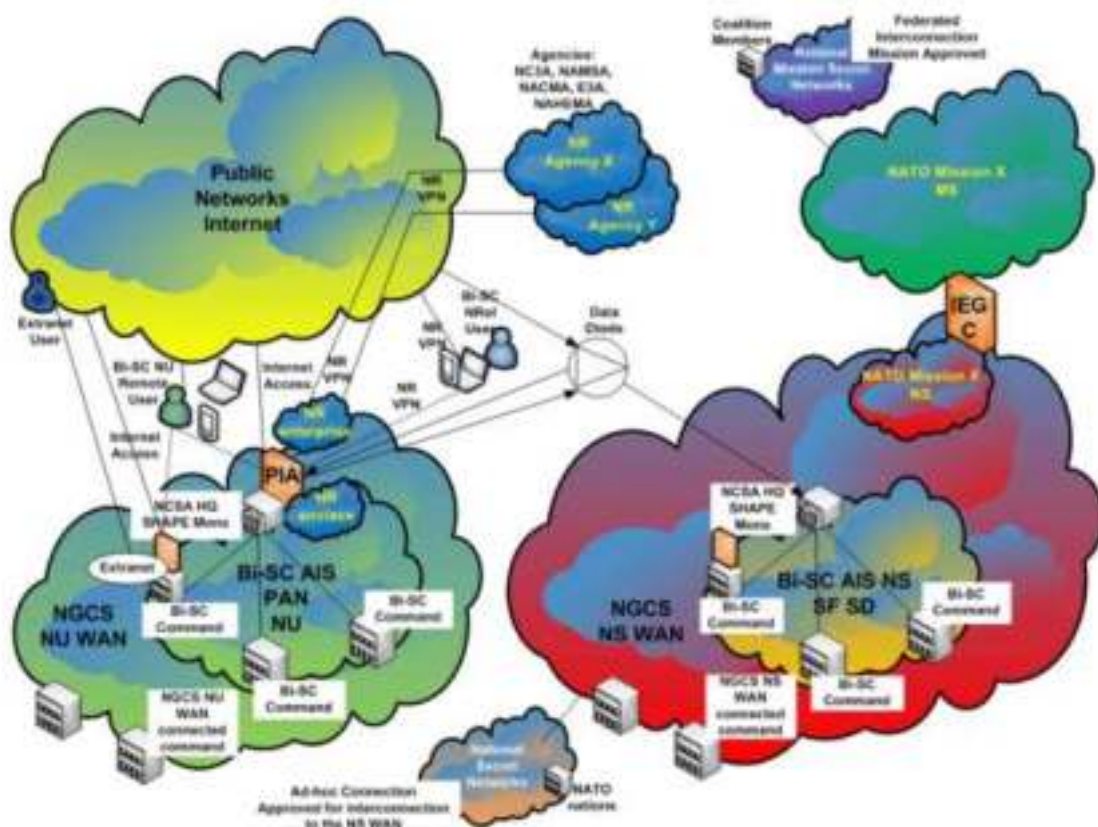
Figure 17: Bi-SC current NU-NR-NS Environment

C.4.2. Information Assurance Documentation

C.4.2.1.   Besides the already listed IA related documentation in this SoW, additional security configuration guidelines are available that will be released to the winning Contractor at CAW. The Security Configuration Catalogue contains a list of the most recent security configuration guidelines.

C.4.3. Firewall Management

C.4.3.1.   The NCI Agency centrally manages Firewalls and Guards devices that interconnect to the NATO-wide networks. Some firewalls will remain as they are located in sites or on networks that are outside the scope of ITM and SOA & IdM Platform.

C.4.3.2.   All NATO managed Firewalls are centrally managed by NCI Agency from management servers on NU and NS level from facilities currently at SHAPE (and backup facilities at Brunssum, NL). These will be centralised and moved to the Service Operations Centres as part of application migration.

C.4.3.3. NCI Agency supports two firewall products: CheckPoint and Palo Alto Networks. Both of them are managed from appropriate management servers (Provider-1 and Panorama respectively). In general local staff (from sites where firewall enforcement modules are installed) have no administrator rights and can only conduct basic tasks related with enabling connectivity with management servers and accessing logs from the local firewall.

C.4.3.4. Local staff view logs via a third party log aggregation tool known as Splunk and view Policies via a third-party tool known as Firemon. Two complete sets of infrastructure are currently employed on the NS and NU networks.

C.4.3.5. Firewall monitoring is integrated with NCIRC. Security events from firewalls are initially submitted to the associated Firewall Management Server, and later to the appropriate ArcSight Connector and Enterprise Management System (EMS). Figure 18 illustrates how it works for the CheckPoint Firewalls:

C.4.3.6. The logs from the firewall enforcement module, and firewall system health status information are sent to a central management server Provider-1 for CheckPoint and Panorama for Palo Alto. From Provider 1 and Panorama, logs are sent via an ArcSight Connector to the ArcSight Logger for analysis and correlation with logs from other devices.

C.4.3.7. The ArcSight Logger is able to correlate, filter, compress and schedule the logs are to be transferred to the ArcSight Security Incident Event Management (SIEM) database at NCIRC.

C.4.3.8. The connection to ArcSight is via a custom built connector known as a FlexConnector. The Provider-1 connection utilises CheckPoint's proprietary Log Export API (LEA) protocol and Panorama is based on Syslog.
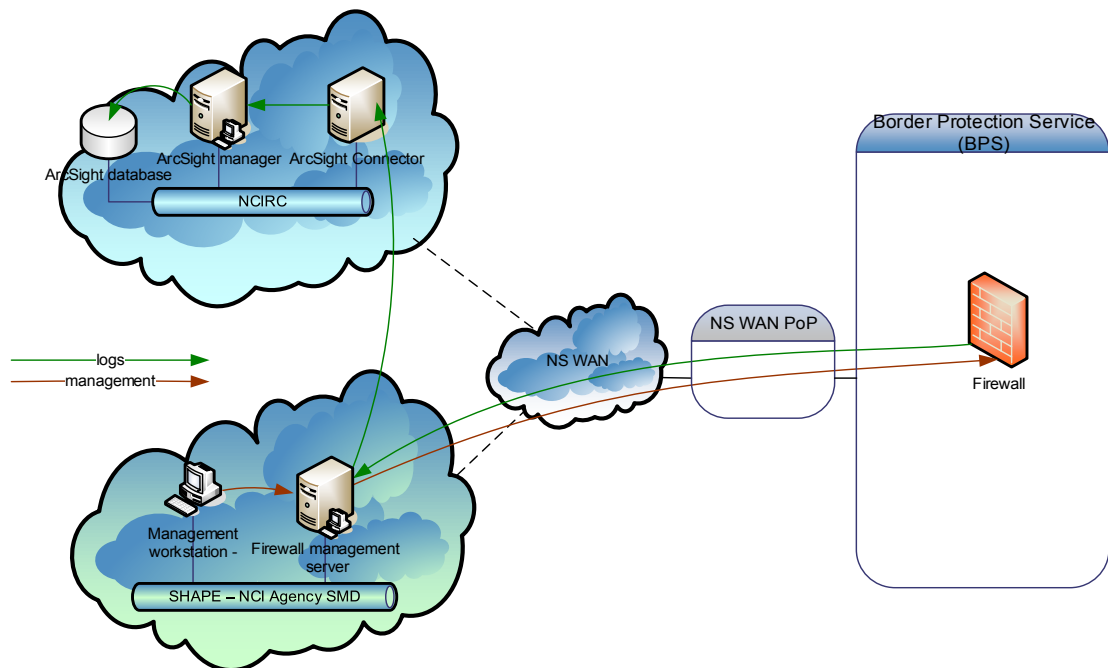
Figure 18: Current Central Firewall Management Solution

C.4.4. NATO Enterprise SMC Systems

C.4.4.1.　　NATO Configuration Management System (NATO CMS)

C.4.4.1.1　　NATO IT infrastructure is distributed, complex and is composed of diverse systems. Therefore there are multiple configuration and asset sources integrated with current NATO CMS. The Purchaser aims at federating all available CMDBs under the NATO enterprise-level CMS (currently being built on the BMC Atrium toolset) to ensure best possible coverage of the process.

C.4.4.1.2　　The IT Modernisation project is expected to simplify the diversity of infrastructure and the asset and configuration management. However, it is also expected that the transition period will be long enough so integration with legacy asset and configuration databases should be kept during the project. The Contractor should use NATO CMS to manage the transition to new infrastructure and migration of hosted services.
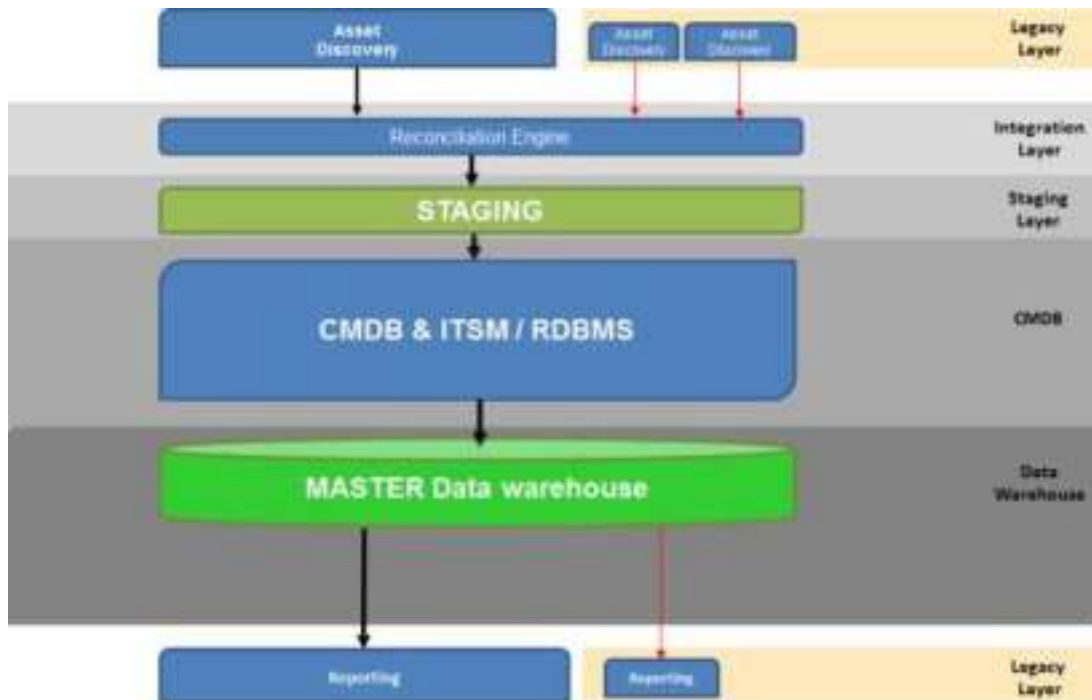
Figure 19: NATO Enterprise level CMS Logical Architecture

C.4.4.1.3   NATO Enterprise level CMS is based on BMC Atrium CMDB wrapped by a staging and data ware house layers. There are multiple configuration data sources that require filtering and reconciliation before ending in the CMDB. The Integration and Staging layer provides this functionality. Master Data warehouse provides interface(s) to several consumers of configuration management system. There are legacy reporting tools currently fed by configuration data from CMS. Master Data warehouse will also be used to interface CMDB with Enterprise Business Applications

C.4.4.1.4   Figure 20 below provides the configuration details for current (March 2015) NATO Enterprise CMS configuration baseline. BMC ITSM 9.1 upgrade is planned for 2016 which will change the components above. Bidders will be provided with latest configuration details.

IFB_CO-14176-SOA-IDM
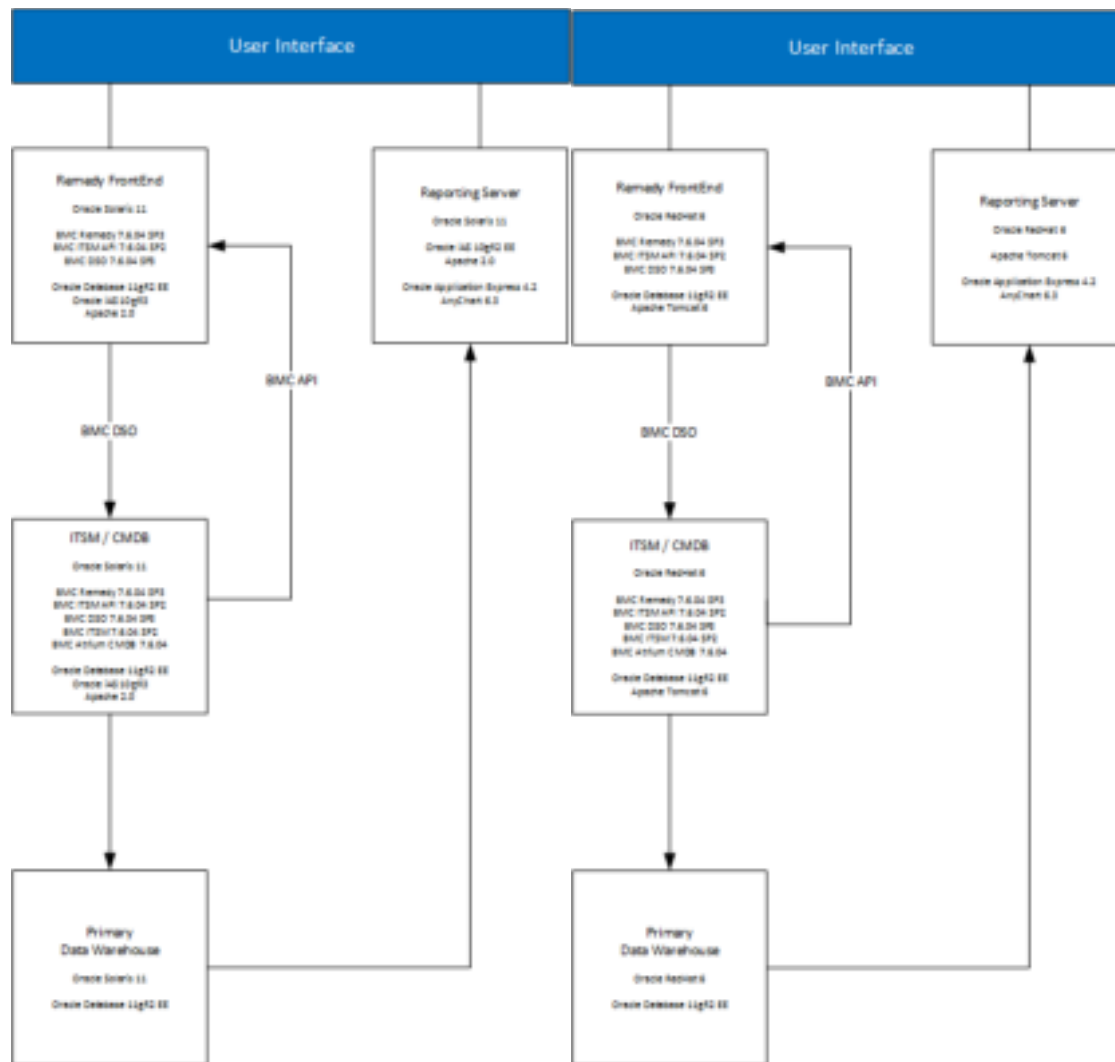
Figure 20: Configuration Management System ON & PBN

C.4.4.2.　　　Domain Level Service Asset and Configuration Tools

Domain	Tools
Physical Asset Management	Cablesolve is used to track physical assets and local network circuits.
Wide Area Network (WAN) CMS	Legacy Database for the time being. This functionality will be moved to BMC ITSM Change Management.
Software License Management	License management is executed on the contractual level, where enterprise agreements are being established. License usage is tracked mainly through BMC Atrium CMS which pulls software information from MS System Centre Configuration Manager and BMC Atrium Discovery and Dependency Mapping tools. The IT infrastructure-level configuration management is carried out through element managers.
Microsoft Applications	Active Directory Group Policies, System Centre Configuration Manager (SCCM) and System Centre Operations Manager (SCOM) configuration automation is used.
Cisco Network Devices	Cisco Prime
C2 & Business Applications	It is executed from applications consoles and are supervisor by System Manager Roles. Some application configuration data which is related to users is maintained in the current helpdesk toolset – BMC Service Desk Express to the extent allowing agents to support users

Table 17: Domain level service asset management and configuration tools currently in use in NCI Agency

C.4.4.3.　　　Automated Information System Enterprise Management System (AIS EMS)

C.4.4.3.1　　The NCI Agency manages the AIS AD enabled EMS services using Microsoft's SCCM, Windows Server Update Services (WSUS), and SCOM for AIS wide configuration, software update, and monitoring purposes on the ON and the PBN. This central enterprise management system is currently based on Microsoft System Centre Enterprise.

C.4.4.3.2　　The EMS Design [NCSA EMS SCCM Technical Design; v1.1, January 2010] will be provided to the Contractor at CAW.

C.4.4.4.　　　Purchasers BMC ITSM Licenses

Below, in Table 18 is the list of BMC ITSM licenses in Purchaser's software inventory.

BMC Software License	Type	Quantity
BMC ProactiveNet Perf Mgt Suite - Lic	Base	1
BMC ProactiveNet Perf Mgt Suite - Serv & Tra	Per Server	60
Seamless Tech Event Integr for BMC		5
Discovery (formerly Atrium Discovery and Dependency Mapping; ADDM)	Per Server	1200
Dashboards and Analytics License	Fixed	20
ITSM Suite	Server	2
Service Management Specialist User	Fixed	41
Service Management Specialist User	Floating	40
Service Desk User	Fixed	10
Service Desk User	Floating	123
Asset Management User	Floating	40
Asset Management User	Fixed	1
Self Service User	Floating	2
Change Management User	Fixed	1
Change Management User	Floating	60
Service Level Management User	Fixed	10
Service Level Management User	Floating	20
Knowledge Management User (Track 3)	Floating	5

Table 18: Purchaser BMC ITSM licence holdings

C.5. Related Projects

The following sections provide background information regarding projects considered by the Purchaser to be relevant in the context of the design and implementation activities in SOA & IdM Platform system.

C.5.1. NATO Enterprise Directory Services (NEDS) Project

C.5.1.1.   NCI Agency is the Host Nation for the NEDS project. This project will provide Directory synchronisation between different.

C.5.1.2.   The NEDS will be deployed on the NS and Business domains by the NEDS Contractor. The NEDS capability supports E-NPKI needs.

C.5.1.3.   The NEDS will act as an information broker between the various NATO directory/data repositories, called the "NEDS Affiliates". Through a 'Repository' function as well as a filtering and synchronisation function NEDS allows "NEDS Affiliates" to make information available for sharing with other directories/data repositories, and allows them to subscribe to NEDS information published by other directories/data repositories. Each piece of

information contained in the NEDS is derived from an authoritative NATO source.

C.5.2. Public Internet Access (PIA) Project.

C.5.2.1. The PIA Project provides a reliable, secure, resilient and managed Internet Services Gateway (ISG) from a commercial service provider to access Public Information Services. The ISG includes relay, protect, and filter internet access (browsing, web publishing, extranet), and internet email traffic to and from Connected NATO entities. The ISG enables remote users to access the network services and internal resources provided by the ITM Business Network. It also provides access to the Internet.

C.5.2.2. The scope of the PIA Project is to provide centrally managed Internet access for all Bi-SC AIS Commands and other entities that are part of the NU WAN, to provide Remote Access for roaming users to their Commands and to provide NU/NR WAN Enterprise Services to allow NU/NR email exchange and functional services to/from the Internet.

C.5.2.3. The PIA's ISG is installed on NATO premises and support outsourced to the PIA Contractor. The infrastructure to provide the PIA services is owned by the PIA Contractor. The PIA Contractor is responsible for the provision of the services as well as operation and maintenance of the equipment, i.e. the PIA Contractor is responsible for the overall lifecycle of the PIA infrastructure during the period of performance of the PIA contract.

C.5.2.4. The PIA Gateway connects into the NGCS/NCI layer and interfaces with the ITM (Business and Public) domains through the NGCS/NCI interfaces.

a. The following services are provided through the PIA:
b. Public Internet Access;
c. Remote user Access;
d. Site-to-Site Virtual Private Network (VPN);
e. External DNS;
f. Proxy Service;
g. Reverse Proxy Service;
h. Email Proxy Service;
i. Web Hosting and Publishing Service;
j. Information Assurance Services;
k. Virtual machine Hosting Service;
l. Mobile Messaging and Web Proxy Service.

C.5.2.5. The initial classification of the PIA will be NATO UNCLASSIFIED but may be upgraded to NR.

C.5.3. Information Exchange Gateway (IEG)

C.5.3.1. During the execution of SOA & IdM Platform the Purchaser will implement a project that is to deliver Information Exchange Gateways on the ON infrastructure. The IEGs will support the exchange of information between NATO's Mission Secret networks and the NATO Secret network (ON) (IEG Case C).

C.5.3.2.   The IEG project will replace existing guards that are currently providing the interim capability. The new guards will support the technical and implementation directive for confidentiality labelling of NATO information. The existing (mail) guards only support First Line of Text (FLOT) labelling.

C.5.4. IT Modernisation (ITM) Project (WP6)

C.5.4.1.   The three main objectives of the ITM project are to:

a. Improve the operational responsiveness of NATO's IT Infrastructure by providing increased robustness, performance and resilience;
b. Improve the life-cycle efficiency of NATO's IT Infrastructure so that infrastructure services can be provided at lowest cost. This objective implies that the Contractor needs to find the right balance between implementation cost and service operations costs. A large part of the current service operation cost is manpower driven. Therefore, an optimum balance between the level of automation introduced for the service management and control, and the life-cycle cost of supporting and maintaining that automation against the manpower savings that it might bring, needs to be achieved;
c. Implement a service based paradigm of operation and support for NATO's IT Networks within which Infrastructure as a Service is recognised and practised.

C.5.4.2.   The current NCIRC Full Operational Capability (FOC) design and implementation needs to be modified to address the proposed ITM architecture. With the introduction of Datacentres and the centralisation of applications and data, the NCIRC sensor placement will require modification to cope with the change in data and information streams.

C.5.4.3.   IT Modersation will deliver a private, on premises cloud, providing Infrastructure as a Service (IaaS). These services will be used to support all of NATO's business needs for static elements. The single, resilient, logically integrated but geographically dispersed, infrastructure will host all of NATO's applications supporting static locations, negating the need for individual projects to provide hardware to support their capabilities.

C.5.4.4.   IT Modernisation will transform NATO's fixed IT infrastructure into a modernised single enterprise, customer-funded service delivery system, with a common management and operations surveillance layer, limited operating system/hardware combinations, increased levels of virtualisation, modern cloud technology, and include appropriate disaster-recovery / survivability considerations. Only through an enterprise approach of this sort can the NCI Agency respond reliably, flexibly and rapidly to NATO customers' demands, charge for its services in a transparent and predictable way, and be able to benchmark its services against outside orgasations. With such an infrastructure in place, the NCI Agency will be able to measure its cost-efficiency, using industry benchmarks, and optimise its infrastructure and processes in order to continually find

improvement in cost and quality of the services provided. Figure 21 illustrates the conceptual future posture, where the Enterprise core services (Infrastructure and Core Services) have been abstracted into a common shared layer.
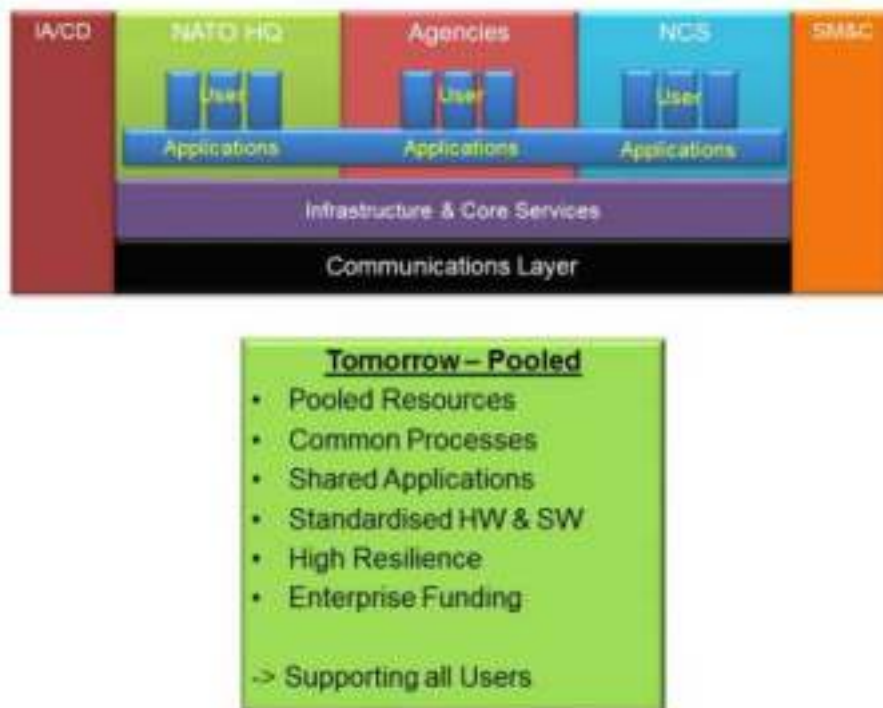
Figure 21: IT posture following IT Modersation

C.5.4.5.   The words that characterise the IT posture NATO will have following IT Modersation are "POOLED" or "SHARED". Assets will be pooled and available to the users according to priority. Excess capacity can be redirected as needed to satisfy operational demands. Sustainability will be enhanced due to standardisation of software, hardware, process and thus also training and logistics needs. Resilience will be provided 'out of the box', with data and services being available at multiple points in the network at all times facilitating 'Disaster Recovery as a Service'.

C.5.4.6.   Pooling is an essential concept of cloud computing. It is the main driver for the adoption of the cloud business model. In NATO today we have processing, storage, etc., capacities at each site that are scaled to the worst case requirement at each site, on a functional service by functional service basis.   As a result spare capacity cannot be exploited as an enterprise resource. If a site is out of capacity or even a particular functional service within a site is short of storage or other resource, it is usually not possible to leverage excess capacity elsewhere to satisfy the shortfall. Pooling allows the sizing of the infrastructure to be reduced overall, while at the same time facilitating deployment of capacity to the users dynamically, according to the operationally assigned priorities.
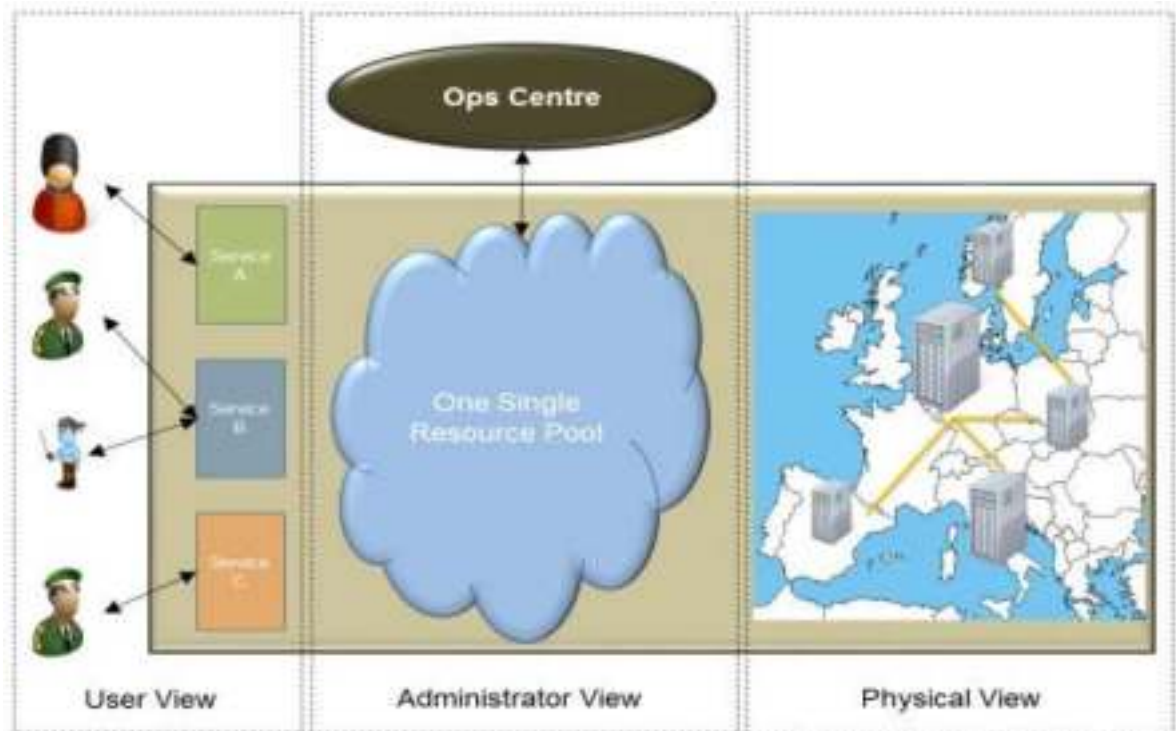
Figure 22: The three views of the new infrastructure

C.5.4.7.   Three views of the future infrastructure are illustrated in Figure 22. At the extreme left is the User View of the service. Users should not be interested in how the services are provided, only that they meet their requirements, such as: resiliency, performance, cost, etc. For example, a pilot might come to work in the morning and wish to see the weather forecast for the next 24 hours. The pilot does not need to concern themselves with all of the activities that go on behind the scenes to collect data, enter it into databases, process it, analyse it, store it and produce finished graphics of the forecast; they are only concerned with the finished product and that it satisfies their needs in terms of timeliness, accuracy, and so on. That is the user view of the service; the experience it provides and the benefit it brings to the user.

C.5.4.8.   IT Modersation envisions presenting a single 'pane of glass' view to the system administrators. The administrators will be able to manage all the pooled assets in the cloud in a transparent way, not having to worry about locations, the specifics of the hardware brand, etc., and will thus be able to focus on provisioning the assets to meet current priorities and optimise the performance of the services. Assets not in use can be powered down in order to save on energy usage. The measurement tools needed to understand the current status of the infrastructure as well as the tools needed to manage the infrastructure in order to be able to provide the services to the user at the agreed service levels constitutes the "Administrator View".

C.5.4.9.   Of course underlying these abstract views is the reality of the physical configuration of the hardware; that is, the Physical View. What is important is that neither the users, nor the Service Operations Centre administrators need to be concerned with the

"Physical View" – they can conduct their roles maintaining only their views which are tailored to their needs and abstracted from physical reality in a way that makes it easier for them to conduct their work. Of course at some level, further back in the organisation the physical view is necessary in order to maintain inventories, replace obsolescence, or conduct physical repairs to equipment, planned maintenance, etc., but this is not a level of detail that users or first or even second Level administrators need concern themselves with.

C.5.5. NATO Computer Incident Response Centre (NCIRC) Full Operational Capability (FOC) Project

C.5.5.1. The NCI Agency is responsible for the NCIRC FOC project which provides the central agent for maintaining the end-to-end security of NATO networks.

C.5.5.2. NCIRC FOC provides NATO-wide protection, detection and response mechanisms to cyber-attacks wherever NATO CIS systems are located (static or deployed). NCIRC provides coverage for the NS, NU and NR network domains at 55 sites, consisting of an integrated and centrally managed set of services around a three-tier architecture:

- a. Tier-1: NCIRC Coordination Centre at NATO HQ
  - i. Tools in support of the Cyber Threat Assessment Cell
- b. Tier-2: NCI Agency's NCIRC Technical Centre in Mons
  - i. Central management of tier-3 sensors
  - ii. Malware, Vulnerability and Forensic Analysis tools
  - iii. Rapid Reaction Team Kits
  - iv. Security Incident Event Management
  - v. Cyber Defence Decision Support System
- c. Tier-3: NATO-wide remote Users sites
  - i. Intrusion Detection and Prevention
  - ii. Full Packet Capture
  - iii. Online Vulnerability Assessment
  - iv. Online Computer Forensics
  - v. Audit Log Aggregation service
- d. Tier-4
  - i. Intrusion Detection and Prevention
  - ii. Full Packet Capture
  - iii. Online Vulnerability Assessment
  - iv. Online Computer Forensics

C.5.5.3. The NCIRC FOC Management network is out of scope for SOA & IdM Platform; however, the five (5) sensors or probes in the Tier-3 sites are fed from resources of the ON and PBN infrastructure.

C.5.5.4. The Intrusion Detection and Prevention (IDP) probes are either installed inline (active prevention) or via a network tap or Switch Switchec Port Analyser (SPAN) port (passive detection). The inline connections can support 1G/10G fibre and 1G/100M/10M copper connections.

C.5.5.5. The Flexible Physical Interface Cards (PIC) Concentrators (FPC) devices are always connected via an aggregator to either network

taps of SPAN ports. Network taps support 1G/10G fibre and 1G/100M/10M copper connections. SPAN ports are usually configured by the local site administrators. Where FPC is deployed at a site, every point monitored by the IDP (either active or passive) is also monitored by the FPC (only passive).

C.5.5.6. For online vulnerability assessment the sensor (probe) deployed at a tier 3 site requires full access to all ports as to properly scan all hosts for known vulnerabilities. This is normally accomplished using one or more of the following (in order of priority):

 a. Change the network configuration so as to allow the Online Vulnerability Assessment (OVA) sensor to be able to reach all ports on all hosts, this normally involves changing a combination of routing, Network Address Translation (NAT) and firewall rules;
 b. Deploy an OVA sensor with several interfaces and connect them to the different sub-networks; or
 c. Deploy as many separate instances of the OVA sensor as required to connect to the different sub-networks.

C.5.5.7. Online Computer Forensics agents are normally installed on every client and server. In order for the tier 3 probe to access all agents at a tier-3 site it may be necessary the change the network configuration at the site.

C.5.5.8. Data sources to be aggregated by the LogA sensor are normally selected based on the criticality ranking of services, in consultation with stakeholders. It may be necessary to change the network configuration (NAT, routing, firewall rules) to allow the LogA sensor to be able to access the chosen logs on all subnets. Logs can be accessed via an Arcsight connector using one of the following protocols:

 a. Syslog over User Datagram Protocol (UDP)/Transmission Control Protocol (TCP);
 b. Windows Management Instrumentation (WMI);
 c. Simple Network Management Protocol (SNMP);
 d. File Transfer Protocol (FTP);
 e. Secure File Transfer Protocol (SFTP);
 f. Secure Copy Protocol (SCP); and
 g. Simple Mail Transfer Protocol (SMTP).

C.5.6. Programme Management and Integration Capability (PMIC) Project

C.5.6.1. The PMIC laboratory provides integration test services for NATO wide networks, IA and AIS services.

C.5.6.2. Access to the PMIC will be given by the Purchaser.

C.5.6.3. The SOA & IdM Platform Contractor should interface the ITS with the PMIC laboratory to support end-to-end services testing where integration or interoperability with NATO wide network, IA or AIS services is/are required.

C.5.7. Enterprise NATO Public Key Infrastructure (E-NPKI) Project

C.5.7.1. The E-NPKI project will implement a PKI environment for NATO.

C.5.7.2. The purpose of E-NPKI is to generate, distribute and manage cryptographic keys, electronic certificates and CRLs, which in turn allows for securing the electronic IT environment.

C.5.7.3. As a part of this E-NPKI architecture the ITM and SOA & IdM Platform locations will have their Registration Authority (RA) provided by the E-NPKI project.

C.5.7.4. E-NPKI will ultimately be fully integrated and interoperable with virtually every other NATO CIS system. Interoperability with NATO systems will be achieved through implementation of common data structures based on international standards (X.509 certificates and CRLs) and common protocols. Final interoperability will be achieved through tight cryptographic integration at the operating system level to ensure full compatibility:

   a. E-NPKI Capabilities will be provided by the Purchaser for the ITM Sites and users;
   b. E-NPKI certificates and CRL information are stored and distributed using NEDS;
   c. Certificate validation is also provided by the use of Online Certificate Status Protocol (OCSP) servers.

C.5.7.5. The E-NPKI architecture is predominantly hosted on the NATO wide NS and NR infrastructures. The NATO HQ infrastructures are aligned with the E-NPKI for all four security domains where for the NS and NR the RA function is delegated to the local HQ security Authority.

C.5.7.6. The Contractor will be provided with E-NPKI issued certificates and services for the different ITM provided services.

ANNEX D : Acronyms

Acronym	Meaning
ABAC	Attribute Based Access Control
ABL	Allocated Baseline
ACL	Access Control List
ACMP	Allied Configuration Management Publication
ACO	Allied Command Operations
ACT	Allied Command Transformation
ADFS	Active Directory Federation Services
ADDM	Atrium Discovery and Dependency Mapping
ADL	Advanced Distributed Learning
AES	Advanced Encryption Standard
AFPL	Approved Fielded Product List
AGS	Alliance Ground Surveillance
AIS	Automated Information System
AJAX	Asynchronous JavaScript and XML
AMIS	ACO/ACT and Missions Identification System
ANWI	Active Network infrastructure
API	Application Programming Interface
APMS	Automated Personnel Management System
ASCII	American Standard Code for Information Interchange
ATC	Aggregated Transport Class
AVI	Audio Video Interleave
Bi-SC	Bi-Strategic Command (ACO & ACT)
Bi-SC AIS	Bi-Strategic Command Automated Information System

BCP	Business Continuity Planning
BLAT	Base Line Acceptance Tests
BMS	Building Management
BPEL	Business Process Execution Language
BPMN	Business Process Model and Notation
BPS	Boundary Protection Services
CAB	Change Advisory Board
CAGE	Commercial and Government Entity
CAPEX	Capital Expenditure
CAW	Contract Award
CBT	Changed Block Tracking
CBT	Computer Based Training
CCB	Configuration Control Board
CDR	Critical Design Review
CD-ROM	Compact Disc - Read-Only-Memory
CET	Central European Time
CFSP	Crypto Forward Support Point
CGI	Common Gateway Interface
CIMIC	Civil Military Cooperation
CIR	Committed information Rate
CIS	Computer Information System
CLI	Common Language Infrastructure
CLIN	Contract Line Number
CLS	Contract for Logistic Support
CM	Configuration Management
CMDB	Configuration Management Database
CMP	Configuration Management Plan

CMS	Configuration Management System
CoC	Certificate of Conformity
COCO	Contractor-Owned / Contractor-Operated
COI	Community of Interest
COM	Component Object Model
COTS	Commercial-Off-The-Shelf
CP	Capability Package
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
CSRS	Community Security Requirements Statement
CSV	Comma-Separated Values
DA	Deployment Authorization (Milestone)
DAM	Data Activity Monitoring
DAC	Discretionary Access Control
DACC	Deployable Air Control Centre
DCIS	Deployable CIS
DCM	Deployable CIS Module
DIF	Difficulty, Importance, Frequency
DISP	Directory Information Shadowing Protocol
DLP	Data Loss Prevention
DML	Defined Media Library
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DVD-ROM	Digital Versatile Disc - Read-Only-Memory
EAI	Enterprise Application Integration

ECAB	Emergency Change Advisory Board
ECP	Engineering Change Proposal
EDC	Effective Date of Contract
EMS	Enterprise Management System
E-NPKI	Enterprise NATO PKI
ESS	Electronic Security System
EULA	End User Licence Agreement
EVC	Ether Virtual Connection
EVPL	Ether Virtual Private Line
FAQ	Frequently Asked Question
FAS	Functional (Area) Service
FBL	Functional Baseline
FCA	Functional Configuration Audit
FFI	Friendly Force Information
FLOT	First Line of Text
FMECA	Failure Modes, Effects and Criticality Analysis
FOC	Full Operational Capability
FOSS	Free Open Source Software
FPC	Flexible PIC Concentrators
FS	Functional Service
FSA	Final System Acceptance
FTE	Full Time Equivalent
FTP	File Transfer Protocol
GFE	Government Furnished Equipment
GIF	Graphics Interchange Format
GSS	Generic Security Services
GQAR	Government Quality Assurance Representatinve

GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HMI	Human Machine Interface
HSTS	HTTP Strict Transport Security
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP within a connection encrypted by TLS/SSL
HWCI	Hardware Configuration Item
IAM	Identity and Access Management
ICD	Interface Control Document
ICWG	Interface Control Working Group
IdM	Identity Management
ICT	Information and Communication Technology
IDP	Intrusion Detection and Prevention
IEG	Information Exchange Gateway
IFB	Invitation for Bid
IIOP	Internet Inter-ORB Protocol
IIS	Internet Information Services
ILS	Integrated Logistics and Support
ILSP	Integrated Logistics and Support Plan
IMP	Issue Management Plan
IPMT	Integrated Project Management Team
IPS	Image Packaging System
IRC	Internal Release Candidate
IREEN	Independent Verification and Validation (IV&V) Reference Environment
ISA	Interim Security Accreditation
ISG	Internet Services Gateway

ITIL	Information Technology Infrastructure Library
ITM	Information Technology Modernisation
ITS	Integration Test Service
ITSM	Information Technology Service Management
JCOP	Joint COP
JFC	Joint Force Command
JMS	Java Message Service
JSLG	Joint Logistics Support Group
JSON	JavaScript Object Notation
JSR	Java Specification Request
JTF	Joint Task Force
JWC	Joint Warfare Centre
KML	Keyhole Markup Language
KPI	Key Performance Indicator
LAMP	Linux, Apache, MySQL, and PHP
LAN	Local Area Network
LANDCOM	Land Command
LDAP	Lightweight Directory Access Protocol
LDT	Logistics Delay Time
LEA	Log Export API
LOG FS	Logistics Functional Services
LoRA	Level of Repair Analysis
LRU	Lowest Replaceable Unit
LSA	Logistics Support Analysis
MAF	Mission Anchor Function
MARCOM	Maritime Command
MCCIS	Maritime Functional Services

MCF	Main Computing Facilities
MDS	Material Datasheet
MDT	Mean Downtime
MEP	Message Exchange Pattern
MHWPS	Minimim Hardware Procurement Specifications
MIM	MIP Information Model
MIP	Multilateral Interoperability Programme
MTBCF	Mean Time Between Critical Failures
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenance
MTF	Message Text Format
MTTR	Mean Time to Repair
NAC	Network Access Control
NAEW&C	NATO Airborne Early Warning and Control
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NCI	NATO Communications Infrastructure
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCISS	NATO Communications and Information School
NCOP	NATO Common Operational Picture
NCS	NATO Command Structure
NDC	NATO Defense College
NDI	Non-Developmental Items
NEDB-NG	NATO Emitter Database - Next Generation
NEDS	NATO Enterprise Directory Service
NFIP	NATO FMN Implementation Plan

NFR	Non-functional Requirements
NGCS	NATO General Communications System
NGO	Non-Governmental Organisation
NHQ	NATO Headquarter
NICE	NATO IP Cryptographic Equipment
NIP	NATO Information Profile
NISP	NATO Interoperability Standards and Profiles
NMRR	NATO Metadata Registry and Repository
NNEC	NATO Network Enabled Capability
NNHQ	New NATO Headquarters
NOR	Notice of Revisions
NOV	NATO Operational View
NPKI	NATO PKI
NSO	NATO School Oberammergau
NSV	NATO Systems View
NQAR	National QAR
NRF	NATO Response Force
NSAB	NATO CIS Security Accreditation Board
NSAM	NATO Security Architecture Methodology
NSCM	NATO Supply Code for Manufacturers
NSPA	NATO Support and Procurement Agency
NSV	NATO System View
NTM	Notice to Move
OAC	Operational Acceptance Criteria
OASIS	Organization for the Advancement of Structured Information Standards
OBL	Operational Baseline
OCR	Optical Character Recognition

OCSP	Online Certificate Status Protocol
ODBC	Open Database Connectivity
OEM	Original Equipment Manufacturer
OLA	Operational Level Agreement
OMG	Object Management Group
OPEX	Operating Expenses
OSS	Open Source Software
OVA	Online Vulnerability Assessment
OWL	Web Ontology Language
PaaS	Platform as a Service
PACS	Physical Access Control System
PAN	Public Access Network
PAP	Policy Administration Point
PBAC	Policy Based Access Control
PBN	Protected Business Network
PBL	Product(-ion) Baseline
PBS	Product Breakedown Structure
PCA	Physical Configuration Audit
PCA	Protected Core Access
PCR	Project Checkpoint Review
PDED	Process Definition and Execution Document
PDF	Portable Document Format
PDM	Product Delivery Meeting
PDP	Policy Decision Point
PDR	Preliminary Desgin Review
PEP	Policy Enforcement Point
PFD	Product Flow Diagram

PFE	Purchaser Furnished Equipment
PHP	PHP: Hypertext Preprocessor
PHST/PHS&T	Packaging, Handling, Storage and Transportation
PIA	Public Internet Access
PIC	Physical Interface Cards
PIN	Personal Identification Number
PHP	Hypertext Preprocessor
PIC	Physical Interface Card
PIP	Policy Information Point
PIP	Project Implementation Plan
PKI	Public Key Infrastructure
PM	Project Manager
PMI	Project Management Institute
PMIC	Programme Management and Integration Capability
PMO	Project Management Office
PMP	Project Management Plan
PMP	PMI Project Management Professional
PMS	Project Master Schedule
PMTP	Project Master Test Plan
PNG	Portable Network Graphics
POC	Point of Contact
PRINCE 2	Projects IN Controlled Environments 2
PRM	Project Review Meeting
PSA	Provisional System Acceptance
PSR	Project Status Report
PTP	Project Test Plan
QA	Quality Assurance

QAP	Quality Assurance Plan
QAR	Quality Assurance Representative
QBT	Quality Based Testing
RACI	Responsible, Accountable, Consulted, Informed
RAM	Release Acceptance Milestone
RAMT	Reliability, Availability, Maintainability, and Testability
RAS	Reusable Asset Specification
RBAC	Role-based Access Control
RC	Release Candidate
RDF	Resource Description Framework
REC	Reference Environment Certification
REST	Representational State Transfer
RFC	Request for Change
RFC	Request for Comments
RFD	Requests for Deviation
RIL	Recommended Item List
RFW	Requests for Waver
RMP	Risk Management Plan
ROI	Return On Investment
ROM	Read Only Memory
RPM	RPM Package Manager
RPO	Recovery Point Objective
RTF	Rich Text Format
RTM	Requirements Traceability Matrix
RTTL	Recommended Tools and Test equipment List
RUP	Roaming User Profile
SAA	Security Accreditation Authority

SACT	Supreme Allied Commander Transformation
SACEUR	Supreme Allied Commander EURope
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAP	Security Accreditation Plan (or Process)
SASL	Simple Authentication and Security Layer
SAT	Site Acceptance Test
SATCOM	Satellite Communication
SBL	System Baseline
SBT	Service-Based Testing
SCCM	System Centre Configuration Manager
SCOM	System Centre Operations Manager
SCORM	Shareable Content Object Reference Model
SCP	Secure Copy Protocol
SDL	Software Development Library
SDR	System Design Review
SDS	System Design Specification
SECAN	Military Committee Communications Security & Evaluation Agency
SFTP	Secure File Transfer Protocol
SHAPE	Supreme Headquarters Allied Powers Europe
SIEM	Security Incident Event Management
SIP	Service Interface Profile
SISRS	System Interconnection Security Requirements Statement
SIVP	Security/Site Implementation and Verification Procedures
SLA	Service Level Agreement
SLP	Standardised Language Proficiency
SLT	Service Level Target

SMC	Service Management and Control
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service Operations Centre
SOM	System Operation Manual
SOP	Standard Operating Procedure
SOW	Statement Of Work
SPAN	Switched Port Analyser
SPARQL	SPARQL Protocol and RDF Query Language
SQL	Structured Query Language
SRA	Security Risk Assesment
SRR	System Requirements Review
SRS	System Requirement Specification
SSE	Senior Systems Engineer
SSL	Secure Sockets Layer
SSRS	System- (Specific) Security Requirements Statement
SSO	Single Sign-On
SSS	Schedule of Supplies and Services
SSWB	Site Survey Workbook
STANAG	NATO STANdardisation AGreement
STDP	System Test Documentation Package
STR	Status Test Review
STS	Security Token Service
STVP	Security Test and Verification Plan

STVR	Security Test and Verification Report
SVDD	System Version Definition Document
SWCI	Software Configuration Item
SWDL	Software Distribution List
SWG	Security Working Group
SWID	Software Identification
TA	Target Architecture
TAP	Test and Acceptance Plan
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDY	Temporary Duty
TL	Technical Lead
TLS	Transport Layer Security
TNA	Training Needs Analysis
TOPFAS	Planning Functional Services
TRR	Test Readiness Review
UAT	User Acceptance Testing
UCC	Unified Communication and Collaboration
UDDI	Universal Description, Discovery and Integration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UNC	Uniform Naming Convention
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VOIP	Voice over Internet Protocol

VPN	Virtual Private Network
VTC	Video Teleconference
WAN	Wide Area Network
WCF	Windows Communication Foundation
WMI	Windows Management Instrumentation
WSDL	Web Services Description Language
WSUS	Windows Server Update Services
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XSLT	eXtensible Stylesheet Language Transformations

Table 19: Acronyms

ANNEX E: Definitions

Term	Meaning
Accountability	Degree to which actions of an *Entity* can be traced uniquely to the *Entity*.
Adaptability	Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.
Alert	A warning that a threshold has been reached, something has changed, or a *Failure* has occurred. The two types of *Alerts* are: • "Warning" (indicating that it is necessary to take action in order to prevent an exception occurring) • "Exception" (indicating that the *Service* is currently operating below the normal predefined parameters/indicators)
Analysability	Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of *Failures*, or to identify parts to be modified.
Artefact	Document containing data in machine processable format, for example an XSD schema, a JSON schema document.
Artefact Collection	A governance namespace for a set of Artefacts and/or Artefact sub-collections. An artefact collection has a name. A collection manager manages an artefact collection, and all artefacts and sub-collections it contains.
Assertion (alternative terms: claim, identity assertion)	A package of information that contains *Identity* and security information about a subject. An *Assertion* can be classed as either a *Simple Token* or a *Security Token*.

Attribute	Characteristic or property of an *Entity* that can be used to describe its state, appearance, or other aspects.
Attribute-Based Access Control	An access control paradigm whereby access rights are granted to *Entities* through the use of policies which evaluate *Attributes* (possibly combining *Attributes* together) to grant or deny access.
Attribute-Based Access Control	Represents a point in the space of logical access control that includes access control lists, role-based access control, and the ABAC method for providing access based on the evaluation of attributes.
Audit Log	An audit log is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event
Authentication	A *Process* to achieve a certain level of assurance in the binding between an *Entity* and an *Identity*.
Authenticity	Degree to which the *Identity* of a subject or resource can be proved to be the one claimed.
Authoritative Data Source	The repository or system that contains the data and attributes about an individual that are considered to be the primary source for this information. If two systems with an individual's data have mismatched information, the authoritative data source is used as the most correct
Authorisation	The *Process* of establishing whether an *Entity* is permitted to perform a particular operation on a resource.
Authorisation Server	OAuth 2.0 terminology describing an entity that authenticates and authorizes a Client and issues an access token to that Client to be used in a request for a protected resource.

Authorised User	An Entity that has access rights for a piece of Platform functionality at "run time". This functionality may include viewing, creating, collaborating and updating/maintaining information.
Availability	Degree to which a system, product or *Component* is operational and accessible when required for use. Inherent *Availability* (intrinsic) assumes ideal support (i.e. unlimited spares, no delays, etc.); only design related *Failures* are considered.
Business Rules	Statements describing a business/enterprise policy or procedure (e.g. discount calculation) and can be represented using formal language.
Capability	*Services* that are used by an end-*User* in support of their operational business.
Capacity	Degree to which the maximum limits of a product or system parameter meet requirements.
Choreography	Describes the sequence and conditions in which the data exchanged between two or more participants in order to meet some useful purpose. The logic of the *Message*-based interactions among the participants are specified from a global perspective.
Civil Military Cooperation	Means by which a military commander connects with civilian agencies active in a theatre of operations.
Claims	The Attributes of an entity that are asserted by an entity contained within a Security Token.
Commercial-Off-The-Shelf	The purchase of packaged solutions which are then adapted to satisfy the needs of the purchasing organisation, rather than the commissioning of custom made, or bespoke, solutions
Community of Interest	A group of people interested on a particular *Topic* or area, i.e. intel community, security community.

Component	An IT system can be divided into *Components*, each of which provides a particular function or group of related functions.
Composition	The *Process* of combining a set of *Services*, and arranging them in a specific, well-defined way.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or *Entities*.
Configuration Item	*Components* of an infrastructure that currently is, or soon will be under *Configuration Management*. *Configuration Items* may be a single module such as a monitor or tape drive, or more complex items, such as a complete system.
Configuration Management	The *Process* responsible for maintaining information about the *Configuration Items* required to deliver a *Service*, including their relationships with one another.
Consumer (related to publish-subscribe)	An end-point, represented by a WS-Addressing end-point reference, designated to receive notifications produced by a notification producer as a result of a subscription.
Context (related to IAM; alternative terms: domain, domain of applicability)	Environment where an *Entity* can use a set of *Attributes* for *Identification* and other purposes.
Contractor	Future successful bidder who awarded the contract with the Purchaser for delivery of the scope describe by the document.
Credential	Set of data presented as evidence of a claimed or asserted *Identity* and/or entitlements.
Data Centre	A repository that houses computing facilities like servers, routers, switches and firewalls, as well as supporting *Components* like backup equipment, fire suppression facilities and air conditioning. It may be a key centralised IaaS location where the bulk of computing will take place.

NATO UNCLASSIFIED

IFB_CO-14176-SOA-IDM

Data Element	A single unit of information (e.g. a speed, altitude) that has a useful meaning in some context.
Data Provider	A *Service* that produces data for other *Services*.
Deployable CIS	Provides a *Capability* for deployed forces in-theatre and extends *Services* from the fixed infrastructure to deployed *Users*.
Disaster	A business or service continuity event which cannot be managed by the incident management capabilities, requiring invocation of the IT Service Continuity Plans employing the contingency Service Assets. The disaster scenarios are identified as a part of the Business Impact Assessment and risk assessment. For the purpose of initial ITM project planning a disaster can be defined as an event leading to any of the following effects: - losing WAN communication from any of the Datacentres, nodes or client-only sites; - destruction of any site; - disabling more than 30% of back-end IaaS components - disabling more than 30% of client components - unavailability of any service (hosted on IaaS) of Business Criticality 1 for more than 24h
Enhanced Node	An IaaS location with enhanced computing capabilities in order to support applications that cannot be centralised for technical or other reasons, to provide a level of graceful degradation should communications be interrupted, or to provide a higher level of *User* experience.
Enrolment	Process to make an entity known within a particular context.

NATO UNCLASSIFIED

Book 2, Part IV, Page IV-216

Entity	Item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence.
Error	A design flaw or malfunction that causes a *Failure* of one or more *Configuration Items*. A mistake made by a person or a faulty *Process* that affects a *Configuration Item* is also an *Error* (human *Error*).
Event	Any detectable or discernible occurrence that has significance for the management of the infrastructure or the delivery of a *Service.*
Event Management	*Process* that monitors all *Events* that occur throughout the Platform. It allows for normal operation, but also detects and escalates exception conditions.
Failure	Loss of ability to operate to specification, or to deliver the required output. The term *Failure* may be used when referring to *Services*, *Processes*, activities, *Configuration Items*, etc.
Fault	see *Error.*
Fault Detection	The capability of a system to determine that a Fault exists in a circuit, using an automatic process.
Fault Isolation	The capability of a system to identify, using an automatic process, which is the component or parameter of the system that is responsible for Fault.
Fault Tolerance	Degree to which a system, product or *Component* operates as intended despite the presence of hardware or software *Faults*.
Federated Identity	*Identity* for use in multiple *Contexts*, which together form an *Identity Federation*.
Federation	Association of users, service providers and identity providers.
Functional Service	Represents a group of functionalities within a specific *Community of Interest*, to which applications and *Services* are assigned.

Functional Baseline	A set of documents that specifies the functional and non-functional requirements of a service or product and that is used as the approved basis for comparison.
Graceful Degradation	The ability of a computer, machine, electronic system or network to maintain limited functionality even when a portion of it has been destroyed or rendered inoperative (either by a fault or deliberately).
Identification (related to IAM)	The *Process* of recognizing an *Entity* in a particular *Context* as distinct from other *Entities*.
Identity	Set of *Attributes* related to an *Entity*.
Identity and Access Management	The people, *Processes* and products necessary to manage *Identities* throughout their life-cycle and the access to resources.
Identity Federation	Agreement between two or more *Contexts* specifying how *Identity Information* will be exchanged and managed for cross-*Context Identification* purposes.
Identity Information	Set of values of *Attributes* optionally with any associated *Metadata* in an *Identity*.
Identity Management	The *Processes* and policies involved in managing the lifecycle and value, type and optional *Metadata* of *Attributes* in *Identities* known in a particular *Context*.
Identity registration	Process of recording an entity's identity information in an identity register.
Identity Repository (alternative terms: identity store)	Repository of *Identities* for different *Entities.*
Identity Service Provider	Entity that verifies, maintains, manages, and may create and assign identity information of other entities.
ILS Plan	A standalone Product Lifecycle documents that will survive the project post-FSA. As such, these documents are not to be submitted as part of the PIP, but will be part of the Technical Proposal

Incident	An unplanned interruption to an IT *Service* or reduction in the quality of an IT *Service*. *Failure* of a *Configuration Item* that has not yet affected *Service* is also an *Incident* — for example, *Failure* of one disk from a mirror set.
Independent Verification and Validation	NCI Agency Service Line organizational unit responsible for ensuring that all NCI Agency services have gone through the required procedures to ensure that they are fit for purpose and use and that they are assured for interoperability purposes
Information Catalogue	An information catalogue is a list of information products that an organization provides to its users or to IT-infrastructure resources, such as applications or other services. Each information product within the catalog typically includes: a description of the information product, timeframes, who is entitled to request the information product, costs (if any), and how to obtain the information product. The catalogue information is metadata associated with the information product. Information products should be identifyable across the organization by using a unique identifier.
Information Consumer	Retriever of semantically enriched information directly from an *Information Provider* or from an intermediary knowledge store.
Information Provider	Make semantically enriched information available, including the actual payload data as well as the structural (schemas) and semantic (ontologies) *Metadata*.
Infrastructure as a Service	A concept of provisioning IT platforms to *Users* or other *Services* in the form of a utility covered by the agreed level of warranty.
Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
Interoperability	Degree to which two or more systems, products or *Components* can exchange information and use the information that has been exchanged.

IT Modernisation	A project aiming at modernizing, consolidating, and centralising NATO's enterprise infrastructure and service management, and by pooling and abstracting resources.
Key Performance Indicator	A measure (quantitative or qualitative) that enables the overall delivery of a *Service* to be assessed by both business and IT representatives.
Logging	Act of keeping a log, which is a file that records either *Events* that occur in software or *Messages* between different *Users.*
Maintainability	Degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers.
Message Exchange Pattern	A template that establishes a pattern for the exchange of *Messages* between two communicating parties.
Metadata	Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage a data asset; often called data about data or information about information.
Metadata Registry	A system that manages both descriptive and structural *Metadata*. Typically, a registry is a software application that uses a database (Repository) to store and search data assets, document formats, definitions of data, and relationships among data.
Metadata Repository	A database created to store *Metadata*.
Metering	The act of controlling software use by the number of specific nodes (workstations where a single *User* is logged on and terminal server sessions) that are simultaneously using a specific application.
Modularity	Degree to which a system or computer program is composed of discrete *Components* such that a change to one component has minimal impact on other *Components.*

Monitoring	The supervising of overall *Processes* that are performed on a computing system, and providing reporting *Services* to the system or system administrator.
Multi-tenancy	A software architecture in which a single instance of software runs on a server and serves multiple tenants. A tenant is a group of *Users* who share a common access with specific *Privileges* to the software instance.
NATO Network Enabled Capability	The Alliance's cognitive and technical ability to federate the various *Components* of the operational environment from the strategic level (including NATO HQ) down to the tactical level, through a networking and information infrastructure
NATO Public Key Infrastructure	The PKI environment for NATO that fully complies with the NATO Certificate Policy.
Non-repudiation	The measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients.
Notification	A one-way *Message* sent to indicate that an *Event* has occurred.
Notification Broker	A *Service* that acts as an intermediary between *Notification Consumers* and *Publishers* in order to permit the *Notification Consumer* to subscribe to *Notifications* produced by *Publishers* that are not offering the *Subscription* interface. In this role it acts as *Notification Producer* and *Notification Consumer* and can offer the interface for the *Publisher* registration.
Notification Cache	A *Service* capable of consuming *Notifications*, to store them in a repository, and to retrieve and resend them – on request – to *Notification Consumers* or to *Notification Requestors*.

Notification Producer	A *Service* capable of producing *Notifications* for those *Notification Consumers* for which *Subscriptions* have been registered, based on *Events* that occur and on the parameters supplied with the requests from which the *Subscriptions* were created. It may directly produce *Notifications* itself, or it may be a *Notification Broker*, reproducing *Notifications* that were produced by a separate *Publisher* and/or *Notification Producer*.
Off-Specification Report	Report describing items that should be provided by the project, but currently are not (or are forecasted not to be) provided. This might be a missing product or a product not meeting its specification.
Operational Network	Provides IT *Services* at NATO SECRET level in direct support of war fighting *Processes*, *Processes* requiring higher levels of assurance and *Processes* of military and political communications.
Orchestration	A procedure consisting of the steps, their sequence, and the conditions which one *Service* executes in order to coordinate and invoke other *Services* with the aim to realize some useful function.
Performance	A measure of what is achieved or delivered by a system, person, team, *Process* or IT *Service.*
Performance Efficiency	*Performance* relative to the amount of resources used under stated conditions.
Policy-Based Access Control	Defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.).
Policy Decision Point (PDP)	A *Service* that provides Authorization decisions by evaluating policies against the *Attributes* of an *Entity*.
Policy Enforcement Point (PEP)	A security software *Component* that ensures that security policies are applied.

Portability	Degree of effectiveness and efficiency with which a system, product or *Component* can be transferred from one hardware, software or other operational or usage environment to another.
Privilege	A right that, when granted to an *Entity*, permits the *Entity* to perform an action.
Privilege Management	*Process* of establishing and maintaining *Entity Privileges* to protected resources: accounts, entitlements and *Roles* that comprise an *Entity*'s access profile.
Problem	A cause of one or more *Incidents*. The cause is not usually known at the time the *Incident* happens.
Project Master Schedule	Summary of all the individual project schedules for the Bond Program and is intended to indicate the position of a project to the other projects on a global basis.
Protected Business Network	Provides IT *Services* at the NATO UNCLASSIFIED and NATO RESTRICTED classification level in support of administrative business processes, appropriate operational *Processes* and those *Processes* requiring interaction over the Internet. Within the PBN infrastructure there are also security domains that are providing NATO UNCLASSIFED information *Services* like extranet applications or VOIP/VTC *Services* and PUBLIC information *Services* like internet access via WiFi.
Publisher	A *Component* capable to produce *Notifications* sent to subscribed *Notification Consumers* or to a *Notification Broker* for further distribution to subscribed *Notification Consumers*.
Publish-Subscribe	A messaging pattern where senders of *Messages*, called *Publishers*, do not program the *Messages* to be sent directly to specific receivers, called *Subscribers*, but instead characterize published *Messages* into classes without knowledge of which *Subscribers*, if any, there may be. Similarly, *Subscribers* express interest in one or more classes and only receive *Messages* that are of interest, without knowledge of which *Publishers*, if any, there are.

Purchaser	NCI Agency acting as a Host Nation for this procurement on behalf of NATO organizations
Purchaser Furnished Equipment	Equipment provided to the contractor doing the project by the purchaser of the project.
Recoverability	Degree to which, in the *Event* of an interruption or a *Failure*, a product or system can recover the data directly affected and re-establish the desired state of the system.
Recovery Point Objective (RPO)	This is the threshold of how much data can be afforded to be lost since the last backup. RPO is measured in hours of data loss
Reliability	Degree to which a system, product or *Component* performs specified functions under specified conditions for a specified period of time.
Relying Party	This is the service that is protected by the PEP. It relies on the Authentication information presented in the Security Token. It is thus usually the Data Provider.
Request-Response	One of the basic methods computers use to communicate with each other, in which the first computer sends a request for some data and the second computer responds to the request.
Resource Server	OAuth 2.0 terminology describing an *Entity* that: hosts the protected resource; is capable of accepting and responding to protected resource requests; and, validates access tokens ensuring the protected resource request conforms to the access control policy.
Resource Utilisation	degree to which the amounts and types of resources used by a product or system, when performing its functions, meet requirements
Role (regarding IAM)	Set of properties or *Attributes* that describe the capabilities or the functions performed by an *Entity*.

Scalability	Ability of a system to increase (or decrease) total throughput under an increased load when resources (typically hardware) are added (or subtracted), so the *Scalability* quality figures are defined accordingly.
Security Token	A structure for distributing assertions between *Entities*.
Security Token Service (STS)	A *Service* that issues *Security Tokens*.
Service	A piece of functionality that is characterized by a syntactic interface specification as well as a semantic interface specification, i.e. its behavior and *User*-observable functionality.
Service Endpoint	
Service Interface Profile	A detailed technical specification of an *Interoperability* interface.
Service Oriented Architecture	An architectural style in which *Services* are provided to the other *Components* by application *Components*, through a communication protocol over a network.
Standard Node	Location with limited amount of computing in support of local *User Services* access.
Stylesheet	An XML document that specifies an XSLT. Named after its XML root element.
Subscriber	Any *Entity* that can create and manage *Subscriptions* interacting with *Notification Producer* and *Subscription Manager Services*. Note that a *Subscriber* may be a different *Entity* from the *Notification Consumer* for which *Notifications* are actually produced.
Subscription	Relationship between a *Notification Consumer* and a *Notification Producer*, including any filtering parameters such as *Topic* and various other optional filter expressions, along with any relevant policies and context information.

Subscription Manager	Provides operations that allow a *Service Requestor* to query and manipulate *Subscriptions* that it manages. A *Subscription Manager* is subordinate to the *Notification Producer*/*Notification Broker*, and may be implemented by the *Notification Producer*/*Notification Broker Service* provider.
Sub-service	A service that is part of a composed service. The sub-service can be either an independent, atomic service or itself a composed service.
Time Behaviour	Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.
Topic	Categorization that can be attached by a *Notification Producer* to a *Notification*. A *Notification* can be associated with one or more *Topics*. *Topics* can be used by a *Notification Producer* to determine which subscribed *Notification Consumers* should receive the *Notification*.
Topic Manager	Maintains and coordinates the ownership of Topics
Trust	Belief in the *Reliability* and truth of information; or in the competence of an *Entity* to act appropriately, within a specified *Context*.
Trust framework	Set of requirements and enforcement mechanisms for parties exchanging identity information.
User	*Entity* that makes use of a resource, e.g., system, equipment, terminal, *Process*, application, or corporate network. Each *User* of the Platform is assigned access rights based on its *Role*, the permissions within that *Role*, and optionally the organisation of the *User*.
Verification	Process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular context at some point in time.

Table 20: Definitions

ANNEX F : References

F.1. Applicable References

The abbreviated document titles given in square brackets, […], are used to refer to documents in the reference list.

F.1.1. NATO Documents

F.1.1.1.   Reference documents for Quality Assurance purposes

[NATO AQAP-2000, 2009]	NATO - Allied Quality Assurance Publication 2000, "NATO Policy on an integrated system approach to Quality through the life Cycle", Edition 3, 2009
[NATO AQAP-2009, 2010]	NATO - Allied Quality Assurance Publication 2009, "NATO guidance on the use of the AQAP 2000 series", Edition 3, 2010
[NATO AQAP-2070, 2015]	NATO - Allied Quality Assurance Publication 2070, "NATO Mutual Government Quality Assurance (GQA) Process", Edition B, Version 3, 2015
[NATO AQAP-2105, 2011]	NATO - Allied Quality Assurance Publication 2105, "NATO requirements for Deliverable Q plans", Edition 2, 2011
[NATOAQAP-2110, 2016]	NATO - Allied Quality Assurance Publication 2110, "NATO QA Requirements for Design, Development and Production", Edition D, Version 1, 2016
[NATO AQAP-2120, 2010]	NATO - Allied Quality Assurance Publication 2120, "NATO QA requirements for production", Edition 3, 2010
[NATP AQAP-2130 2009]	NATO - Allied Quality Assurance Publication 2130, "NATO QA Requirements for inspection & Test", Edition 3, 2009
[NATO AQAP-2131, 2011]	NATO - Allied Quality Assurance Publication 2131, "NATO QA requirements for final inspection", Edition 2, 2011
[NATO AQAP-2210, 2015]	NATO - Allied Quality Assurance Publication 2210, "NATO Supplementary Software Quality Assurance Requirements to AQAP-2110", Edition A, Version 2, 2015

Table 21: Reference documents for Quality Assurance purposes

F.1.1.2.   Documents for Configuration Management Purposes

[NATO STANAG 4427, 2014]	NATO Standardisation Agreement 4427, "Configuration Management in System Life Cycle Management", Ed. 3
[NATO ACMP-2000, 2017]	Policy on configuration management, Ed.A, Version 2
[NATO ACMP 2009, 2017]	Guidance on Configuration Management, Ed. A, Version 2
[NATO ACMP-2100, 2017]	Configuration Management Contractual Requirements, Ed. A, Version 2
[NCIA AI TECH 06.03.01, 2015]	NATO Communications and Information Agency - Agency Instruction 06.03.01, "Identification of Software Assets", 2015

[NCIA AI TECH 06.03.04, 2015]	NATO Communications and Information Agency - Agency Instruction 06.03.04, "Test, Verification and Validation", 2015

Table 22: Documents for Configuration Management Purposes

F.1.1.3.   Standard Guidance

[NATO STANAG 4107, 2016]	NATO Standardisation Agreement 4107, "Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications", Ed. 9, 2016
[NATO STANAG 6001, 2014]	NATO Standardisation Agreement 6001, "Language Proficiency Levels", Ed. 5, 2014
[NAC AC/317-D/71 (Revised), 1996]	AC/317-D/71 (Revised) "NATO COTS Software Policy and Acquisition Guidelines", 1996

Table 23: Standard Guidance

F.1.1.4.   Bi-strategic Command (Bi-SC) Documents

[NCIA SOP 06.03.01, 2015]	NCI Agency Standard Operating Procedure SOP 06.03.01, "Operational Naming and Addressing of NATO ICT Infrastructure", 2015

Table 24: Bi-strategic Command (Bi-SC) Documents

F.1.1.5.   NATO Security Documents

[NAC C-M(2002)49, 2002]	North Atlantic Council Document C-M(2002)49, "Security within the North Atlantic Treaty Organisation" 2002 with Corrigendum, NATO UNCLASSIFIED
[NAC AC/35-D/2000-REV7, 2013]	North Atlantic Council Document AC/35-D/2000-REV7, "Directive on Personnel Security", 2013, NATO UNCLASSIFIED
[NAC AC/35-D/2001-REV2, 2008]	North Atlantic Council Document AC/35-D/2001-REV2, "Directive on Physical Security , 2008, NATO UNCLASSIFIED
[NAC AC/35-D/2002-REV4, 2012]	North Atlantic Council Document AC/35-D/2002-REV4, "Directive on Security of Information", 2012, NATO UNCLASSIFIED
[NAC AC/35-D/2003-REV5, 2015]	North Atlantic Council Document AC/35 – D/2003 –REV5, "Directive on Classified Project and Industrial Security", 2015, NATO UNCLASSIFIED
[NAC AC/35-D/2004-REV3, 2013]	North Atlantic Council Document AC/35-D/2004-REV3, "Primary Directive on CIS Security", 2013, NATO UNCLASSIFIED
[NAC AC/322-D(2006)0041-REV1, 2009]	North Atlantic Council Document AC/322-D(2006)0041-REV1, "Directive on the Selection and procurement of NATO Common-Funded Cryptographic Systems, Products and Mechanisms", 2009

[NAC AC/322-D/0047-REV2(INV), 2009]	North Atlantic Council Document AC/322-D/0047-REV2 (INV), "INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms , 2009, NATO RESTRICTED
[NAC AC/322-D/0048-REV2, 2011]	North Atlantic Council Document AC/322-D/0048-REV2, "INFOSEC Technical & Implementation Directive for Computer and Local Area network (LAN) Security", 2011, NATO RESTRICTED
[NAC AC/322-D(2007)0036, 2007]	North Atlantic Council Document AC/322-D(2007)0036, "INFOSEC Technical & Implementation Directive on Emission Security", 2007, NATO RESTRICTED
[NAC AC/35-D/2005-REV3, 2015]	North Atlantic Council Document AC/35-D/2005-REV3, "Management Directive on CIS Security (CIS)", 2015, NATO UNCLASSIFIED
[NAC AC/35-D/1015-REV3, 2012]	North Atlantic Council Document AC/35-D/1015 –REV3, "Guidelines for the Development of Security Requirement Statements (SRSs)", 2012, NATO RESTRICTED
[NAC AC/35-D/1017-REV3, 2017]	North Atlantic Council Document AC/35-D/1017-REV3, Guidelines for Security Risk Management (SRM) of Communication and Information Systems (CIS), 2017, NATO UNCLASSIFIED
[NAC AC/35-D/1021-REV3, 2012]	North Atlantic Council Document AC/35-D/1021–REV3, Guidelines for the Security Accreditation of Communication and Information Systems (CIS), 2012, NATO UNCLASSIFIED
[NAC AC/35-D/1014-REV3, 2012]	North Atlantic Council Document AC/35-D/1014-REV3, "Guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for CIS, 2012, NATO UNCLASSIFIED
[NAC AC/322-D/0030-REV5, 2011]	North Atlantic Council Document AC/322-D/0030-REV5, "INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS)", 2011, NATO RESTRICTED
[NAC AC/322-D(2004)0022(INV), 2004]	North Atlantic Council Document AC/322-D(2004)0022(INV, "INFOSEC & Technical and Implementation Guidance for Consistent Marking of NATO Information in C3 Systems", 2004, NATO UNCLASSIFIED
[NAC AC/322-D(2007)0047, 2007]	North Atlantic Council Document AC/322-D(2007)0047, "INFOSEC Technical and Implementation Supporting Document on the Use of Shared Peripheral Switches", 2007, NATO RESTRICTED
[NAC AC/322-D(2008)0002, 2008]	North Atlantic Council Document AC/322-D(2008)0002, "INFOSEC Technical and Implementation Supporting Document on Securing Domain Name System Services", 2008, NATO RESTRICTED
[NAC AC/322-N(2014)0158-ADD3, 2015]	North Atlantic Council Document AC/322-N(2014)0158-ADD3, "SECAN Doctrine and Information Publication (SDIP) 29, Selection and Installation of Equipment for the

	Processing of Classified Information", 2015, NATO RESTRICTED
[ITM NS AIS CSRS, 2017]	Community Security Requirements Statement (CSRS) for NATO SECRET Automated Information System (AIS) provided by IT Modernization (ITM NS AIS), 2017, NATO RESTRICTED
[ITM NR AIS CSRS, 2017]	Community Security Requirement Statement (CSRS) for NATO RESTRICTED Automated Information System (AIS) provided by IT Modernization (ITM NS AIS), 2013, NATO RESTRICTED
[NS AIS (ITM) CSRS]	Community Security Requirement Statement (CSRS) for NATO SECRET Automated Information System (NS AIS) (IT Modernization) (version and date TBD)
[NS AIS SecOPS, 2014]	Generic Security Operating Procedures (SecOPs) for "NATO SECRET (NS) Automated Information System (AIS)", 2014
[NS CIS Security Reference Baseline, 2017]	"NATO SECRET CIS Security Reference Baseline", Version 2.0, 2017, NATO RESTRICTED
[NCIA NSAP SOA & IdM, 2017]	NATO Communications and Information, "NATO Security Accreditation Plan for SOA & IdM Platform", 2017

Table 25: NATO Security Documents

F.1.1.6.   Technical Guidance

[NAC AC/317-D/71 (Revised), 1996]	North Atlantic Council Document AC/317-D/71 (Revised) "NATO COTS Software Policy and Acquisition Guidelines", 1996
[NAC AC/322-D(2004)0024-REV2, 2008]	North Atlantic Council Document AC/322-D(2004)0024-REV2, "NATO Public Key Infrastructure (NPKI) Certificate Policy", 2008
[NAC AC/322-D(2005)0037, 2005]	North Atlantic Council Document AC/322-D(2005)0037, "Bi-SC AIS Reference Architecture (RA), Version 2", 2005, NATO RESTRICTED
[NAC AC/322-D(2011)0015, 2011]	North Atlantic Council Document AC/322-D(2011)0015, "NATO Network Enabled Capability Tenets and Principles", 2011
[NAC AC/322-D(2005)0053-REV2, 2009]	North Atlantic Council Document AC/322-D(2005)0053-REV2 "NNEC Data Strategy", 2009
[NAC AC/322-N(2011)0205, 2011]	North Atlantic Council Document AC/322-N(2011)0205, "Core Enterprise Services Standards Recommendations. The Service Oriented Architecture (SOA) Baseline Profile", 2011
[AC/322-D(2015)0014-REV3-AS1, 2015]	North Atlantic Council Document AC/322-D(2015)0014-REV3, "The NATO Enterprise Approach for the Delivery of C3 Capabilities and the Provision of ICT Service", 2015
[NAC ADatP-34(G)-REV1, 2013]	North Atlantic Council Document ADatP-34(G)-REV1, "NATO Interoperability Standards and Profiles", 2013
[NC3B AC/322-N(2016)0021-AS1, 2016]	NATO C3 Board AC/322-N(2016)0021-AS1, "C3 Taxonomy Perspective Baseline 2.0", 2016
[NCIA TR/2014/NCB009779/05, 2015]	NATO Communications and Information Agency Technical Report/2014/NCB009779/05, "Communication and Information System Security Capability Breakdown – Comprehensive Approach, Revision 2.0", 2015
[NCIA TR/2015/NCB009779/09, 2015]	NATO Communications and Information Agency Technical Report /2015/NCB009779/09, "Considerations for a NATO Enterprise Identity and Access Management Strategic Plan", 2015

[SHAPE 3050/SH/CCD CIS/CAR/335/13-301388, 2013]	Supreme Headquarters Allied Powers Europe 3050/SH/CCD CIS/CAR/335/13-301388 and SACT: 5000 TSC-FCR0010/TT-8846/Ser: NU0005 "Bi-SC AIS Service Employment in Support of the NATO Command Structure", 2013
[NCIA SOA & IdM TA, 2017]	NATO Communications and Information Agency, "Target Architecture - Provide Service Oriented Architecture and Identity Management System", 2017
[NCIA SMC TA, 2018]	NATO Communications and Information Agency, "Target Architecture - Enterprise Service Management and Control", 2018

Table 26: Technical Guidance

F.1.1.7.   NATO Templates

[NTEMP-1]	Interface Control Document template
[NTEMP-2]	Security Accreditation Plan template
[NTEMP-3]	System Description template
[NTEMP-4]	Security Risk Assessment (SRA) Report (PILAR) template
[NTEMP-5]	Delta System Security Requirements Statement (dSSRS) template
[NTEMP-6]	Security Test and Verification Report template
[NTEMP-7]	System Interconnection Security Requirements Statement (SISRS) template
[NTEMP-8]	Secure AIS STVP Template

Table 27: NATO Templates

F.1.1.8.   Others

[ACT D-75-10, 2007]	Allied Command Transformation Directive 75-10, "Training Needs Analysis", 2007
[BiSC D-075-007, 2015]	Bi-Strategic Command Directive 075-007, "Education and Individual Training Directive", 2015
[NAC AC/322-D(2007)0048, 2007]	North Atlantic Council Document AC/322-D(2007)0048, "NATO Architecture Framework (NAF) V.3", 2015
[NCIA PDED 06.00.03, 2015]	NATO Communications and Information Agency Process Definition and Execution Document 06.00.03, "Manage Risk", 2015
[NCIA AD 06.03.02, 2015]	NATO Communications and Information Agency Directive 06.03.02, "Service Change Management through the Lifecycle", 2015
[NCIA AD 06.03.04, 2015]	NATO Communications and Information Agency Directive 06.03.04, "Test Verification and Validation", 2015
[NCIA PDED 06.00.04, 2015]	NATO Communications and Information Agency Process Definition and Execution Document 06.03.04, "Test, Verification and Validation", 2015
[NCIA AD 06.00.05]	NATO Communications and Information Agency Directive 06.00.05, "Glossary of Terms and Definitions", EMB Review Draft v 2.0, 2015

Table 28: Other Documents

F.1.2. Project Documents

[NAC AC/322-N(2011)0154, 2011]	North Atlantic Council Document AC/322-N(2011)0154, "Capability Package 9C0150 Core Information Services for Command and Control", 2011, NATO RESTRICTED
[SHAPE SH/CCD J6/SM FCIS/163/17-317951, 2017]	Supreme Headquarters Allied Powers Europe SH/CCD J6/SM FCIS/163/17-317951, "SOA and IDM Platform – Operational Acceptance Criteria", 2017

Table 29: Project documents

F.1.3. Deployable CIS References

[NAC AC/322(SC/6-WG/2)N(2010)0014, 2010]	North Atlantic Council Document AC/322(SC/6-WG/2)N(2010)0014, "DCIS Target Architecture", 2010
[MCM-0043-2013, 2013]	Military Committee Memorandum 0043-2013, "BiSC Conceptual Framework for Alliance Operations (CFAO)", 2013
[SHAPE SH/CCD/J6/SM/FCIS/394/15-305978, 2015]	Supreme Headquarters Allied Powers Europe SH/CCD/J6/SM/FCIS/394/15-305978, "Deployable Communications and Information Systems (DCIS) Concept of Operations (CONOPS)", 2015
[MC 0593, 2015]	Military Commitee 0593, "Minimum Level of Command and Control Service Capabilities in Support of Combined Joint NATO led Operations", 2015
[NAC C-M(2015)0003-AS1, 2015]	North Atlantic Council Document C-M(2015)0003-AS1, "NATO Federated Mission Networking Implementation Plan", 2015
[CP0A0149 Rev1]	CP0A0149 Rev1, "NATO Deployable C2 Assets" (DCIS)
[NC3A TN-1078, 2008]	NATO C3 Agency Technical Note 1078, "Climatic and environmental specification for NATO CP0149, 'Deployable C2 assets'", 2009

Table 30: Deployeble CIS references

F.1.4. External References

[AIA/ASD SX000i, 2016]	Aerospace Industries Association/Aerospace and Defence Industries Association of Europe SX000i, "International guide for the use of the S-Series Integrated Logistic Support (ILS) specifications (issue 1.1)", 2016
[AIA/ASD S3000L, 2014]	Aerospace Industries Association/Aerospace and Defence Industries Association of Europe S3000L - International specification for Logistics Support Analysis – LSA (issue 1.1), 2014
[IEEE 610, 1990]	Institute of Electrical and Electronics Engineers Standard 610.12, "Standard Glossary of Software Engineering Terminology", 1990

[IEEE 1008, 1993]	Institute of Electrical and Electronics Engineers Standard 1008, "Standard for Software Unit Testing", 1993
[IEEE 1028, 2008]	Institute of Electrical and Electronics Engineers 1028, "Standard for Software Reviews and Audits"2008
[IEEE 1044, 2009]	Institute of Electrical and Electronics Engineers 1044, "Standard Classification for Software Anomalies", 2009
[IETF RFC 2119, 1997)]	Internet Engineering Task Force Request for Comments 2119, "Key Words for Use in RFCs to Indicate Requirement Levels", 1997
[ISO 9000, 2015]	International Organization for Standardization 9000 Series, "Quality Management Principles (Version 2015)", 2015
[ISO 10012, 2003]	International Organization for Standardization 10012 (Version 2003), "Measurement Management Systems – Requirements for measurement processes and measuring equipment", 2003
[ISO/IEC 12207, 2017]	International Organization for Standardization/International Electrotechnical Commission 12207, "Information Technology – Software Lifecycle Processes", 2008
[ISO/IEC 25010, 2011]	International Organization for Standardization/International Electrotechnical Commission 25010, "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models", 2011
[ISO/IEC/IEEE 29119, 2013]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers 29119-Part 1, "Concepts and definitions. Part 2 Test processes. Part 3 Test documentation", 2013
[OGC ITIL v3, 2007]	Office of Government Commerce, "Information Technology Infrastructure Library (ITIL) V.3", 2007
[MIL-STD 882E, 2011]	US Department of Defense Military Standard 882E, "System Safety", 2011
[Hohpe and Woolf, 2012]	G. Hohpe, B. Woolf, "Enterprise Integration Patterns: Designing, Building and Deploying Messaging Solutions", 2012

Table 31: External references

F.2. Applicable Standards

F.2.1. Technical Standards

F.2.1.1.   NATO Service Interface Profile (SIP) Standards

[NCIA AI 06.02.01, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.01, "Service Interface Profile for Security Services", 2015
[NCIA AI 06.02.02, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.02, "Service Interface Profile for REST Security Services", 2015
[NCIA AI 06.02.03, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.03, "Service Interface Profile for Security Token Services", 2015
[NCIA AI 06.02.04, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.04, "Service Interface Profile for Policy Enforcement Points", 2015
[NCIA AI 06.02.05, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.05, "Service Interface Profile for Enterprise Directory Services", 2015
[NCIA AI 06.02.06, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.06, "Service Interface Profile for Messaging", 2015
[NCIA AI 06.02.07, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.07, "Service Interface Profile for REST Messaging", 2015
[NCIA AI 06.02.08, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.08, "Service Interface Profile for Publish-Subscribe Services", 2015
[NCIA AI 06.02.09, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.09, "Service Interface Profile for a Publish/Subscribe Notification Broker with Subscription Manager", 2015
[NCIA AI 06.02.10, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.10, "Service Interface Profile for a Publish/Subscribe Notification Consumer", 2015
[NCIA AI 06.02.11, 2015]	NATO Communications and Information Agency Instruction - INSTR TECH 06.02.11, "Service Interface Profile for a Notification Cache Service", 2015
[NC3A RD-3297, 2011]	NATO Consultation, Command and Control Agency Reference Document 3297, "Information Discovery Service Interface Protocol Proposal 1.0", 2011
[NCIA TR/2011/CPW007253/01, 2013]	NATO Communications and Information Agency Technical Report /2011/CPW007253/01, "Metadata Registry Service Interface Profile Proposal", 2013

[NCIA TR/2011/CPW007253/04, 2013]	NATO Communications and Information Agency Technical Report /2011/CPW007253/04, "Query Manager Service Interface Profile Proposal", 2013
[NCIA TR/2012/SPW008423/20, 2012]	NATO Communications and Information Agency Technical Report /2012/SPW008423/20, "BPEL Composition Service – Standardization Profile Proposal", 2012
[NCIA TR/2012/SPW008423/23, 2013]	NATO Communications and Information Agency Technical Report /2012/SPW008423/23, "XSLT-Based Mediation Services – Service Interface Profile (SIP) Proposal", 2013

Table 32: NATO Service Interface Profile (SIP) standards

F.2.1.2. General

[WS-I Basic Profile 1.2, 2010]	Web Services Interoperability Organization (on-line), http://www.ws-i.org, "Basic Profile Version 1.2", at http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html, 2010.
[WS-I Basic Profile 2.0, 2010]	Web Services Interoperability Organization (on-line), http://www.ws-i.org, "Basic Profile Version 2.0", at http://www.ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html, 2010
[IETF RFC 3986 2005]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 3986, "Uniform Resource Identifier (URI): Generic Syntax", at http://tools.ietf.org/html/rfc3986, 2005

Table 33: General (standards)

F.2.1.3. Use of XML

[W3C XML 1.0, 2008]	World Wide Consortium, "eXtensible Markup Language (XML) Version 1.0 (Fifth Edition)" at http://www.w3.org/TR/REC-xml/, 2008
[W3C Namespaces in XML 1.0, 2009]	World Wide Consortium, "Namespaces in XML 1.0 (Third Edition)" at http://www.w3.org/TR/REC-xml-names/, 2009
[W3C XML Schema, 2004]	World Wide Consortium, "XML Schema Part 0: Primer Second Edition" at http://www.w3.org/TR/xmlschema-0/, 2004

Table 34: Use of XML

F.2.1.4. Integration Services

[IETF RFC 2616, 1999]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 2616, "Hypertext Transfer Protocol -- HTTP/1.1" at http://tools.ietf.org/html/rfc2616, 1999
[IETF RFC 2965, 2000]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 2965, "HTTP State Management Mechanism" at http://tools.ietf.org/html/rfc2965, 2000

[W3C SOAP 1.1, 2000]	World Wide Consortium (on-line), http://www.w3.org, "Simple Object Access Protocol (SOAP) 1.1" at http://www.w3.org/TR/2000/NOTE-SOAP-20000508, 2000
[W3C SOAP 1.2, 2007]	World Wide Consortium (on-line), http://www.w3.org, "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)" at http://www.w3.org/TR/soap12-part1/, 2007
[IETF RFC 5246, 2008]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", at http://tools.ietf.org/html/rfc5246, 2008
[IETF RFC 2818, 2000]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 2818, "HTTP over TLS" at http://tools.ietf.org/html/rfc2818, 2000
[OASIS WS-BaseNotification, 2006]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "Web Services Base Notification 1.3 (WS-BaseNotification)" at http://docs.oasis-open.org/wsn/wsn-ws_base_notification-1.3-spec-os.pdf, 2006
[OASIS WS-BrokeredNotification, 2006]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "Web Services Brokered Notification 1.3 (WS- BrokeredNotification)" at http://docs.oasis-open.org/wsn/wsn-ws_brokered_notification-1.3-spec-os.pdf, 2006
[OASIS WS-Topics, 2006]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "Web Services Topics 1.3 (WS-Topics)" at http://docs.oasis-open.org/wsn/wsn-ws_topics-1.3-spec-os.pdf, 2006
[WS-I Simple SOAP Binding Profile 1.0, 2004]	Web Services Interoperability Organization (on-line), http://www.ws-i.org, "Simple SOAP Binding Profile Version 1.0", at http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html, 2004
[WS-I Attachments Profile 1.0, 2006]	Web Services Interoperability Organization (on-line), http://www.ws-i.org, "Attachments Profile Version 1.0", at http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html, 2006
[OASIS WS-ReliableMessaging, 2009]	OASIS standard (on-line), https://www.oasis-open.org/, "Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2", at http://docs.oasis-open.org/ws-rx/wsrm/v1.2/wsrm.html, 2009
[W3C WS-Addressing, 2006]	World Wide Consortium (on-line), http://www.w3.org, "Web Services Addressing 1.0 - Core" at http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/, 2006
[W3C XSLT 1.0, 1999]	World Wide Consortium (on-line), http://www.w3.org, "XSL Transformations (XSLT) Version 1.0 ", at http://www.w3.org/TR/xslt, 1999
[W3C XSLT 2.0, 2007]	World Wide Consortium (on-line), http://www.w3.org, "XSL Transformations (XSLT) Version 2.0 ", at http://www.w3.org/TR/xslt20/, 2007

[W3C XQuery 3.1, 2015]	World Wide Consortium (on-line), http://www.w3.org, "XQuery 3.1: An XML Query Language", at http://www.w3.org/TR/xquery-3/, 2015
[W3C Xpath, 1999]	World Wide Consortium (on-line), http://www.w3.org, "XML Path Language (XPath) Version 1.0", at http://www.w3.org/TR/xpath, 1999

Table 35: Integration Services

F.2.1.5.　　　Registry and Repository Services

[OASIS UDDI, 2004]	Organization for the Advancement of Structured Information Standards (on-line), https://www.oasis-open.org/, "UDDI Version 3.0.2", at http://www.uddi.org/pubs/uddi_v3.htm, 2004
[W3C WSDL, 2001]	World Wide Web Consortium, "Web Services Description Language (WSDL) 1.1", at http://www.w3.org/TR/wsdl, 2001
[W3C XPointer, 2003]	World Wide Web Consortium, "XPointer Framework", at http://www.w3.org/TR/2003/REC-xptr-framework-20030325/, 2003

Table 36: Registry and repository services

F.2.1.6.　　　SMC Services

[ISO/IEC 17963, 2013]	International Organization for Standardization/International Electrotechnical Commission 17963, "Web Services for Management (WS-Management) Specification", 2013

Table 37: SMC services

F.2.1.7.　　　Information Services

[OASIS WS-BPEL V2.0, 2007]	OASIS standard (on-line), https://www.oasis-open.org/ OASIS Standard wsbpel-v2.0-OS, "OASIS Services Business Process Execution Language (BPEL) Version 2.0", at http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.pdf, 2007
[OMG BPMN V2.0.2, 2013]	Object Management Group standard (on-line), http://www.omg.org/, "Business Process Model and Notation (BPMN) Version 2.0.2", at http://www.omg.org/spec/BPMN, 2013
[W3C OWL 2, 2009]	World Wide Web Consortium, "OWL 2 Web Ontology Language, Document Overview", at http://www.w3.org/TR/owl2-overview, 2009
[W3C RDF Concepts, 2004]	World Wide Web Consortium, "Resource Description Framework (RDF): Concepts and Abstract Syntax", G. Klyne et al, at http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/, 2004
[W3C SPARQL Query Language, 2008]	World Wide Web Consortium, "SPARQL Query Language for RDF", Eric Prud'hommeaux, Andy Seaborne, at http://www.w3.org/TR/rdf-sparql-query, 2008

[W3C SPARQL Protocol, 2008]	World Wide Web Consortium, "SPARQL Protocol for RDF", K.G. Clark, L. Feigenbaum, E. Torres, at http://www.w3.org/TR/rdf-sparql-protocol, 2008

Table 38: Information Services

F.2.1.8.   Identity and Security Services

[CCEB ACP133D, 2014]	Combined Communications-Electronics Board Allied Communications Publication 133 (D), "Common Directory Services and Procedures", 2014
[IETF RFC 2617, 1999]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 2617, "HTTP Authentication: Basic and Digest Access Authentication", at http://tools.ietf.org/html/rfc2617, 1999
[IETF RFC 4121, 2005]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 4121, "The Kerberos Version 5 Generic Security Service Application
Programming Interface (GSS-API) Mechanism	Version 2", at http://www.ietf.org/html/rfc4121, 2005
[IETF RFC 4422, 2006]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 4422, "Simple Authentication and Security Layer (SASL)" at http://www.ietf.org/html/rfc4422, 2006
[IETF RFC 4505, 2006]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 4505, "Anonymous Simple Authentication and Security Layer (SASL) Mechanism", at http://www.ietf.org/html/rfc4505, 2006
[IETF RFC 4616, 2006]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 4616, "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism" at http://www.ietf.org/html/rfc4616, 2006
[IETF RFC 4752, 2006]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 4752, "The Kerberos VS ("GSSAPI") Simple Authentication and Security Layer: (SASL) Mechanism", at http://www.ietf.org/html/rfc4752, 2006
[IETF RFC 5246, 2008]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", at http://www.ietf.org/html/rfc5246, 2008
[IETF RFC 6749, 2012]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 6749, "The OAuth 2.0 Authorization Framework", at http://tools.ietf.org/html/rfc6749, 2012
[IETF RFC 6750, 2012]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 6750, "The

	OAuth 2.0 Authorization Framework: Bearer Token Usage", at http://tools.ietf.org/html/rfc6750, 2012
[OASIS WS-Trust, 2009]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "WS-Trust 1.4" at http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.doc, 2009
[OASIS WS-Federation, 2009]	OASIS (on-line), "Web Services Federation Language (WS-Federation) Version 1.2"at http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf, 2009
[OASIS SAML, 2005]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0." at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005
[OASIS SAML Token Profile, 2006]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "Web Services Security: SAML Token Profile 1.1" at http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf, 2006
[OASIS XACML 3.0, 2010]	Organization for the Advancement of Structured Information Standards (on-line), http://www.oasis-open.org, "eXtensible Access Control Markup Language (XACML) Version 3.0" at http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf, 2010
[W3C XML-Signature, 2008]	World Wide Consortium (on-line), http://www.w3.org, "XML-Signature Syntax and Processing" at http://www.w3.org/TR/xmldsig-core/, 2008
[WS-I Security, 2010]	Web Services Interoperability Organization (on-line), http://www.ws-i.org, "Basic Security Profile Version 1.1", at http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html, 2010
[XML Encryption]	World Wide Consortium (on-line), http://www.w3.org, "XML Encryption Syntax and Processing" at http://www.w3.org/TR/xmlenc-core/, 2002

Table 39: Identity and Security Services

F.2.1.9.   Document Format Standards

[ISO 32000-1, 2008]	International Organization for Standardization 3200-1, " Document management -- Portable document format -- Part 1: PDF 1.7", 2008
[ISO 19005-1, 2005]	International Organization for Standardization 19005-1, " Document Management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)", 2005

[ISO 19005-2, 2011]	International Organization for Standardization, 19005-2, "Document Management - Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1 (PDF/A-2)", 2011
[ISO 19005-3, 2012]	International Organization for Standardization 19005-3, "Document Management - Electronic document file format for long-term preservation - Part 3: Use of ISO 32000-1 with support for embedded files (PDF/A-3)", 2012
[ISO/IEC 29500, 2008]	International Organization for Standardization and International Electrotechnical Commission 29500, " Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference", 2008
[MS RTF, 1997]	Microsoft Corporation, Microsoft Application Note GC0165, "Rich Text Format (RTF) Version 1.5 Specification", 1997
[NCIA Visual Identity Guidelines, 2013]	NATO Communications and Information Agency, "NCI Agency Visual Identity Guidelines 1.3", 2012
[NCIA HMI Style Guide, 2015]	NATO Communications and Information Agency, "HMI Style Guide for Rich C4ISR Applications", 2012
[NATO Visual Identity Guidelines, 2016]	NATO, "NATO Agency Visual Identity Guidelines B Version 3", 2016

Table 40: Document format standards

F.2.2. Quality Standards

[ISO/IEC 25010, 2011]	International Organization for Standardization/International Electrotechnical Commission 25010 "Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) System and software quality models", 2011

Table 41: Document quality standards

F.2.3. Programming Standards

[IETF RFC 2078, 1997]	Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 2078, " Generic Security Service Application Program Interface, Version 2" at http://www.ietf.org/html/rfc2078, 1997
[ISO/IEC 23270, 2006]	International Organization for Standardization/International Electrotechnical Commission, 23270, "Information technology -- Programming languages -- C#", 2006

[ISO/IEC 14882, 2003]	International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 14882, "Information technology -- Programming languages -- C++", 2014
[ISO/IEC 23271, 2003]	International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 23271, "Information technology -- Common Language Infrastructure (CLI)", 2012
[ISO/IEC 23272, 2011]	International Organization for Standardization/International Electrotechnical Commission 23272, "Information technology -- Common Language Infrastructure (CLI) -- Information Derived from Partition IV XML File", 2012
[ISO/IEC 15445, 2000]	International Organization for Standardization/International Electrotechnical Commission 15445, "Information technology -- Document description and processing languages -- HyperText Markup Language (HTML)", 2000
[ISO/TS 18152]	International Organization for Standardization/Technical Specification 18152, "Ergonomics of human-system interaction -- Specification for the process assessment of human-system issues", 2010
[ISO 9241-12, 1998]	International Organization for Standardization 9241-12, "Ergonomic requirements for office work with visual display terminals (VDTs) Part 12: Presentation of information", 1998
[ISO 9241-13, 1998]	International Organization for Standardization, 9241-13, "Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 13: User guidance", 1998
[ISO 9241-14, 1997]	International Organization for Standardization, 9241-14, "Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 14: Menu dialogues", 1997
[ISO 9241-16, 1999]	International Organization for Standardization, 9241-16, "Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 16: Direct manipulation dialogues, 1999
[ISO 9241-143, 2012]	International Organization for Standardization, 9241-143, "Ergonomics of human-system interaction -- Part 143: Forms", 2012
[ISO 9241-171, 2008]	International Organization for Standardization, 9241-171, "Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility", 2008
[ISO 9241-110, 2006]	International Organization for Standardization, 9241-110, "Ergonomics of human-system interaction -- Part 110: Dialogue principles", 2006
[JCP JSR 270]	Java Community Process, Java Specification Request 270, "Java SE 6 Release", 2006

Table 42: Programming standards

ANNEX G : Templates and format to be delivered by the Contractor

G.1. **This annex Provides some templates for some of the documents to be delivered by the contractor.**

G.1.1. All templates are for the Contractor to propose and for the Purchaser to decide. However, certain topics must be included as follows in this Annex.

G.1.2. List of templates available to the Contractor:

ID #	Title abbreviation	Tiitle name
1	PMP	Project Management Plan
2	RMP	Risk Management Plan
3	PSR	Project Status Report
4	Minutes of PRM	Minutes of Project Review Meetings
5	PIP	Project Implementation Plan
	IMP	Issue Management Plan
6	TAP	Test and Acceptance Plan
7	TFR	Test Failure Report
8	OSR	Off-specification Report
9	SVDD	System Version Definition Document
10	ICD	Security Mechanism Group

Table 43: List of templates available to the Contractor

G.2. **Project Management**

G.2.1. Project Management Plan (PMP)

Section #	Section Title	Section Description
	Executive Summary	Provides the managerial level description of the approach for the project and how the project will be managed.
1	Introduction	This section provides a high level overview of the project management and how the Contractor will manage the project
1.1	Purpose and Scope	State the scope of the project.
1.2	Document Organisation	This section describes the organisation of the project management plan
1.3	Points of Contact	Provides the title and organisation of the key points of contact for the project
1.4	Glossary	Includes a glossary of all terms and abbreviations used in this document. If the

		glossary is several pages in length, it may be included as an appendix.
		To the extent possible the terms defined in [NCIA AD 06.00.05] will be used.
2	Project Team	This section identifies the Contractors/partners that comprise the Contractor team
2.1	Project Management Structure	This section identifies the relationship among the various Contractors and provides a diagram of the organisational structure of the team
2.2	Prime Contractor	This section identifies the scope of the main Contractor and defines the roles and responsibilities of key staff provided by the Contractor
2.3	Consortium Partner	This section identifies the scope of the consortium partner(s) and defines the roles and responsibilities of key staff provided by the Contractor
2.4	Sub-Contractors	This section identifies the scope of the sub-Contractors and defines the roles and responsibilities of key staff provided by the sub-Contractor
3	Management Processes	This section defines the main project management processes, procedures and templates that will be used during the ITM project.
3.1	Project Management Methodology	This section describes the formal methodology to be employed by the Contractor.
3.2	Control of Schedule and Resources	This section describes how project milestones will be achieved and project resources will be used efficiently.
3.3	Risk Management	This section describes how risk will be managed and introduces the risk management plan.
3.4	Configuration Management	This section describes the Contractor's Configuration Management process that will be used in managing the project; as well as identifying the approval process for changes; who and how they are submitted; and how they will be tracked and monitored
3.5	Communications Management	This section defines the communication requirements for the project and how information flows and will be distributed. Communications management provides the following in a RACI matrix: Communication requirements by roles;

		What information is to be communicated; How the information is communicated; When will information be distributed; Who is responsible for the communication; and Who receives the communication.
3.6	Scope Management	This section identifies how the Contractor will define, track and manage the project scope and then how the Contractor will measure and verify the scope (i.e. Quality Checklists, Scope Baseline, Work Performance Measurements, etc.)
3.7	Relationship to other plans	This section address how the other project related plans (PIP, RMP, CMP, etc.) are managed, reviewed and updated.
4	Project Management Activities and Controls	This section identifies the management tasks that are to be fulfilled as part of the SOA & IdM Platform project and how they will be controlled.
4.1	Project Key Dates	This section provides a discussion of how the PIP's key project dates are identified and will be controlled.
4.2	Project Control & Corrective Actions	This section identifies how the Contractor will manage and control the project and support the integration of NATO PFE
4.2.1	Managerial Reporting Activities	This section identifies the Contractor's reporting procedures for status reports from his sub-Contractors and how they will be validated.
4.2.2	Project Web Site	This section describes the Project Web Site and how it will be used in the context of Project Management. Means of access to the website by the Purchaser should also be covered.
4.2.3	Reference environment	This section identifies how the Contractor is going to manage and control the Reference environment to ensure synchronisation of test activities with all dependent project parties, and applications
4.2.4	Project Review Meeting (PRM)	This section explains how the Contractor will use the PPRM to provide information, raise issues/concerns and report progress.
4.2.5	Design Reviews	This section explains how the Contractor will use the design process and design reviews to manage the implemented solution to ensure that the SOA & IdM Platform supports innovation, delivery of current technology and

		is properly integrated with NATO PFE and SMC.
4.2.6	Contractor Meetings	This section outlines how the Contractor plans to work with the other dependent projects to ensure that the SOA & IdM Platform can interface with the provided services
4.2.7	Problem Reporting & Monitoring	This section identifies how the Contractor will identify, report and manage SOA & IdM Platform problems that require the Purchaser's support
4.2.8	SOA & IdM Platform Project Team	This annex contains the Curriculum Vitae of the project's key personnel
A.1	SOA & IdM Platform Project Manager (PM)	Contains the CV of the Purchaser approved PM
A.2	SOA & IdM Platform Technical Lead (TL)	Contains the CV of the Purchaser approved TL
A.3	SOA & IdM Platform Test Director (TD)	Contains the CV of the Purchaser approved TD
A.4	Additional	This section identifies other personnel needed, outlining a description of their functions, duties and responsibilities as well as how they will be used in the project. This list can include but is not limited to: Quality Assurance Manager; Site Implementation and Support Manager(s); Trainer(s); or Test Expert.

Table 44: Project Management Plan (PMP)

G.2.2. Risk Management Plan (RMP)

Section #	Section Title	Section Description
	Executive Summary	Provides a managerial description of the project's risk management concept and how risks will be addressed throughout the project.
1	Introduction	
1.1.	Purpose	This section identifies and explains the purpose of the risk management plan.
1.2	Intended Audience	Describes the intended audience of the plan, including the sub-Contractor team.
1.3	Glossary	Includes a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.
		To the extent possible the terms defined in ANNEX E will be used.
2	Risk Management Approach	This section identifies the overall risk management approach and should follow the standard risk management approach of: analyse, plan monitor and control-identification. The section should indicate how and to what extent the approach is consistent with related Agency Risk Management processes described in Ref. 57, and 58.
2.1	Risk Identification	This section will explain how the sources of risk, possible risk events and risk symptoms will be determined (details and specifics are addressed later in the document).
2.2	Risk Analysis	This section explains how the following will be determined: the value of opportunities to pursue vs. the threats to avoid and the opportunities to ignore vs. the threats to accept (details and specifics are addressed later in the document).
2.3	Response Planning	This section explains the response planning process and its relationship between risk management and contingency plans (details and specifics are addressed later in the document).
2.4	Risk Monitoring and Control per milestone	This section explains the risk monitoring and control process and how corrective action plans are developed, implemented, and monitored (details and specifics are addressed later in the document).
3	Roles and Responsibilities	For each project role, this section will describe the responsibilities with respect to risk; additional roles can be added.

Section #	Section Title	Section Description
3.1	Project Manager	The section formalises that the project manager is responsible for approval of the risk management plan (this document), leads and participates in the risk management process, and takes ownership of risk mitigation/contingency planning and execution, ultimately making the project manager responsible for the decisions on risk actions, in coordination with the project sponsors.
3.2.	Project Team	The section explains how the project team members (analysts/product managers, designers, developers, testers, and deployment team members) will participate in the risk identification, monitoring and mitigation process/activities.
3.3.	Quality Assurance Lead	This section addresses how the quality assurance (QA) lead will be involved in ensuring that identified risks are being managed per the risk management plan and his/her involvement in identifying new risks and/or proposing mitigation strategies and contingency plans, along with proposing improvements to the risk management plan and processes.
3.4.	Project Sponsors	Project sponsors participate in risk identification and risk activities, as necessary. Project sponsors also receive escalated risks and assist with mitigation and contingency actions for escalated risks
3.5.	Project Stakeholders	Stakeholders assist in monitoring risk action effectiveness and participate in risk escalation, as necessary.
4.	**Risk Identification**	
4.1	Sources	This section provides the detailed description of how risk identification will be done throughout the project's life-cycle even though the majority of the risks should be identified early on in the project. The following may be considered as tools and techniques for risk identification: Analysis of high-level deliverables; Analysis of the PIP; Analysis of change requests; Analysis of project assumptions; Project team input; Lessons learned;

Section #	Section Title	Section Description
		QA audits and reviews; Performance and status reports; or Diagramming techniques.
4.2	Risk Log (Register)	This section identifies and documents the selection logic for the risk sources, events and symptoms and collects the risks' information and builds/establishes the principle and need for the risk log (maintain as a separate document) where the following information should be noted: Risk category; Risk trigger; Potential outcome; Raised By; Date Raised; and Source.
4.2.1	Taxonomy of the Identified Risks	This should be explained here and provided in RMP Appendix A
4.2.2	Operational Risks	This section identifies the list of operational risks
4.2.3	Support Risks	This section identifies the list of support related risks
4.2.4	External Risks	This section identifies the list of dependency and external (project) risks
5.	Risk Analysis/Assessment	
5.1.	Background	This section describes the summary of the Risk Management Process against the following criteria: Methods of Risk Assessment, Probability estimation of the risk occurrence, Impact estimation of the risk, if it occurs, Cost estimation,

Section #	Section Title	Section Description
		Schedule estimation, External risks, and Risk Ranking for the phases of the project: design, implementation, operations, and support.
5.1.1.	Qualitative Analysis	This section describes the qualitative analysis process used to determine: The likelihood of the risk occurring, The qualitative impact on the project, and The quality of the risk data being utilised.
5.1.2.	Quantitative Analysis	If quantitative analysis is to be used, this section should contain information on: The criteria for which risks will undergo quantitative analysis Technique(s) to be utilised: The impact to cost or schedule for risks", The probability of meeting project cost and/or schedule targets, and Realistic project targets on cost, schedule, and/or scope, and Expected outputs of analysis
5.2.	Documentation	The results of risk analysis should be documented in the risk log/register. The following information need to be entered in the log (register): Risk impact; Risk probability; Risk matrix score – computed by the risk log (register) spreadsheet after impact and probability are entered; Risk priority – computed by the risk log (register) spreadsheet after impact and probability are entered, and Qualitative impact – descriptive comments about the potential risk impact.
6.	Response Planning	

Section #	Section Title	Section Description

6.1.	Background	This section describes the risk strategy and planning process to minimise the effects of the risk and how it will be controlled and managed:-
		
		    Risk Handling Process,
		    Evaluation and Selection of options, and
		    Tracking of the process.

6.2.	Risk Strategies	This section describes the methods for responding to risks and defines the various terms.
6.2.1.	Avoid	
6.2.2.	Transfer	
6.2.3.	Mitigate	
6.2.4.	Accept	

6.3.	Documentation	This paragraph addresses the risk log (register) showing:
		
		    Issues,
		    Response strategy (avoid, transfer, mitigate, or accept),
		    Response notes, and
		    Risk owner.

7.	Risk Monitoring and Control	

7.1.	Background	This section identifies the monitoring and control of the risk environment and describes the following tasks are performed:
		
		    Identification and planning for new risks;
		    Tracking of identified risks and their trigger conditions;
		    Periodically review risk and issue status/review as part of project performance information;
		    Re-analyse existing risks to see if the response plan must change, and

Section #	Section Title	Section Description
		Review the effectiveness of the RMP.
7.2.	Timing	This section discusses how often the risk monitoring and control process will occur over the lifetime of the project.
7.3.	Documentation	This section identifies the updating of the risk log (register) with information based on the status of the risk item: Identified – Risk documented, but analysis not performed, Analysis Complete – Risk analysis done, but response planning not performed, Planning Complete – Response planning complete, Triggered – Risk trigger has occurred and threat has been realised, Resolved – Realised risk has been contained, Retired – Identified risk no longer requires active monitoring (e.g. risk trigger has passed), Trigger Date – if the risk has been triggered, and Comments/notes.

Table 45: Risk Management Plan (RMP)

G.2.3. Project Status Report (PSR)

Item	Title	Section Description
	Header	Identifies the report identification number, author and date of release
1	Period of Report	This section identifies the start and end date of the reporting period
2	Activities	This section lists the Contractor activities that occurred during the reporting period and includes the status of current and pending tasks/action items
3	Schedule Impact	This section identifies the status of the plan and associated deliverables and whether they are on time or delayed
4	Products Completed	This section lists the products and deliverables with their status (delivered, reviewed, approved) as well as invoices sent
5	Tests Carried Out	This section lists the tests conducted in the ITS during the reporting period and their status (in progress, tested pass, tested failed)
6	Change Status	Summary and status of Change Requests requested, pending or approved during the period
7	Actual/Potential Issues and Risks	This section describes any identified problems, anomalies and high risk areas with proposed solutions or corrective actions identified in the reporting period – and linked to project issue and/or Risk Log (Register)
8	Next Period's Planned Work	This section identifies the activities scheduled for the upcoming reporting period (which may be a PPRM)
9	Upcoming Deliverables	This section identifies the SSS items that will be delivered in the upcoming period
10	Measurements	This section identifies the development and testing measurements baseline by period, in order to track progress and product status

Table 46: Project Status Report (PSR)

G.2.4. Minutes of Project Review Meetings

Item	Description	Comment
1	Project Management Plan Status	Identify any upcoming changes to the PMP
2	Record of Decisions	A record of all decisions reached at the meeting. Any supporting material should be included with the minutes as annexes; i.e., trade-off analyses, etc., so that the decision is documented, but also the context for the decision.

NATO UNCLASSIFIED

3	Review of On-Going Action Items	Review the status of the project's open action items
4	Project Schedule: Status of On-Going Tasks and WBS	Identify the status of the PIP and state of current activities
5	Accomplishments &Status of Current Contract Deliverables	List major tasks/accomplishments completed and/or milestones achieved since the last meeting
6	Invoices	Review of new acceptance documents and status of invoices
7	Testing Status	Review testing timeline and status of testing
8	Status of Problems with Delivered Capabilities	Review deliverable and test problems/deficiencies and corrective action status
9	Risk Review	Review the Risk Log (Register) for the current phase/stage of the project
10	Problems and Issues	New or potential problems/issues for action/decision
11	Changes	Review status of Change Requests
12	Activities for the Next Period	Identify major tasks/accomplishments to be completed and/or milestones to achieve before the next meeting
13	Any Other Business	Identify the date of the next meeting and any other points for discussion

Table 47: Minutes of Project Review Meetings

G.2.5.   I
ssue Management Plan (standalone deliverable)

Section #	Section Title	Section description
1	Control Mechanism	The IMP need to describe the issue control mechanisms to be used
2	Categorisation	The issues need to be categorised as one of the following: a) Request for change (handled by the project change management procedure) b) Off-specification (handled under Quality Management Plan) c) Problem (handled within Issue Management) d) Concern (interfacing to Risk Management) Question / Query / Suggestion
3	Issue Management Process	The IMP need to detail the issue management process, including the capture, examination (consisting of: validation, assessment, and analysis of impact), review, through to issue completion. Where

		completion can be rejection, statement of containment, service request, or change request
4	Issue Log (Register)	The follow-on actions for the identified and analysed issues will be subject to the Purchaser confirmation: The IMP have to include the Issue Log (Register) template. The Contractor have to maintain the Issue Log (Register) and follow-on actions in synchronisation with the Project Review Meetings schedule

Table 48: Issue Management Plan

G.3. System Implementation

G.3.1. Project Implementation Plan (PIP)

Section #	Section Title	Section Description
	Executive Summary	Provides a managerial level description of how the plan for how the project will be implemented.
1	Introduction	This section explains the purpose and overall objective of the PIP and identifies the major activities to be undertaken in the SOA & IdM Platform project.
1.1	Purpose and Scope	State the purpose of the PIP and explicitly state that this is a living document and that it is to be updated as the project evolves.
1.2	Document Organisation	This section describes the organisation of the PIP.
1.3	Points of Contact	Provides the title and organisation of the key points of contact for the production, analysis and assertions made in the PIP
1.4	Glossary	Includes a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix. To the extent possible the terms defined in Ref. NCIA AD 06.00.05 will be used.
2	Assumptions and Constraints	This section describes the assumptions and constraints concerning the development and execution of the implementation plan addressing items like: Schedule; Hardware; Software and other technology to be reused or purchased; or Interfaces constraints.
3	Implementation Plan	This section provides the framework for the approach taken to create the project schedule.

3.1	Major Tasks	This section describes the major SOA&IDM Project tasks required to deliver the SOA&IDM in the form of a Work Breakdown Structure and Product Breakdown Structure as required in section 4.3.2.
3.2	Project master schedule	This subsection of the Project Implementation Plan provides a schedule of activities to be accomplished. Show the required tasks (described in Subsection 3.1, Major Tasks) in chronological order, with the beginning and end dates of each task. If MS Project is used to plan the implementation, include the project Gantt chart. Include any milestones from the projects that are dependent on this project and vice-versa

This includes the scheduling tool/format, schedule milestones, and schedule development roles and responsibilities. |
3.3	Project Milestone List	This section provides a discussion of the milestones and a summary list of project milestones and their associated dates.

3.4	Security	This section provides an overview and discussion of the security aspects related to the SOA & IdM Platform implementation concerning security:
		
		      Personnel clearances;
		      Screening of equipment;
		      Storage of equipment;
		      Movement and transportation;
		      Security testing & evaluation;
		      Documentation and review;

3.5	Design	This section addresses the tasks needed to produce the SOA & IdM Platform designs and supporting reviews.
4	Implementation	This section describes the site-specific implementation requirements and procedures.
4.1	SOA & IdM Platform Sites	This section defines the requirements that must be satisfied for the orderly implementation of the SOA & IdM Platform services and system for the Wave I

		sites. The PIP have to describe the implementation and how this relates to the all of the Wave I Sites.
4.1.1	Operational Network (NS)	This section addresses the implementation specifics of the ON including an overview description of the implementation: team, schedule, procedures, and data.
4.1.3	Protected Business Network (NU/NR)	This section addresses the implementation specifics for the Business including an overview description of the implementation: team, schedule, procedures, and data.
4.4	Risk and Contingency Planning	This section identifies the risks and actions to take in the event the implementation fails or needs to be altered at any point and includes the factors to be used for making the decision (refer to the Risk Management Plan as needed)
4.5	Acceptance Criteria	This subsection of the Project Implementation Plan establishes the exit or acceptance criteria for transitioning the system into production. Identify the criteria that will be used to determine the acceptability of the deliverables as well as any required technical processes, methods, tools, and/ or performance benchmarks required for product acceptance
5	Implementation Support	This section describes the general support required for the implementation.
5.1	Hardware	This section provides a list of all hardware needed for installing and testing the SOA & IdM Platform services. Identify the hardware by make, model and configuration; also add information about warranty/maintenance contract(s). If this information is provided in another document identify that item here and reference appropriately otherwise add as an Annex to this document.
5.2	Software	This section provides a list of all software (software, operating systems, utilities, etc. and identify the software as COTS, custom developed or legacy) required to implementation the SOA & IdM Platform. Identify the software by name/acronym, version & release numbers, and configuration settings; as well

			as add information about vendor support, licensing, usage, and maintenance contract and associated costs. If this information is provided in another document identify that item here and reference appropriately otherwise add as an Annex to this document.
5.3		Facilities	This section identifies the physical facilities (space), accommodations, location(s) and time (hours per day needed, number of days, and anticipated dates) required to support the storing, staging, implementing and support of the SOA & IdM Platform.
5.4		Issues	This section addresses any known issues or problems with respect to implementation planning.
5.5		Performance Monitoring	This section describes how the Contractor will monitor the performance and determine if the implementation's progress
5.6		Configuration Management Interface	This section addresses the relationship between implementation and Configuration Management (e.g. when versions will be distributed)
6		Implementation Impact	This section describes how the migration is expected to impact the SOA & IdM Platform's implementation for the HQ with respect to Network / infrastructure User community Service Level Agreements requirements (performance, availability, security) System backups, expected transaction rates Storage requirements (with expected growth rate) Help desk support requirements
7		SOA & IdM Platform	

	project Gantt Chart	

Table 49: Project Implementation Plan (PIP)

G.4. Testing and Acceptance

G.4.1. Test and Acceptance Plan (TAP)

Section #	Section Title	Section Description
	Executive Summary	Provides a managerial description of the project's Test and Acceptance concept.
1	Introduction	
1.1.	Purpose	This section identifies and explains the purpose of the TAP.
1.2	Intended Audience	Describes the intended audience of the TAP, including the sub-Contractor team, the Purchaser's representatives and dependent projects/PFE testing.
1.3	Glossary	Includes a glossary of all terms and abbreviations used in this document. If the glossary is several pages in length, it may be included as an appendix.
2	Reference environment	This section explains the role and environment of the Independent Verification and Validation to be conducted on the appropriate Reference Environment, as well as its manning and support requirements.
3	Testing	This section identifies the test process from component through to service testing as controlled and defined in the configuration management process. It need to describe how the Contractor proposes to work with the Customer's representatives during all phases of testing.
3.1	Approach	This section identifies the overall test strategy and is related to configuration management, change management, configurations, metrics, tools needed, unique hard/software, regression testing, and process. It will include a description of how the Contractor will perform testing to ensure the required quality criteria is achieved. Reference should be made to [NCIA AI TECH 06.03.04, 2015] Agency IV&V Directive.
3.2	Responsibilities	This section describes the roles and responsibilities of the staff needed to support the testing facility's Reference System, Reference environment, testing staff and actors involved in the testing process (scheduling, de-conflicting, decision making, etc.) with respect to the suite of SOA & IdM Platform testing steps. It should identify all required personnel needed, including Contractor personnel and Purchaser personnel, and NCI Agency user and customer personnel, as necessary.

Section #	Section Title	Section Description
3.2.1	Test Manager	
3.2.2	Testing Team	
3.2.3	NATO QAR	
3.2.4	Purchaser Independent Verification and Validation	
3.3	Schedule	This section identifies the scheduling process and creation of a realistic schedule (showing planning, development of test cases, setup, testing, etc.). Will also address the planning impact of schedule slips, failed or stopped tests and how these will be resolved to minimise the overall impact to the SOA & IdM Platform schedule.
3.4	Environmental Needs	This section identifies any special needs (power, space, equipment, software, etc.) and dependent PFE availability.
3.5	Reports	This section defines the reports and records developed, produced and maintained as a result of the testing process.
3.5.1	Test Items	This section identifies all items to be tested and implemented in the Datacentres or Node sites, whether it is a client facing or back-end service.
3.5.2	Risk Issues	This section identifies the critical areas for testing, including but not limited to: Interfaces, Security compliance, COTS products, Contractor developed integration products, Complex functions,

Section #	Section Title	Section Description
		Reliability,
		Maintainability,
		Usability,
		Efficiency,
		Modifications due to changes,
		Poorly documented modules, and
		as well as misunderstanding SOA & IdM Platform original requirements.
		Additional areas to be tested, can be found in [NCIA AI TECH 06.03.04, 2015].
3.5.3	Features to be Tested	This section lists the user and service functions to test based on what the SOA & IdM Platform is to do with associated risk level for each component, software item, integration aspect and service.
3.5.4	Features not to be Tested	This section lists what is not to be tested from a configuration management /version control view of the component or service or system. It will include an explanation why the item is not to be tested.
3.5.5	Test Case Reports	This section defines how the test cases are to be documented and recorded.
3.6	Staffing and Training Needs	This section identifies the need for special skills and Purchaser support.
4	Testing Prerequisites	This section outlines the requirements to be satisfied and implemented prior to testing
4.1	Quality Assurance	Refers to the QAP needs and requirements for testing a service.
4.2	Test Cases	This section addresses the review and acceptance process of the test cases.
4.3	Test Data	This section identifies any test data requirements and who is responsible for providing what data.
5	Test Procedures	

Section #	Section Title	Section Description
5.1	Test Schedule	This section identifies the testing periods.
5.2	Planning Risks and Contingencies	This section relates testing to the Risk Management Plan and addresses how the risks are to be addressed and/or mitigated.
5.3	Test Results	This section identifies the documenting of the test results.
5.3.1	Item Pass/Fail Criteria	This section identifies the completion criteria for the service in terms of entrance and exit criteria and resolution of test deficiencies.
5.3.2	Suspension Criteria and Resumption Requirements	This section explains when a test will be paused; specifies what constitutes a stoppage; and what is the acceptable level of deficiencies/defects that are accepted before a test is stopped. This section also explains the actions that will take place when testing is paused or stopped.
5.3.3	Test Deliverables	This section identifies the test deliverables before during and after: Test plan; Test cases; Test design specification & configuration; Interfaces; Restore points; Logs (error and execution); and Reports (errors, problems, corrective actions, successes).
5.3.4	Remaining Test Tasks	This section describes the steps/stages of the SOA & IdM Platform testing from components to integrated system, to services.
5.4	Corrective Actions	This section addresses how corrective actions will be addressed and processed.
5.5	Acceptance and Release	This section defines the steps needed to determine if a component or service has passed all tests and is ready for the production environment and acceptance by the Purchaser.
5.6	Suspend Testing	This section identifies the criteria to end testing and close the IREEN.
5.7	Documentation	Provides the comprehensive list of documentation defined as the STDP.

G.4.2. Test Failure Report

Section #	Section Title	Section Description
	Executive Summary	This section provides a managerial summary of the failure and the classification of the Failure as either Class A, Class B, or Class C.
1	Failure Identification	A descriptive title for the failure.
2	Failure classification	Class A, Class B, or Class C.
3	Failure Description	A description of the failure
4	Impact assessment	An assessment of the impact of the failure, related to, as a minimum: schedule, cost, or quality, or added risk to the same.
5	Proposed Actions	The actions proposed to be taken by the Contractor.

Table 50: Project Master Test Plan (PMTP)

G.4.3.   Off-Specification Report

Section #	Section Title	Section Description
	Executive Summary	This section provides a managerial summary of the off-specification.
1	Title	A descriptive title for the off-specification.
2	Off-specification Description	A description of the off-specification.
3	Related Test	Identification of the related test (if identification occurred during testing)
4	Severity	Classification of the off-specification as 'Major' or Minor', where all major off-specifications need to be rectified prior to deployment or going live.
5	Configuration Item Affected	Identification of the CI(s) affected.
6	Action Taken	A description of any actions taken.
7	Resolution Status	A description of the status of the off-specification.

Table 51: Off-Specification Report

G.4.4.   System Version Definition Document

Section #	Section Title	Section Description
	Executive Summary	This section provides a managerial summary of the version.
1	Version Identification	A version number conforming to a defined numbering scheme (if software then [NCIA AI TECH 06.03.01, 2015] should be used)
2	(Changed) Capabilities	The capabilities of the version. If the version is an update then only the delta changes need to be identified.
3	Installation Guidelines	A short description of the installation procedure. This should only cover differences between this version and the instructions contained in the Maintenance Manual.

4	CI(s)	A list of the CI(s) making up the version.

Table 52: System Version Definition Document

G.5. Security Mechanism Groups

G.5.1. Security Mechanism Groups

Security mechanism Group (SG)	Security mechanism Group (SG) Name	SM #	Security Mechanism (SM) Name
SG01	Malware Protection	SM01a	Malware Protection for Server (e.g. AV for servers)
		SM01b	Malware Protection for Application Server (e.g. SharePoint, etc)
		SM01c	Malware Protection for Multifunction Printing (MFP) device
		SM01d	Malware Protection for Server Database
		SM02	Malware Protection for Client (e.g. AV for clients)
		SM02b	Second but different Malware Protection for Client (e.g. AV for clients)
		SM03	Malware Protection for handheld devices (e.g. smartphones)
		SM04	Malware Protection for Email server (e.g. AV for e-mail services)
		SM05	Malware Protection for Web server (e.g. AV for Web Services)
		SM08	HTTP AV Proxy
		SM09	FTP AV Proxy
SG02	Boundary Protection Devices and Systems(Content Check, Proxy and Firewall)	SM06	Messaging Content Filtering (MCF)
		SM07a	Web Content Filtering (WCF) - Categorization
		SM07b	Web Content Filtering (WCF) - Content Inspection
		SM07c	Web Content Filtering (WCF) - SSL Intercept
		SM14	Firewall (FW) for Outer Perimeter/ Border Protection
		SM15	Firewall (FW) for Inner Perimeter
		SM18	IP Filtering & Management
		SM19	Network/Port Address Translation (NAT/PAT)
		SM20	(Web) Application Firewall and other proxy/reverse proxy
		SM23	Voice over Internet Protocol (VoIP) protection
		SM24	Wireless Network Protection (and Jamming)
		SM31	Logical Security Zones
		SM34	Information Protection Control (IPC) - Classification/Marking
		SM35	Information Protection Control (IPC) - Data Loss/Leak Prevention (DLP)

Security mechanism Group (SG)	Security mechanism Group (SG) Name	SM #	Security Mechanism (SM) Name
		SM39	Development/Test/Pre-production Environments
		SM56	Data diode
SG03	Integrity Check	SM10	Integrity Checker
		SM55	Data processing
SG04	Cryptography	SM11	SSL (TLS) and SSH
		SM29	Cryptographic security (e.g. Encryption / Decryption)
		SM46	Data Scramble
SG05	Identity Management and Access Protection	SM12	Strong Authentication (User Token)
		SM13	Enterprise Single Sign-On/Off (ESSO)
		SM16N	Intrusion Detection and Prevention System (IDS/IPS) - Network (N) Based
		SM16H	Intrusion Detection and Prevention System (IDS/IPS) - Host (H) Based
		SM17	Network Access Control (NAC) / Network Access Protection (NAP) and Network Access Quarantine (NAQ)
		SM23	Voice over Internet Protocol (VoIP) protection
		SM24	Wireless Network Protection (and Jamming)
		SM30a	NPKI - User certificate
		SM30b	NPKI - Device certificate
		SM39	Development/Test/Pre-production Environments
		SM41	CAPTCHA (and its alternatives)
		SM42	Identity & Access Management (IAM or IdM)
		SM48	Password Management
		SM49	Identity & Authentication, Access Control (IAAC)
SG06	Monitoring, Logging and Auditing	SM21	System and Security Logging & Auditing - Infrastructure and Servers
		SM21b	System and Security Logging & Auditing - Applications
		SM27	Network Management System (NMS) / Systems Management System (SMS)
		SM28	IT Forensic and Incident Handling
		SM47	Data Safeguarding (e.g. DAM, FSAM)
SG07		SM25	Storage Compartmented Security Mode (SCSM)

Security mechanism Group (SG)	Security mechanism Group (SG) Name	SM #	Security Mechanism (SM) Name
	Storage and Digital Preservation	SM26	Backup, Recovery and Contingency planning
		SM45	Storage Areas security
SG08	Interruptibility and Availability	SM26	Backup, Recovery and Contingency planning
		SM33	Load Balancing (LB) / Failover (FO)
		SM38	Quality of Service (QoS)
		SM50	Protection against (D)DoS
SG09	Compliance and Configuration Control (incl. Documentation)	SM22	Hardening of Network Devices
		SM27	Network Management System (NMS) / Systems Management System (SMS)
		SM32	Policies, directives, guidance and procedures
		SM36	Vulnerability Scanning & Compliancy Check
		SM37	OS security settings
		SM40	Configuration Management
		SM43	Management of the Security Mechanisms
		SM44	Time Synchronization (e.g. NTP)
SG10	Security Service Orchestration	SM43	Management of the Security Mechanisms
		SM49	Identity & Authentication, Access Control (IAAC)
SG11	Physical security	SM51	Physical security
		SM54	Emission security
SG12	Personnel security	SM52	Personnel security
SG13	Environmental security	SM53	Environmental security

Table 53: Security Mechanism Groups

ANNEX H: ITM Security MechAnisms

The following table explains the security mechanisms that shall be provided by ITM.

SM nr.	SM Name	Security Mechanism (SM) Definition
SM01a	Malware Protection for Server (e.g. AV for servers)	The system shall incorporate protection measures against malware. The protection measures shall incorporate anti-virus (AV), anti-spyware, anti-adware, anti-spam and anti-phishing. Malware protection shall be implemented at all data sources and endpoints of the system including Clients (desktops, laptops, handheld devices, etc.) and Servers (Application servers, Database Servers, File Servers, Email Servers, Web Servers, Print Servers, etc.). A different malware protection product than the one running on the DMZ shall be deployed in the internal network. The products shall be selected from the NATO Information Assurance Product Catalogue (NIAPC) and shall be approved for the security classification of the data processed.
SM01b	Malware Protection for Application Server (e.g. SharePoint)	A different malware protection product than the one running on the DMZ shall be deployed in the internal network.
SM01c	Malware Protection for Multifunction Printing (MFP) device	
SM01d	Malware Protection for Server Database	The products shall be selected from the NATO Information Assurance Product Catalogue (NIAPC) and shall be approved for the security classification of the data processed.

SM02a	Malware Protection for Client (e.g. AV for clients)	
SM02b	Second but different Malware Protection for Client (e.g. AV for clients)	
SM03	Malware Protection for handheld devices (e.g. smartphones)	
SM04	Malware Protection for Email server (AV for email services)	
SM05	Malware Protection for Web server (AV for Web Services)	
SM06	Messaging Content Filtering (MCF)/(SMTP AV Proxy)	The Messaging Content Filtering (MCF) shall be able to evaluate inbound and outbound email messages on the basis of user-defined rules. Each rule shall contain a list of regular expressions, keywords or phrases. The Content filter shall be able to evaluate the header and/or content of messages by comparing the messages with the pre-defined rules. When the content filter finds matching rules, it shall be able to take actions as defined by the rule. The persons affected by the action shall be notified of the actions affecting the message as defined in the rule. It is required to enforce policies by blocking or allowing content based on analysis. The solution is needed to monitor, encrypt, filter, and block content contained in email, instant messaging, peer-to-peer file transfer, web postings, and other types of traffic.

		This includes the SMTP AV Proxy.
SM07a	Web Content Filtering (WCF) - Categorization	Web Content Filtering (WCF) is required to monitor, filter, and block content contained in web-mail, instant messaging, peer-to-peer file transfer, web postings, and other types of HTTP or HTTPS traffic. The content filter can be installed at different levels (browser, client or network). For the ITM project network content filtering is required.
SM07b	Web Content Filtering (WCF) - Content Inspection	
SM07c	Web Content Filtering (WCF) - SSL Intercept	
SM08	HTTP AV Proxy	AV proxies shall offer dynamic real time scanning of all incoming traffic before delivering the data to the end system.
SM09	FTP AV Proxy	
SM10	Integrity Checker	An Integrity Checker shall continuously run in the background of a device creating cryptographic hash values for all new and modified files and storing these hash values in a private database on a centralized server. At any time, it shall be possible to request a validation scan which compares the current hash of each file to the previously known hash in order to detect unauthorized modifications.
SM11	SSL VPN or SSL/TLS VPN	SSL/TSL based protocols and tools shall be deployed and used.

		Secure VPN tunnels are required in order to secure network communications between NATO bodies, Remote Offices and Mobile User, where SSL and TLS are security layer protocols found in all standard Web browsers.
		This security mechanism shall make use of an approved (or authorized) public-key infrastructure (i.e., NPKI).
SM12	Strong Authentication (User Token)	ITM shall deploy infrastructure/services to enable strong authentication to the NATO systems and networks. Strong authentication shall be two-factor and token-based.
		This security mechanism shall make use of an approved (or authorized) public-key infrastructure (i.e., NPKI).
SM13	Enterprise Single Sign-On (ESSO)	ITM shall deploy federation services capable of providing Single Sign On to the NATO infrastructure.
SM14	Firewall (FW) for Outer Perimeter/ Border Protection	Firewalls shall be deployed in each private-public network edges as well as in the internal NATO network, including:
SM15	Firewall (FW) for Inner Perimeter for NR Zones	• The NATO network perimeter (where the Datacentre meets the WAN and Internet). • Between NATO departments, to segregate access according to policy among user groups. • Between NATO LAN switch ports and Web, application, and database server farms in the Datacentre. • Where the wired LAN meets the wireless LAN (between Ethernet LAN switches and wireless LAN controllers). • In laptops, smartphones, and other intelligent mobile devices that store NATO data (in the form of personal firewall software) in the case of telecommuters and mobile workers.
SM16N	Intrusion Detection and Prevention System (IDS/IPS) - Network (N) Based	ITM shall integrate its infrastructure in the NCIRC FOC monitoring capabilities, by providing network taps for network based NCIRC FOC IDS/IPS probes and installing and configuring host based IDS/IPS software.

		The network taps shall be placed such that they provide NCIRC with a complete view of all network segments and should in particular enable placement of probes between any two connected security zones without a significant impact on the performance of the network.
SM16H	Intrusion Detection and Prevention System (IDS/IPS) - Host (H) Based	
SM17	Network Access Control (NAC) / Network Access Protection (NAP) and Network Access Quarantine (NAQ) (def to be modified to cover COM.op.1.5.3)	The capability to restrict the accessibility and availability of network resources to endpoint devices, whether on the campus or outside it, that comply with a defined security policy. Users and/or endpoint devices must authenticate themselves before getting access to the network, even if they are roaming. The authentication methods may vary depending on the device and connectivity types (i.e. hard-coded address, challenge-response, cryptographic methods and others. The network can then make further policy decisions based upon user and device identity characteristics. Before gaining network access, endpoint devices must be checked for vulnerabilities, security software configuration parameters (e.g. whether antivirus signatures are current), and malicious code signatures. Further network decisions are based upon the results of this examination. For instance, a device that is not compliant with a defined security policy has to be isolated/quarantined and undergo a remediation and sanitization process. Only when successful, the device may be granted access to the network and in accordance with its identity characteristics. The solution has to be centrally managed and configured to limit a device to specific network assets or tasks in accordance with policies and business requirements. For example, an IP phone may be restricted to a particular network VLAN and IP telephony gateway.

SM18	IP Filtering	IP Filtering is a mechanism that decides which of IP datagrams will be processed normally and which will be discarded. By discarded it is meant that the datagram is deleted and completely ignored as if it had never been received.
SM19	Network Address Translation (NAT)	NAT/PAT shall be used on all private-public network edges.
SM20	(Web) Application Firewall and other proxy/reverse proxy	Web servers shall be protected against known attacks using the current definitions of the "OWASP ModSecurity Core Rule Set" (Ref-69) or an equivalent set of attack detection rules.
SM21a	System and Security Logging & Auditing - Infrastructure and Servers	Logging and auditing requirements are to be satisfied on each network component and application. Event messages and alerts shall be transmitted over the network, and a tailored subset of these shall be centrally managed and stored. The standardization of the event log format and the correlation of logs is recommended as to enable an "automated smart analysis" of the logging also when combining logs coming from multiple systems. A full control over the administrative channels is required as to enforce global regulations, irrespectively of the User Types (or Categories/Roles), as to monitor, log and audit the whole network infrastructure in a transparent and integral way. This will allow collecting reliable information concerning the security monitoring, logging and auditing of any activity concerning ICT services, systems and their components.
SM21b	System and Security Logging & Auditing - Applications	Logs shall be retained as specified in the primary directive on CIS Security. NCIRC guidance and support is furthermore provided for the retention of security-related logs.
SM22	Hardening of Networked Devices	All network devices shall be hardened using NCIRC recommended configuration settings. For those devices for which no recommended configuration exist NCIRC shall be tasked with the development of a recommended configuration before deployment.

SM23	Voice over Internet Protocol (VoIP) protection	VoIP network segments shall be monitored and protected by network and security appliances as described in the NIATC, NCIRC-TC security recommendation on IP Telephony systems architecture, deployment and configuration, dated 27 September 2010.
SM24	Wireless Network Protection (and Jamming)	Wireless network shall be monitored and protected by network and security appliances as described in the Ref-67.
SM25	Storage Compartmented Security Mode (SCSM)	The purpose of SCSM is to split the information up into separate virtual compartments or security levels. Storage will use secure compartmented data access as information of different classification levels is to be stored using compartmentalized access and access control over trusted and untrusted networks. To create secure compartments, the storage area will use trusted virtualization, application-level firewalls and other security devices that may be used for this purpose.
SM26	Backup, Recovery and Contingency planning	ITM shall provide a proven, cost-effective and robust backup, replication and recovery solution between the different Datacentres. On-site and off-site backup/replication storage needs to be properly implemented and handled, including data encryption and dedicated/redundant bandwidth. As far as the Business Continuity Planning (BCP) and Contingency Planning are concerned, it is necessary to distinguish between "Local" (i.e. within the site) and "Non local" (i.e. across sites) backup.
SM27	Network Management System (NMS) /Systems Management System (SMS)	A Network Management System, as a combination of hardware and software, is needed to provide activity monitoring, network utilization, controlling, auditing, assessing performance of devices, managing, configuring and administering portions of (or the entire) ICT infrastructure.

		It needs to provide discovery capabilities, inventory, configuration and mapping dependency –mainly up to an including layer 3 of the OSI Reference Model.
		A Systems Management System (SMS) is required to provide systems integration as to orchestrate all systems providing services to the business, to coordinate the execution of multiple technical services and systems as to make them appearing as a "single" entity to service request.
		It needs to provide application monitoring, capacity monitoring, storage management, security management, auditing, assessing performance of systems and applications, managing, configuring and administering portions or all systems. Additionally, it shall provide discovery capabilities, inventory, configuration and mapping dependency –mainly from layer 4 and up to an including layer 7 of the OSI Reference Model.
		The SMS needs to integrate and/or interoperate with the NMS.
SM28	IT Forensic and Incident Handling	The IT Forensic security mechanism is needed to assure that digital evidence is accurately collected and that there is a clear chain of custody from the scene of the crime to the investigator, and ultimately to the concerning Authority.
		Digital artefacts that are relevant to forensics include computer systems, storage media, electronic documents, sequence of computer packets, etc. IT Forensic also helps with achieving regulatory compliance and managing response capabilities to IT incidents.
		As part of this security mechanism, NCIRC provided forensic agents will need to be installed and configured. The mechanism also covers Full Packet Capture of network
SM29	Encryption-Decryption /Cryptography	Cryptography is used to obfuscate and authenticate data in order to safeguard its confidentiality, authenticity and integrity. It should be used to encrypt data at rest (e.g. for mobile user devices) as well as data in transit (typically in combination with SSL/TLS and VPN tunneling).

		Depending on the classification level a different type of encryption/decryption mechanism may be required. For this security mechanism, only products approved for usage in NATO for a given classification level are allowed (see Ref-65 NIAPC).
		The maintenance of crypto equipment is part of this SM.
		This security mechanism also applies to the protection of passwords in storage or in transit, in accordance with security policies and best practices. It should be combined with other security mechanisms (e.g. SM13 and 30) as required.
SM30a	NPKI - User certificate	ITM shall provide infrastructure to integrate NPKI certificates and to use them for proving the identity, integrity or authenticity of users, devices or data.
SM30b	Public Key Infrastructure (PKI). NPKI Devices, in conjunction with SM17.	
SM31	Security Zones	The segregation in Security Zones (e.g., Public Security Zone, NU Security Zone, NR Security Zone etc.) enhances security as whole.
		This can be achieved at one or more network layers (mainly at Layer 2 and 3 according
		and using one or a combination of different types of
		Virtual Local Area Network (VLAN);
		• Private Virtual Local Area Network (PVLAN);
		• Access Control List (ACL);
		• VLAN Access Control List (VACL);
		• Multiprotocol Label Switching (MPLS);
		• Virtual Private Network (VPN);

• Virtual Private LAN Service (VPLS);

• Virtual Device Context (VDC);

• Firewall and IDS/IPS capabilities distinct at each layer;

• Distinct Firewall leg and port; and

• Distinct Virtual Switch (vSwitch).

The implementation of the "Security Zones" is called "Security Zoning" and may also include an air gap between CIS.

There is a specific architectural requirement to enable the placement of physical network probes between any two connected security zones without significant impact on the performance.

SM32	Policies, directives, guidance and procedures (PDP)	Policies, directives, guidance and procedures are to be developed where not existing, or regularly updated and published where existing: - Training; - Certified products; - Hardening guides; and - Security settings. This includes the NIATC hardening guides, excluding security-related setting for OS and routers/switches since they are covered respectively with SM37 and SM22.
SM33	Load Balancing / Fail over	A backup operation that automatically switches to a standby database, server, device or network if the primary system fails or it is temporarily unavailable (e.g. for servicing) is needed for all the core and/or critical components of the IT infrastructure. Depending on the type of service, this should include a distributing processing and communications activity evenly across a computer network so that no single device is overwhelmed. (Note: This SM may be provided as part of the ICT infrastructure, or specific for business applications

SM34	Classification Level / Data Labelling (aka Information Protection Control or IPC)	This SM is tightly linked to so-called Information Protection Control (IPC).
		It is needed to electronically label all IT resources thus to indicate the security classification level that the IT resource is permitted to handle. In addition, all data has to be marked with the classification level in accordance with the need-to-know policy.
		This SM needs to generate/share classification metadata –via single or bulk processing- that can be reused by other applications as well as by other security mechanisms, and that can be based on user attributes and roles.
		Depending on the business requirements, this SM may also need to confer the genuineness of data or "Data authenticity".
		This SM needs to work/interoperate with SM35, Data Loss Prevention. The Draft NATO Labelling and Binding Standards are provided for Contractor consideration under Ref-70 (subject to change until ratified).
SM35	Data Loss/Leak Prevention (DLP) for Devices	The Information Protection and Control (IPC) solutions, of which Data Loss/Leak Prevention (DLP) is a key component, is needed as a solution that monitors, encrypts, filters, and blocks content contained in email, instant messaging, peer-to-peer file transfer, web postings, and other types of traffic and to help preventing unauthorized access to sensitive information – anytime, anywhere.
		For effective DLP a tight integration or interoperability of different DLP elements is intended, so as to work together to provide a solid data defence. These elements can be categorized as follows:
		• Data discovery, classification and fingerprinting;
		• Encryption;
		• Gateway detection and blocking;
		• Email integration (e.g. SM34); and
		• Device and media management.

SM36	Vulnerability Scanning & Compliancy	A systematic examination of the AIS components and products is needed to determine the adequacy of the security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
SM37	OS security settings and Group Policy Object (GPO)	All Operating Systems shall be hardened using NCIRC recommended configuration settings. For those operating systems for which no recommended configuration exist NCIRC shall be tasked with the development of a recommended configuration before deployment.
SM38	Quality of Service (QoS)	QoS is mainly the expectation or requirement of service regarding a system. More precisely, QoS needs to provide the ability of implementing, monitoring and managing QoS of different priorities to different applications, users or data flows in a network. Most of the time, this SM makes use of the categories defined as follows: • Voice; • Video; • Important_Data; • Routine_Data; and • Best_Effort_Data.
SM39	Pre-production Environment /Test Environment	This environment is needed to ensure that no application, system, etc. goes into production prior to thorough testing, Quality Assurance checking and successful evaluation during pre-production. In other words, the pre-production environment is used for the functional final testing before the actual deployment into production, irrespective of whether hardware or software modifications are involved. Complex enterprise applications may require specific tests performed within a test environment, either physically or logically separated, from the production environment.

		However, while having a Pre-production Environment is a requirement, a Test Environment may only be implemented if the subsequent operation, support & management allow for it.
SM40	Configuration Management (Database) or CMDB	All configuration items of all technical and/or business services provided by ITM shall be managed centrally and stored in a configuration management data base. ITM shall ensure that the configuration management processes required to maintain the configuration management data base are in place.
SM41	CAPTCHA (and its alternatives)	Not applicable to ITM
SM42	Identity & Access Management (IAM)	This security mechanism is an administrative process coupled with a technological solution. It is needed to identify, validate and provide unambiguous, assured identity credentials for all enterprise human and non-human entities, e.g., services, processes, and devices – through authentication and/or strong authentication mechanisms- and guarantee to different type of users of devices the appropriate authorization to access different security zones.

To this extent, this SM is very much linked and needs to interoperate with SM12 (Strong Authentication). It is required to standardize the identity and access management components as much as possible between the different systems in order to guarantee optimal interoperability.

This service has many interdependencies with other services/security mechanisms. Major components of the IAM are as follows: User Provisioning, Access Management, Delegated Administration, Self-registration and Self-service, Workflow, Auditing and Logging and Reporting, Authentication, Integration. |
| SM43 | Management of the Security Mechanisms | All ITM security mechanisms shall be integrated with the NCIRC FOC infrastructure wherever possible. |

SM44	Time Synchronisation (e.g., Network Time Protocol (NTP))	All the clocks used by the ITM infrastructure shall be synchronized. Ideally this synchronization shall be performed using an internal time server so that no external connections are required.
SM45	Storage Areas security	This SM includes any storage areas such as Logical Unit Number (LUN) Management for Storage Area Network (SAN) security, and others. Software management tool for LUN is essential to enabled efficient LUN creation, management, reporting and auditing.
SM46	Data Scramble	This security mechanism uses an application intuitive scrambling technology that masks critical data sets and so ensures that the protection and referential integrity of sensitive data in production, non-production and end-point environments remains usable and intact whether protecting structured or unstructured data. The security mechanism needs to maintain data integrity without going directly against the database when updating and concealing the sensitive information.
SM47	Data Safeguarding (e.g. DAM, FSAM)	Data Activity Monitoring (DAM) and File Server Activity Monitoring (FSAM) using the Data Safeguarding mechanism. This security mechanism needs to look after the critical data infrastructure, efficiently and securely managing the actions.
SM48	Password Management	It is required to enforce the password policy, thus ensuring that users are choosing strong passwords as defined by the primary directive on CIS Security. The mechanism needs to check every new password for compliance with the policy. Passwords that are not compliant are to be rejected and a password policy message should be displayed that helps users choose compliant passwords. This SM is also supporting SM37.
SM49	Identity & Authentication, Access Control (IAAC)	ITM shall integrate the Identity Management solutions provided as NATO PFE

SM50	Protection against (Distributed) Denial-of-Service ((D)DoS)	Web servers shall be protected against DoS attacks as described on the directive for the security of websites (which is currently under development).
SM51	Physical security	Physical security measures shall be implemented in accordance with [AC/35-D/2001-REV2 from 7 January 2008].
SM52	Personnel security	Personnel security measures shall be implemented in accordance with [AC/35-D/2000-REV7 from 7 January 2013]
SM53	Environmental security	Environmental security measures shall be implemented in accordance with TIA-942 "Telecommunications Infrastructure Standards for Datacentres".
SM54	Emission security	TEMPEST Zoning and the other security measures shall be implemented in accordance with: - AC/322-D(2007)0036 - INFOSEC Technical & Implementation Directive on Emission Security", from 10July2007 (NR); - SDIP-27/1 "NATO Tempest Requirements and Evaluation Procedures"; - SDIP-28/1 "NATO Zoning Procedures"; and - SDIP-29/1 "Facility Design Criteria and Installation of Equipment for the Processing of Classified Information".
SM55	Data processing	The security of data processing (aka data manipulation) is required when data entry and processing, as performed by the applications, requires an active and automated control to ensure that the data (or code) is handled/processed in accordance with the rule sets as established by the business, and therefore consistent with the business objectives.
SM56	Data Diode	This refers to a Boundary Protection Component (or BPC) that ensures that information can only flow in a single direction across a network interconnection point. This mechanism is typically required for data transfer from a low to a high security domain (when there is a

		difference in sensitivity or classification between the two networks (e.g., from NR to NS)), and/or when there is a greater threat from the other CIS (e.g. from a public network to NS). Implementation needs to adhere to the Data-Diode security accreditation package, which also contains the configuration guidance as endorsed by the NSAB.

Table 54: Security Mechanisms that shall be provided by ITM

INVITATION FOR BID

IFB-CO-14176-SOA-IDM

PROVIDE SERVICE ORIENTED ARCHITECTURE AND IDENTITY MANAGEMENT PLATFORM

NATO Communications and Information Agency

BOOK II – PART IV Annex A

SYSTEM REQUIREMENT STATEMENT (SRS)

Table of Contents

Figures

Tables

1 Introduction

1.1 Purpose

This System Requirement Specification (SRS) describes all functional and non-functional requirements, design constraints and other factors necessary to provide a comprehensive description of the system to be delivered under the SOA & IdM Platform project, hereinafter referred to as 'the Platform'.

1.2 Scope

This SRS supports the NATO Capability Package (CP) 9C0150 Core Information Services for Command and Control that identifies the *Capability* and resources required to provide information services that need to be accessible to all *Users,* applications and services on the supported domains, regardless of *Community of Interest* (COI). Core information services provide the common foundation and standard interfaces to support inter-domain *Interoperability* within NATO and with NATO partner nations. The Capability Package reflects the minimum requirement to support the command and control of all military functions.

The basic SRS as contained in the requirement management tool (DOORS) contains the currently identified set of requirements for the Platform covered by:

a. Project 2014/0IS03094 ("Provide Web Enabling Services"), which covers the design of an initial enterprise-level core data management service *Capability* to the NATO Command Structure that is consistent with the requirements of Deployable Computer Information System (DCIS), development and implementation across the enterprise of the initial *Capability* to provide service discovery, information assurance, messaging, *Mediation*, *Orchestration*, *Choreography*, *Metadata Repository*, information access and information discovery web services on the *Operational Network* (ON) and the *Protected Business Network* (PBN);

b. Project 2014/0IS03099 ("Upgrade NATO Enterprise Directory Services"), which covers the upgrade and implementation of NATO enterprise directory services to provide SOA compliant enterprise-wide directory services that support *Identity Management* (through integration with human resource data management services) and extend services and interfaces to include *Role-Based Access Control* on the ON and PBN domains.

The two projects are closely interdependent at the technical level, with shared services and common interfaces, and have therefore been combined under a single contract, and any distinction between the projects is not relevant for the contract. This allows *Functional Services* (FS) and other systems/projects to benefit from a uniform service-oriented functional platform supported by Enterprise-wide *Identity Management* services. As a result, the name of the project addressed by this SRS is "SOA and *Identity Management* Platform".

1.3 Acronyms and Abbreviations

The acronyms and abbreviations used in this SRS are defined in Annex D of the Statement of Work.

1.4 Definitions

The definitions used in this SRS are defined in Annex E of the Statement of Work, and will be indicated in *italics* throughout this document.

1.5 Overview

This SRS comprises 4 sections:

- Section 1 provides an introduction and the use of this document.

- Section 2 provides an overall description of the Platform Services, *Roles* involved and project constraints.

- Sections 3 providing the Functional Requirements and section 4 providing the Non-Functional Requirements, together comprising the required functionality and their associated requirement attributes.

The following subjects are described in separate Annexes.

- Statement of Work Annex D, Abbreviations

- Statement of Work Annex E, Glossary with definitions for common terms used in this SRS

- Statement of Work Annex F, References (including standards and specifications)

During the system requirements analysis and design (Design Stage), further elaboration of Platform Information Objects will be required, and, almost certainly, additional Information Objects, products, attributes and relationships will be identified to implement the requirements.

1.6 SRS Conventions

The system requirements, defined in this document, are individually identified by a unique number which shall be used at all times as the specific reference for each.

No meaning is associated with the order of serial numbering. There could be gaps in numbering and requirement identifiers in a group do not have to be sequential.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].

Words in *italics* indicate terms referenced in Annex E of the SoW.

1.7 Applicable References

The abbreviated document titles given in square brackets, […], are used to refer to documents in the reference list (Annex F of the Statement of Work). These documents are meant to provide guidance and background information.

1.8 Applicable Standards and Specifications

The Platform supports agreed NATO standards and other open standards and specifications identified in the NATO Interoperability Standards and Profiles (NISP) [NAC ADatP-34(G)-REV1, 2013] and SOA Baseline Profile [NAC AC/322-N(2011)0205, 2011] whenever feasible. This especially applies to providing *Interoperability* with external federated systems (e.g. National systems, NATO industries, partner Nations).

Key service interfaces necessary to achieve *Interoperability* within a *Federation* of systems are further defined by detailed *Service Interface Profiles* (SIP).

External systems built according to SOA principles use Platform-provided services via interfaces described by SIPs. Older, non-SOA systems are integrated with the Platform using existing *Commercial off-the Shelf* (COTS) connectors based on e-mail, database access, and file transfer mechanisms.

Some given references are for draft versions of documents (e.g., "Edition 4 Ratification Draft"). Where this is done, the *Contractor* is obliged to use the draft document as given with the expectation that it will be ratified without any substantial change.

Changes in standards/specifications as part of a normal technological maintenance path (e.g., Windows Vista to Windows 7, .NET Framework 3.5 to.NET Framework 4.0) should not be considered to be major.

Requirement ID	SRS-1960
Verification method	Inspection
Requirement	The Platform SHALL be compliant with [NAC ADatP-34(G)-REV1, 2013] base standards and profiles for information exchange

Requirement ID	SRS-1959
Verification method	Inspection
Requirement	The Platform SHALL be compliant with [NAC ADatP-34(G)-REV1, 2013] base standards and profiles for XML implementation.

1.8.1 Technical Standards

Requirement ID	SRS-1962
Verification method	Inspection
Requirement	The Platform SHALL comply with the standards referenced in section 2.1 "Technical Standards" in Annex F of the Statement of Work.

Requirement ID	SRS-4231
Verification method	Inspection
Requirement	Any variations from the Technical Standards SHALL be approved by the *Purchaser*.

1.8.2 Quality Standards

Requirement ID	SRS-2000
Verification method	Inspection
Requirement	The Platform SHALL comply with the standards referenced in section 2.2 "Quality Standards" in Annex F of the Statement of Work.

Requirement ID	SRS-4232
Verification method	Inspection
Requirement	Any variations from the Quality Standards SHALL be approved by the *Purchaser*.

1.8.3 Programming Standards

Requirement ID	SRS-2002
Verification method	Analysis
Requirement	The Platform SHALL comply with the standards referenced in section 2.3 "Programming Standards" in Annex F of the Statement of Work.

Requirement ID	SRS-4233
Verification method	Analysis
Requirement	Any variations from the Programming Standards SHALL be approved by the *Purchaser*.

1.9 Verification Methods

The requirements in this SRS will be verified through qualification, herein defined as an endorsement with a guarantee and supporting documentation that the item being qualified satisfies the specified requirement(s). The different verification methods applicable to the requirements herein are described in the following paragraphs.

Note: In some cases, more than one verification method might be required in order to verify fulfilment of a requirement.

1.9.1 Inspection

Inspection is the visual examination of an item and associated descriptive documentation.

For Non-Developmental Items (NDI), Modified NDI and Developmental Items software inspection is used to determine if physical quantity lists are met.

1.9.2 Analysis

Analysis is the review and processing of design products (documentation, drawings, presentations, etc.) or accumulated data obtained from other qualification methods, such as manufacturer's tests of a product to be mass-produced, to verify that the system/*Component* design meets required design criteria.

1.9.3 Testing

Testing is the operation of the system, or a part of the system, under controlled and specified conditions, generally using instrumentation, other special test equipment or specific test patterns to collect data for later analysis. This verification method usually requires recorded results to verify that the requirements have been satisfied.

2 General System Description

2.1 Product Perspective

2.1.1.1 Platform Principles

The Platform is architected with a set of guiding principles which provide the foundation for its implementation. They are as follows:

a. Service Orientation: In order to support the implementation of SOA within NATO systems, the Platform itself is built using the principles of SOA. This means that, for the majority of functions, there are both a Service *Component*, running as a separate, loosely-coupled instance and a compiled *Component* that can be readily incorporated into applications. The services are all based on clearly defined, open standards, so that they can, if required, be used independently of the compiled *Components*.

b. Runtime Environment: The Platform does not constrain the development of FS in terms of programming language or runtime environment. This means that the building blocks need to be available in most common development environments, such as Java and .Net. The interfaces that are offered by the supported *Components* are standardised across development environments, both by the *Components* and the supporting services.

c. Enterprise Application Integration (EAI): NATO has already made considerable investment into its CIS *Capabilities*. In order to service-enable these systems, the Platform enables discovery and disclosure of information contained within the system, thus allowing sharing of data and business processes among any connected application or data source in the NATO enterprise.

d. Microservices: At the other end of the spectrum is the concept of "microservices" – very small, extremely focused pieces of software performing a distinct function. Microservices tend to be very lightweight and self-contained, with their own internal data management functionality, which makes them very easy to deploy and distribute. As a logical refinement of the SOA approach, their characteristics make microservices popular for usage both in mobile applications as well as in highly componentised larger-scale applications where there is a need to de-centralise services to the maximum. The Platform will provide a framework that will support the implementation of a microservices architecture where required.

e. Service *Composition*: In order to rapidly scale and build new services, the Platform provides the ability to orchestrate services into compound services, or use message routing to control information flow. By defining business processes, services can be reused and integrated into different contexts, or rearranged to deliver a more efficient operating environment.

f. *Multi-tenancy*: There will be multiple CoIs and applications ("tenants") using the Platform, and these need to be isolated from each other, while at the same time being able to easily share information. The execution and memory storage are separated, granting the isolation between FSs, avoiding any adverse impact on *Performance* and security.

g. *Performance* and *Scalability*: The Platform is integrated with NATO's *Information as a Service* (IaaS) so that it can be rapidly scaled to cope with new operating environments or operational conditions. This means that it is able to scale up (i.e. increase the level of resources available to a set of machines) or scale out (i.e. increase the number of machines providing the service). This process of scaling is automated, within agreed parameters, so that additional *Capacity* can be dynamically provisioned at runtime or from remote management centres.

h. Event-driven Architecture: As well as supporting messaging in a SOA environment, the Platform supports event-driven communication. In this case, the control and routing of information is in response to events or changes of state. The software-defined process reacts only when certain events have occurred, and these may trigger additional processes or activities.

i. Common Security: The Platform offers NATO information systems – including current and new FSs and business applications – a set of common *Identity and Access Management* (IAM) services, with common and consistent processes and *Capabilities* across the enterprise.

j. Federated Integration: Although the scope of delivery for the Platform is the NATO enterprise only, for many of the services, there is a *Federation* aspect. This means that services are able to provide and consume information from outside of the NATO domain, with authorised partners. The services that can be federated must comply with agreed, open interfaces that can be shared with and agreed by a range of partners using potentially heterogeneous systems (i.e. different technologies than on the Platform).

k. Documentation and Guidance: Individual FSs need guidance and support in preparing their systems for incorporation into the Platform. This takes the form of documentation (such as *Service Interface Profiles* and Interface Control Documents), toolsets (for verifying interface implementations) and manpower to guide them through the full lifecycle of development and deployment.

2.1.2 Scope

The Platform services are organised into six categories, as shown in Figure 7.

The six categories of Platform services are:

- Integration Services

- Information Services

- Registry and Repository Services

- Platform Hosting Services

- Service Management and Control Services

- *Identity* and Security Services

2.1.3 Intended Users/Roles

2.1.3.1 Key Definitions

User: Refers to an *Entity* that may make use of a resource, e.g., system, equipment, terminal, process, application, or corporate network.

Role: Defined by a set of properties or *Attributes* that describe the capabilities or the functions performed by an *Entity*.

Each *User* of the Platform may be assigned access rights for a given functionality based on its *Role* and/or *Attributes* (such as the organisation of the *User*) and the permissions within that *Role* and/or associated with those *Attributes*.

An **Authorised User** is an *Entity* that has access rights for a piece of Platform functionality at "run time". This functionality may include viewing, creating, collaborating and updating/maintaining information.

Typical Platform *Users* interact with *User* facing services and applications, but not directly with the Platform services themselves, which are largely transparent to them. However, the permissions for Platform services are configured for special *Authorised Users* (in a *Role* known as an **Administrator**) to access and manage certain of the Platform's services directly.

There are several types of Administrators in the NATO context, to include:

a. **Platform Organisational Node Administrator**: a person having Access Rights for the Platform Organisational Node Administrator Functionality. This functionality includes managing the Platform Accounts, Access Rights, defining the Application or Information Portal Structure, and defining Information Exchange Contracts.

Platform Organisational Node Administrators are generally members of the staff responsible for *User* management, domain value management and system configuration for that particular Platform organisational node.

Platform Organisational Node Administrators are also responsible for adapting and localising production workflow sequences to guide and control processes.

Platform Organisational Node Administrators can assign User permissions on types of information objects (e.g., Overlay) and functions (e.g., Read, Create, Modify, Delete) on those objects for that particular organisational node. To simplify administration, a Role may be specified from more basic Roles and permission sets.

Platform Organisational Node Administrators will have the Capability to perform content management functions, including data cleansing and archiving.

b. **Platform Enterprise Administrator**: a person having Access Rights for the Platform Enterprise Administrator Functionality. This functionality includes maintaining the enterprise-wide configuration (e.g., domain values).

Platform Enterprise Administrators are responsible for overall management and administration of the system, including both technical and procedural aspects. In general, Platform Enterprise Administrators are identified for each mission/domain.

Procedural and administrative responsibilities of the Platform Enterprise Administrators include the creation, documentation and enforcement of operating policies and procedures associated with functional system configuration; domain management; User access and Privilege Management; data stewardship; workflow management; and identification and resolution of functional issues.

Platform Enterprise Administrators are responsible for overseeing development and maintenance of Standard Operating Procedures (SOPs) and coordination with Platform Organisational Node Administrators.

The technical responsibilities of Platform Enterprise Administrators include enterprise domain management; collection of Performance and accounting data; and ensuring that security mechanisms are working.

Platform Enterprise Administrators are also responsible for identifying standard production workflow sequences.

c. **Platform System Administrator**: a person having Access Rights for the Platform System Administrator Functionality. This functionality includes the functionality for the Platform System Administration and the Platform System Maintenance. The Platform System Administration Functionality includes deploying, configuring and updating the Platform.

Platform System Administrators are generally NATO Communications and Information Agency (NCI Agency) personnel or other local CIS support personnel responsible for system and network technical issues, and for ensuring the proper configuration, network connectivity and Recoverability of the system.

Responsibilities of the Platform System Administrators include network and domain management; back-up and recovery of file systems and databases; and administration of the Platform applications and servers.

Platform System administrators are responsible for maintaining Windows User groups and adding new Users to the Windows domain, and (re)installing the system as required.

In addition, others types of Users will interact with the Platform:

d. **Solution Architects and Developers** use the Platform services at "design time", developing their systems to interact with these services and benefiting from their functionality and well-understood architectural patterns.

The ability to leverage existing core SOA and IAM services – as well as previously developed COI-enabling and COI-specific services – means that new User Applications and Services are quicker and more cost-effective to develop and integrate within NATO CIS. Increased access to distributed data sources means that a more comprehensive and integrated view can be presented to Users, while maximising the return on investment of NATO systems.

e. **External Partners** benefit from *Federation* capabilities offered by the SOA & IdM Platform services.

The Platform provides a consistent way to integrate federated systems, so that information extends across NATO and partner networks (NATO Enterprise [AC/322-D(2015)0014-REV3, 2015] , Alliance Enterprise and Coalition Enterprise), when used in conjunction with existing cross-domain solutions. It provides services that can be used to deliver a wide range of heterogeneous data types to multiple partners, both military and Civil Military Cooperation (CIMIC).

This provides support for achieving information superiority ("Responsibility to Share"), while simultaneously helping to ensure that information is released only to those with a "Need to Know".

f. **SOA Services** take advantage of the common web-based application platform provided by the Platform Hosting Services to support the development and deployment of services.
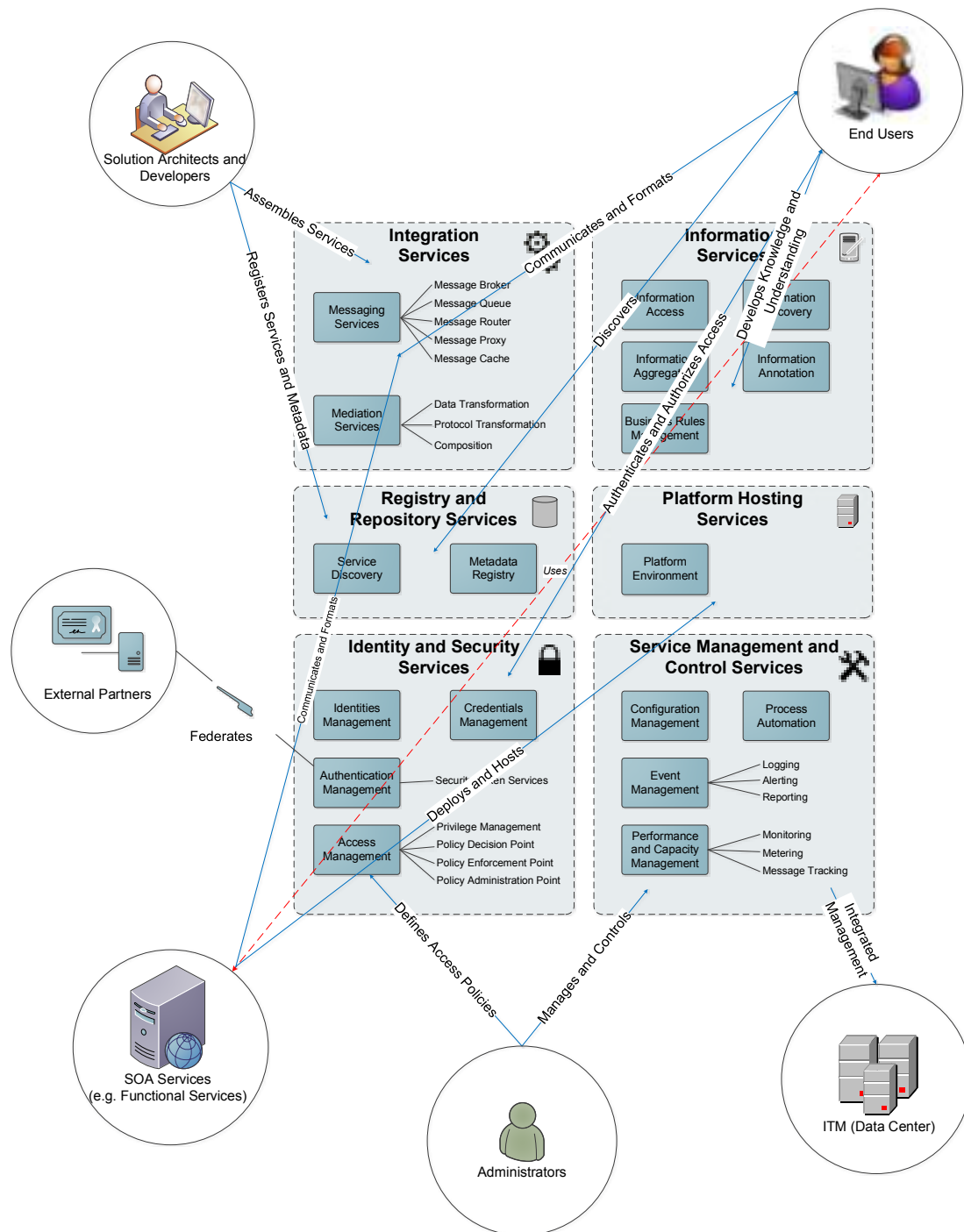
Figure 1 - Organizational Relationships

2.1.3.2 Solution/Development Constraints

The implementation of physical *Components* on special purpose networks (exercises/training/mission) is outside the scope of this project.

Implementation of comprehensive cross domain services are outside of the scope of this project.

Implementation of *Components* and/or configuration of connections in Nations, if required for interfacing purposes, are out of scope of this project.

2.1.4 Operating Environment

2.1.4.1 Operational Network and Protected Business Network Connectivity

The Platform services will be installed for two major networks (as defined in [SHAPE 3050/SH/CCD CIS/CAR/335/13-301388, 2013]):

a. The PBN provides IT services at the NU and NR classification level in support of administrative business processes, appropriate operational processes and those processes requiring interaction over the Internet. Within the PBN infrastructure there are also security domains that are providing NATO UNCLASSIFED information services like extranet applications or VOIP/VTC services and PUBLIC information services like internet access via WiFi;

b. The ON provides IT services at NS level in direct support of war fighting processes, processes requiring higher levels of assurance and processes of military and political communications.

As presented in Figure 2, both networks will be implemented with the same logical *Components*, but with separated physical *Components*. The two physical infrastructures will be connected to support required cross-domain information exchanges compliant with, and within the limits of, applicable NATO security policy.
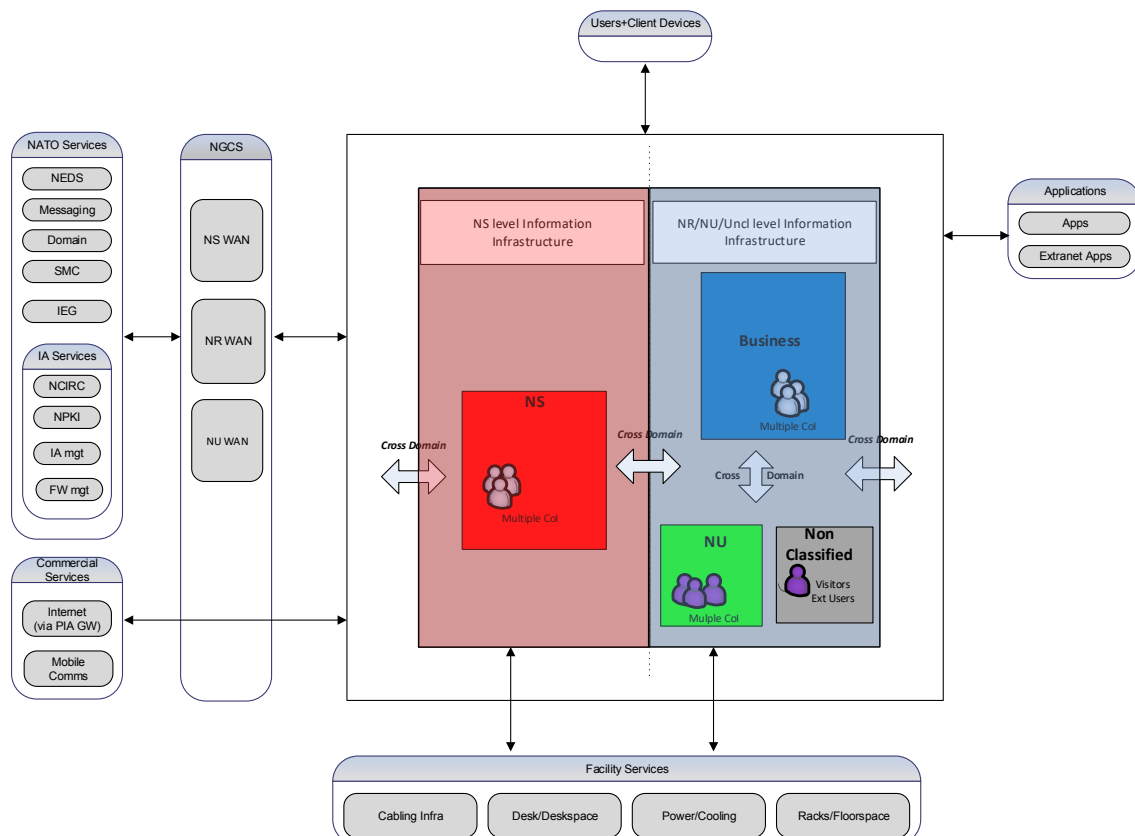
Figure 2 - ON and PBN interconnectivity within a computing facility

2.1.4.1.1 Nodes

The Platform services will be installed on computing nodes provided by the *IT Modernisation* (ITM) as depicted in Figure 3 and 4 below:

Data Centre **Nodes** – The ITM project plans to deliver *Data Centres* to serve as Main Computing Facilities (MCF) The MCFs will provide the complete suite of Platform services.

Enhanced Nodes provide a minimal set of selected Platform services in situations where agreed service levels cannot be met when services are provided from the MCFs. It is anticipated that there will be different service requirements for different types of *Enhanced Nodes*.

Standard Nodes will be receiving all their services from the MCFs. No Platform services are installed there.
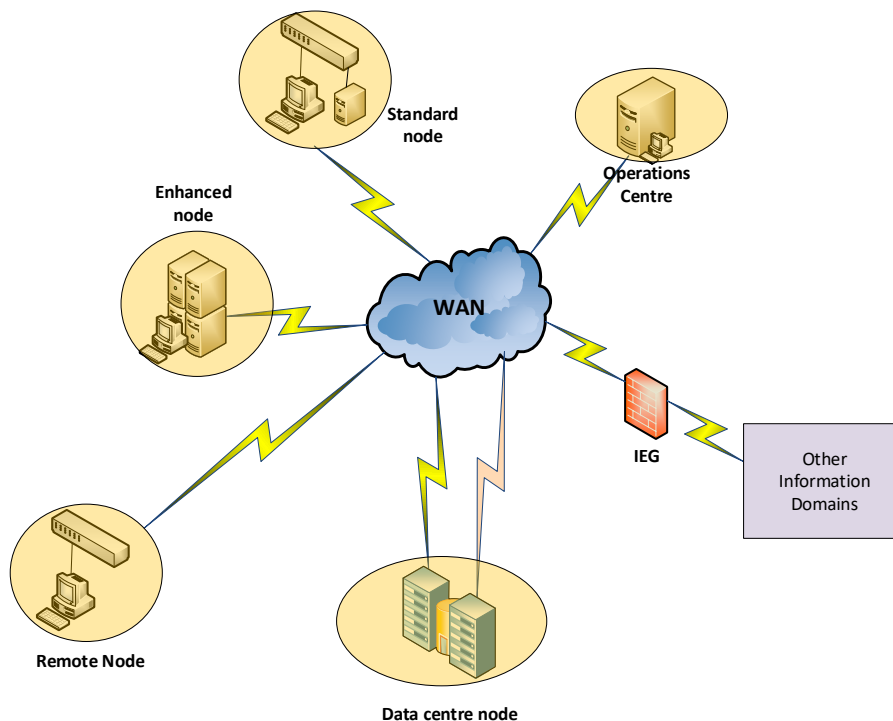
Figure 3 - ON ITM WAN-LAN topology
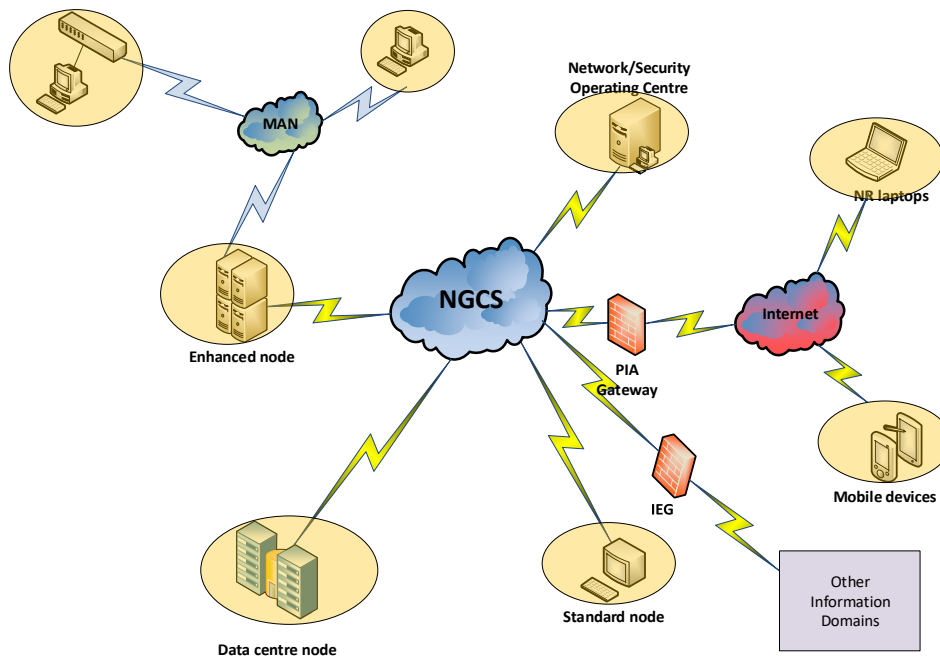
Figure 4 - PBN ITM WAN-LAN topology

An **Integration and test facility**, as for example in the Programme Management and Integration Capability (PMIC) environments, will be provided to enable other projects already at their software development phase consistent integration with the Platform services.

A **Reference facility** maintained by the NCI Agency will be used to ensure proper change management and evaluation before installation of NATO information systems integrated with the Platform into operational environment. This will not be on the main ON and PBN networks themselves, but are expected to be located on equipment of the same specification in the *Data Centres*.

All services are required to be able to run on the *Deployable CIS* platform.

The services that are actually provisioned on a *Deployable CIS* node depend on the nature of the mission involved. It is anticipated that a single *Deployable CIS* node varies between requiring the full suite of Platform services (comparable to a *Data Centre*), selected Platform Services (comparable to an *Enhanced Node*) or none (a *Standard Node*).

2.1.4.2 Service Provision

Platform services will be used by other projects and systems. To enable this, early integration and compatibility testing is necessary. Therefore, integration testing will be conducted on the PMIC Test Facility and preparation for deployment (including Change Management and Change Evaluation) will be conducted within the Reference Facility.

The Platform will be centralised as much as possible, mostly at the *Data Centres*, and selected *Components* at the *Enhanced Nodes* as delivered by the ITM Project.

The *Enhanced* and *Standard Nodes* will receive most of their services from the *Data Centre* Nodes. In exceptional cases, services with special requirements (e.g., regarding *Availability* or *Performance*) that cannot be met when provided from the *Data Centre* Node will be provided locally by on-site installation, but typically still will be administered remotely.

2.1.4.3 Interfaces

The following diagram describes the interfaces between the different nodes and the different system *Components*.
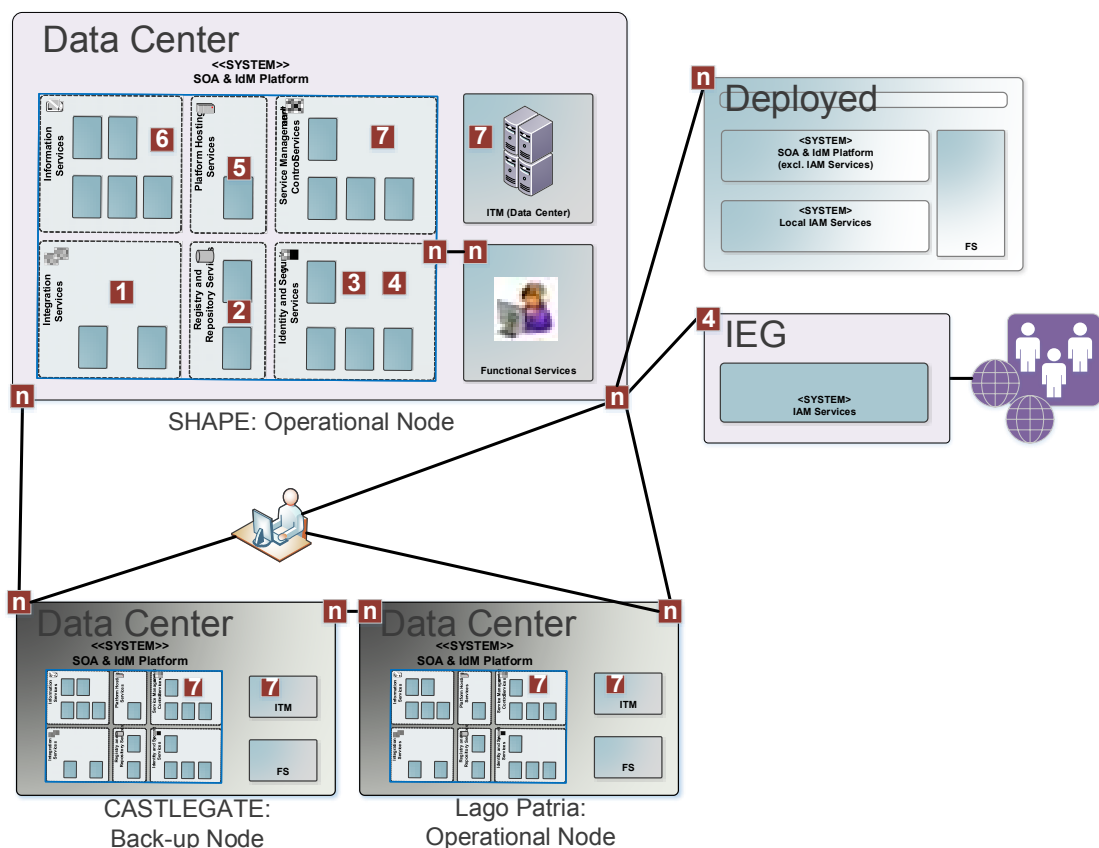
Figure 5 - Internal Interfaces

The interfaces represent:

1 - Hypertext Mark-up Language (HTTP)/Simple Object Access Protocol (SOAP)

2 - HTTP/SOAP/Universal Description, Discovery and Integration (UDDI)

3 - HTTP/SOAP/WS-Security

4 – Lightweight Directory Access Protocol (LDAP) or Directory Information Shadowing Protocol (DISP)

5 - HTTP

6 - HTTP/SOAP/SPARQL Protocol and Resource Description Framework (RDF) Query Language (SPARQL)

7 - Service Management and Control information

N - Any of the above, or a combination of.

2.1.4.4 External Interfaces

The Platform is able to provide its services and interfaces to external systems.

The **Integration Services** enable information sharing between heterogeneous and decoupled systems, such as FS.

Different **Authoritative *Identity* Data Sources** exchange information with the Platform's **NEDS** *Component*. The NATO Public Key Infrastructure (NPKI) is one of these sources, but is also acting in another role in underpinning *Trust* for the **Security Services**.

External information sources provide the **Information Services** access to data that can be integrated and exposed in a single, standards-based format together with descriptive metadata to aid the understanding of the information, and enable automated processing.

Several services can also be made available to external partners, provided that cross-domain solutions are in place. These are among others the **Registry and Repository**, the **NEDS** directory via its **Allied Replication Hub**, **Messaging Services**, and *Security Token Service*.

The following diagram shows the interfaces to external systems, also indicating in which security domain these are located.
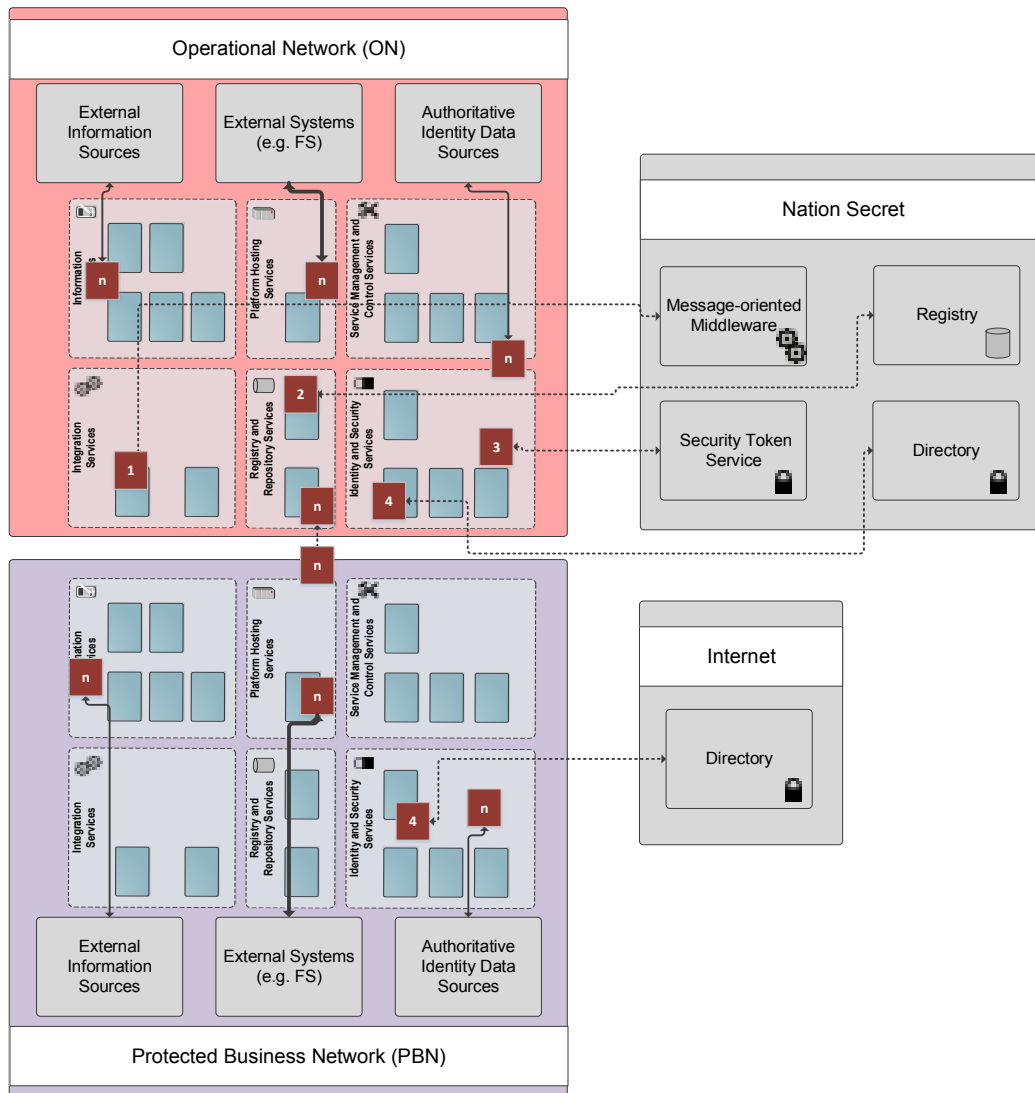
Figure 6 - External Interfaces

Specific information is pushed between Platform elements (e.g. NEDS) from PBN to ON through data diodes that are already available NATO networks.

2.2 Assumptions

It is assumed that the following projects will have delivered, or at least are available for integration to the Platform project:

   a. ITM

   b. NPKI

   c. Information Exchange Gateway (IEG) or other cross-domain services for *Federation* capabilities

It is assumed that future NATO FSs and other information systems integrated by the Platform will be centralised in the *Data Centres* provided by the ITM project.

In exceptional cases, systems not installed in the *Data Centres* – such as via *Deployable CIS* – will have sufficient network connectivity (bandwidth and latency) to integrate through the Platform. The Platform will have sufficient robustness (e.g. guaranteed message delivery) to deal with the potential intermittent connectivity and latency issues that are part of this environment.

It is assumed that in parallel with the implementation of the Platform project, the NCI Agency staff transformation will take place which will provide the competencies and skill sets, at the locations needed, to support the new Platform.

The modifications of any other systems (beyond those covered by the pilots) are out of scope of the implementation of this Platform.

3 Functional Requirements

This section provides technical and functional requirements for the services that comprise the Platform.

As already introduced in the Product Perspective, the Platform services are organised into six categories, as shown in the figure below.
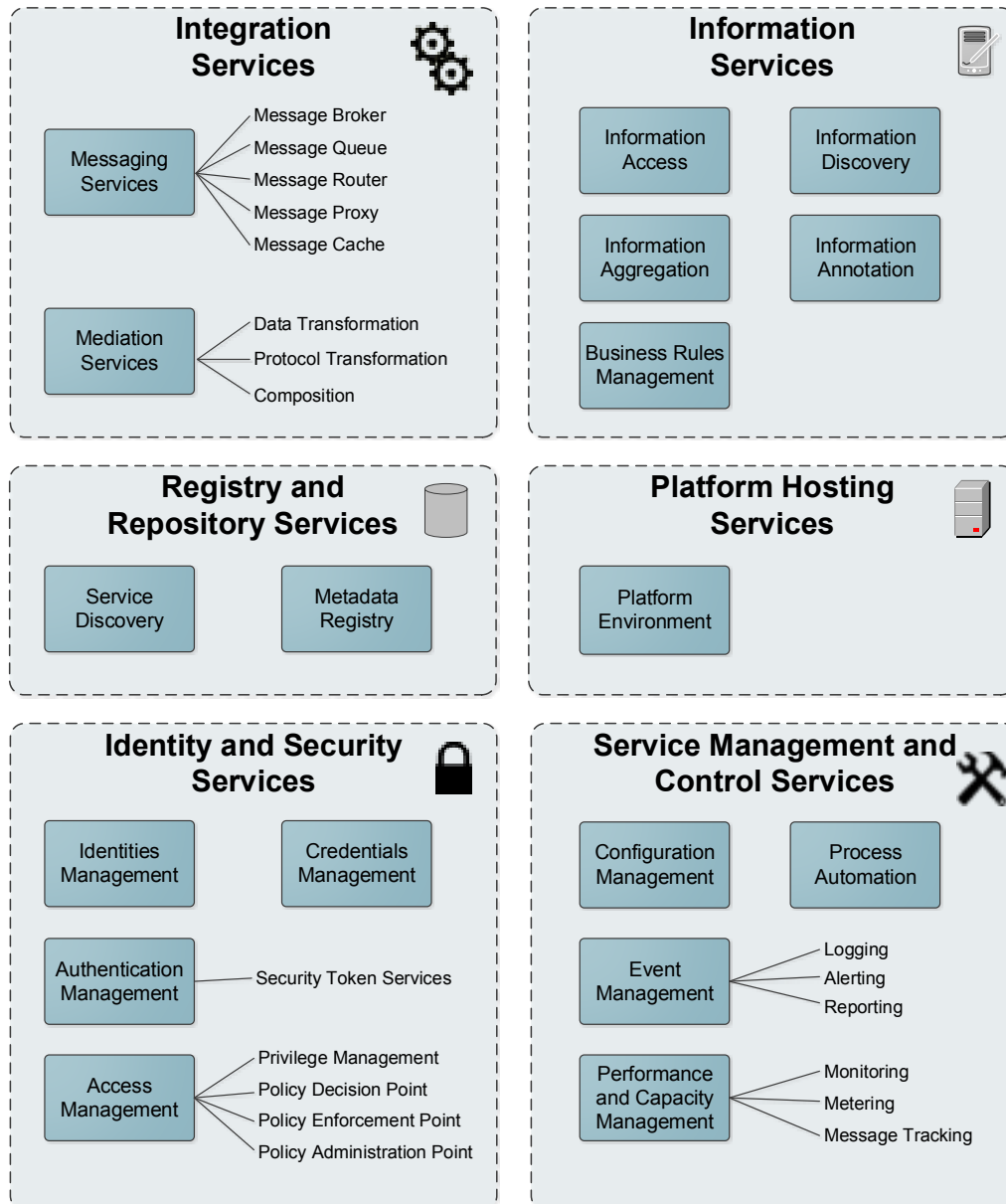
Figure 7 - Platform Services

Requirement ID	SRS-280
Verification method	Testing
Requirement	The Platform SHALL support *Multi-tenancy* in terms of isolation of the software *Components* (services, applications) by providing Middleware services for each individual tenant (*Users*).

3.1 Integration Services

One of the primary functions of the Platform is to provide *Interoperability* between systems, so that data from one system can be easily and efficiently distributed with others regardless of the data payload (images, text, video etc.).

The Integration Services provide the key information exchange *Capabilities* of the Platform. They provide the connections between different service providers and consumers in a transparent, easy to use and reliable way (Messaging). They are data agnostic, though can be configured to support different outcomes according to values or structures within the data, including prioritisation of critical messages (Routing).. Likewise, they can perform *Mediation* between providers and consumers, in terms of data structures or protocols, seamlessly allowing the exchange of data between diverse heterogeneous systems (*Mediation*).

Integration Services support both simple and complex modelling of the interactions, leveraging the use of Messaging, Routing, and *Mediation* to produce compound services that are common combinations of other services. These can be further combined to provide greater and more powerful *Capabilities* in more rapid and agile ways. This includes the ability to incorporate existing proprietary services into the information ecosystem by offering a standard interface that can be easily consumed (Proxying).

In addition, the consumers of services are not necessarily known when the service is created – there are always unanticipated *Users*. This means that the Platform needs to be able to provide easy to implement *Mediation*, both between data formats (such as Friendly Force Information (FFI) to Keyhole Markup Language (KML)) and protocols (File Transfer Protocol (FTP) to Hypertext Transfer Protocol (HTTP)). The mapping between the various *Data Elements* is reusable, so the *Mediation* services are able to access the Registry directly to retrieve the correct *Stylesheets*. Some *Mediations* are delivered as part of the platform, whilst tools are provided to enable different CoIs to deliver their own *Mediations* as part of FS integration.

The Integration Services thus provide the *Capability* to deliver messages between endpoints and to mediate - which includes transformation, routing, and protocol conversion - in order to successfully transport service requests from the service requester to the correct service provider (and vice versa). It can be further decomposed into Messaging Services and *Mediation* Services.

Requirement ID	SRS-293
Verification method	Analysis
Requirement	The Platform SHALL implement mechanisms that enable the provision of new services from existing services by: • composing them • providing proxies • by using data and protocol transformations.

Requirement ID	SRS-3180
Verification method	Testing
Requirement	The Platform SHALL enable the processing of messages, including data extraction from the messages.

Requirement ID	SRS-4234
Verification method	Testing
Requirement	The Platform SHALL enable data aggregation from different services and service providers.

Requirement ID	SRS-295
Verification method	Inspection
Requirement	The Platform SHALL provide a library of built-in *Mediation* patterns to be used for the provision of new services including, at least, the patterns officially known as "Enterprise Integration Patterns" [Hohpe and Woolf, 2012]: • Integration Styles • Messaging Systems • Messaging Channels • Message Construction • Simple Messaging • Message Routing • Message Transformation • Composed Messaging • Messaging Endpoints • System Management patterns

Requirement ID	SRS-454
Verification method	Testing
Requirement	The Platform SHALL support multiple Web Service communication protocols to include REST and SOAP.

Requirement ID	SRS-3655
Verification method	Testing
Requirement	The Platform SHALL support data exchange via XML and JSON.

3.1.1 Messaging Infrastructure

Service Oriented Architecture (SOA) is an approach whereby service "consumers" interact with service "providers" to exchange information or perform actions. Simply defined, the consumer is an application, service, or some other type of software module that requires a service; the provider is a service that accepts and executes requests from consumers.

Messaging underpins SOA. The consumer formats a request message and binds the message to a communications channel that the service supports, which is sent over the network to the "end-point" which represents the address at which the service provider can be reached. The service provider executes the service and returns a message to the consumer.

For the Platform, its Messaging Services are able to take a service call and messages to the end-point as well as to correlate a response with the original request; i.e., to fully and comprehensively enable a service consumer to connect/interact with service providers.

Along the way, messages may need to be transformed or enhanced in order to be understood by or be useful for the receiver. These activities are collectively referred to as *Mediation* (see below).

There exist a number of different Messaging "patterns" – referred to as *Message Exchange Patterns* (MEP) – which are standard ways of interacting between service consumers and providers:

In order to support a wide range of scenarios, the Platform needs to support a common set of MEP. These include, but are not limited to, *Request-Response*, *Publish-Subscribe*, Message Streaming and Message Queues. Additional messaging features may also be applied on top of these MEPs, such as Reliable Messaging and Message Routing, based on the contents or metadata of the message.

- The *Request-Response* (or synchronous) MEP is used in case a Consumer requires the Producer to process and return synchronously or asynchronously a response to the Consumer request.
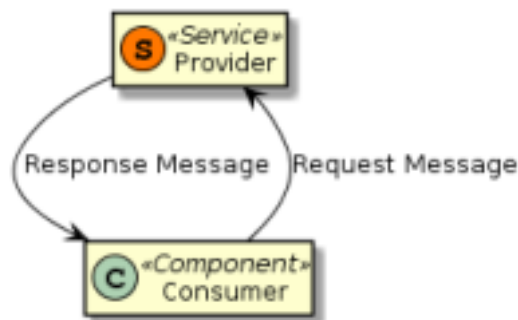
Figure 8 - The *Request-Response Message Exchange Pattern*

- *Publish-Subscribe* (or asynchronous) MEP is a messaging pattern where consumers may be dynamically subscribed to receive *Notifications* "pushed" from producers. A *Subscription* indicates the consumer's interest in one or more message types. Consumers only receive messages that are of interest. The consumers may receive *Notification* messages from producers directly or indirectly via *Notification Brokers*.

  The *Publish-Subscribe* MEP is most suitable when there is a need to immediately and simultaneously notify one or several Messages

Consumers about new messages (data changes) available at the
Message producer.
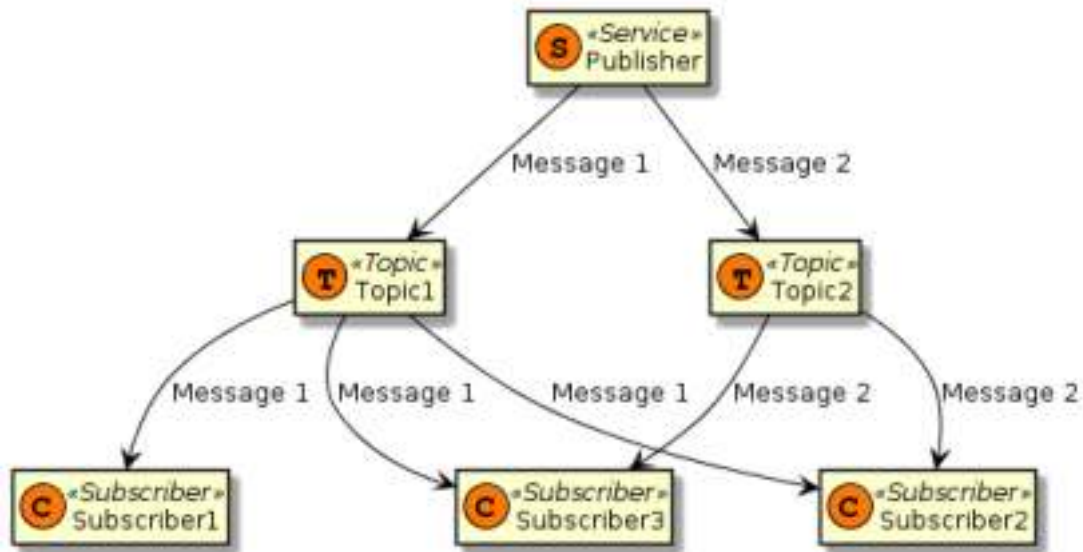
Figure 9 - The *Publish-Subscribe Message Exchange Pattern*

The following are *Components* of the Messaging services:

- The Message Queue is responsible for storing and forwarding
  messages, providing the underlying "plumbing" to transport messages
  between service consumers and providers. It supports both reliable
  transport and guaranteed delivery. Message queuing is a common
  example of a mechanism used to support asynchronous messaging,
  although it can also be used to support all kinds of messaging, as shown
  in the *Composition* diagram below.

Figure 10 - Message Queue *Composition* diagram

- The Message Router is responsible for routing messages between the service consumer/requestor and service provider, including those based on both content-based routing and straight through message passing.
  - It may change the routing of a message, selecting among service providers that support the intent of the requester.
  - Selection criteria for the provider can include content and context of the message as well as knowledge about *Capabilities* of the target candidates and even versioning of service implementation
  - If a message is routed to one provider, which responds with a *Failure*, the message can be re-routed to another provider. In certain circumstances it may be used to route messages without the involvement of the Mediator Services (see section 3.1.2) to realise straight message pass-through.
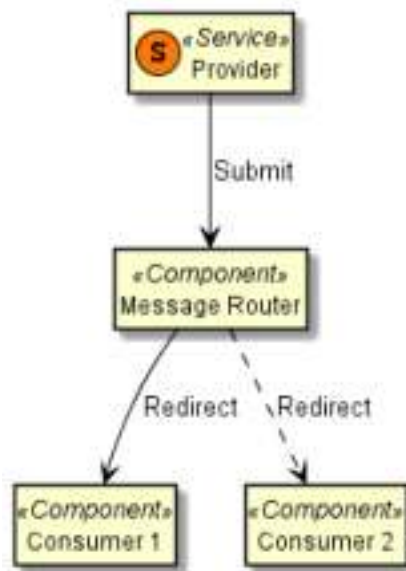
Figure 11 - Message Router *Composition* diagram

- The Message Proxy acts as an intermediary for other services, hiding their actual location (endpoint) and implementation from the service consumers. The proxy services can communicate on a behalf of the underlying service. It can expose a virtual endpoint for the underlying service, giving the consumers a point to call without the need to know exactly where the ultimate service instance resides (or even if the service is in the same domain). They supports the loose coupling and service abstraction principles of the SOA design.
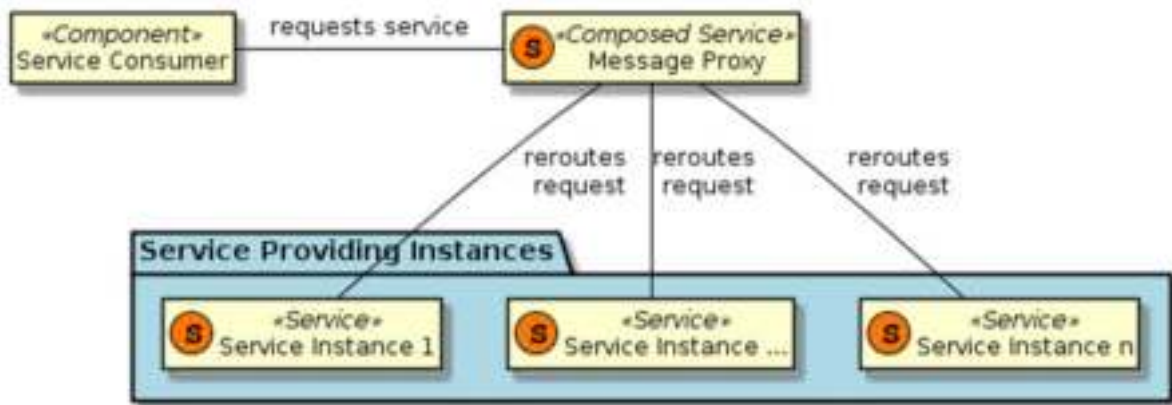
Figure 12 - Message Proxy *Composition* diagram

- The Message Cache provides the functionality to conditionally store messages sent between producers and consumers. The messages can be later served to consumers if they need to resynchronise their state or were unavailable and lost some messages. A related service specific for the *Publish-Subscribe* MEP, the *Notification Cache*, is described under section Annex F in the SoW.
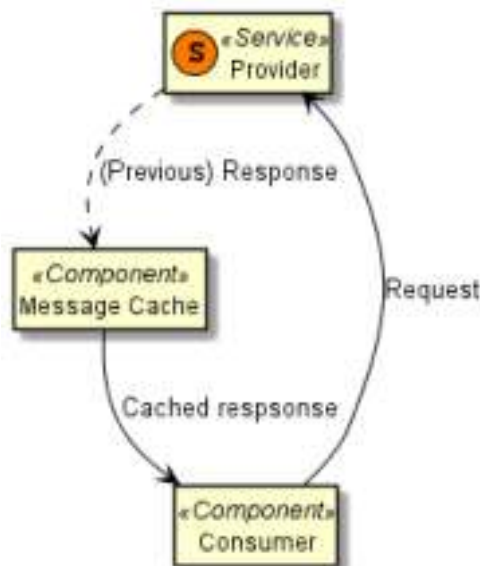
Figure 13 - Message Cache *Composition* diagram

The entire set of Messaging *Components* for the *Request-Response* pattern are shown integrated in the *Composition* diagram below.
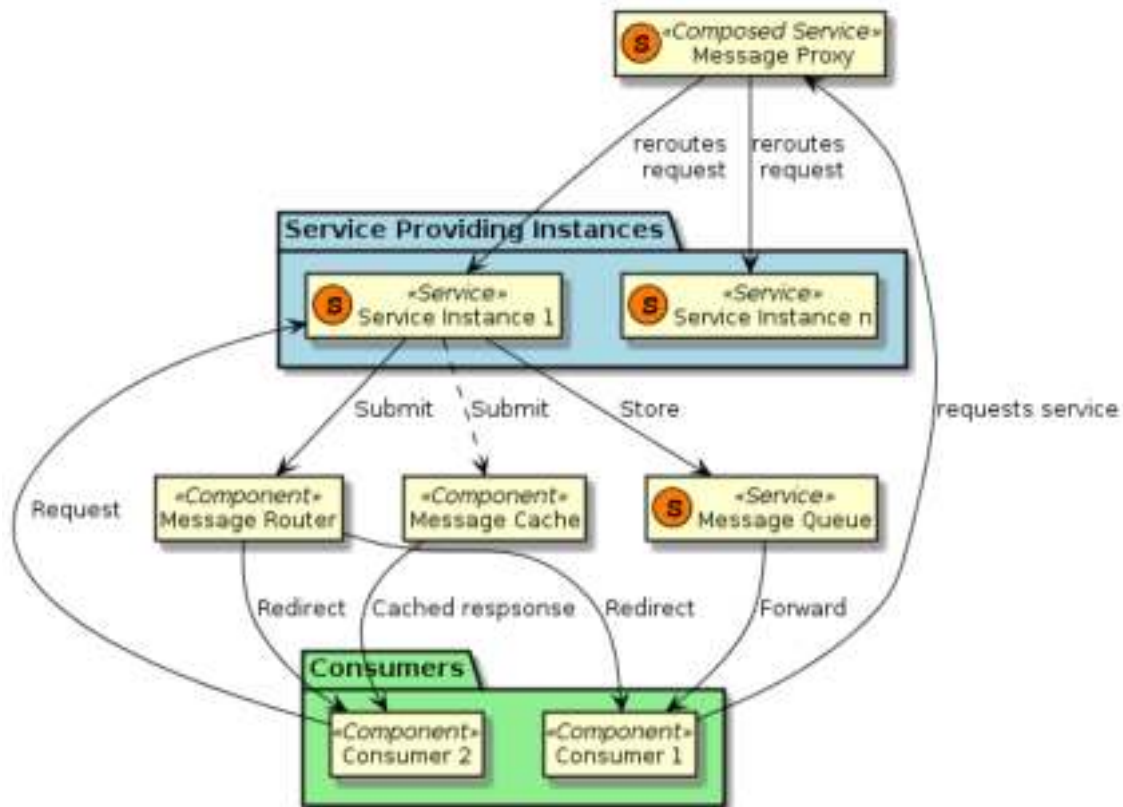
Figure 14 - Messaging Service *Composition* diagram: *Request-Response*

To enable the *Publish-Subscribe* pattern the following architectural *Components* are additionally needed:

- The Message Broker *Component* acts as an intermediary between the *Publishers* and *Consumer*. In this case the *Publisher* does not send *Notifications* directly to the *Consumer*, but sends them to Message Brokering Services for further distribution to registered *Consumers*.

- A *Subscription Manager* provides operations that allow a service requestor to query and manipulate *Subscriptions* that it manages. A *Subscription Manager* is subordinate to the *Notification Producer*/*Notification Broker*, and may be implemented by the *Notification Producer/Notification Broker* service provider. However, it is permitted for it to be implemented by a separate service provider.

- A *Topic Manager* maintains and coordinates the ownership of *Topics*.

- A *Notification Cache* service offers optional functionality for Publish-Subscribe-based messaging. Extending the functionality of a classic WS-Notification *Publish-Subscribe* scenario (see [OASIS WSN, 2006]), the *Notification Cache* service covers the requirement to cache *Notification* messages, and to provide retrospective access to them.

The *Composition* diagram below illustrates how the *Components* work together to enable *Publish-Subscribe* functionality.
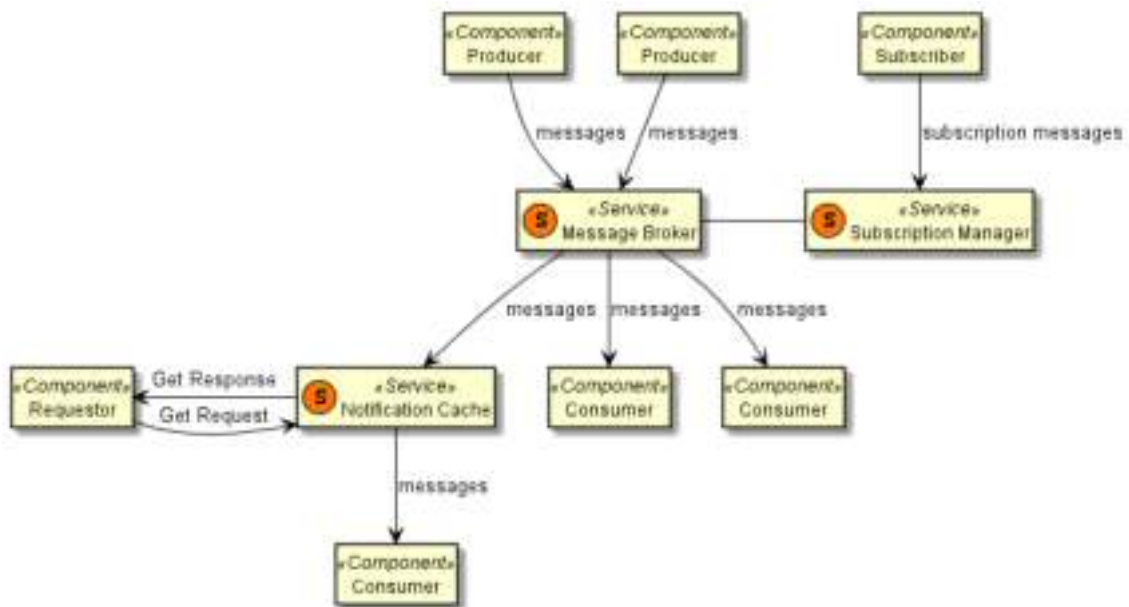
Figure 15 - Messaging Services *Composition* diagram: *Publish-Subscribe*

Requirement ID	SRS-2161
Verification method	Inspection
Requirement	The Platform SHALL support a variety of messaging styles (also known as MEP) at a minimum: • *Request-Response* (further specified in section 3.1.1.1) • *Publish-Subscribe*, (further specified in section 3.1.1.2) • Solicit Response (reverse of *Request-Response*) • Fire and Forget (one-way messages) • Store and Forward • Broadcast • Streaming

Requirement ID	SRS-2187
Verification method	Testing
Requirement	The Platform SHALL support the following delivery modes: • Synchronous messaging • Asynchronous messaging • Long running messaging.

Requirement ID	SRS-4220
Verification method	Testing
Requirement	The Platform SHALL be able to prioritise messages in order to ensure that high priority requests take precedence over lower-priority ones.
Requirement ID	SRS-2162

Verification method	Testing
Requirement	The Platform SHALL be able to add messages and retrieve messages from a Message Queue through a standard interface.

Requirement ID	SRS-2160
Verification method	Testing
Requirement	The Platform SHALL be able to prioritise messages in order to ensure that high priority requests take precedence over lower-priority ones.

Requirement ID	SRS-2162
Verification method	Testing
Requirement	The Platform SHALL support communication through a variety of transport standards, formats and protocols and their secure versions, at a minimum: • TCP/IP • UDP/IP • HTTP • SMTP • FTP • SOAP

Requirement ID	SRS-400
Verification method	Testing
Requirement	The Platform SHALL enable management of its endpoints, executable both by the operator via GUI or via service definition file processing, allowing for the following operations: • Associate an information source with an endpoint • Associate an information sink with an endpoint • Support the dynamic creation of endpoints • Support the dynamic modification of endpoints • Support the dynamic removal of endpoints

Requirement ID	SRS-4245
Verification method	Testing
Requirement	The platform SHALL be able to support a variety of service definition standards, at a minimum: • WSDL 1.1 • WSDL 2.0 • WADL

Requirement ID	SRS-406

Verification method	Testing
Requirement	The Platform SHALL provide the means to logically connect two endpoints for the purpose of establishing information flow from the producer to the consumer.

Requirement ID	SRS-4246
Verification method	Testing
Requirement	The Platform SHALL provide tools to define, manage (i.e., start, stop, suspend, resume), optimize and debug services and information flows between information providers and consumers, and intermediate operations.

Requirement ID	SRS-3978
Verification method	Testing
Requirement	The Platform SHALL be able to perform the following operations on information as it flows between the consumer and producer: • Augmentation • Filtering • Modification • Combination • Deletion

Requirement ID	SRS-4247
Verification method	Testing
Requirement	The Platform SHALL be able to execute background, periodic or user requested tasks for: • data ingestion • data notifications/generation • data processing

3.1.1.1 Request-response

Requirement ID	SRS-2174
Verification method	Testing
Requirement	The Platform Services SHALL use the Hypertext Transfer Protocol (HTTP; see [IETF RFC 2616, 1999]) as a transport mechanism to exchange messages.

Requirement ID	SRS-2175
Verification method	Testing
Requirement	The Platform Services SHALL employ the Uniform Resource Identifiers (URI; see Ref. [IETF RFC 3986, 2005]) to identify resources.

Requirement ID	SRS-2177

Verification method	Analysis
Requirement	The Platform Web Services using the REST Style when invoking other Web Services SHALL comply with the technical specifications as defined in the SIP for REST Messaging (see [NCIA AI 06.02.07, 2015]).

Requirement ID	SRS-2178
Verification method	Analysis
Requirement	The Platform Web Services using the SOAP Style when invoking other Web Services SHALL comply with the technical specifications as defined in the SIP for SOAP Messaging (see [NCIA AI 06.02.06, 2015]).

3.1.1.2 Publish-subscribe

Requirement ID	SRS-2182
Verification method	Analysis
Requirement	The *Publish-Subscribe* interfaces SHALL comply with the technical specifications as defined in the SIP for *Publish-Subscribe* Services (see [NCIA AI 06.02.08, 2015], [NCIA AI 06.02.09, 2015], and [NCIA AI 06.02.10, 2015]).

Requirement ID	SRS-
Verification method	
Requirement	

3.1.1.2.1 Message Broker

Requirement ID	SRS-2226
Verification method	Testing
Requirement	The Platform SHALL be able to act as a Message Broker propagating *Notifications* from *Publishers* to *Consumers*.

Requirement ID	SRS-428
Verification method	Testing
Requirement	The Platform SHALL provide the means to disseminate information to multiple *Consumers*.

Requirement ID	SRS-2202
Verification method	Testing
Requirement	The Platform SHALL expose a *Consumer* interface to receive *Notifications* from *Publishers*.

Requirement ID	SRS-2203
Verification method	Testing

Requirement	The Platform SHALL publish *Notifications* to the interface exposed by subscribed *Consumers*.

Requirement ID	SRS-426
Verification method	Testing
Requirement	The Platform SHALL allow producers to publish messages.

Requirement ID	SRS-430
Verification method	Testing
Requirement	The Platform SHALL allow *Consumers* to modify and cancel existing *Subscriptions*.

Requirement ID	SRS-2207
Verification method	Testing
Requirement	The Platform SHALL allow *Subscribers* to subscribe to a subset of information products matching a specific filter (e.g. *Topic*).

3.1.1.2.2 Subscription Manager

Requirement ID	SRS-2205
Verification method	Testing
Requirement	The Platform SHALL expose the *Subscription Manager* interface to which a *Consumer* can be subscribed.

3.1.1.2.3 Topic Manager

Requirement ID	SRS-397
Verification method	Testing
Requirement	The Platform SHALL provide the means for *Consumers* to receive information according to operationally defined *Topics*.

Requirement ID	SRS-395
Verification method	Testing
Requirement	The Platform SHALL provide the means to manage the *Topics* supported, including: • Organise a *Topic* hierarchy • Create a *Topic* • Move a *Topic* within the hierarchy • Remove a *Topic* • Manage *Topic* Filters

3.1.1.2.4 Notification Cache

Requirement ID	SRS-2184
Verification method	Testing

Requirement	The Platform SHALL provide a *Notification Cache* which complies with the technical specifications as defined in [NCIA AI 06.02.11, 2015].

3.1.1.3 Message Queue

Requirement ID	SRS-2126
Verification method	Testing
Requirement	The Platform SHALL provide the means for a producer to submit messages to the message queues.

Requirement ID	SRS-441
Verification method	Testing
Requirement	The Platform SHALL provide the means for a consumer to retrieve (and remove) messages from the message queue(s).

Requirement ID	SRS-440
Verification method	Testing
Requirement	The Platform SHALL provide the means to create, modify and delete message queues.

3.1.1.4 Message Router

Requirement ID	SRS-2165
Verification method	Testing
Requirement	The Platform SHALL be able to route messages to the intended service provider.

Requirement ID	SRS-432
Verification method	Testing
Requirement	The Platform SHALL be able to route messages correctly based on the address.

Requirement ID	SRS-433
Verification method	Testing
Requirement	The Platform SHALL be able route messages based on message *Metadata* (e.g., addressee) or message content.

Requirement ID	SRS-434
Verification method	Testing
Requirement	The Platform SHALL support message delivery to a single consumer.

Requirement ID	SRS-435
Verification method	Testing

Requirement	The Platform SHALL support message delivery to multiple consumers.

Requirement ID	SRS-3188
Verification method	Testing
Requirement	The Platform SHALL support guaranteed delivery of messages.

3.1.1.4.1 Message Proxy

Requirement ID	SRS-284
Verification method	Testing
Requirement	The Platform SHALL be able to provide a single point of access to services.

Requirement ID	SRS-437
Verification method	Testing
Requirement	The Platform SHALL provide the means to proxy request messages from a consumer to an *Information Provider*.

Requirement ID	SRS-438
Verification method	Testing
Requirement	The Platform SHALL provide the means to proxy response messages from an *Information Provider* to a consumer.

3.1.1.4.2 Message Cache

Requirement ID	SRS-3187
Verification method	Testing
Requirement	The Platform Message Cache SHALL store frequently called data and make it available for reuse, based on configurable parameters.

Requirement ID	SRS-4229
Verification method	Testing
Requirement	The Platform Message Cache SHALL be configurable to include as a minimum the replacement method, cache heap space, number of entries, and size of object.

Requirement ID	SRS-447
Verification method	Testing
Requirement	The Platform Message Cache SHALL provide the means for a requester to receive responses stored by the Message Cache.

Requirement ID	SRS-444
Verification method	Testing
Requirement	The Platform SHALL provide the means for an authorised requester to clear a Message Cache.

Requirement ID	SRS-445
Verification method	Testing
Requirement	The Platform SHALL allow for automatic clearing of the Message Cache based on the size, number and expiry time of messages.

3.1.2 Mediation

A central goal of the *Mediation* Services is to remove the tight coupling between services, by supporting the transformation of messages between service providers and service consumers. Messages dispatched by a consumer are transformed into messages understood by a provider, and vice versa.

These services therefore enable the communication between services that use different data formats or protocols. Its elements include:

- Data Transformation

- Protocol Transformation

- Composition
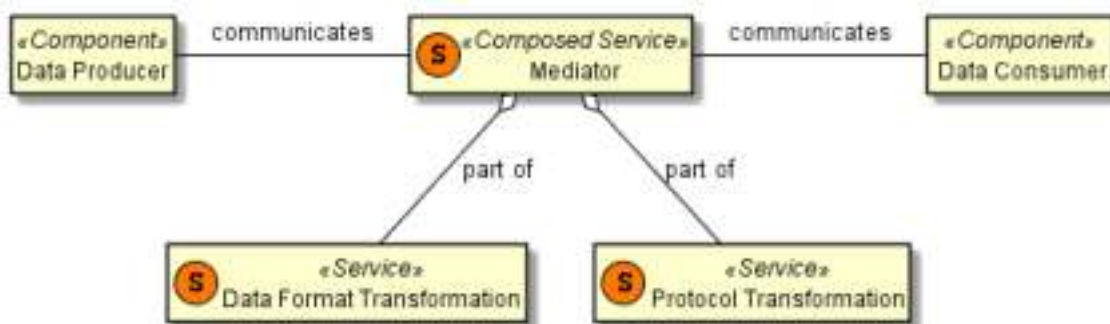
Figure 16 - *Mediation* **Services** *Composition* **diagram**

Requirement ID	SRS-178
Verification method	Analysis
Requirement	The Platform SHALL be able to take data in the format or protocol used by an information producer and transform the data into another format or protocol, according to a predefined set of extensible rules, that can be understood by the intended *Information Consumer*.

Requirement ID	SRS-175
Verification method	Testing

| Requirement | The Platform SHALL provide the means to expose a transformation as a service. |

Requirement ID	SRS-176
Verification method	Testing
Requirement	The Platform SHALL provide the means to make use of a transformation service.

Requirement ID	SRS-177
Verification method	Testing
Requirement	The Platform SHALL provide the means to activate and deactivate a transformation service.

3.1.2.1 Data Transformation

Data Transformation supports the encoding of – and transformation between – information in different formats. This is needed when *Information Consumers* cannot directly process the information in the format chosen by the *Information Provider*.

Important aspects of data transformation include format conversion where data is encoded differently using another format. Both data encodings represent the same information and are usually compatible. Important aspects of data transformation include format conversion where data is encoded differently using another format.

It should be able to take source data that has to be transformed, a specification of the source format, a specification of the target format, and a specification of how data *Artefacts* from the source format are mapped to *Artefacts* of the target format, and transforms the data into a new representation complying with the target data format.

Requirement ID	SRS-2128
Verification method	Analysis
Requirement	The Platform SHALL provide the means to convert data from one value into another, compatible value.

Requirement ID	SRS-3189
Verification method	Testing
Requirement	The Platform SHALL be able to transform data formats independently from their representation; at a minimum, supported representations include binary, MTF, XML, JSON, and plain (unformatted) text.

| Requirement ID | SRS-2218 |
| Verification method | Testing |

Requirement	The Platform SHALL allow for Extensible Stylesheet Language Transformations (XSLT), when mediating between different XML data formats.

Requirement ID	SRS-4236
Verification method	Testing
Requirement	The Platform SHALL retrieve all stylesheet based transformations from the Metadata Registry and Repository.

Requirement ID	SRS-2219
Verification method	Analysis
Requirement	Each XSLT *Stylesheet* SHALL be created as a separate *Artefact*, and not embedded in the implementation of the service.

Requirement ID	SRS-2221
Verification method	Analysis
Requirement	The Platform services using XSLT *Stylesheets* for *Mediation* SHALL comply with the XSLT-Based *Mediation* SIP Proposal (see [NCIA TR/2012/SPW008423/23, 2012]).

Requirement ID	SRS-3192
Verification method	Testing
Requirement	The Platform services SHALL be able to run data transformations using externally provided: • XSLT • Executables • Transformation Services.

3.1.2.2 Protocol Transformation

Protocol Transformation mediates between communication parties by adjusting the way in which data is exchanged between both parties. Protocol Transformation Services enable the use of different protocols for handling information between *Information Providers* and consumers over a possibly heterogeneous network. Protocol Transformation Services are important when different types of communication patterns are being used (e.g., static, deployable or mobile) that would require special protocols to ensure that the information is being transferred in the most efficient possible way.

Protocol transformation services mediate between various transport protocols, which for example in a web services setting usually comprise single protocols like HTTP, HTTP within a connection encrypted by TLS (HTTPS), TLS, SMTP and FTP, but also entire message-oriented middle-ware solutions. An example

of a binary transport protocol would be Joint Range Extension Applications Protocol (JREAP).

Protocol Transformation Services are important when different types of communication patterns are being used (e.g. static, deployable or mobile) that would require special protocols to ensure that the information is being transferred in the most efficient possible way.

Requirement ID	SRS-2164
Verification method	Analysis
Requirement	The Platform will be able to transform between transport protocol formats and format versions according to predefined rules.

Requirement ID	SRS-3197
Verification method	Analysis
Requirement	The Platform SHALL be able to adapt between different *Message Exchange Patterns*.

3.1.3 Composition

Composition **Services** enable the provision of a service or *Capability* by combining other services. Services can therefore be used as building blocks which interact each other following a defined process. The result can be the *Orchestration* or *Choreography* of services, depending whether the process is managed by a central service or not. The *Composition* Services make use of other *Components* such as Message Router and *Mediation* Services.
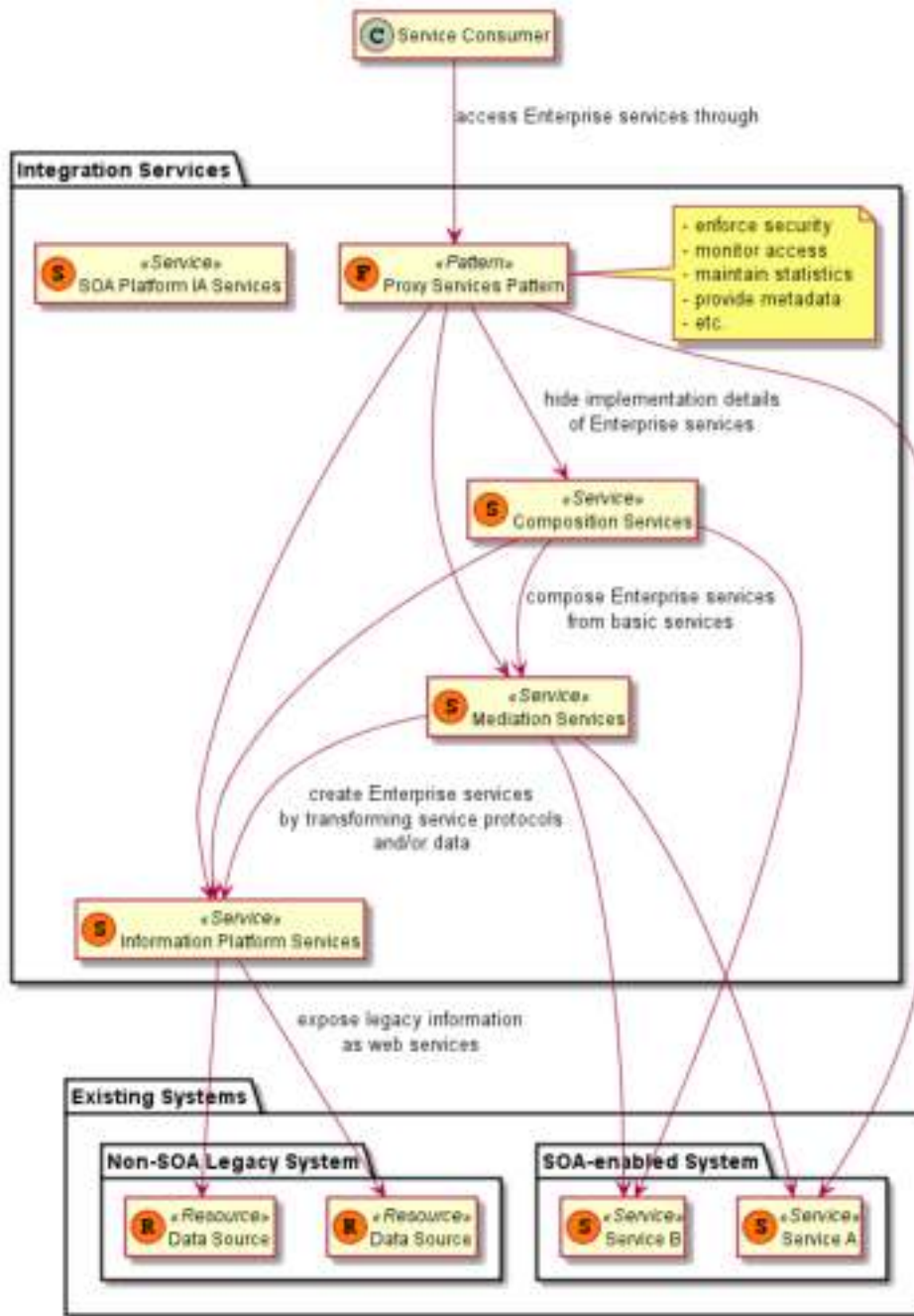
Figure 17 - Complete *Mediation* Services *Composition* diagram

Requirement ID	SRS-511
Verification method	Testing
Requirement	The Platform SHALL provide functionality to compose existing services.

Requirement ID	SRS-512
Verification method	Testing
Requirement	The Platform SHALL provide functionality to propagate and coordinate interactions between services being composed.

Requirement ID	SRS-513
Verification method	Testing
Requirement	The Platform SHALL provide functionality to correlate messages that are exchanged between composed services.

Requirement ID	SRS-514
Verification method	Testing
Requirement	The Platform SHALL provide functionality to monitor the state of the active *Compositions*.

Requirement ID	SRS-3198
Verification method	Analysis
Requirement	The Platform SHALL be able to support *Choreography* modelling.

Requirement ID	SRS-2223
Verification method	Analysis
Requirement	The Platform SHALL be able to compose services following the Business Process Execution Language (BPEL, [OASIS WS-BPEL V2.0, 2007]) specification.

Requirement ID	SRS-4250
Verification method	Testing
Requirement	The Platform SHALL be able validate a BPEL file, and all supporting needed schemas and descriptors.

Requirement ID	SRS-2224
Verification method	Analysis
Requirement	The Platform SHALL be able to compose services BPEL *Composition* SIP Proposal (see [NCIA TR/2012/SPW008423/20, 2012]).

Requirement ID	SRS-516
Verification method	Testing
Requirement	The Platform SHALL be able to compose multiple individual services into a single business-process represented by an *Orchestration*.

Requirement ID	SRS-517
Verification method	Analysis

Requirement	The Platform SHALL be able to expose an *Orchestration* (i.e. composed process) as a service with an exposed interface.

Requirement ID	SRS-519
Verification method	Testing
Requirement	The Platform SHALL be able to support as a minimum the following process control flow constructs: • Sequence • Parallel execution • Process joins • Loops • Conditional execution • Action synchronisation • Asynchronous eventing

Requirement ID	SRS-521
Verification method	Testing
Requirement	The Platform SHALL provide functionality to execute multiple *Orchestration* instances.

Requirement ID	SRS-524
Verification method	Testing
Requirement	The Platform SHALL be able to create *Orchestration* instances and manage their execution, including start/stop/suspend/resume.

Requirement ID	SRS-525
Verification method	Testing
Requirement	The Platform *Orchestration* SHALL coordinate *Sub-services* calls and process data produced by *Sub-services*.

Requirement ID	SRS-527
Verification method	Testing
Requirement	The Platform *Orchestration* SHALL support multiple versions of the same process definition running in parallel.

Requirement ID	SRS-528
Verification method	Testing
Requirement	The Platform SHALL provide mechanism to handle *Orchestration* execution *Faults*.

Requirement ID	SRS-529
Verification method	Testing
Requirement	The Platform SHALL maintain state of *Orchestrations* being executed.

Requirement ID	SRS-3858
Verification method	Testing
Requirement	The Platform *Orchestration* Services SHALL support long running processes.

Requirement ID	SRS-530
Verification method	Testing
Requirement	The Platform *Orchestration* Services SHALL support temporal suspension of long running processes to secondary memory (aka dehydration).

3.2 Registry and Repository Services

Service Discovery is the process of locating service providers, and retrieving the services' descriptions and access parameters which have been previously published. The primary mechanism involved in performing of Service Discovery is a service registry, which contains relevant data about available and upcoming services, as well as pointers to the corresponding service contract documents including SLAs.

Typically, the *Metadata* that is important for calling a service – for example, information about the data format used in the response – is stored in a *Metadata Repository*. The repository also provides a home for other artefacts, including Extensible Markup Language (XML) schemas and documentation that are important to the Platform.

These services thus work together to store and provide information that is important for discovering and using services. They can be accessed by services, service developers and *Users* at both design time and run time.

This information includes *Metadata* about services, such as the endpoint and interface implemented by a particular service, the schemas of particular XML data models (in different versions), ontologies, transformations and so on. It supports the advance and dynamic discovery of services and information sources.

It includes the following *Components*:

- Service Discovery

- Metadata Registry and Repository

3.2.1 Service Discovery

The **Service Discovery** services enables a requester to discover a target service that matches certain requirements. The resulting service description is sufficient to inform a consumer on the mechanism required to bind to an instance of the target service.
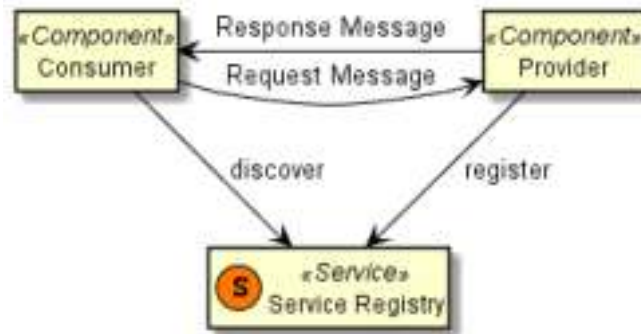
Figure 18 - Service Discovery *Composition* Diagram

As depicted in the diagram below there are two ways to discover and register services:

A Graphical User Interface (GUI), which is typically used (manually) at design-time

Web service interfaces (REST and SOAP) for web services, which are typically invoked dynamically (automatically) at run-time.

Note that the GUI uses the same underlying interfaces exposed to web services so that the GUI and the web service interfaces implementations are consistent, but are independent and de-coupled.
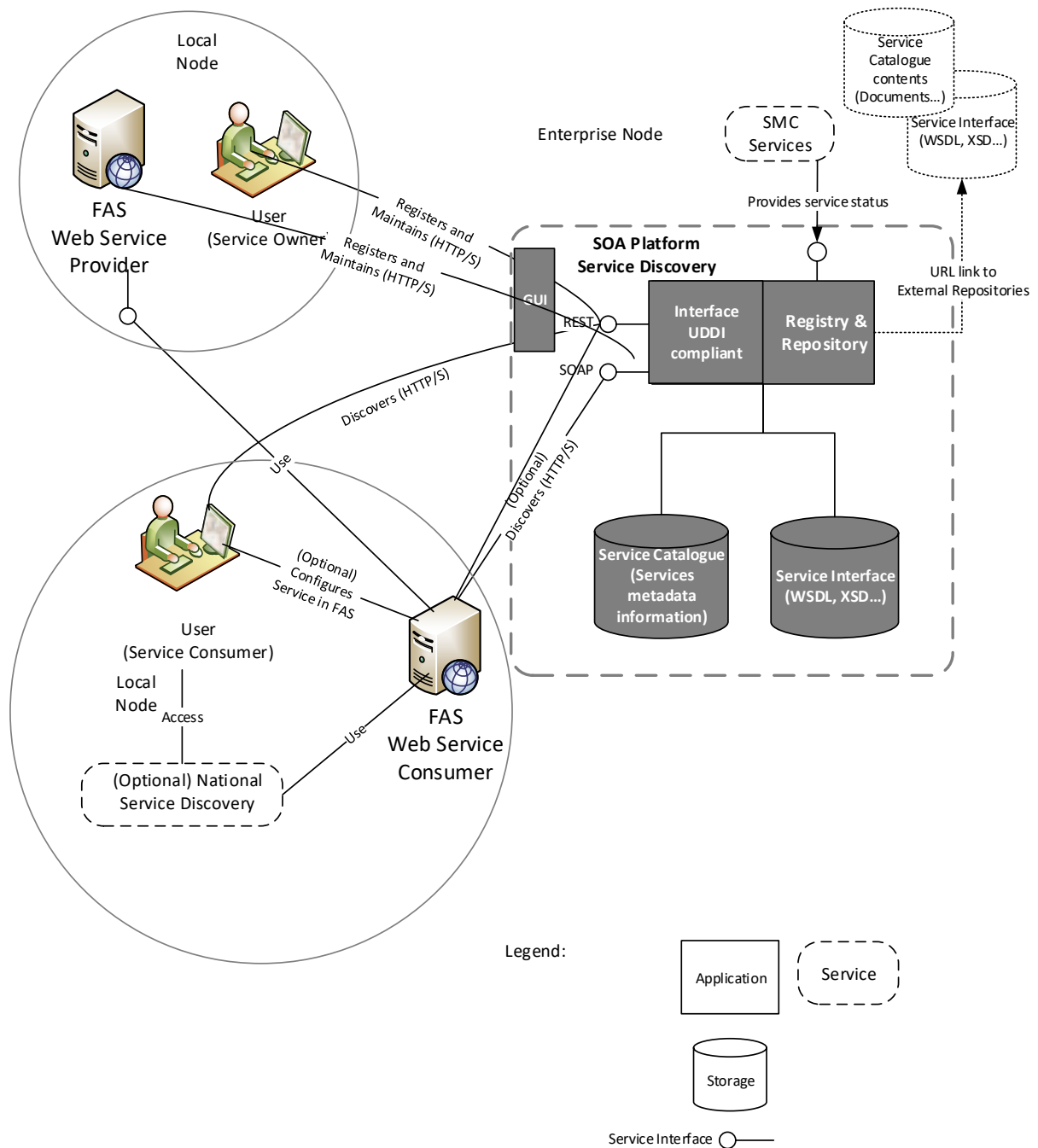
Figure 19 - Service Discovery Interfaces

Requirement ID	SRS-3678
Verification method	Testing

Requirement	The Platform SHALL allow a Service Provider to register a web service at both runtime and design time, with at least the following *Metadata* (e.g., description, keywords) information: • service end-point URL • service name • service description • service contract • keywords • point of contact details

Requirement ID	SRS-3677
Verification method	Testing
Requirement	The Platform SHALL allow a *Consumer* to discover published services using the service metadata as filters via a programmatic service interface and via user accessible GUI.

Requirement ID	SRS-373
Verification method	Testing
Requirement	The Platform SHALL return sufficient information to the requesting service to bind with it at run-time.

Requirement ID	SRS-2113
Verification method	Testing
Requirement	The Platform SHALL provide functionality to identify and register separate service instances that can provide identical results.

Requirement ID	SRS-285
Verification method	Testing
Requirement	The Platform SHALL maintain a managed list of internal and external services as a Service Catalogue, accessible by Service *Consumers*.

Requirement ID	SRS-3680
Verification method	Testing
Requirement	The Service Catalogue SHOULD be complemented with information from the Platform SMC services (see Section 3.3) on the status, *Availability*, usage and other operational information of registered web services.

Requirement ID	SRS-3681
Verification method	Testing
Requirement	The Platform SHALL provide a web-based GUI for the *Users* to visualise, manage and search for services and their corresponding information.

Requirement ID	SRS-3682
Verification method	Analysis
Requirement	The Platform SHALL provide a UDDI v.3 compliant Interface for the GUI and the web services interaction with the Service Registry *Component*.

Requirement ID	SRS-3770
Verification method	Analysis
Requirement	The Platform SHALL comply with the Service Discovery SIP Proposal (see Ref. [NC3A RD-3185, 2011]).

3.2.2 Application Programming Interfaces (APIs)

An Application Programming Interface (API) is an entry point for a system or application, allowing other programs or systems to access it. It is similar to a "service interface" as used in the context of other Platform services, although less formally structured and with a broader suite of possible technologies.

APIs should be managed and organised. Similar to service discovery and management, "API Management" is the process of publishing, documenting and overseeing APIs in a secure, scalable environment. The goal of API Management is to monitor the interface's lifecycle, assist in discovering and accessing APIs, and make sure the needs of developers and applications using the API are being met.

Requirement ID	SRS-4118
Verification method	Inspection
Requirement	The Platform SHALL implement an API Management *Capability* to enable lifecycle management (including versioning) of APIs, adequate documentation of interfaces, and implementation of the *Identity* and Security Services to protect access to the API.

Requirement ID	SRS-4033
Verification method	Analysis
Requirement	For each API *Component* the Platform SHALL fully document the interface, including: • Mechanisms for securely invoking the API • Available methods and functionality • Available information elements, including *Attributes* and enumeration values

	• *Error* handling

Requirement ID	SRS-2533
Verification method	Testing
Requirement	The Platform SHALL allow authorised *Components* and systems to access the API supporting the Platform *Capability*.

Requirement ID	SRS-4063
Verification method	Analysis
Requirement	The Platform SHALL expose an API using open standards or widely accepted industry standards.

3.2.3 Metadata Registry and Repository

The *Metadata Registry and Repository* is a system that contains information that describes the structure, format and definitions of data. Typically, a registry is a software application that uses a database to store and search data, document formats, definitions of data, and relationships among data.

The Platform includes a *Metadata Registry and Repository* to provide a consistent, controlled and reliable means to store, manage and access XML *Artefacts* and *Artefact Collections*, including *Metadata* and data specifications.

An ***Artefact*** in the context of the *Metadata Registry* is usually a structured document like an XML schema. But unstructured information, such as supporting documentation for APIs, can also be considered to be an Artefact.

An ***Artefact Collection*** is a governance namespace for a set of *Artefacts* and/or *Artefact* sub-collections. An *Artefact* collection has a name. A collection manager manages an *Artefact* collection, and all *Artefacts* and sub-collections it contains.

Artefact Metadata describes information about an *Artefact* or *Artefact Collection*. Example *Metadata* for *Artefacts* are name, originator, version, publication date, point of contact, security classification, life-cycle status. Example *Metadata* for collections are name, description, collection manager. NATO and domain specific *Metadata* is expected, so the *Metadata* model needs to be extensible.

The *Metadata Registry and Repository* will also need to support workflows to manage the life-cycle of an *Artefact*. The possible life-cycle statuses will depend on the *Artefact*; and example are the NATO STANAG related *Artefacts* that can have the following status: Final Draft, Ratification Draft, Withdrawn, Promulgated, Superseded, and more.
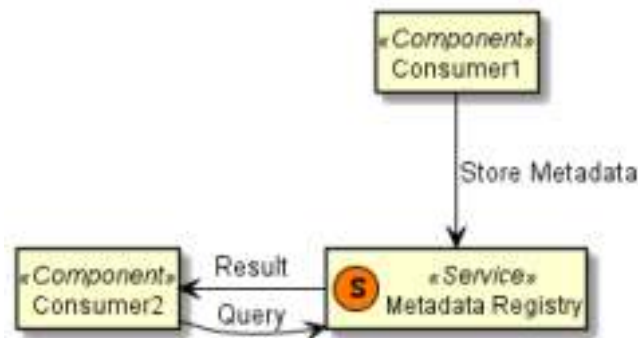
Figure 20 - Metadata Registry *Composition* diagram

Requirement ID	SRS-3202
Verification method	Inspection
Requirement	The Platform SHALL expose a service API to be used as interface by other services and *Users* (through a GUI) interface to provide access to the *Metadata Registry* and *Repository* functionality.

Requirement ID	SRS-3200
Verification method	Testing
Requirement	The Platform SHALL provide the ability to register, make available, update, and delete *Artefacts*, *Artefact Collections,* and associated *Metadata*.

Requirement ID	SRS-4095
Verification method	Testing
Requirement	The Platform SHALL provide the ability to update *Metadata* of multiple *Artefacts* simultaneously (i.e. bulk operation).

Requirement ID	SRS-4070
Verification method	Testing
Requirement	The Platform SHALL support registration, search, update, and deletion of *Artefacts*, including: - XML schema - WSDL - supporting documentation (like PDF) with design or usage information.

Requirement ID	SRS-488
Verification method	Testing
Requirement	The Platform SHALL provide the ability to control at a *User* level, read, write, edit and delete access to *Artefacts*, *Artefact Collections*, and *Metadata*.

Requirement ID	SRS-4084
Verification method	Testing
Requirement	The Platform SHALL be able to extract *Artefact Metadata* from: • the *Artefact* itself • a separate metadata-document (XML *Artefact*).

Requirement ID	SRS-3309
Verification method	Testing
Requirement	On registration of an *Artefact* the Platform SHALL provide the ability to also register referenced *Artefacts*, including XML schema and WSDL.

Requirement ID	SRS-492
Verification method	Testing
Requirement	The Platform SHALL be able to differentiate between different object types based on *Artefact* content (e.g. WSDL, OWL, RDF, XML schema).

Requirement ID	SRS-4237
Verification method	Testing
Requirement	The Platform SHALL be able to manage XSLTs.

Requirement ID	SRS-4248
Verification method	Testing
Requirement	The Platform SHALL be able to validate uploaded XSLT against XML schemas.

Requirement ID	SRS-3310
Verification method	Testing
Requirement	The Platform SHALL be able to validate an *Artefact,* based on syntax and availability of referenced *Artefacts*, and depending on: • the Artefact type • the operation an *Artefact* is involved in.

Requirement ID	SRS-493
Verification method	Testing
Requirement	The Platform SHALL provide the ability to search, list and retrieve *Artefacts,* including different versions, using a filter on the *Artefact* content and/or on the *Artefact Metadata.*

Requirement ID	SRS-3311

Verification method	Testing
Requirement	The Platform SHALL provide filtered search on contents of XML *Artefacts* using XPath and/or XQuery.

Requirement ID	SRS-4071
Verification method	Testing
Requirement	The Platform SHALL be able to store and manage different versions of an *Artefact*, *Artefact Collection* and associated *Metadata*.

Requirement ID	SRS-489
Verification method	Testing
Requirement	The Platform SHALL provide the ability to create and manage workflows with customisable life-cycle statuses for *Artefacts* and *Artefact Collections*.

Requirement ID	SRS-3305
Verification method	Testing
Requirement	The Platform SHALL provide functionalities to assign a workflow to *Artefacts* and to *Artefact Collections*.

Requirement ID	SRS-3306
Verification method	Testing
Requirement	The Platform SHALL assign a default workflow to *Artefacts* and *Artefact Collections* based on the *Artefact* type or the *Artefact Collection*(s) to which it belongs, if no specific workflow is provided.

Requirement ID	SRS-4085
Verification method	Testing
Requirement	The Platform SHALL be able to inform *Users* and services about changes to an *Artefact* or *Artefact Collection*.

Requirement ID	SRS-4086
Verification method	Testing
Requirement	The Platform SHALL be able to inform subscribed *Users* about *Artefact* or *Artefact Collection* changes via: • e-mail • GUI.

Requirement ID	SRS-3308
Verification method	Testing

Requirement	In order to be notified about *Artefact* and/or *Artefact Collection* changes, the Platform SHALL provide the ability to:
	• subscribe and unsubscribe • view and manage *Subscriptions* • select *Notification* delivery preferences

Requirement ID	SRS-3314
Verification method	Testing
Requirement	The Platform SHALL provide the ability to reference and retrieve specific versions of an *Artefact* via an accessible unique and non-editable URL.

Requirement ID	SRS-4096
Verification method	Testing
Requirement	The Platform SHALL provide the ability to search and list *Artefacts* together with the *Artefact Metadata*, and export the result as a structured document (for example as XML document).

Requirement ID	SRS-485
Verification method	Analysis
Requirement	The Platform SHOULD support federated searches using open standards for federated or aggregated search, in order to allow searching of other *Metadata Registry and Repositories*.

Requirement ID	SRS-3315
Verification method	Testing
Requirement	The Platform SHALL provide functionality to reference to *Artefacts* from other *Metadata Registry and Repositories*.

Requirement ID	SRS-3312
Verification method	Testing
Requirement	In case of an XML *Artefact* the Platform SHALL provide functionality to retrieve and export: • XML *Artefacts* together with referenced XML *Artefacts* called out by import or include statements • specific *Artefact* fragments (XML fragments) using XPath end XQuery.

Requirement ID	SRS-4094
Verification method	Testing

Requirement	The Platform SHALL be able to create, view, search and manage associations between *Artefacts,* which can be both dependent or independent of the *Artefact* version. Examples of an associations between *Artefacts* are "is superseded by", "refers to", "is derived from".

3.3 SMC Services

Effective management of the Platform and its hosted services is critical. The ability to monitor and manage services' *Performance* and *Availability*, configure and control service implementations, and automate and improve end-to-end processes is a core function of the Platform.

In order to optimise the efficiency and *Availability* of services, it is important that their status is continuously monitored, not only at the machine level, but also at the service level. Therefore the Platform is integrated with the Enterprise Service Management and Control (SMC) system, mostly based on BMC Remedy and Truesight, that is in place across NATO. This is also linked to other services, such as the Registry, to allow the dynamic allocation of service endpoints based on current service *Performance*. The *Monitoring* of services also supports meeting SLA targets, and – if necessary – the *Metering* (and charging) of services.

The Platform's SMC Services provide a suite of *Capabilities* needed to ensure that SOA services are up and running, accessible and available to *Users*, protected and secure, and that they are operating and performing within agreed upon quality of service and Service Level Agreement (SLA) parameters.

Platform management is more than just service *Monitoring*, however. It also includes *Capabilities* and tools for provisioning of new services / service instances, managing and *Monitoring* composite applications and/or orchestrated sets of services, as well as the supporting infrastructure across the architecture layers.

In addition, the Platform must be able to provide visibility into message content and routing, as well as transactional workflows, and have the ability to identify and automatically correct *Performance* bottlenecks.

Service Management includes the following *Components*:

- Configuration Management

- Event Management

- Performance and Capacity Management

- Process Automation

Requirement ID	SRS-3981
Verification method	Testing

Requirement	The Platform SHALL deliver the necessary interfaces to exchange information in both directions with the Enterprise SMC *Capability*, with the necessary flexibility to present the data in accordance with evolving enterprise level data structures and vocabularies.

Requirement ID	SRS-238
Verification method	Testing
Requirement	The Platform SHALL provide *Capabilities* to define, deploy, manage and enforce quality of service and Service Level Agreements (SLAs) for individual services and service groups.

Requirement ID	SRS-239
Verification method	Analysis
Requirement	The Platform SHALL be able to define, deploy and manage SLA parameters for whole end-to-end processes.

Requirement ID	SRS-274
Verification method	Testing
Requirement	The Platform SHALL provide the *Capability* to manage the full life-cycle of services, from provisioning to controlling to decommissioning, including versioning.

Requirement ID	SRS-2417
Verification method	Testing
Requirement	The Platform SHALL support remote deployment of all the Platform *Components* and updates using Microsoft System Center Configuration Manager.

Requirement ID	SRS-4252
Verification method	Testing
Requirement	The Platform SHALL support configuration reporting of Platform Components using Microsoft System Center Configuration Manager.

Requirement ID	SRS-2419
Verification method	Testing
Requirement	The Platform SHALL support collection and reporting of asset inventory metrics for all the Platform *Components* using Microsoft System Center Configuration Manager, including: • Memory

	• Operating System • Peripherals • Services • Login tracking • Software existence and usage • Licensing

3.3.1 Configuration Management

In Information Technology Infrastructure Library (ITIL) terms, *Configuration Management* is the process responsible for maintaining information about the *Configuration Items* (CI) required to deliver a Service, including their Relationships with one another. This information is managed throughout the lifecycle of the CI, and it typically stored in a *Configuration Management* Database (CMDB).

The *Configuration Management* process is most concerned with configuring, deploying and later decommissioning Services. The Platform needs to provide the ability to change, capture, duplicate, backup or restore the configuration of Services.

An Enterprise CMDB already exists in the NATO Enterprise provided as part of the IaaS platform from the ITM project, and is used as the underpinning of the Platform's *Configuration Management* as well.

There is also a relationship between SOA *Configuration Management* and Service Discovery. Configuration Management, and tools like the CMDB, tend to focus on somewhat more stable, static elements of a service, managing the configuration as it is understood from inception (for example its installation attributes, versions and constraints). Service discovery, on the other hand, tends to be more dynamic, and is more concerned with allowing the service to be found and accessed at run-time. In both cases, the service is being managed; there is thus overlap between SMC and Service Discovery.

Requirement ID	SRS-3571
Verification method	Analysis
Requirement	The Platform SHALL re-use the Enterprise SMC *Configuration Management Component* (BMC IT Service Management Atrium (ITSM) CMDB) to track Platform assets and their configuration information when possible, and be compatible with it when re-use is not possible.

Requirement ID	SRS-244
Verification method	Testing
Requirement	The Platform SHALL provide the capability to search for Platform assets based on available *Metadata* information.

Requirement ID	SRS-3546
Verification method	Testing
Requirement	The Platform SHALL provide a dashboard with an overall view of the Platform inventory items.

3.3.2 Event Management

In ITIL terms, an *Event* can be defined as any detectable or discernible occurrence that has significance for the management of the infrastructure or the delivery of a Service.

Event Management is the process that monitors all *Events* that occur throughout the Platform. It allows for normal operation, but also detects and escalates exception conditions.

For the Platform, *Event Management* includes:

- Logging,

- Alerting

- Reporting

Requirement ID	SRS-3588
Verification method	Testing
Requirement	The Platform SHALL integrate with the *Event Management* system that will be provided by the Enterprise SMC *Capability*.

Requirement ID	SRS-3556
Verification method	Testing
Requirement	The Platform SHALL collect *Events* generated from all Platform *Components* and forward them to the Enterprise *Event Management* System.

Requirement ID	SRS-3555
Verification method	Testing
Requirement	The Platform SHALL provide a toolset which allows *Authorised Users* to define, filter, correlate and group *Events* according to their context, criticality, source and impacts.

3.3.2.1 Logging

Logging is the act of keeping a log, which is a repository that records either *Events* that occur in software or messages between different *Users*. These log messages may be written to a single logfile, stored in a database, or managed in other ways.

Having a *Logging Component* in the Platform should allow for future analysis of *Events*, for example the recovery of the full chain of evidence for any system access or update.

3.3.2.2 Alerting

The Platform and the services hosted on it, have certain expectations of service *Availability*, *Performance*, security and other parameters. These may be expressed as *Key Performance Indicators* (KPI), Service Level Agreements (SLA) or other metrics.

The *Alerting* functionality of the SMC Services is closely tied to the *Monitoring* functionality, in which the "health" of the system is continually evaluated. In all cases, when the acceptable threshold for a service (or the Platform) is detected to be approaching or reached, the system will automatically generate an *Alert Event*.

An *Alert* can either be a:

- "Warning" (indicating that it is necessary to take action in order to prevent an exception occurring)

- "Exception" (indicating that the service is currently operating below the normal predefined parameters/indicators)

While this functionality is closely related to the existing ITM *Event Management* system, there are some unique requirements for the Platform, including the ability to *Alert* on stalled or failed service *Compositions*/*Orchestrations*.

Requirement ID	SRS-3557
Verification method	Testing
Requirement	The Platform SHALL provide a toolset to configure policy and rule based *Event* filtering, and to automate *Alert* triggering capabilities.

Requirement ID	SRS-291
Verification method	Testing
Requirement	The Platform SHALL provide functionality to generate *Alerts* associated with SOA services to include: • breach of *Performance* or *Capacity* thresholds • stalled processes • unauthorised access to services • SLA parameters can't be met • specific mechanisms to enforce SLAs were activated (e.g., throttling)

3.3.2.3 Reporting

An SMC system needs to provide thorough reports for compliance, auditing, billing, service value determination, and so on. The Reporting function is customizable so expert *Authorised Users* can add, delete or modify Reports.

The Reporting I is distinct from the *Monitoring Component* in that *Monitoring* occurs in real time, while Reporting (usually) happens *post facto*.

Requirement ID	SRS-251
Verification method	Testing
Requirement	The Platform SHALL be able to generate: • SLA compliance reports • *Error*/exception reports • operational and historical reports on *Events* • overall *Performance* trends • service usage reports • other customizable reports based on captured metrics which can be filtered and sorted based on various criteria

3.3.3 Performance and Capacity Management

This aspect of the SMC Services is about defining and tracking the metrics to be captured during service operation to measure *Performance* and use of *Capacity*.

This includes *Monitoring* tools, which are used to measure the "health" of the Platform and its hosted services (as well as the Web Hosting Services which the Platform sits on top of) by monitoring service *Availability*, *Capacity* and *Performance* as defined by the relevant KPIs. These in turn may provide input to the *Event Management* processes, in particular *Alerting*.

It also includes *Metering* tools, which are more focused on service utilisation and consumption of services per *User*/*Entity*, for the purposes of cost recovery or reporting.

3.3.3.1 Monitoring (including dashboards)

Monitoring observes and tracks the operations and activities of *Users*, applications and services on the Platform, thus providing a way to supervise the overall processes that are performed.

Requirement ID	SRS-2118
Verification method	Testing
Requirement	The Platform SHALL monitor the status and quality of service, (including *Availability*, *Performance*, and utilisation) of the Platform infrastructure, the underlying Web Hosting Services and the services hosted on the Platform.

Requirement ID	SRS-381
Verification method	Testing
Requirement	The Platform SHALL provide functionality for real time monitoring of services against expected KPI, SLA, or other configurable metric thresholds.

Requirement ID	SRS-3563
Verification method	Testing
Requirement	The Platform SHALL report on usage patterns over daily, monthly and variable periods.

Requirement ID	SRS-2896
Verification method	Testing
Requirement	The Platform SHALL automatically detect degraded *Performance*.

Requirement ID	SRS-3562
Verification method	Testing
Requirement	The Platform SHALL provide customizable dashboards for monitoring selected statistics and metrics for Platform, Web Hosting, and hosted services.

Requirement ID	SRS-288
Verification method	Testing
Requirement	The Platform SHALL provide the *Capability* to monitor access attempts to Platform services.

Requirement ID	SRS-382
Verification method	Testing
Requirement	The Platform SHALL provide functionality to monitor composed and/or orchestrated services, as well as to drill down to monitor individual services of a *Composition* and/or *Orchestration*.

Requirement ID	SRS-383
Verification method	Testing
Requirement	The Platform SHALL provide functionality to monitor service *Faults* and exceptions.

3.3.3.2 Metering

Metering measures levels of *Resource Utilisation* consumed by service *Subscribers*. Measured data is stored for summarizing and analysing.

Requirement ID	SRS-252
Verification method	Testing
Requirement	The Platform SHALL be able to collect and present the statistics on service utilisation broken down by *User*/tenant.

Requirement ID	SRS-390

Verification method	Testing
Requirement	The Platform SHALL aggregate collected statistics for a given *User*/tenant or group of *Users*/tenants over specified periods of time.

Requirement ID	SRS-4249
Verification method	Testing
Requirement	The Platform SHALL be able to use statistics on service utilisation for *Metering*, billing and other purposes.

Requirement ID	SRS-392
Verification method	Testing
Requirement	The Platform SHALL make collected and aggregated statistics available for retrieval.

3.3.3.3 Message Tracking

Because the Platform SMC Services must provide end-to-end visibility of all service requests and responses, it is therefore responsible for tracking, *Monitoring* and *Logging* all message routing and service invocation activities.

The responsibility for Message Tracking also includes the need for the SMC Services to be able to dynamically and automatically identify (and implement; see Process Automation section) improvements in message routing, both for a single service call and as part of a service *Composition*/*Orchestration*.

Requirement ID	SRS-2197
Verification method	Testing
Requirement	The Platform SHALL track and monitor the message routing for service invocation and responses.

Requirement ID	SRS-241
Verification method	Testing
Requirement	The Platform SHALL provide the functionality to diagnose faulty message flows and identify improvements to prevent disruption of transactions.

3.3.4 Process Automation

The Platform SMC Services are expected to be able to react to *Errors* or potential *Errors* in the system – as indicated by the *Event Management* or *Performance* and *Capacity* Management *Components* – and to identify and automatically implement resolutions. These can include *Performance*, *Capacity*, message traffic, or other types of issues which the SMC Services automatically attempt to resolve.

Requirement ID	SRS-3578
Verification method	Testing

Requirement	The Platform SHALL be able to automatically manage services by defining, configuring and triggering automated actions when certain *Alerts* (triggers) are received.

Requirement ID	SRS-3565
Verification method	Testing
Requirement	The Platform SHALL accept triggers from *Alerting*, *Monitoring*, and Message Tracking Services.

Requirement ID	SRS-367
Verification method	Testing
Requirement	The Platform SHALL be able to automatically execute as a minimum the following actions: • service call prioritisation • selective routing based on configurable criteria • service throttling

3.4 Platform Hosting

As part of the concept of *Multi-tenancy* (see Section 1.1.3), there is an important trend in the IT industry towards the development of SOA Integration Platforms. These allow *Users* to access multiple applications through a common platform. They also offer application developers an opportunity to quickly develop and deploy new applications.

With this model, a single version of the platform, with all necessary configurations (hardware, network, operating system, software stack) can be used for all customers (applications). Additional versions of the platform are set up to offer identical environments for testing and pre-release purposes.

The hosting services also make available a service container that manages the service life cycle and underlying resources (such as memory, storage and Central Processing Unit (CPU)) to deliver the required service. The application or web service execution can take place within the container's run time environment.

3.4.1 Platform Attributes

The Platform provides a complete development and deployment setting for SOA-based applications and services in NATO, enabling the delivery of a complete service context: from simple single-function services to sophisticated *Compositions* of services resulting in complex *Capability*.

The Platform provides an enterprise-wide system/application delivery and provisioning mechanism, along with functionality to manage and decommission hosted services, and an approval workflow to support the provisioning of the SOA and IAM services

With this functionality, the Platform will provide an environment whereby common tools and automated procedures can be deployed to help create, modify, test and deploy (migrate and install) application code, libraries and services across environments (e.g., from development to testing) and to automate the release process(es) of services across environments.

It is expected that the Platform supports environments based on the following core NATO software stacks:

- LAMP to include Ruby, PHP and Python frameworks

- Apache HTTP Service

- Microsoft .NET Framework with Windows Communication Foundation (WCF) and Internet Information Services (IIS)

- SharePoint 2013/2016

- Java Application Framework on Apache Tomcat

Requirement ID	SRS-449
Verification method	Inspection
Requirement	The Platform SHALL provide the functionality to provision, manage and decommission hosted services.

Requirement ID	SRS-3701
Verification method	Testing
Requirement	The Platform SHALL provide a Web Interface for *Users* for automated provision of Platform services, including of pre-configured templates.

Requirement ID	SRS-3702
Verification method	Testing
Requirement	The Platform SHALL allow for development of an approval workflow to support the provisioning of the Platform services.

Requirement ID	SRS-3607
Verification method	Testing
Requirement	The Platform SHALL provide an operational environment which supports *Scalability* of deployed software (Services), featuring as a minimum load balancing and failover.

Requirement ID	SRS-3602
Verification method	Testing
Requirement	The Platform SHALL provide the following environments as pre-configured templates for various development environments, specifically:

	• LAMP to include Ruby, PHP and Python frameworks with Apache HTTP Service • .NET Framework applications on IIS • SharePoint 2013/2016 • Java Application Framework on Apache Tomcat The exact configuration of the templates will be finalised during the design review phase.

Requirement ID	SRS-3603
Verification method	Analysis
Requirement	Development Platform environments SHALL be able to make use of Platform provided services via their service interfaces, independent of their run-time environment.

Requirement ID	SRS-3614
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to configure basic features of the hosted environments, to include as a minimum CPU, RAM and Storage parameters.

3.5 Information Services

NATO systems provide vast amounts of information, which are usually only available within specific CoIs or in formats that are not immediately accessible to, or exchangeable with, the data stores of other systems. The Platform provides the mechanisms to make information sources discoverable and accessible across organizational boundaries and communities of interest.

The Information Services provide *Capabilities* required to manage the enterprise information sphere. They provide a uniform way of representing, accessing, maintaining, managing, analysing, and integrating data and content across heterogeneous information sources.

The Information Services integrate the appropriate information in a timely and consistent manner, analysing and attempting to improve the quality of data, and ensuring consistency and *Integrity* of business-critical data and facts across the enterprise. They are able to consume and integrate information across the enterprise, and are able to validate and enforce pre-defined data quality rules.

The *Components* of the Information Services include:

- Information Access

- Information Aggregation

- Information Discovery

- Information Annotation

- Business Rules Management
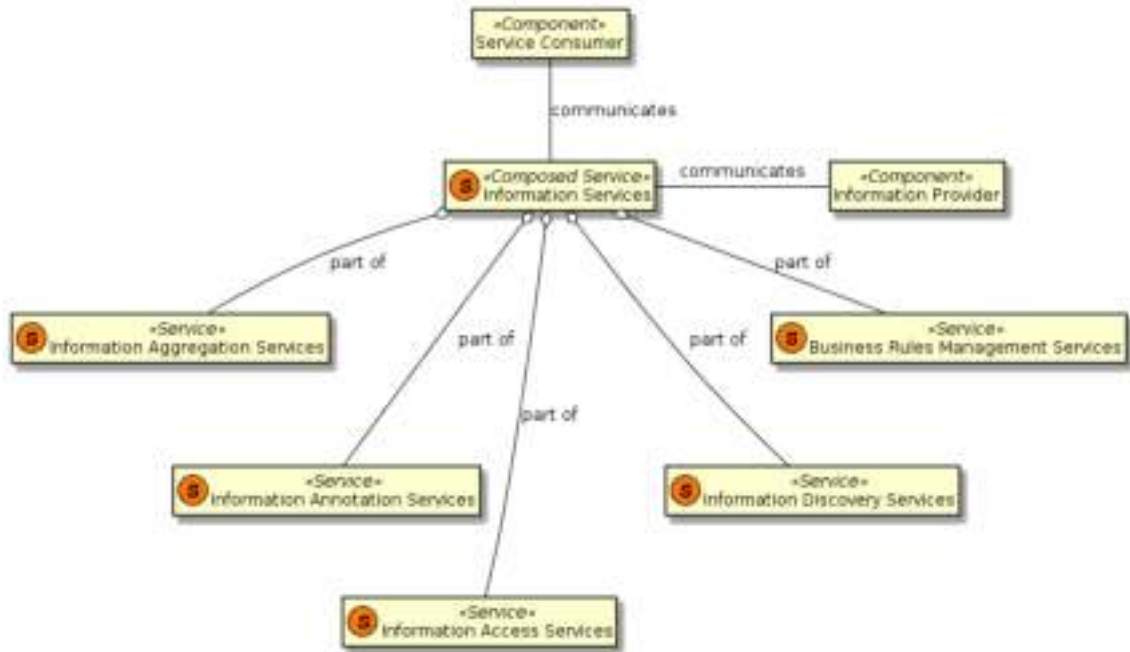
Figure 21 - Information Services *Composition* diagram

Requirement ID	SRS-3385
Verification method	Analysis
Requirement	The Platform SHALL make the semantics and structure of information products available using the Web Ontology Language (OWL).

Requirement ID	SRS-3386
Verification method	Analysis
Requirement	The Platform SHALL support the retrieval and manipulation of Resource Description Framework (RDF) data based on SPARQL Protocol and RDF Query Language (SPARQL) interface recommendations.

Requirement ID	SRS-3387
Verification method	Analysis
Requirement	The Platform will be compatible with Information Discovery Services SIP Proposal (see Ref. [NC3A RD-3297, 2011]).

3.5.1 Information Access

Information Access Services provide a generic *Capability* that can be configured as required to expose new information stores or sources in the required service

protocols and formats. The intent is to minimise custom services and allow agile provisioning of new *Capabilities* based on evolving operational requirements.

The Information Access Services expose information stores or sources into web enabled services.

By focusing on providing access to information from existing stores and sources, rather than on providing applications which use that information, Information Access Services de-couple the access to information from the use of the information. Since applications can use information in any number of ways to support any number of use cases, de-coupling the access to information from its use improves re-use.

Requirement ID	SRS-267
Verification method	Analysis
Requirement	The Platform SHALL implement mechanisms to expose data from data sources and data stores as web services.

Requirement ID	SRS-465
Verification method	Testing
Requirement	The Platform SHALL provide functionality for mapping or identifying synonymous information products (i.e. information products in different *Information Catalogues* providing the same information content). It will leave the information products intact and creates only the linkages between products.

Requirement ID	SRS-3407
Verification method	Testing
Requirement	The Platform SHALL be able to validate and enforce data quality rules.

3.5.2 Information Aggregation

The Information Aggregation Services pull together related information from multiple (often heterogeneous) sources and present it as a single information set. This allows the easy integration of the aggregated information into other contexts, such as business processes, mash-ups and business intelligence applications.

In support of the transformation needed for the information services, it will make use of the integration services (see Section 3.1).

Requirement ID	SRS-480
Verification method	Testing
Requirement	The Platform SHALL provide the means to define an aggregation of two or more data sources.

Requirement ID	SRS-479
Verification method	Testing
Requirement	The Platform SHALL provide the means to expose the integrated information as a new information source.

Requirement ID	SRS-3511
Verification method	Testing
Requirement	The Platform SHALL manage the data hierarchies, groupings, relationships such as parent-child relationships, and relationships between data.

3.5.3 Information Discovery

The Information Discovery Services provide the functionality to automate the discovery and retrieval of Information Products and their structure.

Information Products, in this regard, are aggregates of structured data. Discovered data is the result of a search upon an entire dataset, a search upon a subset of a dataset, or a search based on dataset and/or content *Metadata*.

Requirement ID	SRS-3413
Verification method	Testing
Requirement	The Platform SHALL provide the ability to query and search for information products.

Requirement ID	SRS-464
Verification method	Testing
Requirement	The Platform SHALL provide functionality for a search across multiple information sources.

Requirement ID	SRS-327
Verification method	Testing
Requirement	The Platform SHALL provide the mechanisms to collect, filter, prioritise and order the search results coming from the different search sources into a single result set.

Requirement ID	SRS-461
Verification method	Testing
Requirement	The Platform SHALL provide functionality to group information products based on their content.

Requirement ID	SRS-458
Verification method	Testing
Requirement	The Platform SHALL provide the means to create and maintain *Information Catalogues*.

Requirement ID	SRS-459
Verification method	Testing
Requirement	The Platform SHALL provide the means to uniquely identify information products associated with a catalogue.

Requirement ID	SRS-460
Verification method	Testing
Requirement	The Platform SHALL provide the means to specify the *Metadata* associated with an information product.

Requirement ID	SRS-462
Verification method	Testing
Requirement	The Platform SHALL provide the means to search *Information Catalogues* for a specific information product.

Requirement ID	SRS-463
Verification method	Testing
Requirement	The Platform SHALL provide details to the *Consumer* on how to obtain discovered information products, which can also encompass a referral to the full information product could be available through another service (i.e. via or service endpoint reference).

3.5.4 Information Annotation

The Information Annotation Services provide functionality for annotating or enhancing information objects with additional information such as: *Metadata*, tags, comments, attachments, relationship with other information objects and/or content.

An annotation is a collection of *Assertions* about one or more information objects and so must be able to uniquely reference those objects. Further, annotations are made by an *Entity*, *User*, system etc. and so information such as who created the annotation, when it was created, the confidence, *Reliability* and *Authenticity* of the *Assertions* must also be recorded.

The Information Annotation Services allow for persisting these annotations. Since the annotations are additional information that makes reference to existing information, an Information Annotation Service can be logically decoupled from the service providing that existing information.

The Information Discovery Services complement the Information Annotation Services by allowing *Information Consumers* to query not only the original information objects but also any annotations which relate to them.

Requirement ID	SRS-322
Verification method	Testing

Requirement	The Platform SHALL allow to enrich and annotate information.

Requirement ID	SRS-504
Verification method	Testing
Requirement	The Platform SHALL provide functionality to create, update, delete and store annotations associated with existing information objects.

Requirement ID	SRS-505
Verification method	Testing
Requirement	The Platform SHALL maintain *Metadata* on the annotations, including but not limited to: - who created it - when was it created - what is the history of the annotation

Requirement ID	SRS-506
Verification method	Testing
Requirement	The Platform SHALL provide functionality to retrieve annotations for individual information objects.

Requirement ID	SRS-507
Verification method	Testing
Requirement	The Platform SHALL provide functionality to retrieve annotations based on *User* defined search criteria.

3.5.5 Business Rules Management

Business Rules Management provides the *Capability* to support the creation, testing, management, deployment and maintenance of *Business Rules* in an operational environment.

Business Rules are statements describing a business/enterprise policy or procedure (e.g., discount calculation) and can be represented using formal language.

3.5.5.1 Authoring Environment

Requirement ID	SRS-3623
Verification method	Testing
Requirement	The Platform SHALL provide an authoring environment and *User* interface that allows for the management of *Business Rules*.

Requirement ID	SRS-510

Verification method	Testing
Requirement	The Platform SHALL provide the *Capability* to create, modify, store, delete, version and retrieve *Business Rules*.

Requirement ID	SRS-3627
Verification method	Testing
Requirement	The Platform SHALL support the archiving of rules that are no longer used in production.

Requirement ID	SRS-509
Verification method	Testing
Requirement	The Platform SHALL provide the *Capability* to evaluate and validate *Business Rules* against expected behaviour and results.

Requirement ID	SRS-3853
Verification method	Testing
Requirement	The Platform SHALL provide the *Capability* to monitor and record *Business Rules* execution.

Requirement ID	SRS-3630
Verification method	Testing
Requirement	The Platform SHALL enable *Business Rule* designers to test/execute rules and rulesets, and allow for running simulations using pre-loaded data.

Requirement ID	SRS-3631
Verification method	Testing
Requirement	The Platform SHALL notify *Business Rule* designers when conflicting *Business Rules* are written.

Requirement ID	SRS-3636
Verification method	Testing
Requirement	The Platform SHALL support intelligent code completion to assist in *Business Rule* authoring.

Requirement ID	SRS-3637
Verification method	Testing
Requirement	The Platform SHALL support contextual display (e.g., colour) of *Business Rules* to assist in human interpretation of the *Business Rules*.

Requirement ID	SRS-3638

Verification method	Testing
Requirement	The Platform SHALL enable rules to be developed using commercial Office tools (e.g., Microsoft Excel, Word).

3.5.5.2 Business Rules Engine

Requirement ID	SRS-3646
Verification method	Testing
Requirement	The Platform SHALL provide a runtime environment (*Business Rules* Engine) that allows applications to invoke *Business Rules*.

Requirement ID	SRS-3647
Verification method	Testing
Requirement	The Platform SHALL accept *Business Rules* in natural language.

Requirement ID	SRS-3648
Verification method	Testing
Requirement	The Platform SHALL accept *Business Rules* in rule tables.

Requirement ID	SRS-3666
Verification method	Testing
Requirement	The Platform SHALL allow *Business Rules* to be time bound such that new rules can be authored and put into production and not take effect until a specific date and time.

Requirement ID	SRS-3649
Verification method	Testing
Requirement	The Platform SHALL allow *Business Rules* to be time bound such that existing rules can be deprecated at a specific date and time.

Requirement ID	SRS-3650
Verification method	Testing
Requirement	The Platform SHALL support full forward and backward chaining.

Requirement ID	SRS-3652
Verification method	Analysis
Requirement	The Platform SHALL enable *Business Rules* to be maintained separately from application code.

Requirement ID	SRS-3657
Verification method	Testing
Requirement	The Platform *Business Rules* Engine SHALL support batch processing of data.

Requirement ID	SRS-3658
Verification method	Testing
Requirement	The Platform *Business Rules* Engine SHALL support online transaction processing of data.

Requirement ID	SRS-3854
Verification method	Analysis
Requirement	The Platform SHALL enable to export *Business Rules* as [OASIS WS-BPEL V2.0, 2007] and/or [OMG BPMN V2.0.2, 2013] for processes and workflow rules.

3.6 Identity and Security Services

The Platform increases the use of a common, centralised security framework. This improves the time to deliver systems, through more streamlined accreditation processes, while at the same time hardening the security posture. Administrators do not have to constantly be provisioning and de-provisioning accounts. Instead, a single *Identity* is used across NATO, with a single set of *Credentials*, providing Single Sign-On (SSO). The *Identity Information* is passed through different systems and services, delivering true, end to end *Authentication*. Access control is again centralised, and based on policy, thus widening the availability of potential consumers ("responsibility to share") while at the same time ensuring only those with the "need to know" can perform action on the data.

The requirements in this document are configured according to the 2016 CIS Security Capability Breakdown [NCIA TR/2014/NCB009779/05, 2015]. They specifically cover the class of *Capabilities* entitled *Identity and Access Management*, as shown in the figure below.
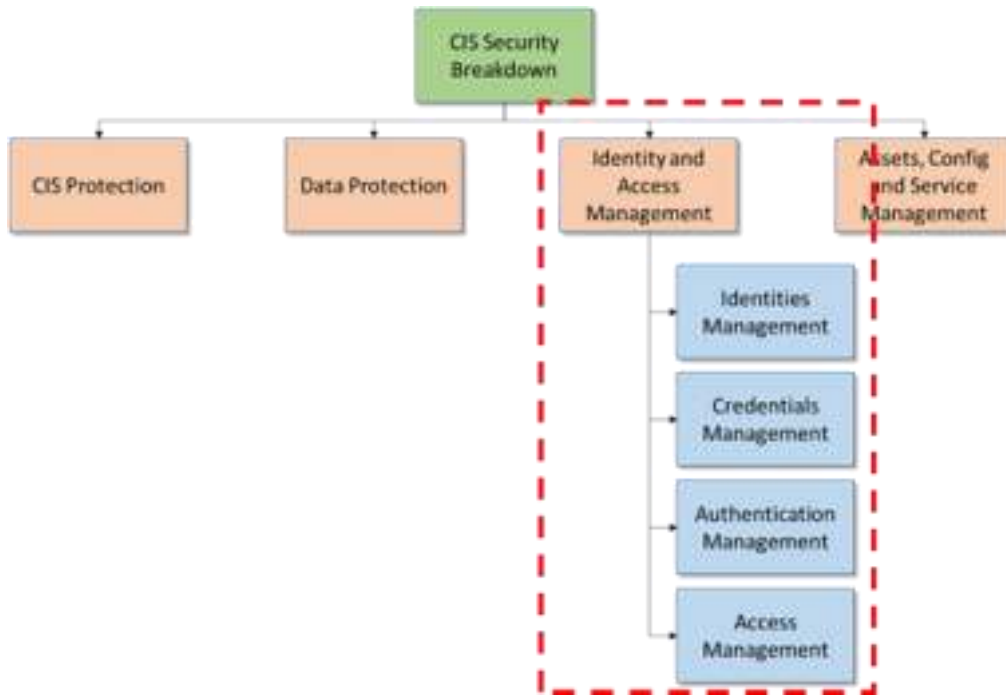
Figure 22 - Security Capability Breakdown

The overall IAM *Capability* is a framework that facilitates the management of electronic identities, and the assignment of their rights and *Privileges*.

Within IAM an *Entity* is an item inside or outside an information and communication technology system, such as a person (*User*), an organisation, a device, a subsystem, or a group of such items that has recognizably distinct existence. An *Identity* is defined as a set of *Attributes* related to an *Entity* [ISO/IEC 24760-1, 2011]. Note that an *Entity* (such as a *User*) can have many different *Identities*, each of which is a distinct collection of *Attributes* related to the *Entity*.
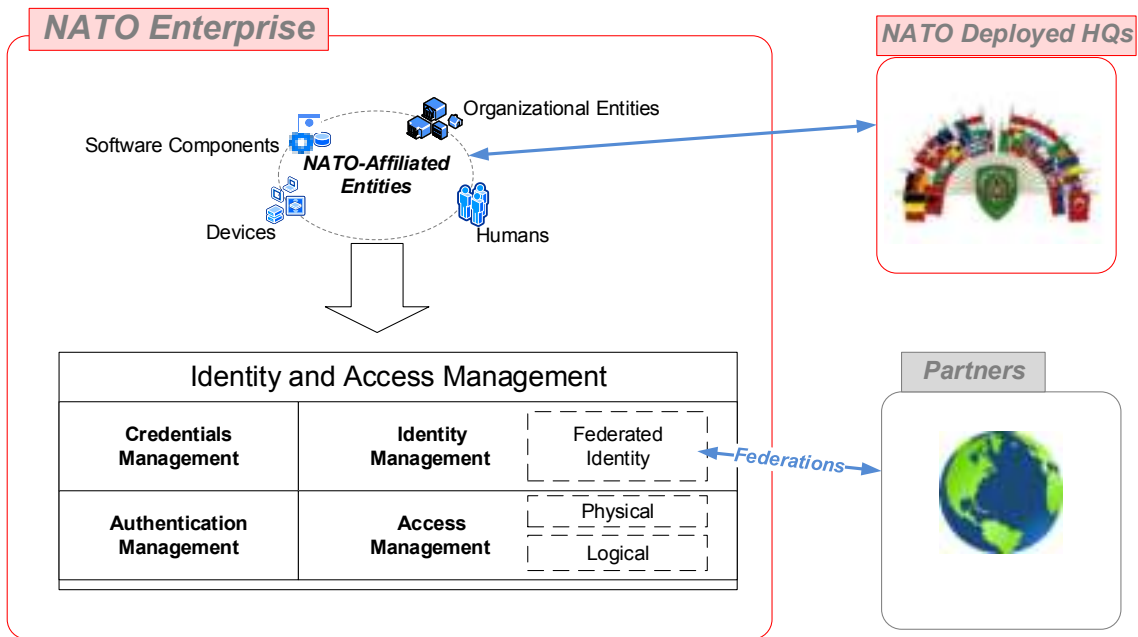
Figure 23 - *Identity and Access Management* **Breakdown**

The management and usage of *Identities* is one of the key aspects of the Platform. The Platform will provide a centralised IAM *Capability* for the NATO Enterprise, in order to:

- Provide the toolset to model and control the NATO internal Enterprise-level IAM business processes, workflows, and data exchange in support of logical and physical access control;

- Integrate and support the existing local IAM *Capabilities* across the NATO Enterprise;

- Support interactions with IAM *Capabilities* external to NATO (e.g., with Partner Nations).

The elements of IAM include:

- Identities Management

- *Credentials* Management

- Authentication Management

- Access Management

Requirement ID	SRS-3711
Verification method	Analysis
Requirement	The Platform SHALL provide a framework for IAM *Capability* at the NATO Enterprise level, consisting of coherent solutions and processes, fully integrated with existing *Capabilities* such as NEDS.

Requirement ID	SRS-3715
Verification method	Analysis

Requirement	The Platform SHALL leverage NEDS mechanisms for affiliation, data processing, and data exchange with the NATO Physical and Logical Access Control system(s).

Requirement ID	SRS-3340
Verification method	Analysis
Requirement	The Platform SHALL comply with the technical specifications as defined in the SIP for Security Services (see Ref. [NCIA AI 06.02.01, 2015]).

Requirement ID	SRS-3343
Verification method	Analysis
Requirement	The Platform SHALL comply with the technical specifications as defined in the SIP for REST Security Services (see Ref. [NCIA AI 06.02.02, 2015]).

Requirement ID	SRS-3341
Verification method	Analysis
Requirement	The Platform SHALL comply with the technical specifications as defined in the SIP for *Security Token Services* (see Ref. [NCIA AI 06.02.03, 2015]).

Requirement ID	SRS-3342
Verification method	Analysis
Requirement	The Platform SHALL comply with the technical specifications as defined in the SIP for *Policy Enforcement Point* (see Ref. [NCIA AI 06.02.04, 2015]), and the technical specifications as defined in the SIP for REST Security Services (see Ref. [NCIA AI 06.02.02, 2015]).

Requirement ID	SRS-3348
Verification method	Analysis
Requirement	The Platform SHALL comply with the technical specifications as defined in the SIP for Enterprise Directory Services (see Ref. [NCIA AI 06.02.05, 2015]).

3.6.1 Identities Management

Entities affiliated with any NATO organisation have a unique and standardised Enterprise *Identity* within the NATO Enterprise.

The Enterprise *Identity* links and synchronises all *Identities* provisioned for the *Entities* in different *Contexts* (networks, systems) and ensures that the status of *Identities* corresponds to the current status of an *Entity's* affiliation with the NATO organisation.

Identity Attributes of *Entities* are coherently managed and synchronised across the NATO Enterprise and shared with other organisations to enable access decisions.

The *Identity and Access Management* processes maintain this unique Enterprise *Identity Information* for all NATO-affiliated *Entities* (which can include people (*Users*), devices, services or organisations). The Enterprise *Identity* is used to reflect the status of *Entity's* affiliation with NATO during the *Identity's* lifecycle, and to bind a NATO-affiliated *Entity* with other (*Context*-specific) *Identities* of the *Entity*.

It also provides services for FS (or other applications) to query *Identity Information* about *Users*.

The IAM *Capability* is supported by governance giving direction through strategy, policy, and standards, and includes the ability to:

- Manage the lifecycle of *Identities* including for example creation of new *Identities*, maintenance of the *Attribute* values over time, and the termination of *Identities*

- Ensure coherence of all *Identities* representing the same *Entity*

- Separate *Identities* representing the same *Entity* where needed (privacy)

- Support the management of credentials (evidence of an *Entity's Identity*) used to authenticate

- Manage the *Trust* (assurance) related to the different *Identities*

- Manage business functions profiles (e.g., organisational *Roles*) for *Entities*

- Authenticate (verify a claimed or asserted *Identity* using *Credentials*)

Requirement ID	SRS-608
Verification method	Testing
Requirement	The Platform SHALL monitor and manage the lifecycle of Enterprise *Identity* for the NATO Enterprise.

Requirement ID	SRS-2977
Verification method	Testing
Requirement	The Platform SHALL allow *Authorised Users* (i.e. the Platform Administrator) to manage (create, update, delete) the Platform *User* Accounts, *Credentials* (e.g., password), details, and manage general access *Privileges* of individual *User* Accounts.

Requirement ID	SRS-584
Verification method	Testing
Requirement	The Platform SHALL allow for the definition and maintenance of the lifecycle state *Attribute* for

	Enterprise Identities (e.g., unknown, established, active, suspended, archived).

Requirement ID	SRS-601
Verification method	Testing
Requirement	The Platform SHALL allow the definition, enforcement and compliancy verification of policies for creation and maintenance of *Identity Attributes*.

Requirement ID	SRS-3722
Verification method	Testing
Requirement	The Platform SHALL use NEDS as the broker of identity data from *Authoritative Data Source* for different types of *entities* as follows: • people • organisational *Entities* • facilities • Roles • groups • devices • software • policy

Requirement ID	SRS-619
Verification method	Testing
Requirement	The Platform SHALL use NEDS to enable searching the *Identity Repository* based on any *Identity Attribute*.

3.6.1.1 Identity Federation

NATO is a "federated" environment, with multiple governance and security domains, provided by the Nations and by NATO itself, potentially linked together. In an *Identity Federation* it is possible that a service *Consumer* and a service provider can belong to different *Contexts* (domains), but still need to be authenticated and authorised. In this case, the information necessary to authenticate an *Entity* may not be resident in the service's domain.
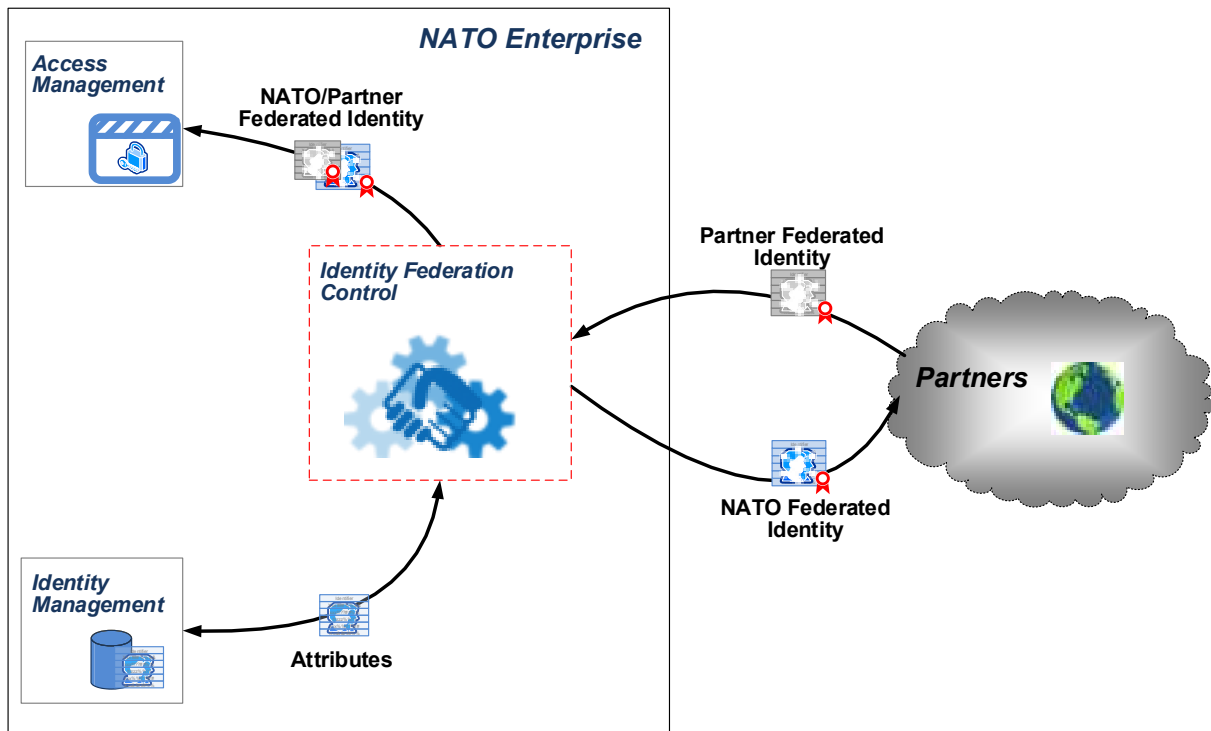
Figure 24 - *Identity Federation*

Federated Identity is a term used when two or more organisational units share *Identities* rather than each creating their own *Identity* representing the same *User*. *Identity Federation* supports the establishment and management of *Identity Trust* across the NATO Enterprise and to the extended network of NATO affiliates and enable *Identity* data to traverse across *Contexts*.

In *Federation* scenarios, the *Identity Federation Capabilities* leverage partner IAM capabilities to manage *Identities* of *Entities* external to NATO and to authenticate them. *Identity Federation Capabilities* also enable re-use of NATO *Identities* beyond the scope of *Identity* original NATO *Context*.

Requirement ID	SRS-359
Verification method	Testing
Requirement	The Platform SHALL provide the *Capability* to define, establish and manage technical *Trust* between *Federated Identity Service Providers*.

3.6.1.2 Allied Replication Hub

Federation with entities external to NATO can also be achieved by sharing a common repository /directory service, which allows partners to publish their information, and retrieve the information shared by others. This is referred to as the Alliance Replication Hub (ARH; see figure 25)

This ARH is to provide the ability for:

a. NEDS to publish data to be shared with NATO Nations and partner

b. NEDS to retrieve data published by NATO Nations and partners

c. Nations and partners to publish data to be shared with the NATO environment

d. Nations and partners to retrieve data published by NATO, NATO Nations and partners
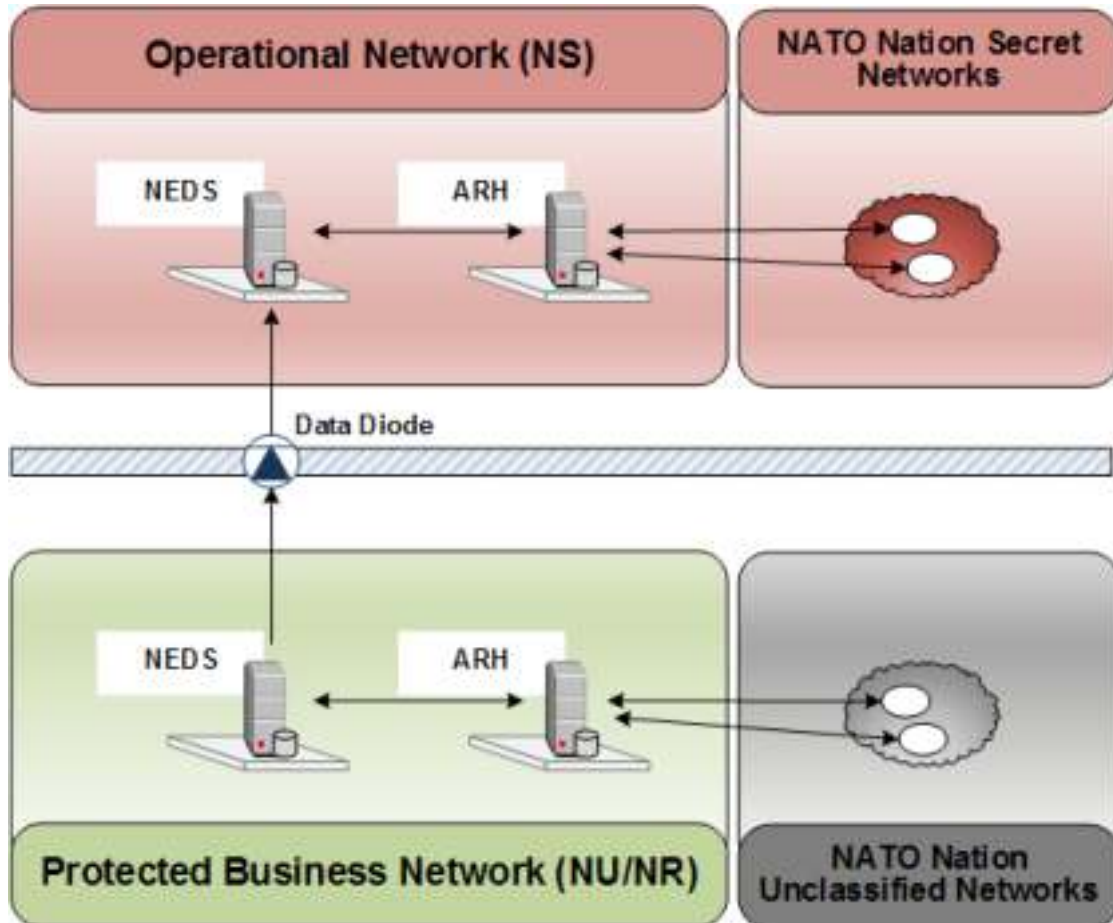
Figure 25 - ARH on the different networks

Requirement ID	SRS-570
Verification method	Testing
Requirement	The Platform SHALL support sharing of *Identity* data with external trusted partners by providing a dedicated instance of a repository.

Requirement ID	SRS-4223
Verification method	Testing
Requirement	The Platform SHALL provide an LDAP over TLS (LDAPS) interface for NATO and partners to push and pull information.

Requirement ID	SRS-4224
Verification method	Analysis

Requirement	The Platform SHALL use the [CCEB ACP133D, 2014] schema.

3.6.2 Credentials Management

Entities are issued with *Credentials* that support a high level of *Identity* assurance. The *Credential* Management *Capability* issues and controls the lifecycle of *Credentials* across the Platform.

Credential controls make use of the integration with *Identity and Access Management Capabilities* and processes for *Identity* correlation and binding. They rely on Enterprise *Identities* to receive and use relevant *Identity Attributes*, extracted from *Authoritative Data Sources*.

Credential Management is fundamentally the ability to collect/create, assess, and handle *Credentials*. These are *Attributes* that can be used as evidence of a claimed or asserted *Identity* and/or entitlements in order to enable an *Entity* to be associated with an *Identity* (see also [NCIA TR/2015/NCB009779/09, 2015]).

For NATO entities, the management of *Credentials* will not be conducted by the Platform. The two most prevalent credential types, Kerberos and X.509 tokens, will be managed by the Active Directory and NATO PKI systems respectively. However, for non-NATO *Entities* that are unable to provide Federated *Credentials* (as described above), some level of *Credential* management will be necessary.

The purpose of the *Credential* Management *Capability* in this case will allow *Users* to authenticate to *Identity Providers* in the NATO domain in order to access NATO assets (resources) and collaborate with NATO *Users*. This will be after the *Identity and Access Management Capability* has controlled the process for creating a new (non-NATO) entity in a dedicated (or separated) area of the *Identity Repository*. The *Credentials* management *Capability* allows the *User* to modify their own *Credentials*, or to request modification by administrators.

Requirement ID	SRS-2996
Verification method	Testing
Requirement	The Platform SHALL manage credential details (e.g., login and password, PKI certificate), enabling authentication for *Users* that cannot be authenticated through Active Directory

3.6.3 Authentication Management

3.6.3.1 Authentication

Authentication is a formalised verification process that, if successful, results in authenticated (confirmed, trusted) *Identity* for an *Entity*.

The *Authentication* process involves test of one or more *Identity Attributes* provided by an *Entity* to determine, with the required level of assurance, their correctness. Simply put, *Authentication* is the process that validates an *Entity* is who it *Claims* to be.

There are five categories of *Users* which may want to access the Platform and its services. They are:

a. Category I.: NATO *Users* who can authenticate to a NATO Active Directory;

b. Category II.: NATO *Users* who cannot authenticate to a NATO Active Directory but can present a SAML token issued by a trusted *Security Token Service*;

c. Category III.: NATO *Users* who cannot authenticate to the a NATO Active Directory and cannot present a SAML token issued by a trusted *Security Token Service*;

d. Category IV.: Non-NATO *Users* (e.g. national users) who can present a SAML token issued by a trusted *Security Token Service*;

e. Category V.: Non-NATO *Users* (e.g. national *Users*) who cannot present a SAML token issued by a trusted *Security Token Service*.

The Platform *Identity* and Security Services deal directly with **Categories I**, **II** and **IV**. The system also supports Category III and V *Users*; however, there is an "out of band" process which initiates the management of these types of *Users*. Category I and II are normal internal *Identity and Access Management* patterns, while Category IV represents the main *Federation* scenario (see below).

Requirement ID	SRS-3028
Verification method	Testing
Requirement	The Platform SHALL allow an access control component to require *Authentication* for access to a specific resource.

Requirement ID	SRS-356
Verification method	Testing
Requirement	The Platform SHALL support as a minimum the following *Authentication* mechanisms: • basic (Username, password) *Authentication* • open standards-based *Claims*-based *Authentication*, to include • SAML for SOAP/WS-Security • OAuth for REST • OpenID Connect • WS-Federation • forms-based Authentication to the Identity Service Provider • PKI certificates-based Authentication to the Identity Service Provider • Kerberos • multi-factor (multi-credential) *Entity Authentication*

Requirement ID	SRS-4069
Verification method	Testing
Requirement	The Platform SHALL allow configuring unauthenticated access to a resource.

Requirement ID	SRS-3048
Verification method	Testing
Requirement	All Platform *Authentication* controls (including libraries that call external *Authentication* services) SHALL have a centralised implementation, used for all resources.

Requirement ID	SRS-
Verification method	
Requirement	

Requirement ID	SRS-3038
Verification method	Testing
Requirement	All *Authentication* controls SHALL be enforced on the server side.

Requirement ID	SRS-2976
Verification method	Testing
Requirement	The Platform SHALL uniquely Identify and Authenticate *Users*.

Requirement ID	SRS-355
Verification method	Testing
Requirement	The Platform SHALL allow *Authentication* of a *User* to an application (*Relying Party*).

Requirement ID	SRS-187
Verification method	Testing
Requirement	The Platform SHALL enable sharing of *Identity* data among multiple relying parties as a part of an authenticated *Entity* session, implementing Single Sign-On (SSO) across the Platform for one or more services.

Requirement ID	SRS-338
Verification method	Testing

Requirement	The Platform SHALL allow the *Entity* to leave the current *Authentication* session (log out), including *Logging* out from multiple applications, services or resources in one step.

Requirement ID	SRS-227
Verification method	Testing
Requirement	The Platform SHALL support different methods of *User Authentication* depending on *Authentication* policies and required level of *Authentication* assurance.

3.6.3.2 Federated Authentication

Federation is described in section 3.6.1.2 above. The approach to federated *Authentication* for the Platform is to implement a *Trust* relationship between the security services in the federated domains. When federated *Trust* is established, an *Identity Service Provider* in one domain can make use of a *Security Token Service* (STS) to issue an *Assertion* of *Identity*, also called a *Security Token*, on behalf of an *Entity*, which can be accepted by the *Authentication* service in another domain.

A *Trust* relationship between federated domains may be one-way (Domain X accepts the *Security Tokens* of Domain Y, but not vice-versa) or two-way (both domains accept the other's *Security Tokens*).

Requirement ID	SRS-3744
Verification method	Testing
Requirement	The Platform SHALL support web-based *Authentication* in *Federations* by: - Providing federated *Identities* for the authenticated NATO-affiliated *Entities* - Validating and accepting federated *Identities* from NATO-trusted partners - Using federated *Identities* in *Authorisation* processes.

Requirement ID	SRS-3437
Verification method	Testing
Requirement	The Platform SHALL be able to establish a *Trust* relationship between *Federated Identity* service providers in order to authenticate *Users* from other domains, by: - using a *Security Token* issued by a trusted *Federated Identity* Provider - mapping *Attributes* from a federated Identity Service Provider to other *Attributes* according to predefined rules

	• reissuing a *Security Token* that is trusted internally containing the appropriate *Attribute* values

Requirement ID	SRS-361
Verification method	Testing
Requirement	The Platform SHALL expose an Identity Service Provider interface to its service providers (e.g., enterprise applications) supporting multiple *Authentication* protocols, as specified in SRS-356.

Requirement ID	SRS-362
Verification method	Testing
Requirement	The Platform SHALL expose a Service Provider interface able to consume *Identity Information* provided by external *Identity Service Providers* after successful *User Authentication*.

Requirement ID	SRS-364
Verification method	Testing
Requirement	The Platform SHALL mediate between *Claims*-based *Authentication* protocols (see SRS-356) used by external *Federated Identity Service Providers* and the identity providers configured in the Platform.

Requirement ID	SRS-363
Verification method	Testing
Requirement	The Platform SHALL enable a *User* to authenticate through a chain of trusted *Identity Service Providers* in order to get access to the protected resources made available to the *User* within an established *Federation*.

3.6.3.3 Security Token Service (Broker and Resource)

The Platform applies a Token-based security mechanism, regardless of whether the implementation of services is based upon SOAP, REST or another protocol.

The usage of *Security Tokens* allows the actors to propagate security data, as the token contains the relevant *Attributes* about an *Entity*, or *Claims*, in a secure manner, providing *Trust* and assuring the *Integrity* of the content.

When a service *Consumer* intends to access a protected service an exchange of tokens takes place that passes on the *Identity*, *Context* and all necessary information a service provider needs to grant access to the *User*.

The *Security Token Service* (STS) generates, validates and exchanges *Security Tokens*, and authenticates the end-user before issuing a token. It can also be

federated with other STS in other domains (see above). In OAuth this is known
as an *Authorisation Server*.
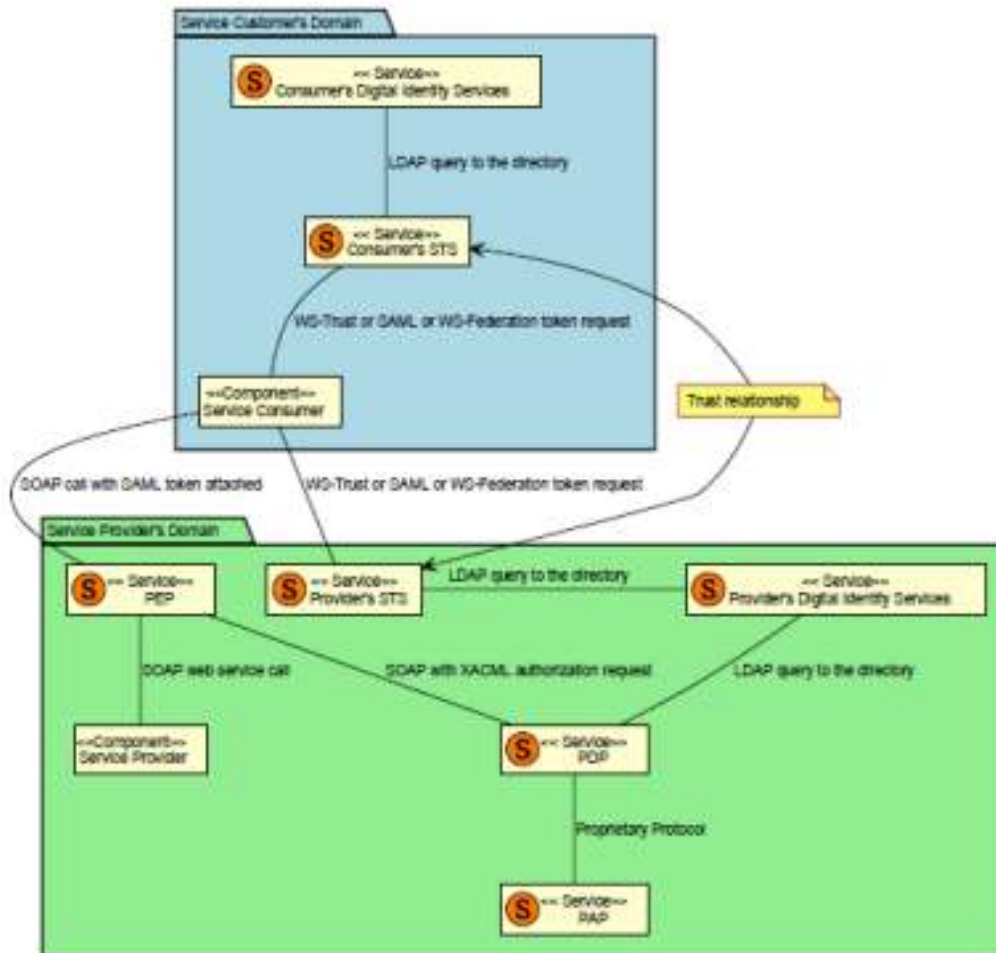
Figure 26 - STS *Federation Composition* diagram

Requirement ID	SRS-331
Verification method	Analysis
Requirement	The Platform SHALL provide a token-based security mechanism.

Requirement ID	SRS-3447
Verification method	Testing
Requirement	The Platform SHALL ensure that the *Security Token Service* on the Platform is configured to support the open standards-based *Claims*-based *Authentication* by default as its *Authentication* methods for all *Relying Parties*.

Requirement ID	SRS-186
Verification method	Testing

Requirement	The Platform SHALL be able to issue a new *Security Token*, including new proof information, based on the *Credential* provided/proven in the request.
Requirement ID	SRS-188
Verification method	Testing
Requirement	The Platform SHALL be able to renew a previously issued token when expiration is presented (and possibly proven) and return a token with new expiration information.

Requirement ID	SRS-3442
Verification method	Testing
Requirement	The Platform SHALL allow an exchange of tokens to take place between the requestor and the *Relying Party* that passes on the *Identity*, *Context* and all necessary information a *Relying Party* needs to grant access.

Requirement ID	SRS-183
Verification method	Testing
Requirement	The Platform SHALL allow *Authorised Users* to configure which *Assertions* are issued to individual *Relying Parties* within each *Security Token*.

Requirement ID	SRS-184
Verification method	Testing
Requirement	The Platform SHALL be able to configure other aspects of token-issuance, such as the lifetime of the token and which certificates are used.

Requirement ID	SRS-3503
Verification method	Analysis
Requirement	The Platform SHALL support both SAML 2.0 and OAuth 2.0 token types.

Requirement ID	SRS-3444
Verification method	Testing
Requirement	The Platform SHALL hide internal *Security Token Service* instances from Entities in domains beyond the NATO Enterprise.

Requirement ID	SRS-3445
Verification method	Testing

Requirement	The Platform SHALL provide dedicated *Security Token Services* for Entities from domains beyond the NATO Enterprise.

Requirement ID	SRS-3448
Verification method	Testing
Requirement	The Platform SHALL be able to configure the *Security Token Service* for enabling a one-way *Trust* with other *Security Token Services*.

Requirement ID	SRS-3438
Verification method	Testing
Requirement	The Platform SHALL perform required *Identity* token transformations (*Attribute* mappings) between tokens obtained from external *Identity Service Providers* and provided to local Service Providers.

Requirement ID	SRS-2121
Verification method	Testing
Requirement	The Platform SHALL allow the *Security Token Service* in the domain of the service provider to place further constraints on the abilities and *Privileges* of consuming services and *Users* from the federated *Consumer* domain.

Requirement ID	SRS-345
Verification method	Testing
Requirement	The Platform SHALL ensure that the *Security Token Service* can be configured to limit issuance of *Security Tokens* for acceptance by a particular *Relying Party* or a particular group of *Relying Parties*.

3.6.4 Access Management

Access Management (which includes *Authorisation*) is provided as an external, centralised *Policy-Based Access Control* service that allows for the "up front" definition of a comprehensive set of access control policies and then grants or denies access to resources based on these policies.

The Platform provides a *Capability* for creating, maintaining and evaluating access control policies that specify how information about resources, *Users*, services and devices (e.g., their entitlements and *Privilege Attributes*), and the environmental *Context* should be combined in order to determine when to grant or deny access to a physical and/or logical resource.

Roles are the basis for *Role-Based Access Control* (RBAC). *Roles* are used in the Access Management process in support of the *Identity* lifecycle, enabling control of provisioning; they can also be used in support of processes related to

the access control, for example to formulate access control policy. Management of *Roles*, and usage of *Roles* for both *Identity* provisioning and access control, is a core function of the Platform.

The decision which model (what type of policies) to use depends on required granularity of access control, required ease of administration, overall organisation policies, etc. In many cases hybrid approach may be utilised: RBAC often provides a sufficient level of granularity to define access policies for internal resources; however, an application that has an extensive remote *User* population may require additional access mechanisms capable of handling *Attribute-Based Access Control* (ABAC) contextual information.
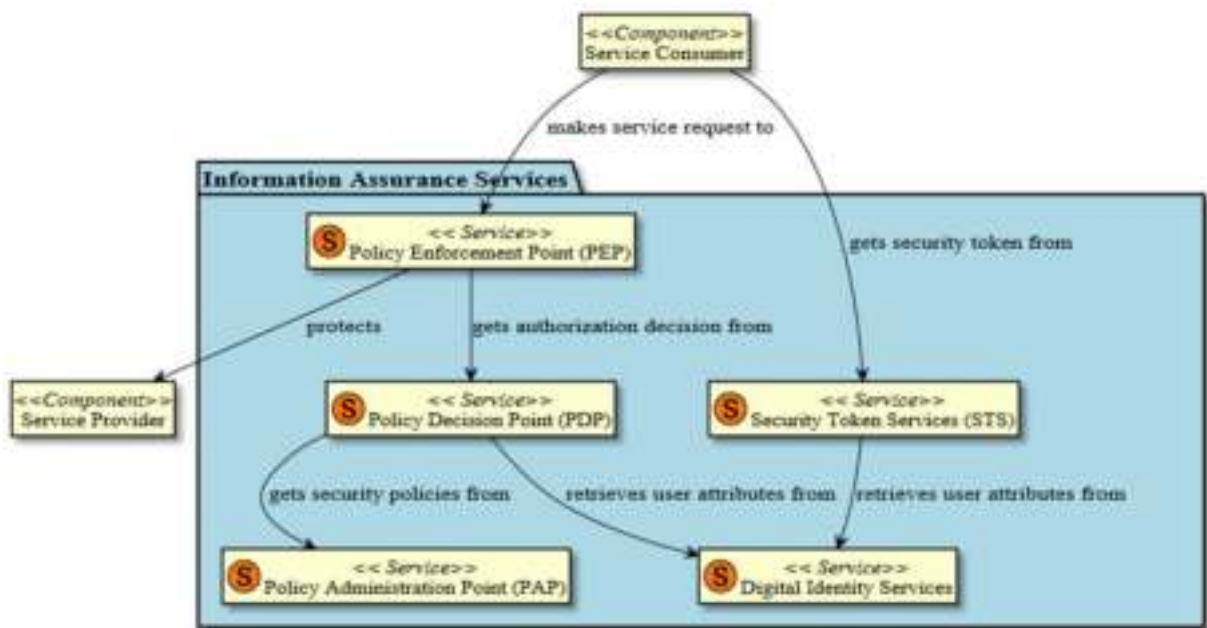
Figure 27 - Security Services (*Authorisation*) *Composition* diagram

The primary *Components* that the Platform will implement in support of *Authorisation* are one or more each of:

- Policy Enforcement Points (PEP)- this can be an Authorisation Server in REST parlance

- Policy Decision Points

- Policy Administration Points

Requirement ID	SRS-3066
Verification method	Testing
Requirement	The Platform SHALL ensure that *Users* can only access functions or services for which they possess specific *Authorisation*.

Requirement ID	SRS-3067
Verification method	Testing

Requirement	The Platform SHALL ensure that *Users* SHALL only access URLs for which they possess specific *Authorisation*.

Requirement ID	SRS-3068
Verification method	Testing
Requirement	The Platform SHALL ensure that *Users* SHALL only access information for which they possess specific *Authorisation*.

Requirement ID	SRS-2133
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to retrieve access rights bound to the Enterprise *Identity* of an *Entity*.

Requirement ID	SRS-223
Verification method	Testing
Requirement	The Platform SHALL support usage of different access control modes, best suited for a given resource, including: - Discretionary Access Control (DAC) - Role-Based Access Control (RBAC) - Attribute-Based Access Control (ABAC) *Context*-Aware Access Control

Requirement ID	SRS-4011
Verification method	Testing
Requirement	The Platform SHALL allow for ABAC according to the following guidelines: *Authorisation* decisions to be based on composable, machine-readable policies. *Authorisation* decisions to be based on *Attributes* of the following: - Actor; - Resource; - Action; - Environment; - Others, by configuration. *Attributes* to be retrieved from known repositories, when they are not included in the request. - Obligations on the PEP to be returned with the *Authorisation* decision.

Requirement ID	SRS-2992
Verification method	Testing
Requirement	The Platform SHALL allow for RBAC according to the following guidelines: • *Users* are associated with *User Roles* and also with organisations. • *User Roles* determine the functions and types of objects available to the *User*. • organisations determine the data available for use by the available functions. • a *User* has permission on a particular data item only if the *User* has an authorised *Role* and is a member of that organisation.

Requirement ID	SRS-3099
Verification method	Testing
Requirement	The Platform Access Control function SHALL deny access by default.

Requirement ID	SRS-3077
Verification method	Testing
Requirement	All Platform *Authorisation* controls (including libraries that call external *Authorisation* services) SHALL have a centralised implementation enforced on the server side, used for all resources.

Requirement ID	SRS-232
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to define and enforce various overall access management policies (e.g., governing creation and maintenance of *Privilege* and entitlement *Attributes*, required *Authentication* levels, required *Event* collection levels, etc.).

Requirement ID	SRS-193
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to configure the location (e.g., URI) of the policy store.

Requirement ID	SRS-194
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to configure the location (e.g., URI) of the *Attribute* store.

Requirement ID	SRS-2980
Verification method	Testing
Requirement	The Platform SHALL lock *User* access after a configurable number of unsuccessful *Authentication* attempts.

3.6.4.1 Policy Enforcement Point

The *Policy Enforcement Point* (PEP) Services protect other services by providing a logical entry point that serves as an intermediary between a call from a service *Consumer* to a service provider.

The PEP can either be deployed as a separate device or appliance (or *Authorisation Server* for REST implementations) that sits between the *Consumer* and provider, or as an inline *Component* that is deployed as part of the container infrastructure of the service (as an integral part of the *Resource Server* for REST implementations).

When trying to access the protected service endpoint, the *Entity* may be asked by the PEP to provide a valid token (which has been authenticated in the platform - see above), or it may be automatically included with the request. The PEP validates the token, and extracts the relevant *Attributes*, which are then sent to the *Policy Decision Point* (see below) for an *Authorisation* decision. The PEP matches the request to the relevant policy, retrieves any additional required *Attributes* from the *Attribute* Service, and returns a signed decision as to whether or not the *Consumer* is granted to access the protected service. If so the *Entity's* request(s) gets redirected to the targeted service.
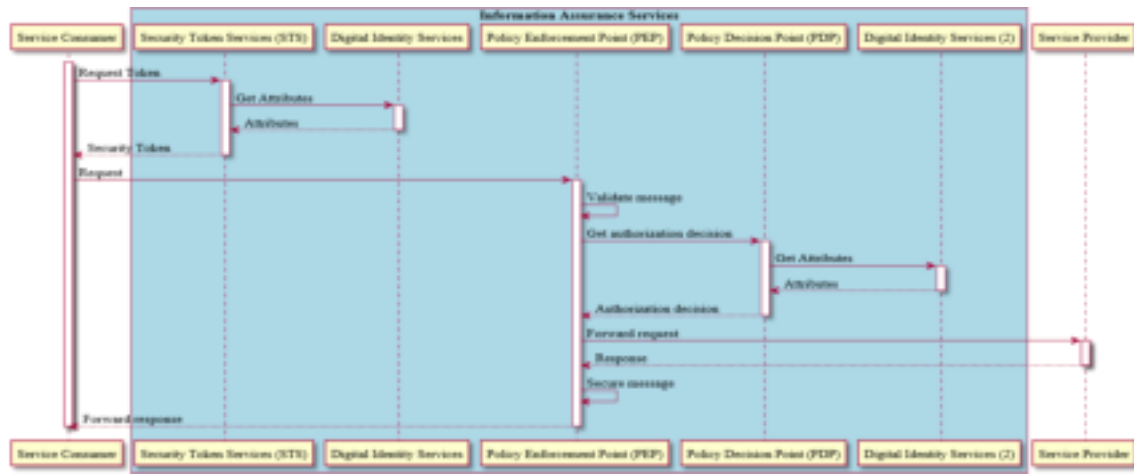
Figure 28 - Security Services (*Authorisation*) sequence diagram
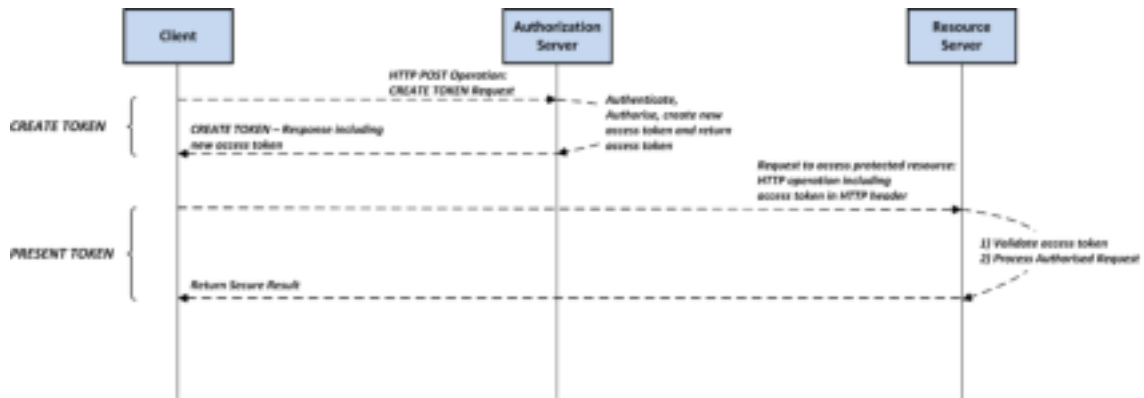
Figure 29 – REST-based Security Services (*Authorisation*) sequence diagram

Requirement ID	SRS-3757
Verification method	Testing
Requirement	The Platform SHALL enforce *Authorisation* decisions for requests to protected resources.

Requirement ID	SRS-190
Verification method	Testing
Requirement	The Platform SHALL apply required security mechanisms to the responses returned from protected services (signing, encryption).

Requirement ID	SRS-191
Verification method	Testing
Requirement	The Platform SHALL validate the security elements of the incoming message, including message encryption and signature, validity of the *Security Token*, and that the *Security Token* is from a trusted issuer.

Requirement ID	SRS-3460
Verification method	Testing
Requirement	The Platform provided PEP instances SHALL as a minimum support .NET framework and Java Runtime Environment.

3.6.4.2 Policy Decision Point

The *Policy Decision Point* (PDP) Services provide *Authorisation* decisions by evaluating digital policies against the *Attributes* of an *Authorisation* request. They base their decisions on *Authorisation* policies obtained from *Policy Administration Points* (PAP).

The request can contain *Attributes* about the subject of the request (the service *Consumer*), the object of the request (the resource that is being accessed), the action that is being performed and other *Attributes* not related to the subject or

resource (the "environment"). A decision is returned to the requesting *Entity*, which can contain further obligations about how the request is to be treated.

Requirement ID	SRS-3756
Verification method	Testing
Requirement	The Platform SHALL provide *Authorisation* (*Policy Decision Point*) functionality to evaluate *Authorisation* decisions based on access policies associated with requested resource, authenticated requestor *Identity Information* and other data required by access policies.

Requirement ID	SRS-3458
Verification method	Analysis
Requirement	The Platform SHALL allow external *Policy Decision Points* to be called for evaluation security policies associated with protected services.

Requirement ID	SRS-196
Verification method	Testing
Requirement	The Platform SHALL return any further obligations that are required in order for the requester to access the service provider.

Requirement ID	SRS-198
Verification method	Testing
Requirement	The Platform SHALL retrieve any further *Attributes* from the appropriate *Attribute* store that are required by the policy in order to make a decision.

Requirement ID	SRS-199
Verification method	Testing
Requirement	The Platform SHALL apply required security mechanisms to access requests (signing, encryption).

3.6.4.3 Policy Administration Point

The *Policy Administration Point* (PAP) Services provide functionality required to compose, modify, manage, and control access control policies in a standard policy exchange format, enabling the policy enforcement through the *Policy Enforcement Point* (PEP) and *Policy Decision Point* (PDP) *Components*.

Requirement ID	SRS-3424
Verification method	Testing
Requirement	The Platform SHALL provide Access Policy Administration functionality to create, disseminate, modify, manage, and maintain hierarchical rule sets to control digital resource management, utilisation, and protection in a standard policy exchange format.

Requirement ID	SRS-221
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to evaluate (test) access control policies for any combination of resource, *Identity* and other access decision factors.

Requirement ID	SRS-235
Verification method	Testing
Requirement	The Platform SHALL provide tools to support verification (testing) of access management data compliancy with overall access management policies.

Requirement ID	SRS-205
Verification method	Testing
Requirement	The Platform SHALL provide the means to store and administer access control policies via one or more policy store repositories.

3.6.4.4 Privilege Management

The Authorization services also make use of the *Privilege Management* (or Digital *Identity*) *Components*.

Privilege Management is the process of establishing and maintaining *Entity Privileges* to protected resources: accounts, entitlements and *Roles* that comprise an *Entity's* access profile. These *Attributes* complement *Identity Attributes*, which represent characteristics about an *Entity* that make it possible to uniquely identify it, and which are used in *Authorisation* processes.

Privilege Management in NATO is anchored by the NATO Enterprise Directory Service (NEDS).

NEDS is a cornerstone *Capability* of the Platform, providing core directory functionalities while acting as the *Authoritative Data Source* of *Identity Information* within the NATO enterprise. The combination of *Identity Information* from NEDS and the policies established via Access Management provide robust *Entity Privilege Management Capabilities*.

NEDS provides highly-available Directory Service elements in distinct networks. These elements are interconnected with each other, and affiliated with both authoritative affiliation sources, which are crucial for *Identity* lifecycle management, as well as systems and applications consuming the identities. The architectural goal is to stimulate systems to interface with NEDS as the enterprise-wide trusted source and broker for *Identity Information*. In this manner *Identity and Access Management* can be centralised, rather than provided through multiple systems.

NEDS also provides the *Capability* to share trusted *Identity* information between different systems and to Enterprise *Users*. The information on *Identities* (e.g. people, organizations, and devices) is retrieved from different, authoritative sources (e.g. the Automated Personnel Management System (APMS)). NEDS covers the whole enterprise (including NATO HQ) and is the standard way to exchange *Identity Information* across NATO.

Information can be synchronised between different affiliate systems and automated workflows can be created, including provisioning and de-provisioning of *User* Accounts. The Security Services also retrieve information from the NEDS directory, which in that context is also known as the Policy Information Point (PIP).

Finally, NEDS' *Federation Capabilities* enable synchronisation with internal and external partners (e.g. NATO Nations).

The Platform augments NEDS with additional services and tools to manage *Identity* within the NATO Enterprise.

Requirement ID	SRS-3752
Verification method	Testing
Requirement	The Platform SHALL provide organisational *Role* Management functionality to include *Role* modelling, manual and automated *Role* assignment, and a routine/scheduled *Role* validation.

Requirement ID	SRS-2994
Verification method	Testing
Requirement	The Platform SHALL allow two or more *Users* to have the same *Roles* within the Platform simultaneously.

3.6.5 IAM Process Management

Identity and Access Management Processes are the business processes to plan and control processing of *Attributes* used for *Entity Identification*, *Authentication*, authorisation, and *Accountability* as well as to control access (logical and physical) to protected resources.

With the current limited IAM *Capabilities* in NATO, IAM-related processes are handled in an uncoordinated manner, only as internal aspects of other business processes within a scope of a local *Context*, such as a campus, an organizational *Entity*, a specific system, etc.

Rationalization and streamlining of IAM processes at the Enterprise level has been recognised as a vital requirement to ensure coherency of the NATO IAM *Capabilities* across all levels of the organizational structure. Automation of IAM business processes, including control of both process flows and approvals (that implies human interactions in processes), is a characteristic of the IAM *Capabilities*, desired in complex organizations such as NATO. Typically, it is

delivered as an integral part of *Identity* administration and governance solutions for big organizations.

Requirement ID	SRS-3716
Verification method	Testing
Requirement	The Platform SHALL provide a toolset for *Authorised Users* to model IAM business processes, including actions such as approvals, notifications, initiation of *Identity* and access data processing requests.

Requirement ID	SRS-3717
Verification method	Testing
Requirement	The Platform SHALL provide automation of the modelled IAM business processes through the ability to execute conditional sequences of (sub)-processes and tasks, arranged in a form of workflows.

Requirement ID	SRS-4105
Verification method	Testing
Requirement	The Platform SHALL support triggering IAM tasks on demand, scheduled, and/or as part of complex workflows.

Requirement ID	SRS-631
Verification method	Testing
Requirement	The Platform SHALL support testing mode of workflows for simulation and validation of newly defined/updated workflows before execution in the production environment.

Requirement ID	SRS-618
Verification method	Testing
Requirement	The Platform SHALL use a data retrieval mechanism to support filling out forms for IAM workflows.

Requirement ID	SRS-533
Verification method	Analysis
Requirement	The Platform SHALL define transition workflows between lifecycle states of Enterprise Identities (e.g. *Enrolment*, activation, maintenance (update), adjustment, suspension, reactivation, deletion, archiving, and restoring).

Requirement ID	SRS-4106
Verification method	Testing

Requirement	The Platform SHALL define workflows related to on-boarding processes, including pre-arrival and at arrival activities.

Requirement ID	SRS-4108
Verification method	Testing
Requirement	The Platform SHALL define workflows related to *Identity Information* update requests, including modification of *User Privileges* when the *Identity* data update implies it (e.g., change of the assignment in the organizational structure).

Requirement ID	SRS-4107
Verification method	Testing
Requirement	The Platform SHALL define workflows related to off-boarding processes, including deactivation and archiving of the Enterprise *Identity* for an employee who has left the organization, deactivation of corresponding *User* accounts, cards, *Credentials*, *Privileges*, etc.

Requirement ID	SRS-3738
Verification method	Testing
Requirement	The Platform SHALL define workflows related to NPKI certificate request processes, including integration with the on-boarding processes.

Requirement ID	SRS-4109
Verification method	Testing
Requirement	The Platform SHALL define workflows related to Pass (Token) (re-)issue request processes, including integration with the on-boarding processes.

Requirement ID	SRS-4110
Verification method	Testing
Requirement	The Platform SHALL define workflows related to Personal Identification Number (PIN) Reset Request.

Requirement ID	SRS-592
Verification method	Testing
Requirement	The Platform SHALL allow authorised *Users* to display and report the status of all executed IAM business processes.

Requirement ID	SRS-3713
Verification method	Testing
Requirement	The Platform SHALL provide a self-service *Capability*, with a secure Web interface, for *Authorised Users* to initiate execution of the defined IAM business processes, including filling out and submitting the required pre-defined electronic forms.

Requirement ID	SRS-3714
Verification method	Testing
Requirement	The Platform SHALL provide a self-service *Capability*, with a secure Web interface, for enabling authenticated *Users* to trigger requests to maintain their own personnel information and to perform certain routine *Identity* lifecycle maintenance tasks (e.g., update their personal contact information), including a change validation process before any data is updated within the system and synchronised.

4 Non-functional Requirements

The Non-Functional Requirements (NFR) categorise system/software product characteristics which cannot be defined as "functional".

For Platform the Non-functional Requirements repository will contain the following requirements categories:

   a. Service Criticality (section 4.1)

   b. *Performance* Requirements (section 4.2)

   c. System Quality (section 4.3)

   d. *Logging* and Auditing (section 4.4)

   e. Security (section 4.5)

   f. Interoperability (section 4.6)

   g. Design constraints (section 4.7)

   h. Documentation Requirements (section 4.8)

   i. Computer Resource Constraints (section 4.9)

4.1 Service Criticality

The Platform services can be grouped into three categories based upon their level of criticality to the overall effectiveness of the Platform:

   a. Level 1: Platform cannot be considered to be functional without these services running (Critical)

   b. Level 2: The Platform can operate without these services, but its effectiveness is degraded (Important)

   c. Level 3: These services provide value-add, but the Platform can be used effectively without them (Standard)

   d. Table 1 illustrates which Platform services fall into each category. This categorization is used as a guideline for developing the Non-Functional Requirements and necessary service levels for the Platform.

Table 1 – Platform services by Service Level (criticality)

Service	Critical Service (L1)	Important Service (L2)	Standard Service (L3)
Integration Services			
- Messaging Services	X		
- Mediation Services		X	
Registry and Repository Services			
- Service Discovery		X	
- Metadata Registry			X
Information Services			

- Information Access, Aggregation, Annotation and Discovery			X
- Business Rules Management			X
Platform Hosting Services			
- Platform Environment	X		
Identity and Security Services			
- Identities Management		X	
- Credentials Management		X	
- Authentication Management	X		
- Access Management	X		
Service Management and Control Services			
- Event Management	X		
- Performance and Capacity Management	X		
- Configuration Management		X	
- Process Automation			X

4.2 Performance Requirements

Performance is the degree to which a software system or component meets its objectives for timeliness.

The following *Performance* metrics are recognised:

a. Latency is defined as any kind of delay that happens in data communication over a network.

b. Throughput is defined as the maximum number of request processed by the system in a specified amount of time

c. Response time is defined as the total amount of time it takes to respond to a request for service. In the context of the table below, transmission time is ignored so the response time is the sum of the service time and wait time.

Whereby,

a. High latency is defined as any kind of delay that happens in data communication over a network exceeding 1100 milliseconds (ms).

b. Limited bandwidth is defined as network bandwidth of less than 512 kbps.

Table 2 – Minimum *Performance* figures per group of services

Business Performance Requirement		Throughput (Request/second)	Maximum response time (Latency) (in seconds)
Integration Services	*Messaging Services*	3000	0.03
	Mediation Services	2000	0.03
Registry & Repository		12	2
SMC Services	*Event Management*	12	2
	Performance and Capacity Management	116	2
Platform Hosting		18	1
Information Services		22	2
Identity and Security Services	*Authentication management*	200	0.03
	Access management	1000	0.03

* The figures presented in table 2 are based on 500 concurrent users, single tenant, average message size 23 kB, with 2,048 kB as a maximum message size.

Requirement ID	SRS-4191
Verification method	Testing
Requirement	The Platform SHALL meet at a minimum the throughput levels defined for the individual services in Table 2.

Requirement ID	SRS-4192
Verification method	Testing
Requirement	The Platform SHALL not exceed the latency defined for the individual services in Table 2.

4.2.1 Scalability

Scalability is defined as the capability of a system to increase (or decrease) total throughput under an increased load when resources (typically hardware) are added (or subtracted), so the scalability quality figures are defined accordingly.

Requirement ID	SRS-4169
Verification method	Analysis
Requirement	The Platform SHALL be able to support a throughput increase of 10% every year with no degradation of the maximum latency.

4.3 System Quality Requirements

The System Quality section of the Non-Functional Requirements categorises system/software **product quality.**

The quality of a system is the degree to which the system satisfies the stated and implied needs of its various stakeholders, and thus provides value. These stated and implied needs are represented by quality models that categorise product quality into characteristics, which in some cases are further subdivided into sub-characteristics. (Some sub-characteristics are divided into sub-sub-characteristics.) This hierarchical decomposition provides a convenient breakdown of product quality.

Characteristic definitions in this section are based on ISO/IEC 25010:2011(E) - System and software quality models.

A tailoring of the standard has been made to assure that the Quality Characteristics necessary for the Platform are correctly selected and defined, in accordance with chapter 3.5 of the Standard.

The quality of a product can be seen in many different way, depending on the stakeholder's point of view.

In this case, the stakeholder's view to be used depends on the **Primary and Secondary *Users* (administrators, maintainers, etc.)** point of view; therefore, in accordance with the ISO 25010 standard, the quality model will be tailored based on these stakeholders.

The following table shall be considered in reading this section:

Table 3 – Influence of Quality Characteristics

Product Quality Characteristic	Influence on Quality (Primary Users)	Influence on Quality (Maintenance Tasks)	Influence on Quality (Other Stakeholders' Concerns)
Performance Efficiency	Yes		Yes
Reliability	Yes		Yes
Availability	Yes	Yes	
Fault Tolerance		Yes	
Recoverability	Yes	Yes	
Portability		Yes	
Adaptability		Yes	
Maintainability		Yes	Yes
Modularity		Yes	
Analysability		Yes	
Testability	Yes	Yes	

4.3.1 Tailoring of Quality Characteristics

Due to the nature of the Platform and due to the objective of this document, the quality characteristics have been tailored, in accordance with the following table:

Table 4 – Quality Characteristics Tailoring

Reference (ISO)	Quality Attribute	Applicable
4.2.1	**functional suitability**	N
4.2.1.1	functional completeness	N
4.2.1.2	functional correctness	N
4.2.1.3	functional appropriateness	N
4.2.2	**performance efficiency**	Y
4.2.2.1	time behaviour	Y
4.2.2.2	resource utilization	Y
4.2.2.3	capacity	Y
4.2.3	**compatibility**	N
4.2.3.1	co-existence	N
4.2.3.2	interoperability	N
4.2.4	**usability**	N
4.2.4.1	appropriateness recognisability	N
4.2.4.2	learnability	N
4.2.4.3	operability	N
4.2.4.4	user error protection	N
4.2.4.5	user interface aesthetics	N
4.2.4.6	accessibility	N
4.2.5	**reliability**	Y
4.2.5.1	maturity	N
4.2.5.2	availability	Y
4.2.5.3	fault tolerance	Y
4.2.5.4	recoverability	Y
4.2.6*	**security**	N
4.2.6.1	confidentiality	N
4.2.6.2	integrity	N
4.2.6.3	non-repudiation	N
4.2.6.4	accountability	N
4.2.6.5	authenticity	N
4.2.7	**maintainability**	Y
4.2.7.1	modularity	Y
4.2.7.2	reusability	N
4.2.7.3	analysability	Y
4.2.7.4	modifiability	Y
4.2.7.5	testability	Y
4.2.8	**portability**	Y
4.2.8.1	adaptability	Y
4.2.8.2	installability	N
4.2.8.3	replaceability	N

* An SRS section about security is defined, but it describes the *Capability* of the platform in order to be secure. The platform security will not be evaluated in terms of "Quality"

4.3.2 Measuring the quality characteristics

For the *Monitoring* of quality characteristics, the following definitions will be used:

a. **Error (or Fault)**: A design or source code or hardware flaw or malfunction that causes a *Failure* of one or more *Configuration Items*. A mistake made by a person or a faulty Process that affects a CI is also an *Error* (human *Error*). For the Platform, Human *Error* is generally not taken into consideration in measuring the quality *Performance*.

b. **Fault:** see Error

c. **Failure**: Loss of ability to Operate to Specification, or to deliver the required output. The term *Failure* may be used when referring to Services, Processes, Activities, or *Configuration Items*.

d. **Incident**: An unplanned interruption to a service or reduction in the quality of an service. *Failure* of a *Configuration Item* that has not yet affected service is also an *Incident* — for example, *Failure* of one disk from a mirror set

e. **Problem**: A cause of one or more *Incidents*. The cause is not usually known at the time the *Incident* happens.

4.3.3 Performance Efficiency

Performance Efficiency is the *Performance* relative to the amount of resources used under stated conditions. Resources can include other software products, the software and hardware configuration of the system, and materials (e.g., print paper, storage media).

4.3.3.1 Capacity

Capacity is the degree to which the maximum limits of a product or system parameter meet requirements. Parameters can include the number of items that can be stored, the number of concurrent *Users*, the communication bandwidth, throughput of transactions, and size of database.

Requirement ID	SRS-3264
Verification method	Testing
Requirement	The Platform SHALL be able to handle any or all of its designed Platform services when the maximum number of concurrent *Users* are using the platform, without any *Fault*/*Error* or timeout, for at least 99.5% of its Operational time.

Requirement ID	SRS-3265
Verification method	Testing
Requirement	The Platform shall be able to handle all Platform services concurrently, using the defined information product for each of them, without any *Fault/Error* or timeout, for at least 99.5% of its Operational time.

Requirement ID	SRS-3266
Verification method	Testing
Requirement	The Platform SHALL be able to handle any or all of its designed Platform services with the maximum amount of allowed data, without any *Fault/Error* or timeout, for at least 99.5% of its Operational time.

4.3.3.2 Resource Utilisation

Resource Utilisation is the degree to which the amounts and types of resources used by a product or system, when performing its functions, meet requirements.

Requirement ID	SRS-4016
Verification method	Testing
Requirement	Platform services SHALL meet the minimum required throughput defined in Table 2, for at least 99.5% of its Operational time.

Requirement ID	SRS-4175
Verification method	Testing
Requirement	None of the Platform services SHALL ever drop below the maximum throughput value defined Table 2 by more than 10%.

4.3.3.3 Time Behaviour

Time Behaviour is the degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

Requirement ID	SRS-3270
Verification method	Testing
Requirement	Each of the Platform services SHALL be able to answer any request within the required time limits defined in Table 2, for at least 99.5% of its Operational time.

Requirement ID	SRS-4176
Verification method	Testing

Requirement	None of the Platform services SHALL ever exceed the maximum time limits value defined in Table 2 by more than 10%.

4.3.4 Reliability

Reliability is the degree to which a system, product or *Component* performs specified functions under specified conditions for a specified period of time.

4.3.4.1 General

MTBF (Mean Time Between *Failures*) is defined as the mean time between two consecutive *Faults* which generate a *Failure*.

A critical *Failure* is a *Failure* which cause the complete system unavailability with consequent loss of the provided service/*Capability*.

Table 5 – Reliability by Service Level

Service Type	MTBF
Level 1	8,760 hours
Level 2	4,380 hours
Level 3	720 hours

Requirement ID	SRS-3291
Verification method	Analysis
Requirement	The Platform SHALL exhibit a Mean-Time-Between-*Failure* (MTBF) characteristic, for each service level, in alignment with ITM of at least the number of operational hours as defined in Table 5.

4.3.4.2 Availability

Availability is the degree to which a system, product or component is operational and accessible when required for use.

Inherent Availability (Intrinsic) assumes ideal support (i.e., unlimited spares, no delays, etc.); only design related *Failures* are considered.

For the Platform only Inherent *Availability* will be considered.

4.3.4.2.1 Inherent Availability

Table 6 – Inherent Availability by Service Level

Service Type	Inherent Availability
Level 1	99.97%
Level 2	99.9%
Level 3	99%

Requirement ID	SRS-2425
Verification method	Analysis
Requirement	The Platform SHALL have an *Inherent Availability* for each service level of at least the percentages defined in Table 6.

Requirement ID	SRS-2447
Verification method	Analysis
Requirement	The Platform SHALL be able to queue requests to an unavailable Service and deliver them when the Service becomes available again.

4.3.4.3 Fault Tolerance

Fault Tolerance is the property that enables a system to continue operating properly in the event of the *Failure* of some of its *Components*. A fault-tolerant design enables a system to continue its intended operation, possibly at a reduced level, rather than failing completely when some part of the system fails.

Related to *Fault Tolerance*, *Graceful Degradation* is the ability of a computer, machine, electronic system or network to maintain limited functionality even when a portion of it has been destroyed or rendered inoperative (either by a *Fault* or deliberately). The purpose of graceful degradation is to prevent catastrophic *Failure*, ensuring that it maintains overall functionality - possibly operating at a reduced level of *Performance* - when portions of the system are down.

Ideally, even the simultaneous loss of multiple *Components* does not cause downtime in a system with this feature. In graceful degradation, the operating efficiency or speed may decline gradually as an increasing number of *Components* fail.

The Platform is designed to be fault-tolerant, in particular regarding its most critical (Level 1) services, based upon the following principles:

- *Graceful degradation*: The core services of the Platform have been categorised by their "criticality"; see Table 1, with corresponding levels of service expected. When *Faults* begin affecting the Platform – for example, reduced throughput or CPU usage at capacity, or *Failure* of a less-important service – the system can begin to take off-line the less-critical services (Level 3, and in some instances even Level 2) in order to preserve the functionality of the most-critical (Level 1) services.

- Redundancy: At a minimum, the most critical services (Level 1) of the Platform have backup/failover instances running which can take over if the main instances of the services fail.

Table 7 – *Fault Tolerance* by Service Level

Service Type	Recovery Time
Level 1	10 seconds
Level 2	4 hours
Level 3	7 hours

Requirement ID	SRS-3302
Verification method	Testing
Requirement	For 99% of the possible *Faults/Errors* in any of the Platform services, the system SHALL be able to recover the service or switch to an alternative service, in no more than the amount of Recovery Time defined in Table 7, without loss of data.

Requirement ID	SRS-2463
Verification method	Testing
Requirement	The Platform SHALL resume/retry services, in case of *Failure* due to high latency/timeout/loss of network connectivity, without loss of data.

Requirement ID	SRS-2464
Verification method	Testing
Requirement	The Platform SHALL continue to function within and between the remaining nodes following the loss of one or more connected Organisational Nodes operating within the Platform implementation architecture using the ON WAN or PBN WAN.

4.3.4.4 Recoverability

Recoverability is the degree to which, in the *Event* of an interruption or a *Failure*, a product or system can recover the data directly affected and re-establish the desired state of the system. Following a *Failure*, a computer system will sometimes be down for a period of time, the length of which is determined by its *Recoverability*.

Requirement ID	SRS-3806
Verification method	Analysis
Requirement	In the event a service is interrupted because of a *Fault/Error,* the Platform SHALL be able to restore the data in no more than the duration of Recovery Point specified in Table 7, at least 99.9% of the faults.

4.3.5 Portability

Portability is the degree of effectiveness and efficiency with which a system, product or *Component* can be transferred from one hardware, software or other operational or usage environment to another.

4.3.5.1 Adaptability

Adaptability is the degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments. *Adaptability* includes the *Scalability* of internal *Capacity* (e.g. screen fields, tables, transaction volumes, report formats, etc.).

Requirement ID	SRS-3810
Verification method	Testing
Requirement	When the Platform is installed in any different environment (deployed, exercise, etc.), 100% of critical (Level 1) services and at least 90% of non-critical (Level 2 and Level 3) services SHALL run without any *Faults/Errors,* at least 99.5% of the time.

Requirement ID	SRS-4170
Verification method	Analysis
Requirement	The Platform SHALL not present any *Fault/Error* after any *Scalability* process, for at least 99.5% of its Operational time.

4.3.6 Maintainability

Maintainability is the degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers.

Modifications can include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications. Modifications include those carried out by specialised support staff, and those carried out by business or operational staff, or end *Users*.

Maintainability includes installation of updates and upgrades.

Maintainability can be interpreted as either an inherent capability of the product or system to facilitate maintenance activities, or the quality in use experienced by the maintainers for the goal of maintaining the product or system.

4.3.6.1 General

MTTR is the Mean Time for the system to be Repaired/Restored after a *Failure*.

Recovery Point Objective (RPO) is the threshold of how much data can be afforded to be lost since the last backup. RPO is measured in hours of data loss.

For the Platform, the MTTR to be considered is the mean time needed to restore the system in the operative condition, excluding administrative and logistics delay times

MaxTTR is defined as the maximum time required to restore the system in the operative condition, excluding administrative and logistics delay times.

The MaxTTR to be considered is the maximum time needed to restore the system in the operative condition, excluding administrative and logistics delay times.

Table 8 – *Maintainability* by Service Level

Service Type	MTTR	MaxTTR	RPO
Level 1	2 hours	4 hours	10 seconds
Level 2	4 hours	8 hours	4 hours
Level 3	7 hours	24 hours	24 hours

Requirement ID	SRS-2400
Verification method	Testing
Requirement	The Platform SHALL provide a MTTR in accordance with the times defined in Table 8.

Requirement ID	SRS-3294
Verification method	Analysis
Requirement	The MaxTTR for the Platform SHALL not exceed the times defined in Table 8 for a single maintenance action.

Requirement ID	SRS-2401
Verification method	Testing
Requirement	The Platform SHALL provide a RPO in case of Disaster Recovery in accordance with the times defined in Table 8.

4.3.6.2 Modularity

Modularity is the degree to which a system or computer program is composed of discrete *Components* such that a change to one *Component* has minimal impact on other *Components*.

Requirement ID	SRS-3286
Verification method	Analysis
Requirement	When a maintenance action is required on a software *Component* of the Platform, this action SHALL not cause any possible *Fault/Error* in other *Components* of the system, at least 99.9% of the time.

Requirement ID	SRS-4068
Verification method	Testing
Requirement	The Platform SHALL allow individual Platform services to be deployed separately, without the need to install the full Platform software.

4.3.6.3 Analysability

Analysability is the degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of *Failures*, or to identify parts to be modified.

Implementation can include providing mechanisms for the product or system to analyse its own *Faults* and provide reports prior to a *Failure* or other *Event*.

Fault Detection is the capability of a system to determine that a *Fault* exists using an automatic process.

Fault Isolation is the capability of a system to identify, using an automatic process, which is the component or parameter of the system that is responsible for *Fault*.

Requirement ID	SRS-3287
Verification method	Analysis
Requirement	The Platform SHALL be able to detect at least 99.5% of the possible problem which can occur, notifying the *User* or Administrator with a general message.

Requirement ID	SRS-3288
Verification method	Analysis
Requirement	The Platform SHALL be able to isolate 85% of the possible problem which can occur, notifying the *User* or Administrator with a specific message which identifies the *Error*/*Fault* which has occurred.

4.3.6.4 Testability

Testability is the degree of effectiveness and efficiency with which test criteria can be established for a system, product or *Component* and tests can be performed to determine whether those criteria have been met.

Observability if defined as the capability of the system of determining if specific inputs affect the outputs

Controllability is defined as the capability of the system of producing a specific input from a specific output

Requirement ID	SRS-4263
Verification method	Analysis
Requirement	90% of the software *Components* of the Platform shall be Observable, using automatic test procedures.

Requirement ID	SRS-4264
Verification method	Analysis
Requirement	80% of the software *Components* of the Platform shall be controllable, using automatic test procedures.

4.4 Logging and auditing

Requirement ID	SRS-3003
Verification method	Testing
Requirement	The Platform SHALL be able to generate and retain logs (audit records) for System *Events*, associated with individual *User Identities*, to include: • system start-up (including re-starts) and shutdown • log-on (including failed log-on attempts) and log-off of individual *Users* • changes to permissions and *Privileges* of *Users* and groups • changes to security relevant system management information (including audit functions) • start-up and shutdown of the audit function • any access to security data • deletion, creation or alteration of the security audit records • changes to system date and time • unsuccessful attempts to access system-level resources

Requirement ID	SRS-4021
Verification method	Testing
Requirement	The Platform SHALL be able to generate and retain logs (audit records) for Service *Events*, associated with individual *User Identities*, to include: • Successful or unsuccessful requests to and responses from services • Successful or unsuccessful authorization (access control) decisions • Service startup or shutdown • Configuration changes to services • Message delivery and non-delivery

Requirement ID	SRS-376
Verification method	Testing
Requirement	The Platform SHALL be able to log all messages, including whole messages or *Attributes* to include: • Message time-stamp • Message source and target address • URL requested • Service requested • Operation requested • Request size

	• Unique request id (extracted from the message or automatically generated by the SOA *Logging* Services)

Requirement ID	SRS-3098
Verification method	Testing
Requirement	The Platform logs SHALL include: • *Event* type • Time stamp from a reliable source • Severity level of the *Event*, if applicable • Service(s) involved in the *Event*, if applicable • The *Identity* of the *User* that caused the *Event* (if applicable) • Status of the *Event* • A description of the *Event*

Requirement ID	SRS-248
Verification method	Testing
Requirement	The Platform SHALL be able to export logging information to the format agreed with the Purchaser.

Requirement ID	SRS-4022
Verification method	Testing
Requirement	The Platform SHALL allow *Authorised Users* to enable, configure verbosity of, and disable the various types of logging.

Requirement ID	SRS-3005
Verification method	Testing
Requirement	The Platform SHALL protect the *Audit Logs* from unauthorised modification or deletion.

Requirement ID	SRS-3173
Verification method	Testing
Requirement	The Platform SHALL not log data that could assist an attacker, including and personal information.

Requirement ID	SRS-3010
Verification method	Testing
Requirement	The Platform SHALL retain *Audit Logs* for a configurable period of time, the period being configurable by *Authorised Users*.

Requirement ID	SRS-4023

Verification method	Testing
Requirement	The Platform SHALL allow *Authorised Users* to configure the maximum permitted size of the *Audit Logs*.

Requirement ID	SRS-3013
Verification method	Testing
Requirement	The Platform SHALL raise an alarm via the Service Management and Control system when the *Audit Logs* reach an *Authorised User* configurable percentage of its maximum permitted size.

Requirement ID	SRS-4024
Verification method	Testing
Requirement	The Platform SHALL provide a log analysis and reporting tool, which will allow *Authorised Users* to browse, search and report on *Audit Logs*, based on combinations of search criteria across all fields in the log record format supported by this system.

Requirement ID	SRS-3009
Verification method	Testing
Requirement	The Platform SHALL enable the archiving of logging that is no longer actively used to a separate data storage device for long-term retention.

4.5 Security

4.5.1 Session Management

Requirement ID	SRS-2122
Verification method	Testing
Requirement	The Platform SHALL use available session information to allow an *Entity* to access another resource without the need for another *Authentication.*

Requirement ID	SRS-4046
Verification method	Testing
Requirement	A session management mechanism to protect session IDs SHALL be used after a successful *Authentication*.

Requirement ID	SRS-4119
Verification method	Testing
Requirement	A session management mechanism related security context SHALL be maintained until the session expires.

Requirement ID	SRS-4047
Verification method	Testing
Requirement	Any change in the security context SHALL require re-*Authentication*.

Requirement ID	SRS-4048
Verification method	Testing
Requirement	The Platform SHALL allow *Authorised Users* to set a "timeout" period which SHALL automatically log-out any sessions which have been inactive for that period of time.

Requirement ID	SRS-4049
Verification method	Testing
Requirement	*Authorised Users* SHALL be able to enable and disable the session timeout feature.

Requirement ID	SRS-3060
Verification method	Testing
Requirement	Session IDs SHALL be generated using a cryptographically secure (pseudo)random number generator and they SHALL be at least 128 bits long.

Requirement ID	SRS-3063
Verification method	Testing
Requirement	The application SHALL not permit duplicate concurrent authenticated *User* sessions originating from different machines or IP addresses.

Requirement ID	SRS-3128
Verification method	Inspection
Requirement	If HTTPS is required, the web application SHALL make use of HTTP Strict Transport Security (HSTS; previously called STS) to enforce HTTPS connections.

4.5.2 Password Processing

Requirement ID	SRS-2978
Verification method	Testing
Requirement	The Platform SHALL apply password policy which will enforce individuals to select a password that is at least a configurable (by *Authorised Users*) minimum number of characters long, comprising a configurable mix of uppercase, lowercase, numerics and symbols.

Requirement ID	SRS-4030

Verification method	Testing
Requirement	The Platform SHALL force passwords to be changed at intervals configurable by *Authorised Users*.

Requirement ID	SRS-2979
Verification method	Testing
Requirement	The Platform SHALL deny the re-use of a configurable (by *Authorised Users*) number of previous passwords.

Requirement ID	SRS-4031
Verification method	Testing
Requirement	The Platform passwords SHALL be stored, encrypted, as NATO SECRET information in an approved location with controlled and recorded access.

Requirement ID	SRS-3029
Verification method	Testing
Requirement	Password fields SHALL not echo the *User*'s password when it is entered, and password fields (or the forms that contain them) have autocomplete disabled.

Requirement ID	SRS-3000
Verification method	Testing
Requirement	The Platform SHALL provide help texts to support the login process together with links to recover lost password and login details.

Requirement ID	SRS-3045
Verification method	Testing
Requirement	Forgotten password and other recovery paths SHALL send a time-limited activation token or use two factor proofs.

Requirement ID	SRS-3032
Verification method	Testing
Requirement	Forgot password functionality and other recovery paths SHALL do not send the existing or new passwords in clear text to the *User*.

Requirement ID	SRS-3034
Verification method	Testing
Requirement	No default passwords SHALL be used, for any Platform *Components*.

Requirement ID	SRS-4032
Verification method	Testing
Requirement	Passwords SHALL never be hard-coded in any source code or executable, not even in an encrypted/hashed form.

Requirement ID	SRS-3046
Verification method	Testing
Requirement	Shared knowledge questions/answers (so called "secret" questions and answers) SHALL not be used.

4.5.3 Data Protection

Requirement ID	SRS-3109
Verification method	Testing
Requirement	The Platform SHALL never cache data identified by the Purchaser as sensitive, and SHALL be cleared (invalidated) on logout and/or when the session expires and/or on re-Authentication.

Requirement ID	SRS-4239
Verification method	Testing
Requirement	The Platform SHALL clear (invalidate) data identified by the Purchaser as sensitive on logout and/or when the session expires and/or on re-Authentication.

Requirement ID	SRS-3107
Verification method	Testing
Requirement	The Platform SHALL send to the server data identified by the Purchaser as sensitive in the HTTP message body (i.e., URL parameters are never used to send sensitive data).

Requirement ID	SRS-3111
Verification method	Testing
Requirement	The *Integrity* of interpreted code, libraries, executables, *Audit Logs*, and configuration files SHALL be verified using checksums or hashes.

Requirement ID	SRS-2962
Verification method	Testing
Requirement	The Platform SHALL maintain referential *Integrity* between entities across data sets.

Requirement ID	SRS-2983
Verification method	Testing

Requirement	The Platform SHALL protect *User Credentials* in transit.

Requirement ID	SRS-2989
Verification method	Testing
Requirement	The Platform SHALL protect the *User's* entire login transaction and session via SSL or similar technologies.

Requirement ID	SRS-3179
Verification method	Analysis
Requirement	All cryptographic functions SHALL be implemented on the server side.

Requirement ID	SRS-2960
Verification method	Testing
Requirement	If a file is being generated or exported in a format that does not use headers/footers, the Platform SHALL include a Security Classification into an appropriate part of the file so that it is clearly visible to the *User*.

4.5.3.1 User account processing

Requirement ID	SRS-2990
Verification method	Testing
Requirement	The Platform SHALL allow the *User* (with the same user-id) to access the same information and functionality from any workstation on the NS WAN (i.e., 'roving user' functionality).

4.5.3.2 Communications Security

Requirement ID	SRS-3171
Verification method	Testing
Requirement	The Platform SHALL enforce: • a trust path to be built from a trusted CA to each Transport Layer Security (TLS) server certificate, as well as • each server certificate to match the Fully Qualified Domain Name of the server, and • each server certificate to be valid.

Requirement ID	SRS-3115
Verification method	Testing
Requirement	The Platform SHALL enforce TLS to be used for all connections, internal (e.g., backend) or external, that involve data or functions identified by the Purchaser as sensitive.

Requirement ID	SRS-3116
Verification method	Testing
Requirement	The Platform SHALL enforce backend TLS connection Failures to be logged.

Requirement ID	SRS-3119
Verification method	Testing
Requirement	The Platform SHALL enforce failed TLS connections to not fall back to an insecure connection.

Requirement ID	SRS-3120
Verification method	Testing
Requirement	The Platform shall enforce certificate paths to be built and verified for all client certificates using configured Trust anchors and revocation information.

Requirement ID	SRS-3121
Verification method	Testing
Requirement	The Platform SHALL use a single standard TLS implementation that is configured to operate in a mode of operation approved by the Purchaser.

Requirement ID	SRS-3122
Verification method	Testing
Requirement	The Platform SHALL enforce specific character encodings to be defined for all TLS connections (e.g., UTF-8).

4.6 Interoperability

4.6.1 Interface Requirements

Interoperability is defined in ISO 25010 as the degree to which two or more systems, products or *Components* can exchange information and use the information that has been exchanged.

Within NATO, *Interoperability* is defined as, the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.

4.6.1.1 Interfaces

Interconnecting different systems is one of the primary roles of the Platform, and as such it will able to establish data exchanges through a variety of interfaces with:

- Bi-Strategic Command Automated Information Services (Bi-SC AIS) FSs

- Fielded Prototype Systems until Bi-SC AIS FSs will be available

- Bi-SC AIS Core Services

- Other NATO fielded systems

4.6.1.1.1 Interface Control Document

Requirement ID	SRS-2509
Verification method	Inspection
Requirement	For each specified interface (i.e., inputs and outputs to the Platform), the Platform SHALL be equipped with an Interface Control Document (ICD) describing the interface provided in a format proposed by the *Contractor* and accepted by the *Purchaser*. The content SHALL include, where applicable, the following information: • A list of the applicable technical standards • A catalogue of the services and interfaces exposed by the Platform • A detailed description of the interfaces, including diagrams, *Data Elements*, data formats, *Performance* values, communication protocols, security settings, etc. • Descriptions of *Data Elements* • units of measure required for the *Data Element*, such as seconds, meters, kilohertz, etc. • limit/range of values required for the data element (for constants provide the actual value) • accuracy required for the *Data Element* • precision or resolution required for the *Data Element* in terms of significant digits, • frequency at which the *Data Element* is calculated or refreshed, such as 10 KHz or 50 msec • legality checks performed on the *Data Element* • data type, such as integer, ASCII, fixed, real, enumerated, etc. • data representation/format • priority of the *Data Element* • Service Descriptors, identifying the services endpoints, a detailed description of the service operations and service parameters • All related *Artefacts* such as WSDL, schema files and descriptors • Message descriptions • Interface priority • Communications protocol

4.6.1.2 Interface Mechanisms

4.6.1.2.1.1 File Exchange

Requirement ID	SRS-2519
Verification method	Analysis
Requirement	The Platform SHALL provide adequate documentation for the content and meaning of the file formats it produces or accepts. An adequate definition is one that enables a programmer or *User* to understand the meaning of the data and determine whether it is suitable for its intended use.

Requirement ID	SRS-4230
Verification method	Analysis
Requirement	The Platform SHALL supply a definition for every element, *Attribute*, and enumeration value defined in the file format.

4.6.1.2.1.2 Direct Database and File Access

In limited instances, direct database access in the Platform may be required to enable information exchange or visualisation.

Requirement ID	SRS-2522
Verification method	Analysis
Requirement	As a design rule, direct database access in the Platform SHOULD be avoided.

4.6.2 External Interface Requirements

The Platform has interfaces with external systems and services in order to be able to exchange information. Some of these interfaces are on the ON, and some of them are on the PBN.

Requirement ID	SRS-4009
Verification method	Analysis
Requirement	The *Contractor* SHALL ensure that the Platform supports traversal of firewalls and gateways through the use of well-known proxy protocols or encapsulation of cryptographic protocols over http/https.

4.6.2.1 NATO Systems and Services

4.6.2.1.1 NATO Bi-SC AIS Core Services

Capability Package 9C0150 includes 12 projects that identify the *Capability* and resources required to provide information services that need to be accessible to all *Users*, regardless of COI. Core Information Services provide the common foundation and standard interfaces to support inter-domain *Interoperability* within NATO and with NATO partner nations. The Capability Package reflects

the minimum requirement to support the command and control of all military functions.

4.6.2.1.1.1 Unified Communication and Collaboration Services (UCC)

UCC is intended to provide interaction and collaboration services (e.g., text chat, voice over IP, VTC over IP) to support the command and control of all military functions.

4.6.2.1.1.1.1   Instant Messaging

Instant messaging supports instantaneous synchronous communication and includes the *Capability* to discover people/contacts including their real-time presence information, ad hoc collaboration and participation in a number of concurrent sessions.

Requirement ID	SRS-2624
Verification method	Testing
Requirement	The Platform SHALL support *Interoperability* with instant messaging based on the Extensible Messaging and Presence Protocol (XMPP).

Requirement ID	SRS-2625
Verification method	Analysis
Requirement	The Platform SHALL conform to the fundamental features and security mechanisms of instant messaging as described in the *Service Interface Profile* for Basic Collaboration Services (AI 06.02.12).

4.6.2.1.1.1.2   E-mail Services

Requirement ID	SRS-2628
Verification method	Testing
Requirement	The Platform SHALL interface with the Bi-SC AIS E-mail Services based on MS Exchange.

Requirement ID	SRS-2629
Verification method	Testing
Requirement	The Platform SHALL comply with Bi-SC AIS E-mail services and protocols.

Requirement ID	SRS-2630
Verification method	Analysis
Requirement	E-mail messages produced by the Platform to be provided to the Bi-SC AIS E-mail Services SHALL comply with the formats used in the Bi-SC AIS (e.g., classification header).

4.6.2.1.1.2NATO Information Portal (NIP) Services

When NATO Information Portal (NIP) is used for information management purposes, the Platform will be able to send or receive Information Products to/from the NIP. The Platform will support the interface standards for the NIP for sending or receiving Information Products.

Requirement ID	SRS-2652
Verification method	Testing
Requirement	The Platform SHALL be able to interface with the NATO Information Portal using the SharePoint 2013/2016 APIs.

4.6.2.1.1.3Information Exchange Services

The Platform services will perform in multiple security domains (NATO UNCLASSIFIED, NATO SECRET) where rules, regulations and category of personnel are different.

When the Platform servers will exchange and synchronise information between (i.e. across) the NS and MS domains, multiple procedures and devices will be available in support of these exchanges. The Platform will provide the appropriate means to support these cross-domain exchanges.

Cross-domain support service is necessary when the Platform is used in a distributed environment for creating and feeding the Information Products from various sources spread across different Security Domains

The NATO IEG supports different scenarios in order to meet operational needs for Cross-domain information exchange as described in AC/322-D0030-Rev5.
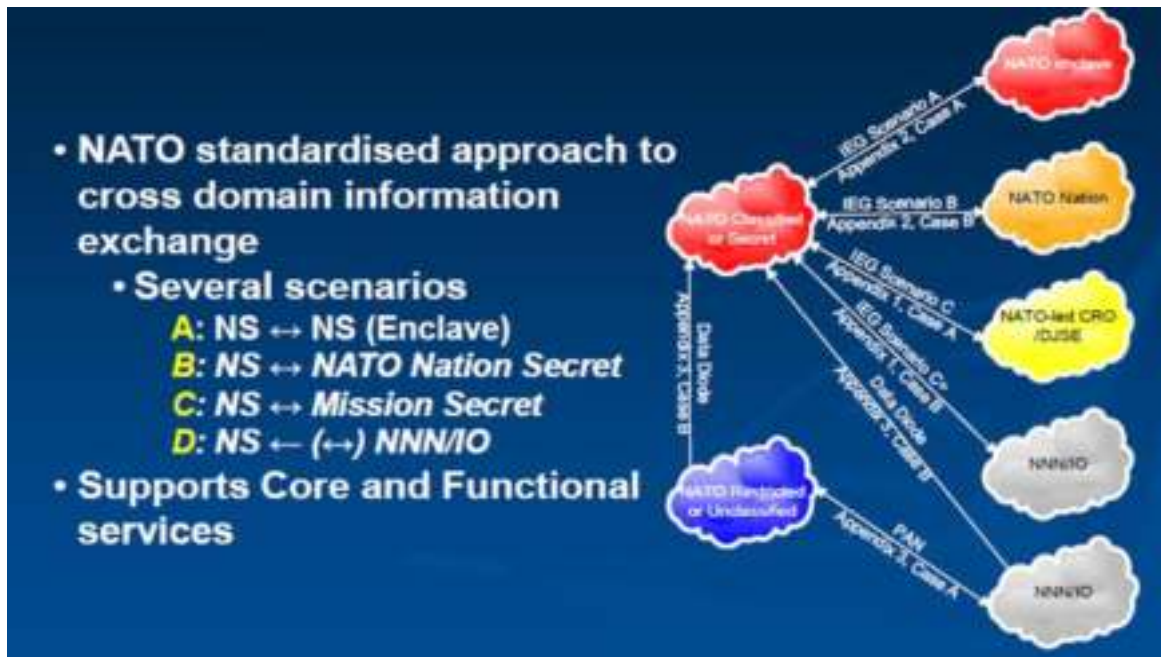
Figure 30 - IEG Scenarios

IEG-C operates as two chained HTTP proxies, one for High to Low information exchanges and another one for Low to High information exchanges. Between the proxies there is a filtering engine that sanitises the information flows in each direction, checking both the header and the body of the HTTP transport messages. The IEG-C targets the content of the HTTP body, which must be an XML document.

IEG-C can filter both SOAP and REST Web Services, or any custom XML protocol that uses HTTP as transport. The IEG-C expects a specific structure for the labelling of the *Data Objects*, and the signatures to bind the security labels *Metadata* to the *Data Objects*.

The current IEG solution cannot handle HTTPS endpoints.

Requirement ID	SRS-2658
Verification method	Analysis
Requirement	All data disseminated to a different Security Domain SHALL contain approved NATO security labels and adhere to NATO labelling standards.

Requirement ID	SRS-2555
Verification method	Testing
Requirement	The Platform SHALL exchange information with IEG-C to cross from NATO Secret to Mission Secret Security domains.

4.6.2.1.1.4 Windows Domain Services

Windows Domain Services provide Security and Directory Services to the Bi-SC AIS Domain.

Requirement ID	SRS-2678
Verification method	Analysis
Requirement	The Platform SHALL integrate with the Bi-SC AIS Directory Services Active Directory.

Requirement ID	SRS-2680
Verification method	Testing
Requirement	If the Platform requires an Active Directory schema change, these schema extensions SHALL be documented and submitted for approval to the *Purchaser* during the Design Stage.

Requirement ID	SRS-2681
Verification method	Testing
Requirement	The Platform SHALL be compatible with Active Directory services and protocols.

Requirement ID	SRS-2684

Verification method	Inspection
Requirement	The Platform SHALL support integration with Windows File and Print Services (including publishing and lookup through Active Directory).

Requirement ID	SRS-2685
Verification method	Inspection
Requirement	The Platform SHALL support integration with Windows built-in services (e.g., Domain Name System (DNS), Internet Information Services, RUP, Terminal Server).

Requirement ID	SRS-2686
Verification method	Inspection
Requirement	The Platform SHALL support integration with Windows Security Services.

Requirement ID	SRS-2687
Verification method	Inspection
Requirement	The Platform SHALL support integration with Active Directory-supported security access control (e.g., ACL, security groups) to Operating System resources.

Requirement ID	SRS-2688
Verification method	Inspection
Requirement	The Platform SHALL be able to operate with the latest security settings from the NATO Information Assurance Technical Centre (NIATC) without change.

4.6.2.1.1.4.1 Malware Detection Services

Requirement ID	SRS-2702
Verification method	Testing
Requirement	The Platform will be able to run with NATO Standard Malware Detection Services and anti-virus software.

Requirement ID	SRS-2703
Verification method	Testing
Requirement	The Platform SHALL work correctly and not adversely impact other applications when Bi-SC AIS standard Anti-Virus software is applied.

Requirement ID	SRS-3619
Verification method	Testing
Requirement	The supplied software SHALL be compatible with the NATO Anti-Virus management centre and approved by the *Purchaser*.

4.6.2.1.1.4.1.1 Generic Security Services Application Program Interfaces (GSS API)

Requirement ID	SRS-2563
Verification method	Testing
Requirement	The Platform MAY use Generic Security Services Application Program Interface as the application programming interface for accessing security services.

Requirement ID	SRS-2564
Verification method	Testing
Requirement	The Platform security application program interface SHALL be compliant with [IETF RFC 2078, 1997].

Requirement ID	SRS-2565
Verification method	Testing
Requirement	The Platform primary security services (access control, *Confidentiality*, *Integrity*, *Authentication*, and *Non-repudiation*) SHALL use X.509.

Requirement ID	SRS-2566
Verification method	Analysis
Requirement	The Platform X.509 support to primary security services SHALL be compliant with NPKI.

4.6.2.1.2 NATO Bi-SC AIS Deployable CIS

4.6.2.1.2.1 Introduction

NATO *Deployable CIS* provides a *Capability* for deployed forces, in-theatre and extends services from the fixed infrastructure to deployed *Users*.

Deployable CIS will support the full range of required CIS services at the deployed HQ. These CIS services include communication and the Bi-SC AIS core and FSs. The communication services provide telephony, video conferencing and fax. The core services provide standard office automation including email and data transfer. The FSs provide services specific military functions. To support deployed operations which may involve C2 participants from Nations which cannot be cleared for access to NATO SECRET (NS) information, it is necessary for the *Deployable CIS* C2 nodes to support a MISSION SECRET (MS) domain. A NS domain is still required to support NATO activities and a NATO UNCLASSIFIED (NU) domain is required to support sharing of information in an unclassified environment.

NATO will provide the operational command structure of NATO lead expeditionary operations:

a. Multinational Force, rotational

b. Mission usually involves forces from non-NATO Nations

c. Liaison with local governments, NGO, etc.

d. 3 information security domains (plus national domains), namely:

    i. a Mission Secret (default secret mission execution domain)

    ii. a Mission Unclassified

    iii. the NATO Secret

e. NATO expeditionary operations have the following characteristics:

f. Rapidly deployable

g. NTM from 2 to 30 days

h. Roll-on Roll-off to tactical airlift

i. Deployment of forces and HQ structure mission tailored:

j. Small mobile teams

k. Deployable HQ from 50 to 500 *Users*

l. Disaster relief to Corps size operation

m. Every mission is different, and never as planned. For this reason, *Deployable CIS* have to maximise *Modularity*, *Scalability* and flexibility.

n. Sustainable with not host nation support

4.6.2.1.2.2 Context

Once a mission is started, all relevant pre-mission information is transferred into the MS Mission Anchor Point. Operational *Users* from the static environment continue mission preparation in the MS environment, while the deployable nodes that will support the mission are selected and prepared. Note that for missions engaging the NRF-in-standby this nodal selection and preparation is already done during the NRF preparation phase.
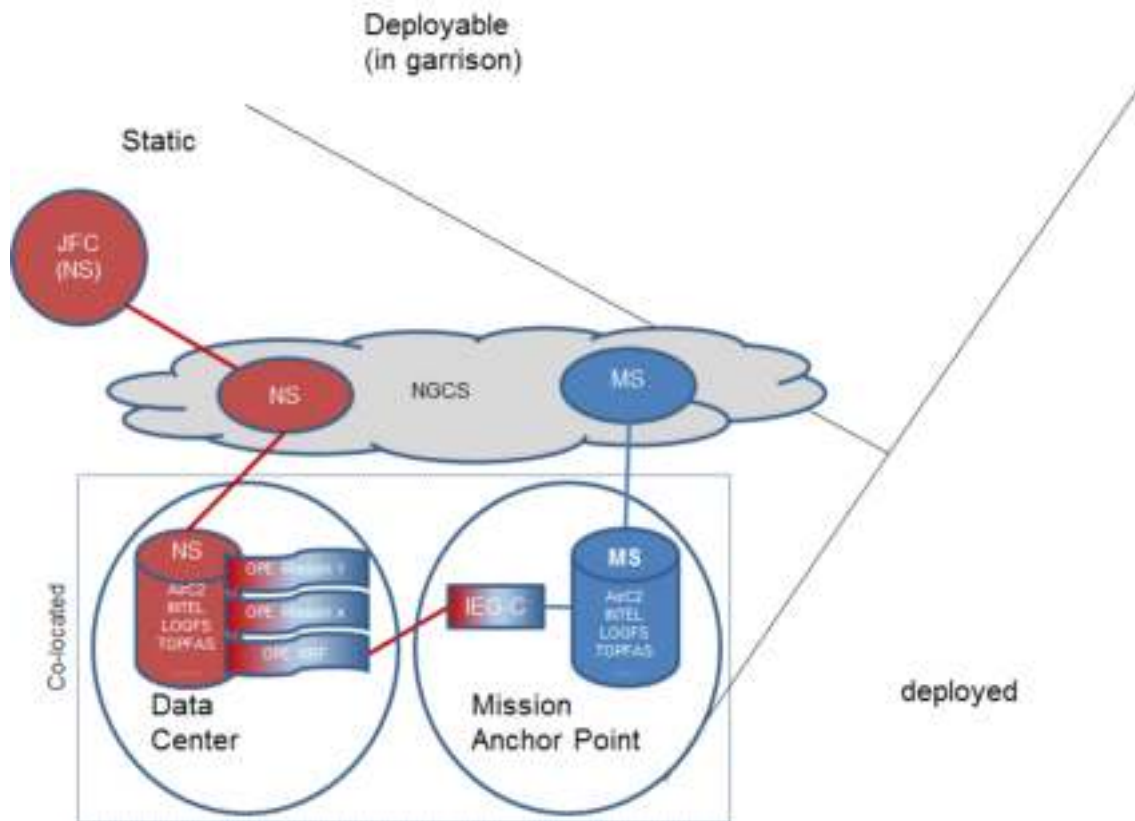
Figure 31 - Phase 1: Mission secret domain used for mission specific planning

Once the deployable nodes that support the deployable C2 are selected and prepared, all mission applications required for the deployable C2 (JTF HQ and JSLG in the example) and the related databases will be installed on the deployable nodes, and while still in garrison, all preparation data will be synchronised to those nodes. It should be possible to switch the roles of the databases. In the early phases, the main database is the in the Mission Anchor Function, and the secondary is the one in the node in garrison. When a node in garrison is deployed, these roles may change.
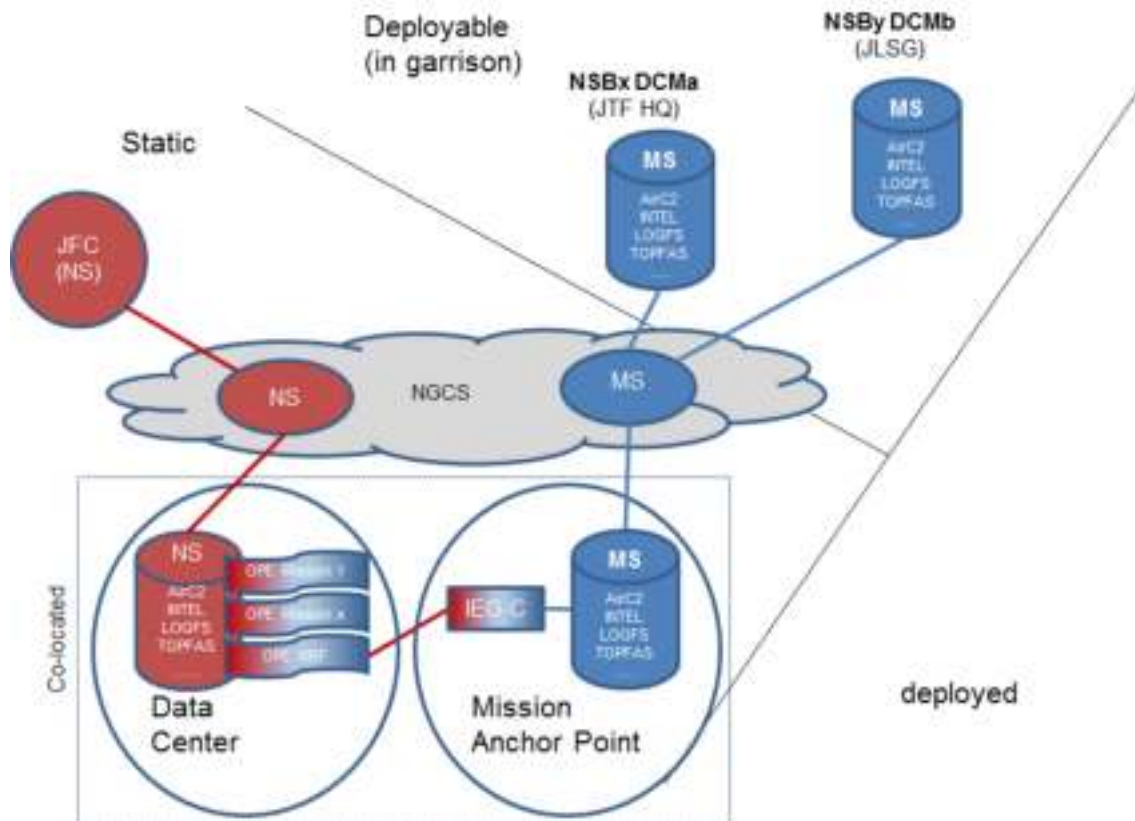
Figure 32 - Phase 2: DCMs are assigned to support NRF C2 entities

When the node deploys into theatre, the applications and databases are not reachable, but planning and preparation by the operational *Users*, still in their peacetime HQ, continues using the MAF.

Once the deployable node becomes operational in theatre, the data in the deployed node is synchronised with the MAF. Operational *Users* in the JTF HQ forward will use the local FS installations for their work, while *Users* supporting the mission from the rear will work on the installations in the MAF, and only the resulting database synchronisation will be executed over the long delay and narrow SATCOM links.
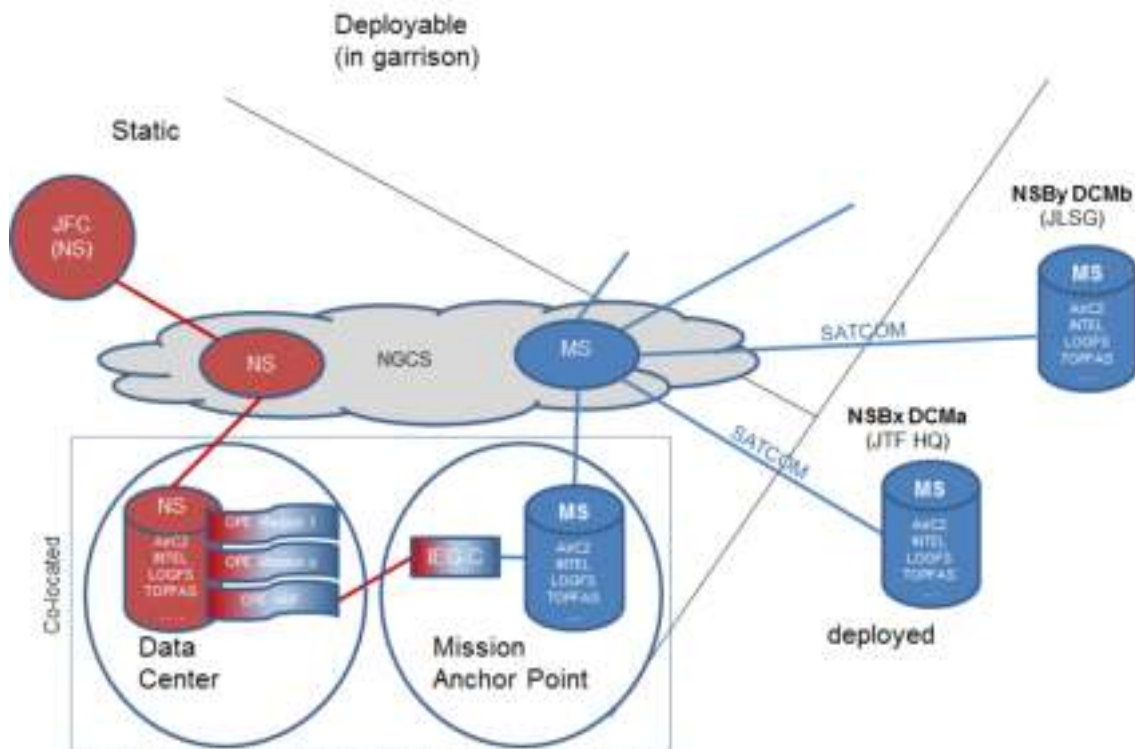
Figure 33 - Phase 3: DCMs deploy forward, deployed node contains primary COI database

FS *Capabilities* will be made available to the *Users* through two options; a full-feature web-based application running on the existing NATO Security Domains (ON, MS and PBN, when applicable) and an equal full-feature client application (for those situations where higher responsiveness is needed, where network latency is too high or where reach-back connectivity is not available).

Any *Contractor* involved in the development of a FS *Capability* that is meant to be deployable will define and develop test programs, plans, and procedures and conduct testing, oriented specifically to test the deployability of the system, as well as evaluate and document the results. The hardware, software, testing equipment, supplies, facilities, and personnel will be available and in place to conduct or support each test. For acceptance and operational testing, the test data will also be included, and mimic the anticipated operational quantities and sizes of information objects that will be identified in the NATO FS NFRs. These tests will be performed in an existing or new *Deployable CIS* Reference environment that accurately simulates the latency and bandwidth network conditions of the *Deployable CIS* infrastructure.

4.6.2.1.2.2.1   Business Level Requirement
The services that are actually provisioned on a *Deployable CIS* node will depend on the nature of the mission involved. It is anticipated that a single *Deployable CIS* node will vary between requiring the full suite of Platform

services (comparable to a *Data Centre*), selected Platform Services (comparable to an *Enhanced Node*) or none (a *Standard Node*).

Requirement ID	SRS-3493
Verification method	Analysis
Requirement	The Platform SHALL be required to be able to run on the *Deployable CIS* platform.

Requirement ID	SRS-2921
Verification method	Analysis
Requirement	The Platform SHALL be deployed depending on the type of *Deployable CIS* node. A single *Deployable CIS* node SHALL vary between the full suite, a selection of Platform service or no Platform Services.

4.6.2.1.2.3 Quality Requirements

4.6.2.1.2.3.1   Usage scope and limitations

Requirement ID	SRS-2888
Verification method	Inspection
Requirement	The Platform SHALL not bear additional licences and charges for deployment of the Platform Product if used in a NATO context (exercise, mission, static and deployable commands, NRF).

4.6.2.1.2.3.2   Availability

For the deployed Platform, five levels of network degradation will be considered due to outages and/or jamming:

- Normal: 90%-100% of the throughput available

- Degraded: 70%-90% of the throughput available

- Severely Degraded: 10%-70% of the throughput available

- Minimum: >0%-10% of the throughput available

- Off-line: 0% of the throughput available

A **degraded network mode of operation** is when the mission-specific WAN or mission-specific LAN is providing a reduced level of service that may impact one or more of the Platform services (or Application and Interface Products). Reduction in service may be due to bandwidth limitations or a communication degradation affecting some part of the LAN and/or WAN.

Requirement ID	SRS-4255
Verification method	Testing
Requirement	The Platform SHALL be able to continue service locally if a WAN connection is disrupted.

Requirement ID	SRS-4257

Verification method	Testing
Requirement	The Platform SHALL be able to resume services to other nodes if a WAN connection is restored after a disruption.

Requirement ID	SRS-4256
Verification method	Testing
Requirement	The Platform SHALL be able to provide services to other nodes if interconnections are over degraded networks.

4.6.2.1.2.3.3   Maintainability

Requirement ID	SRS-2898
Verification method	Testing
Requirement	Each deployable Platform instance SHALL have the *Capability* to be operated by local administration and management, so that if a node is isolated from the central support, local administration and management can be executed.

Requirement ID	SRS-2899
Verification method	Testing
Requirement	The Platform preparation for deployment and movement SHALL not take more than 5 days from receiving the Notice to Move until the equipment is packed up ready to move.

4.6.2.1.2.4 Interface Requirements

Requirement ID	SRS-2915
Verification method	Testing
Requirement	The Platform data resynchronisation in deployment after long periods off-net SHALL resolve consistency conflicts.

Requirement ID	SRS-2916
Verification method	Testing
Requirement	The Platform SHALL implement data compression that guarantees an efficient use of network bandwidth.

Requirement ID	SRS-2917
Verification method	Testing
Requirement	The Platform SHALL implement incremental database synchronisation communication protocol that guarantees an efficient use of network bandwidth.

Requirement ID	SRS-2918

Verification method	Testing
Requirement	The Platform SHALL not encrypt WAN data exchange.

4.6.2.1.2.5 Infrastructure Requirements

Deployable CIS must provide equipment to host the NATO Bi-Strategic Command Automated Information Services (Bi-SC AIS) *Functional Services*, along with any requisite supporting infrastructure. *Deployable CIS* must also both host and provide Bi-SC AIS Core Services. (The AIS *Functional Services* applications themselves are provided from outside the *Deployable CIS* programme).The AIS services must be able to have access to the communications network to allow interaction between elements of the AIS services and to enable the services to be accessed by *Users*. This equipment is grouped into the µISM subsystem. Each security domain is served by a separate µISM module.

Requirement ID	SRS-2924
Verification method	Analysis
Requirement	The backend deployment for NATO locations SHALL be done using the NATO Infrastructure (Processing, Storage, Networking) Services.

Requirement ID	SRS-2925
Verification method	Testing
Requirement	The Platform SHALL be deployable in both MS Hyper-V and VMWare virtualised environments.

4.6.3 Co-existence Requirements

Co-existence is the degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.

Requirement ID	SRS-2611
Verification method	Testing
Requirement	The Platform SHALL operate with other Bi-SC AIS FSs in the same environment without causing an *Error* condition in itself or in other systems.

4.7 Design Constraints

4.7.1 Architectural Constraints

4.7.1.1 General

Requirement ID	SRS-1720
Verification method	Analysis
Requirement	The Platform SHALL be compliant with the standards given in the section "Applicable Standards". Any proposed deviation SHALL be approved by the *Purchaser*.

Requirement ID	SRS-4104
Verification method	Analysis
Requirement	The Platform SHALL be designed and implemented based on the Platform Principles as described in section 2.1.1.

Requirement ID	SRS-1722
Verification method	Analysis
Requirement	The proposed software architecture, development environment, middleware system and the separation of *Components* (Human Machine Interface, Business and Data) for the Platform SHALL be documented and explained in detail.

Requirement ID	SRS-1724
Verification method	Analysis
Requirement	The Platform services SHALL comply with the C3 Classification Taxonomy [NC3B AC/322-N(2016)0021-AS1, 2016], and applicable *Service Interface Profiles*.

Requirement ID	SRS-1726
Verification method	Analysis
Requirement	The Platform design process SHALL balance design implementation with cost for implementation and support to minimise life cycle cost. The Platform design SHALL take into account the technical, support and cost impacts for NATO.

Requirement ID	SRS-2404
Verification method	Analysis
Requirement	The Platform SHALL be composed of discrete *Components* such that a change to one *Component* has minimal impact on other *Components*.

4.7.1.2 Browser-based Functionality

Requirement ID	SRS-1728
Verification method	Analysis
Requirement	The Platform *User* functionality SHALL be browser-based, except as specifically waived by the *Purchaser*.

Requirement ID	SRS-4138
Verification method	Inspection
Requirement	The Platform SHOULD not use plug-ins and runtime environments (e.g. Flash plug-in, Silverlight). The use

	of Hypertext Mark-up Language (HTML) 5 and AJAX is strongly recommended.

Requirement ID	SRS-1746
Verification method	Analysis
Requirement	The Platform SHALL use standard internet addressing, Universal Resource Locator and Universal Resource Identifier.

4.7.1.3 Commercial off-the Shelf (COTS) selection and integration

Requirement ID	SRS-1731
Verification method	Analysis
Requirement	The Platform SHALL be based on COTS in its architecture in place of dedicated solutions when the functionalities of a COTS matches the requirements for a Service with no or minimal adaptation.

Requirement ID	SRS-1732
Verification method	Analysis
Requirement	All functionalities provided by the COTS used for the Platform SHALL be available and not shielded nor masqueraded by an additional layer.

Requirement ID	SRS-1733
Verification method	Analysis
Requirement	The Platform adaptations SHALL be delivered as additional Services, owned by NATO, that complement the COTS native functionalities.

4.7.2 Software Design

4.7.2.1 Programming Languages and Technologies

Requirement ID	SRS-1750
Verification method	Analysis
Requirement	The Platform SHALL comply with the standards and language specifications described below. Any variations from the languages or specifications SHALL be agreed with the *Purchaser*: • C# [ISO/IEC 23270:2003] Java SE Version 9 [JSR 379] • .NET • C++ [ISO/IEC 14882] • Common Language Infrastructure (CLI) [ISO/IEC 23271:2003 and ISO/IEC 23272:2003] • JavaScript [ECMA 262] • HTML [ISO/IEC 15445, 2000]

Requirement ID	SRS-1752
Verification method	Analysis
Requirement	The Platform SHALL not use DCOM, COM, ActiveX and/or COM+ unless specifically authorised in advance by the *Purchaser*.

4.7.2.2 Coding Standards

Requirement ID	SRS-1757
Verification method	Inspection
Requirement	A convention SHALL be adopted and applied consistently across all code *Artefacts* for each programming language employed.

Requirement ID	SRS-1758
Verification method	Inspection
Requirement	Source code *Artefacts* delivered for the Platform SHALL be written using Standard English (e.g., for Classes, Methods, Variables etc.).

Requirement ID	SRS-4120
Verification method	Inspection
Requirement	Industry coding best practices SHALL be used for Platform source code *Artefacts*.

4.7.2.3 Code Documentation

Requirement ID	SRS-1761
Verification method	Inspection
Requirement	Source code delivered for the Platform, including customisation code for COTS products and modifications to Free Open Source Software (FOSS) products but not to existing COTS/FOSS source code, SHALL be documented with in-line comments using standard English. Commercial best practices SHALL be used in the level of commenting.

Requirement ID	SRS-1762
Verification method	Inspection
Requirement	Comments for the source code of the Platform SHALL be used to clarify intent of the code and SHALL be provided for: • Each class definition explaining the purpose of the class • Each member function explaining what the function does • Each member variable explaining what the variable means

	• Each type definition (enums) explaining what the type represents

Requirement ID	SRS-1764
Verification method	Inspection
Requirement	Comments for the source code of the Platform SHALL be able to be extracted and formatted to augment technical documentation.

4.7.2.4 Registry Settings

Requirement ID	SRS-1766
Verification method	Inspection
Requirement	All usage of the Windows Registry by the Platform applications SHALL be fully documented, and requires approval by the *Purchaser* not later than the Design Stage.

4.7.3 Graphical User Interface (GUI)

Bi-SC AIS applications are developed as projects within NCIA to be used by NATO *Users*. Both NCIA and NATO have their own standards and guidelines that will influence or directly affect Bi-SC AIS applications' visual design. Although Bi-SC AIS applications can have their own characteristics, any new application needs to feel like other products NCIA or NATO have previously created and share the same organisational values.

Requirement ID	SRS-4253
Verification method	Inspection
Requirement	The Platform SHALL provide a Web-based toolset to configure the Platform services.

Requirement ID	SRS-4254
Verification method	Testing
Requirement	The Platform toolset SHALL be able to graphically display and configure service parameters.

Requirement ID	SRS-4064
Verification method	Analysis
Requirement	In case the Platform provided toolset makes use of an API to interact with a service, the tool SHALL be able to make use of all API features and *Performance*.

Requirement ID	SRS-4251
Verification method	Analysis
Requirement	In case the Platform provided toolset makes use of an API to interact with a service, the tool SHALL be

	designed to allow for future GUI enhancement or replacement.

4.7.3.1 NCIA and NATO

Requirement ID	SRS-2739
Verification method	Analysis
Requirement	The Platform visual design SHALL follow the recommendations and guidelines stated in the following Documents: • NATO Visual Identity Guidelines [NATO Visual Identity Guidelines, 2016] • NCIA Visual Identity Guidelines [NCIA Visual Identity Guidelines, 2013]

Requirement ID	SRS-2740
Verification method	Analysis
Requirement	The Platform SHALL follow the recommendations and guidelines of the Human Machine Interface (HMI) Style Guide for C4ISR Rich Applications [NCIA HMI Style Guide, 2015] regarding to windows and layouts, *User* interactions, *User* support and feedback, common *User* interface *Components* design, visual design and text use.

4.7.3.2 ISO standards

Requirement ID	SRS-2742
Verification method	Testing
Requirement	The Platform icons included in the designed solution SHALL be compliant with the ISO 18152 standard series.

Requirement ID	SRS-2743
Verification method	Inspection
Requirement	The Platform SHALL be compliant with the ISO 9241 standard series for software usability.

4.7.4 Free and Open Source software (FOSS)

Requirement ID	SRS-1769
Verification method	Analysis
Requirement	FOSS *Components* in the Platform SHALL comply with the NATO strategy on the use of Open Source Software in NATO systems.

Requirement ID	SRS-1770
Verification method	Inspection

Requirement	Any Platform *Components* based on free and open source software SHALL be provided with the source code for the FOSS.

Requirement ID	SRS-1771
Verification method	Analysis
Requirement	Use of a FOSS *Component* SHALL not limit the deployment or use of the Platform in any way and SHALL not require the release of code developed for the Platform.

4.8 Documentation Requirements

4.8.1 General

The requirements describing which technical documentation shall be developed and how the technical documentation shall be managed and taken under configuration control are in the SoW. This section of the SRS will cover the requirements which are applicable to the online technical documentation.

Requirement ID	SRS-3676
Verification method	Inspection
Requirement	The general requirements for technical documentation developed in the SOW SHALL also apply to the on line documentation.

Requirement ID	SRS-1777
Verification method	Inspection
Requirement	The Platform on-line *User* documentation and help system SHALL be compliant with standards identified under section "Applicable Standards".

Requirement ID	SRS-1779
Verification method	Inspection
Requirement	The Platform SHALL adhere to the 'Microsoft standard User interface' methods for accessing on-line documentation resources.

4.8.1.1 On-line Help

4.8.1.1.1 General

The Platform will be used by organisations in various time zones throughout NATO territories and other areas of NATO operations. During crisis use of the Platform will be high and over extended working hours. Full on-line help *Capability* will be required to supplement the Platform help-desks.

Requirement ID	SRS-1826
Verification method	Testing

| Requirement | The Platform SHALL support on-line help describing all functionality of the Platform *Capability*. |

Requirement ID	SRS-1827
Verification method	Testing
Requirement	The Platform on-line help SHALL translate every use case and usage scenario into a browsing sequence.

Requirement ID	SRS-4240
Verification method	Testing
Requirement	The Platform SHALL structure every browsing sequence according to the *User* workflow.

Requirement ID	SRS-1828
Verification method	Testing
Requirement	The Platform on-line help SHALL describe each Platform function, the interrelationships between and the logical sequence of functions.

Requirement ID	SRS-1829
Verification method	Testing
Requirement	The Platform on-line help SHALL explain all menu items, dialog windows, data entry and query fields implemented in the Platform Product Baseline.

Requirement ID	SRS-1830
Verification method	Testing
Requirement	The Platform on-line help SHALL include a glossary providing definitions of all terms and acronyms implemented in the Platform Product Baseline.

Requirement ID	SRS-1831
Verification method	Testing
Requirement	All definitions in the Platform glossary SHALL be available in roll-over, pop-up windows linked to every appearance in on-line help of the corresponding term or acronym.

Requirement ID	SRS-1832
Verification method	Testing
Requirement	In the Platform, each dialogue, menu item, toolbar item, function, field or button (each item on the screen) SHALL have an on-line help option. This SHALL be clearly visible, but not intrusive.

Requirement ID	SRS-1833
Verification method	Testing
Requirement	The Platform on-line help function SHALL provide meaningful advice and hints to *Users* appropriate to the actions they are trying to take.

Requirement ID	SRS-1834
Verification method	Testing
Requirement	The Platform on-line help SHALL be concise, compact and clear to the *User*.

Requirement ID	SRS-1835
Verification method	Testing
Requirement	The on-line help SHALL include snapshots of the Platform screens, windows, and dialogue boxes. The snapshots SHALL be provided in a suitable lightweight format (e.g., Graphics Interchange Format (GIF), PNG) approved by the *Purchaser*.

Requirement ID	SRS-1836
Verification method	Testing
Requirement	Pictures in the Platform on-line help showing more than five GUI elements/controls SHALL have a clickable image map describing each element.

Requirement ID	SRS-1837
Verification method	Testing
Requirement	If the Platform on-line help subject requires a large picture that does not fit on a normal page, a reduced copy SHALL be additionally included on the Help page that will expand to its full size on *User* request.

Requirement ID	SRS-1838
Verification method	Testing
Requirement	The Platform on-line help SHALL be context-sensitive (i.e., based on a specific point in the state of the software and providing help for the situation that is associated with that state on action being performed).

Requirement ID	SRS-1839
Verification method	Testing
Requirement	All context-sensitive GUI elements in the on-line help SHALL be linked to the relevant User Manual subjects.

Requirement ID	SRS-1840

Verification method	Testing
Requirement	In the Platform, all source code elements SHALL be configured to link the GUI elements to their context-sensitive subjects.

Requirement ID	SRS-1841
Verification method	Testing
Requirement	The Platform SHALL contain help functions that provide access to interactive training sessions to guide *Users* through procedures and functions.

Requirement ID	SRS-1842
Verification method	Testing
Requirement	The Platform on-line help SHALL be given by a small pop-up screen or infotip screen. This screen SHALL appear quickly and be very easy to hide, for instance clicking anywhere within it.

Requirement ID	SRS-1843
Verification method	Testing
Requirement	The Platform on-line help SHALL open a dedicated web page when the *User* request access to the full content of the on-line help. The on-line help SHALL not be preventing the *User* to perform on the Platform GUI.

Requirement ID	SRS-1844
Verification method	Testing
Requirement	The Platform SHALL allow the *User* to hide the on-line help screen just by clicking anywhere else, or there SHALL be another single action hiding mechanism.

4.8.1.1.2 Help Search

Requirement ID	SRS-1846
Verification method	Inspection
Requirement	The Platform on-line help SHALL be organised in the following two sections: • Contents, providing access to all help pages and organised in a logical manner by subject or procedure • Index, providing *Users* with both the ability to search for keywords in all Help pages and retrieve a list of those pages in which those keywords appear and the ability to select and trigger such a query from a list of all keywords.

Requirement ID	SRS-1847

Verification method	Testing
Requirement	The Platform SHALL be able to display search query results for finding help items in the online help in a list. The Platform SHALL display the help item when the *User* selects a query result in this list.

4.8.1.1.3 Help Format

Requirement ID	SRS-1849
Verification method	Testing
Requirement	The on-line help shall be available as a web site and includes all project-related source elements and graphics. The web site shall be available as a stand-alone web site to be installed and used on a stand-alone computer if required.

4.8.1.2 Frequently Asked Questions (FAQ)

Requirement ID	SRS-1851
Verification method	Inspection
Requirement	The Platform SHALL provide a list of Frequently Asked Questions (FAQ). FAQs SHALL be available to support the NCIA Help Desk and other support organisations.

Requirement ID	SRS-1852
Verification method	Testing
Requirement	The Platform SHALL allow the *User* to display the Platform FAQ.

Requirement ID	SRS-1853
Verification method	Testing
Requirement	The Platform SHALL allow the *User* to search the Platform FAQ.

Requirement ID	SRS-1854
Verification method	Testing
Requirement	The Platform SHALL allow the Platform *User* or the Platform Administrator to ask questions to the NCIA Help Desk in electronic form by using the Platform FAQ.

Requirement ID	SRS-1855
Verification method	Testing
Requirement	The Platform SHALL allow *Authorised Users* to update the contents of the FAQ.

4.9 Computer Resource Constraints

Requirement ID	SRS-1937

Verification method	Testing
Requirement	The Platform SHALL be able to run on NATO-provided infrastructure including virtual servers and operational workstations.

Requirement ID	SRS-1942
Verification method	Analysis
Requirement	The infrastructure requirements of a service or application SHALL not be designed and deployed with a "per service, per application" approach but SHALL be covered through a harmonised "infrastructure services" approach applicable to all services and applications making use of the infrastructure services.

Requirement ID	SRS-4125
Verification method	Analysis
Requirement	The Platform SHALL be compatible with the x86-64 architecture (32-64 bit applications).

Requirement ID	SRS-4126
Verification method	Analysis
Requirement	The server-side of the Platform SHALL be compatible with the NATO desktop baseline including: • Microsoft Windows Server; • Red Hat Enterprise Linux; or • Solaris.

Requirement ID	SRS-4128
Verification method	Analysis
Requirement	The client-side of the Platform SHALL be compatible with the NATO desktop baseline including: • MS Windows Operating system; • MS Office Professional Plus; • MS Internet Explorer; • MS Silverlight; • Adobe Acrobat Reader; • Java Virtual Machine; • Email security classification Labelling client; • McAfee Anti-Virus and Data Loss Prevention (DLP) agent; • NCIRC desktop Host-based Intrusion Detection System (HIDS) and Forensics analysis based agents; • VPN client for PBN mobile client devices; and • Disk encryption for PBN mobile client devices.

Requirement ID	SRS-4139
Verification method	Analysis
Requirement	The Platform SHALL support multiple browsers, including as a minimum: • MS browser, and • Firefox.

Requirement ID	SRS-4130
Verification method	Analysis
Requirement	The Platform SHALL support the IPv6 protocol.

Requirement ID	SRS-4131
Verification method	Analysis
Requirement	The Platform SHALL support either: • MS IIS, or • Tomcat.

Requirement ID	SRS-4132
Verification method	Analysis
Requirement	The Platform's server deployment package (virtual appliance or installation package) SHALL be compatible with both: • Microsoft Hyper-V, and • VMWare ESXi hypervisor.

Requirement ID	SRS-4133
Verification method	Analysis
Requirement	The software installation package of the Platform SHALL be compatible with either: • Windows Installer program, • Redhat RPM, or • Solaris Image Packaging System (IPS).

Requirement ID	SRS-4134
Verification method	Inspection
Requirement	The Platform software SHALL not have any hard coded: • URL, DNS or IP Address settings. • UNC, File Path, Drive Letter or similar storage location settings.

Requirement ID	SRS-1949
Verification method	Inspection
Requirement	All URL, DNS, IP Addressing and similar network settings SHALL be parametric, configurable, and

	possible to automate for unattended installation, backup, recovery.

Requirement ID	SRS-4135
Verification method	Inspection
Requirement	The Platform SHALL not have any direct dependency on the physical parameters of the storage environment (such as disk type, connection type, SAN topology, SAN protocol).

Requirement ID	SRS-4141
Verification method	Testing
Requirement	The Platform SHALL be able to adapt immediately to changes in resource *Capacity* due to changing priorities (e.g. shrinking RAM).

Requirement ID	SRS-4151
Verification method	Testing
Requirement	The Platform SHALL be able to automatically add a new instance without shutting down.

Requirement ID	SRS-4150
Verification method	Testing
Requirement	All infrastructure states for the Platform environment SHALL be automatically recreatable from templates that describe how the instances need to be configured and updated with data.

Requirement ID	SRS-4142
Verification method	Testing
Requirement	The Platform SHOULD be resource consumption aware to minimise consumption of CPU, memory, network input/output (I/O) and storage I/O.

Requirement ID	SRS-4145
Verification method	Analysis
Requirement	The Platform SHALL allow for geographic distribution of its instances across multiple ITM nodes.

Requirement ID	SRS-4146
Verification method	Analysis
Requirement	The Platform SHALL allow for global load balancing between Datacentres, in order to scale and support increasing volumes.

Requirement ID	SRS-4147
Verification method	Analysis
Requirement	The Platform SHALL support an active/active design local to a datacentre and across datacentre nodes (with replication of session and states for stateful *Components*). In this case both locations are running simultaneously, handling different *Users* and ready to fail over to each other should it become necessary.

Requirement ID	SRS-4148
Verification method	Testing
Requirement	The Platform SHALL be able to perform full and incremental backups (i.e. snapshots) of data and software without impacting system *Availability* and Performance.

Requirement ID	SRS-4158
Verification method	Testing
Requirement	The Platform SHALL be able to backup of both complete repositories as well as selected information element.

Requirement ID	SRS-4157
Verification method	Testing
Requirement	The Platform SHALL allow for backups of full or selected data to occur automatically at a configurable frequency.

Requirement ID	SRS-4156
Verification method	Testing
Requirement	The Platform SHALL make use of offload-host VM backup for backup jobs that create large I/O load and can impact the correct functioning of the production system for more than 5 minutes.

Requirement ID	SRS-4155
Verification method	Analysis
Requirement	The Platform SHALL use offline indexing of image backups for those systems that need to be indexed at the file level.

Requirement ID	SRS-4154
Verification method	Analysis
Requirement	The Platform SHALL use agentless image-based backups with incremental-forever using Changed Block Tracking (CBT).

Requirement ID	SRS-4153
Verification method	Testing
Requirement	The Platform SHALL provide mechanisms to restore software and data lost since last backup.

Requirement ID	SRS-4152
Verification method	Testing
Requirement	The Platform SHALL allow for selection of the backup files and the elements to restore.

Requirement ID	SRS-4149
Verification method	Testing
Requirement	The Platform SHALL be able to archive both a complete repository as well as selected information elements (e.g. objects, records, documents).

Requirement ID	SRS-4160
Verification method	Testing
Requirement	Archived data is searchable/readable and the Platform SHALL provide mechanisms for restoring it to a specified repository as required.

Requirement ID	SRS-4159
Verification method	Testing
Requirement	The Platform SHALL allow an *Authorised User* to recover an archive, or parts of archive, by overwriting or appending.

Bidding Sheets Instructions

INTRODUCTION & IMPORTANT NOTES

All bidders are required to submit pricing details to demonstrate the Purchaser's Pricing Principles are being applied as part of their bids (in the absence of a pre-approved National Format). All data completed in these sheets shall be complete, verifiable and factual and include the required details. Any exclusions may render your bid as non compliant thus removing yourself from the bidding process.

Bidders are **REQUIRED** to complete the Offer Summary tab, the SSS tab, as well as the detailed tabs for Labour, Material, ODCs, and travel. Note that input cells are colour coded **YELLOW in the SSS tab**. Detailed tabs for Labour, Material, ODCs, must be completed as indicated in the detailed instructions for each tab which can be found below, as well as in each detailed tab in the **orange box.** G&A, Overhead, material handling, and other indirect rates do not need to be separately calculated in the detail sheets but **must be included in the totals for each category (Labour/Material/etc.) as appropriate.** A list of the indirect rates applied in the bid must also be provided in the "Rates" tab, although they do no need to be linked to any and the detailed calculations of these rates will be requested in pre-contract award from the winning bidder.

Any formulas provided in these bidding sheets are provided only to assist the bidder. Any changes in formula can be made at the bidder's discretions, as long as the detailed costs are clear, traceable, and accurate as required. **Ultimately the bidder is responsible for ALL values, formulas and calculations** with the bidding sheets that are submitted to the Agency.

Bids in multiple currencies should follow these instructions:
-For the Offer Summary Tab bidders must add columns to the right of the current table; two columns "Currency" and "Firm Fixed Price" for each additional currency of the bid.
-For the CLIN Summary Tab, Bidders have 2 options: A) Columns may be added to the right of the current table; three columns "Quantity", "Unit Price" and "Total Firm Fixed Price" would be added for each additional currency of the bid B) Bidders may duplicate the CLIN Summary tab for each currency bid.
-For the Detailed Tabs Bidders have 2 options: A) Provide all the detailed data for all currencies in the table provided, selecting the individual currencies from the dropdown lists and summing only common currencies together in CLIN Summary/Offer Summary Sheets B) Duplicate the CLIN Summary tab for each currency bid.

DETAILED TABs	DESCRIPTION
MATERIAL LABOUR TRAVEL ODCs	*The detailed tables are to be completed by the bidder with all columns populated, and shall be expanded to include as many rows as necessary to provide the detail requested. Any unnecessary rows should be deleted (no blank entries). The bidder is required to identify for each item the CLIN it is associated with from the drop down menu. Each column should then be populated using the column- specific instructions in the first row. Bidder may not delete columns within tables, or omit information from columns, but may add columns if necessary, although it's not anticipated this will be needed.* *Note CLINs with no costs associated with that item should also be selected within the table, and noted that there is no cost within that table for the CLIN. For example, if there is no labour associated with CLIN X.1, Select CLIN X.1 in the first column and then in the second column note "No Labour is associated with this CLIN". This will help to ensure that all the proper detail has been accounted for and properly allocated.* *Important Note: The Total sum of the "fully burdened" cost column should equal the grand total cost for each category (Labour, Material, etc.) to include profit as well as all indirect rates (G&A/Overhead/Material handling/etc.) associated with that category. These indirect rates must be included in the total firm fixed price on the appropriate detailed tab but are no longer required to be shown as separate calculations at the bidding stage. However, the bidder is required to include the associated indirect costs in the totals of the detailed tab in the base unit costs. Alternatively, the bidder may choose to show these as separate calculations by expanding the table columns to show the additional costs due to these indirect rates (similar to the way profit is calculated). Note again although the detailed indirect rate calculations are not required at the bidding stage, this information will be requested from the winning bidder during pre-contract award discussions.*
Rates	*As discussed previously in these instructions, the detailed indirect rate calculations are not required to be included in the bidding sheets, although the bidders may chose to do so. However, ALL bidders are required to state the G&A/OH/Material handling and any other indirect rates that they have applied to the bid.*

A) COMPLETENESS CHECK for CURRENCY - "OFFER SUMMARY" TAB

Currency has been entered for offer summary tab	**Missing Currency**

B) ACCURACY CHECK #1- OFFER SUMMARY TOTALS MATCH CLIN SUMMARY

		Delta
Total Fixed Price Base Contract	**OK**	0.00
Total Fixed Price Evaluated Options	**OK**	0.00

C) ACCURACY CHECK #2- OFFER SUMMARY TOTALS MATCH DETAIL TABS

Grand Total Offer summary (All CLINS) matches detail	**OK**

D) COMPLETENESS CHECK FOR "CLIN SUMMARY" TAB

All CLINS have a firm fixed price bid- Base Contract	**MISSING PRICING FOR 1 or more CLINS**
All CLINS have a firm fixed price bid- Evaluated Options	**MISSING PRICING FOR 1 or more CLINS**

E) COMPLETENESS CHECK FOR CLIN DETAILS TAB

Labour	**OK**
Material	**OK**
Travel	**OK**
ODCs	**OK**

Automated Checks:

This tab is provided only as a **tool** for the bidders to assist in verifying that they have provided the bid currency as required and that the grand totals are accurate and traceable.

Checks do not guarantee that the bid is accurate or traceable and ultimately the bidder is responsible to meet the requirements outlined in the bidding instructions to ensure completeness, accuracy, and traceability.

Bidder is not required to use this automated checks tab, and is not required to ensure all items are "green" but it's highly recommended by the purchaser that this is used as a tool to ensure accuracy and minimize required corrections to the bid

For multiple currencies, duplicate the "firm fixed price" colum for each currency

CLIN Number	CLIN DESCRIPTION	Firm Fixed Price
Currency		
Wave 1 Base Contract		-
CLIN 2	Work Package 2 -Implement SOA Platform	
CLIN 4	Work Package 4 -Implement IdM Platform	
CLIN 6	Work Package 6 - Support Pilot Integration Cases	
CLIN 7	Work Package 7 - Support integration of other projects	
Wave 2 (Option)		-
CLIN 2	Work Package 2 -Implement SOA Platform	
CLIN 4	Work Package 4 -Implement IdM Platform	
O&M Wave 1 (Option)		-
CLIN 2	Work Package 2 -Implement SOA Platform	
CLIN 4	Work Package 4 -Implement IdM Platform	
CLIN 6	Work Package 6 - Support Pilot Integration Cases	
CLIN 7	Work Package 7 - Support integration of other projects	
O&M Wave 2 (Option)		-
CLIN 2	Work Package 2 -Implement SOA Platform	
CLIN 4	Work Package 4 -Implement IdM Platform	
Total Firm Fixed Price		-

Offer Summary Instructions:
Bidders are to populate all yellow cells. Firm fixed prices need to be provided for every CLIN, with no omissions.

Note any formulas existing in the cells are provided only to assist the bidder, and ultimately all calculations are the bidder's responsibility. As such, the contractor may alter any formulas necessary to provide an accurate, clear and traceable bid as required.

Important Note: The Total sum firm fixed price column in this "Offer Summary" sheet should equal the grand total from the "CLIN Summary" tab. These totals are also required to be traceable to the totals from the details tabs (Labour+Material+Travel+ODCs)= Grand Total= CLIN Summary Tab. The "Automatic Checks" tab provides a limited number of checks to help the bidder ensure the bid is accurate and traceable.

CLIN	WBS Description	Qty/MD Total	Unit Price / Base Cost	Total Price (Indicate Currency Here)	Delivery means	Delivery Date	DESTINATION (Incoterm 2000 DDP at location specified below, unless otherwise stated herein contract)	SoW reference: Sections #

Work Package 2 -Implement SOA (basic) Wave 1

2.1	**Project Management**							
2.1.1.	Project Management Plan(s) and Documents				Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.4., 11.5, 11.6, 12.3, G.2., G.3
2.1.2.	Project Status Report				Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.3, 5.4., G.2.
2.1.3.	Project Management Office				Electronic	EDC + 4 Weeks	Project Website	5.5, 5.6, G.2.
	Total Project Management							
2.2	**Engineering**							**7**
2.2.1.	Orientation Workshop				See Below	See Below	See Below	7.2.
2.2.1.1	Orientation Workshop Documentation				Electronic	1 week before the workshop	Project Website	7.2.
2.2.1.2	Orientation Workshop				Meeting	EDC + 4 weeks	Project Website	7.2.
2.2.2.	System Requirements Analysis and Review				See Below	See Below	See Below	4.4., 7.3.
2.2.2.1	System Requirements Review (SRR)				NCIA	EDC + 2M	NCIA	4.4., 7.3.
2.2.2.2	System Requirements Specifications Change Request				Project Website	EDC + 2M	Project Website	4.4., 7.3.
2.2.3.	Design & Review				See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.3.1	Preliminary Design Review (PDR)				See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.3.1.1.	System Design Documentation Package (SDS, ICDs, Security Accreditation				Electronic	4 Weeks before PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.3.1.2.	Preliminary Design Review (PDR)				Meeting	EDC + 20w	NCIA	4.1., 7.4.
2.2.3.1.3.	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation				Electronic	2 Weeks after PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.3.2	Critical Design Review (CDR)				See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.3.2.1.	System Design Documentation Package (SDS, ICDs, Security Accreditation				Electronic	4 Weeks before CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.3.2.2.	Critical Design Review (CDR)				Meeting	PDR +1M	NCIA	7.4.
2.2.3.2.3.	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation				Electronic	2 Weeks after CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.2.4.	Basic SOA Platform				Electronic	As required	Project Website	6.9
2.2.4.1.	Integration Services (Wave 1)				Electronic	As required	Project Website	6.9
2.2.4.1.1	Messaging Infrastructure				Electronic	As required	Project Website	6.9
2.2.4.1.2	Mediation				Electronic	As required	Project Website	6.9
2.2.4.2.	SMC Services (in support of Wave 1)				Electronic	As required	Project Website	6.9
2.2.4.3.	Platform Hosting Services				Electronic	As required	Project Website	6.9
2.2.5.	Tests (during Product Baseline and before Operational Baseline)				See Below	See Below	See Below	5., 6., 8., 12., 16., G.4.
2.2.5.1	System Tests Documentation Package to support tests				Electronic	3 Weeks before test start date	Project Website	8.1., G.4.
2.2.5.2	OEM Manuals to support tests				Electronic	3 Weeks before test start date	Project Website	5.2, 6.6, 6.8, 8.2, 14.6
2.2.5.3	Technical documentation to support tests				Electronic	3 Weeks before test start date	Project Website	5.2, 6.6, 6.8, 8.2, 14.6
2.2.5.4	TRR meeting and associated report				Meeting / Electronic	before test start date	NCIA, Project Website	8.2., 8.4
2.2.5.5	Baseline test campaigns				As required	start: EDC + 33 Weeks	Project Website	5.2., 6.6., 6.8., 8.2.
2.2.5.6	Updated System Tests Documentation Package as a result of test, in particular Test Report				Electronic	1 Week after test end date	Project Website	8.2., 8.3., 8.4., G.4.
2.2.5.7	Updated Product Baseline				As required	As required	Project Website & NCIA	8.2., 8.4., 12.2
2.2.5.8	FCA report				Electronic	1 Week after test campaign end date	Project Website	8.2., 12.9.
2.2.5.9	Status Test Review (STR) meeting and associated report				Meeting / Electronic	1 week after test campaign	Project Website	8.4.
2.2.6	Site Surveys for PSA sites				Meeting / Electronic	As required	NCIA, Project Website	3.1., 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.
2.2.7	Engineering Documentation				Electronic	1 Week after baseline test campaign	NCIA, Project Website	5.4., 5.5, 5.6., 7., G.2
	Total Engineering							
2.3	**Implementation**							**6**
2.3.1.	Implementation Plan				See below	See below	See below	4.2., 4.5., 5.3, 6.2., 6.4., 6.11., 9.2., 10.1., 13.2.
2.3.1.1	Implementation Plan (final version)				Electronic	PSD+1 Month, and As required	Project Website	4.2., 4.5., 6.2., 6.4., 10.1., G.3
2.3.1.2	Implementation Plan (annexes) - 1 per site				Electronic	8 Weeks before implementation at the site	Project Website	4.2., 4.5., 6.2., 6.4., 10.1., G.3
2.3.2.	Reference System Implementation				See Below	See Below	See Below	4.7, 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.3.2.1	Implementation Plan (initial version, covering Reference System implementation)				Electronic	4 Weeks before HW/SW shipment	Project Website	4.2., 4.5., 6.2., 6.4., 10.1., G.3
2.3.2.2	Inventory / Material Data Sheet				Electronic	10 Days before shipment	Project Website	14.8., C.4.
2.3.2.3	Custom form 302 (if required)				Electronic	10 Days before shipment	Project Website	16.9.
2.3.2.4.	Recommended Tools and Test equipment List (RTTL)				Electronic	10 Days before shipment	Project Website	14.8.
2.3.2.5.	Software Distribution List (SWDL)				Electronic	10 Days before shipment	Project Website	14.8.
2.3.2.6.	Packing List (if applicable)				Electronic	shipment	shipment	14.9.
2.3.2.7.	Personnel Security Clearances (PSC)				Electronic	10 days before delivery	Project Website	6.5., 13.1
2.3.2.8.	Materials (technical services and user services) and associated delivery, installation,				HW/SW	4 Weeks before test start date	NCIA	4.7, 6.6., 7.1., 7.4., 8.2., 12.10., 14.8
2.3.2.9.	Special to Type Tools and Test Equipment: provision and installation (if required)				HW / SW / Labour: Testbed	4 Weeks before test start date	NCIA	4.7, 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.3.2.10.	As-built drawings/documentations				Electronic	Site installation (accordine to SIP)	Project Website	4.7, 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.3.2.11.	PCA report				Electronic	1 Week after test campaign end date	Project Website	4.7, 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.3.2.12.	Localised version of Security Operating Procedures (SecOPs)				Electronic	2 Weeks before test start date	Project Website	6.6., 10.1.
2.3.2.13.	Localised version of Security Test and Verification Plan (STVP)				Electronic	2 Weeks before test start date	Project Website	6.6., 8.2., 10.1
2.3.2.14.	On-site training				Course: per site	As required to align with the SIP	Sites	14.7
2.3.2.15.	Site Installation and Activation checklist				Electronic	1 Week after PCA	Project Website	6.2., 6.4., 6.5., 6.6.
2.3.3.	Site Survey				Electronic	Aligned with the SIP	Project Website	3.1., 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.
2.3.4.	Implementation (PSA and FSA sites)				See Below	See Below	See Below	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.3.4.1	Preparation for installation				Delivered "per site"	10 Days before shipment (Survey report - 1 mo before site installation)	Project Website	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5., 9.2. 9.3. 9.5., 10
2.3.4.1.1.	Site Verification Survey report (if required)				Delivered "per site"	1 Month before site installation	Project Website	6.3., 6.5.
2.3.4.1.2.	Inventory / Material Data Sheet (MDS)				Delivered "per site"	10 Days before shipment	Project Website	14.8
2.3.4.1.3.	Custom form 302 (if required)				Delivered "per site"	10 Days before shipment	Project Website	16.9
2.3.4.2	Integration & Tests				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5. 9.2. 9.3. 9.5., 10.
2.3.4.3	Installation and activation (sites)				SW/meetings/electronic	Site installation (according to SIP)	See below	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5. 9.2. 9.3. 9.5., 10.
2.3.4.4	Deployment				Electronic	1 Week after site activation, aligned with the SIP	Project Website	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5. 9.2. 9.3. 9.5., 10.
2.3.4.4.1	Provision to PMIC lab				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5. 9.2. 9.3. 9.5., 10.
2.3.4.4.2	Provision to PBN				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5. 9.2. 9.3. 9.5., 10.
2.3.4.4.3	Provision to ON				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2. 8.2. 8.4. 8.5. 9.2. 9.3. 9.5., 10.
2.3.5.	Baselines for Wave 1				See Below	See Below	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
2.3.5.1.	System Requirements Review (SRR)				Meeting / Electronic	EDC+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.2.	Critical Design Review (CDR) - Initial Functional Baseline (FBL)				Meeting / Electronic	EDC+2M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.3.	Functional Baseline Review (FBL)				Meeting / Electronic	CDR+1M, CDR+2M, CDR+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.4.	Allocated Baseline Review (ABL)				Meeting / Electronic	CDR+4M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.5.	Internal Release Candidate x.1 (IRCv1 alpha)				Electronic, site, website	CDR+4M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.6.	Production Baseline Review (PBL)				Meeting / Electronic	IRCv1+1M, IRCv1+2M, IRCv1+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.7.	Internal Release Candidate x.2 (IRCv2 beta)				Electronic, site, website	IRCv1+4M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.8.	Release Candidate x.3 (RCv3 final)				Electronic, site, website	IRCv2+4M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.9.	Operational Baseline Review (PBL)				Meeting / Electronic	RCv3+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.10.	Deployment Authorization				NCIA	RCv3+2M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.11.	Partial System Acceptance (PSA) Wave 1				NCIA	OA+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
2.3.5.12.	Final System Acceptance (FSA) Wave 1				NCIA	PSA+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7
	Total Implementation							
2.4	**System Testing and Acceptance**							**8**
2.4.1.	Security Accreditation				See Below	See Below	See Below	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
2.4.1.2	Security Accreditation Documentation				Paper, Electronic: 2 per site (1 for ON, 1 for PBN) + as needed for SSL interception	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10., G.8.
2.4.1.2	Software Approval				Electronic	4 Weeks before test session and as required	See Below	7.4, 8.2
2.4.1.2.1.	Software Approval Documentation Package				Electronic	4 Weeks before test session	Project Website	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
2.4.1.2.2.	Support Software Security and Technical Tests				As required	As required	NCIA	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
2.4.1.2.3.	Support IV&V testing				As required	As required	NCIA	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
2.4.1.2.4.	Updated Product Baseline				As required	As required	Project Website & NCIA	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
2.4.2.	Acceptance Tests				NCIA	As required	Project Website	5.2., 6.6., 6.8., 8.2.
	Total System Acceptance							
2.5	**Integrated Logistics Support (ILS)**							3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
2.5.1.	Integrated Logistics Support Plan (ILSP) +				Electronic	4 weeks before CDR + as required	Project Website	3.1.2., 4.4., 4.5., 5.3, 5.6, 6.3, 6.4, 6.6., 7.2., 7.4 8.2., 9.5., 14.
2.5.1.1.	Maintenance and Support Concept				Electronic	with ILSP	Project Website	6.7.4.
2.5.1.2	Logistic Support Analysis (in form of a report)				Electronic	4 week before CDR + as required	Project Website	14.4
2.5.1.3	Safety Hazard definition and identification analysis				Electronic	4 week before CDR	Project Website	14.5
2.5.1.4	Documentation Business Rules				Electronic	with ILSP	Project Website	3.1.2., 4.4., 4.5., 5.3, 5.6, 6.3, 6.4, 6.6., 7.2., 7.4 8.2., 9.5., 14.
2.5.2.	Technical Documentation				Electronic	4 weeks before SBL and update as needed	Project Website + one per site	12.5., 12.6., 14.6.
2.5.2.1	Operation and user Manuals				Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
2.5.2.2	Maintenance Manuals (including admin and platform manuals)				Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
2.5.2.3	OEM Manuals for COTS				Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
2.5.2.4	On-line documentation (Embedded in the platform)				Electronic	Any SW release	embedded in the SW	14.6.
2.5.3.	Training				See Below	See Below	See below	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8., G.7
2.5.3.1.	Training Requirement Analysis (TRA) report (as part of site surveys)				Electronic	with site survey reports	Project Website	9.5., 14.7
2.5.3.2.	Training Needs Analysis (TNA)				Electronic	2 weeks before SRD and update as needed	Project Website	4.5., 14.7
2.5.3.3.	Training Program/Plan				Electronic	with ILSP	Project Website	4.5., 14.7, G.7.2.
2.5.3.4.	Training Materials				Electronic	4 weeks before first training session	Project Website	8.5., 14.5., 14.7., 14.8., 14.10.
2.5.3.5.	Training Provisioning				On-site & Electronic	with ILSP	Website	14.7.
2.5.4.	Configuration, Issues and Changes Management Package				See below	See below	See below	14
2.5.4.1	Configuration Item Management Database (CMDB)				Electronic	as required to align with the CMP	NCIA	4.9., 5.5., 8.3, 12.4., 12.11.,
2.5.4.2	Software Licenses Repository				Electronic	first version for PSA and updated version on FSA	NCIA	14., 12.2.
2.5.4.3	Change Management Documentation Package (ECP, RFD, RFW)				As required	As required	Project Website	14., 9.4., 10.1., 12.6., 12.7.
2.5.4.4	Issues, Incidents, Risks and Problems Management Documentation Package				Electronic	As required	Project Website	11.4., 11., 14., 4.10., 5.2., 5.3., 5.5., 5.6., 8., 9.4., 10.2., 11.4., 11.7., 12.2.5., 14.6., G.2.
2.5.4.5	CSA (Configuration Status Accounting) Reports				Electronic	As required	Project Website	14., 5.6.1., 7.4.2., 12.6., 12.9
2.5.5.	Warranty				N/A	FSA	Equipment/software	6.12., 14.4., 14.6., 14.8 14.10.
	Total ILS							
2.6	**Software/Equipment**							
2.6.1.	Software and licensing				Electronic: CD/DVD/USB, website	when submittine IRC for review	Equipment/software	3.1.2, 4.6, 4.9, 5.2, 6.4, 6.5, 6.8, 7., 8.2, 8.3, 11.3., 11.6, 12, 12.4, 13.5, 14.6.1, 14.8, 14.9.4, 14.10
	Total Equipment/Software							
2.7	**Operations and Maintenance (OPTIONAL)**							9.4.1, 12.2.4., 14.
2.7.1.	Initial Operational Support				See below	See below	See below	14.3., 14.4.
2.7.1.1.	Governance activities				Labour	from PSA + 1year	Annex C	14.3., 14.4.
2.7.1.2.	System operations activities				Labour	As required	Annex C	14.3., 14.4.
2.7.1.3.	Maintenance and Help-Desk activities				Labour	As required	Annex C	14.3., 14.4.
2.7.1.4.	Non-production-environment activities				Labour	As required	Annex C	14.3., 14.4.
2.7.1.5.	Updates to Service Catalogue for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
2.7.1.6.	Updates to SLA / SLTs / KPIs for Business Services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
2.7.1.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and				Electronic	As required	Project Website	14.3., 14.4.
2.7.1.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
2.7.1.9.	Updates to Service IT-Continuity Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
2.7.1.10.	Service Operation and Continuous Service improvement for Business Services and Support				As required	As required	NCIA	14.3., 14.4.
2.7.1.11.	Updates Interface to ITSM Tools - if required				HW/SW	As required	Annex C	14.3., 14.4.
2.7.1.12.	Service Performance Reports (SLA, KPIs, SLTs)				Paper, Electronic	As required	Project Website	14.3., 14.4.
2.7.1.13.	Service Support Reports (Service specific)				Paper, Electronic	As required	Project Website	14.3., 14.4.
2.7.1.14.	Service Performance Review				Meeting	As required	NCIA	14.3., 14.4.
2.7.1.15.	Service Performance Review Minutes				Meeting + 3 days	As required	Project Website	14.3., 14.4.
2.7.2.	Follow-on Support (Year 2)				See below	From PSA +1year to PSA + 2year	See below	14.3., 14.4.

#	Description	Format	Timing	Location	Ref
2.7.2.1.	Governance activities	Labour	As required	Annex C	14.3 , 14.6
2.7.2.2.	System operations activities	Labour	As required	Annex C	14.3 , 14.6
2.7.2.3.	Maintenance and Help-Desk activities	Labour	As required	Annex C	14.3 , 14.6
2.7.2.4.	Non-production environment activities	Labour	As required	Annex C	14.3 , 14.6
2.7.2.5.	Updates to Service Catalogue for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.2.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.2.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and	Electronic	As required	Project Website	14.3 , 14.6
2.7.2.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.2.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.2.10.	Service Operation and Continuous Service Improvement for Business Services and Support	As required	As required	NCIA	14.3 , 14.6
2.7.2.11.	Updates Interface to ITSM Tools - if required	HW/SW	As required	Annex C	14.3 , 14.6
2.7.2.12.	Service Performance Reports (SLA, KPIs, SLTs)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.2.13.	Service Support Reports (Service specific)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.2.14.	Service Performance Review	Meeting	As required	NCIA	14.3 , 14.6
2.7.2.15.	Service Performance Review Minutes	Electronic	Meeting + 3 days	Project Website	14.3 , 14.6
2.7.3.	**Follow-on Support (Year 3)**	**See Below**	**From PSA + 2year to PSA + 3years**	**See below**	**14.3 , 14.6**
2.7.3.1.	Governance activities	Labour	As required	Annex C	14.3 , 14.6
2.7.3.2.	System operations activities	Labour	As required	Annex C	14.3 , 14.6
2.7.3.3.	Maintenance and Help-Desk activities	Labour	As required	Annex C	14.3 , 14.6
2.7.3.4.	Non-production environment activities	Labour	As required	Annex C	14.3 , 14.6
2.7.3.5.	Updates to Service Catalogue for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.3.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.3.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and	Electronic	As required	Project Website	14.3 , 14.6
2.7.3.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.3.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.3.10.	Service Operation and Continuous Service Improvement for Business Services and Support	As required	As required	NCIA	14.3 , 14.6
2.7.3.11.	Updates Interface to ITSM Tools - if required	HW/SW	As required	Annex C	14.3 , 14.6
2.7.3.12.	Service Performance Reports (SLA, KPIs, SLTs)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.3.13.	Service Support Reports (Service specific)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.3.14.	Service Performance Review	Meeting	As required	NCIA	14.3 , 14.6
2.7.3.15.	Service Performance Review Minutes	Electronic	Meeting + 3 days	Project Website	14.3 , 14.6
2.7.4.	**Follow-on Support (Year 4)**	**See Below**	**From PSA + 3year to PSA + 4year**	**See below**	**14.3 , 14.6**
2.7.4.1.	Governance activities	Labour	As required	Annex C	14.3 , 14.6
2.7.4.2.	System operations activities	Labour	As required	Annex C	14.3 , 14.6
2.7.4.3.	Maintenance and Help-Desk activities	Labour	As required	Annex C	14.3 , 14.6
2.7.4.4.	Non-production environment activities	Labour	As required	Annex C	14.3 , 14.6
2.7.4.5.	Updates to Service Catalogue for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.4.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.4.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and	Electronic	As required	Project Website	14.3 , 14.6
2.7.4.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.4.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.4.10.	Service Operation and Continuous Service Improvement for Business Services and Support	As required	As required	NCIA	14.3 , 14.6
2.7.4.11.	Updates Interface to ITSM Tools - if required	HW/SW	As required	Annex C	14.3 , 14.6
2.7.4.12.	Service Performance Reports (SLA, KPIs, SLTs)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.4.13.	Service Support Reports (Service specific)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.4.14.	Service Performance Review	Meeting	As required	NCIA	14.3 , 14.6
2.7.4.15.	Service Performance Review Minutes	Electronic	Meeting + 3 days	Project Website	14.3 , 14.6
2.7.5.	**Follow-on Support (Year 5)**	**See Below**	**From PSA + 4years to PSA + 5year**	**See below**	**14.3 , 14.6**
2.7.5.1.	Governance activities	Labour	As required	Annex C	14.3 , 14.6
2.7.5.2.	System operations activities	Labour	As required	Annex C	14.3 , 14.6
2.7.5.3.	Maintenance and Help-Desk activities	Labour	As required	Annex C	14.3 , 14.6
2.7.5.4.	Non-production environment activities	Labour	As required	Annex C	14.3 , 14.6
2.7.5.5.	Updates to Service Catalogue for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.5.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.5.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and	Electronic	As required	Project Website	14.3 , 14.6
2.7.5.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required	Electronic	As required	Project Website	14.3 , 14.6
2.7.5.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required	As required	As required	NCIA	14.3 , 14.6
2.7.5.10	Service Operation and Continuous Service Improvement for Business Services and Support	As required	As required	NCIA	14.3 , 14.6
2.7.5.11.	Updates Interface to ITSM Tools - if required	HW/SW	As required	Annex C	14.3 , 14.6
2.7.5.12.	Service Performance Reports (SLA, KPIs, SLTs)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.5.13.	Service Support Reports (Service specific)	Paper, Electronic	As required	Project Website	14.3 , 14.6
2.7.5.14.	Service Performance Review	Meeting	As required	NCIA	14.3 , 14.6
2.7.5.15.	Service Performance Review Minutes	Electronic	Meeting + 3 days	Project Website	14.3 , 14.6
Total O&M					

Total - Work Package 2 - Wave 1

Work Package 2 -Implement SOA (extended) Wave 2

#	Description	Format	Timing	Location	Ref
2.8	**Project Management**				
2.8.1	Project Management Plan(s) and Documents	Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.4. , 11.5, 11.6, 12.3, G.2. , G.3
2.8.2	Project Status Report	Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.3, 5.4., G.2.
2.8.3	Project Management Office	Electronic	EDC + 4 Weeks	Project Website	5.5, 5.6, G.2.
Total Project Management					
2.9	**Engineering**				?
2.9.1	Orientation Workshop	See Below	See Below	See Below	7.2.
2.9.1.1	Orientation Workshop Documentation	Electronic	1 week before the workshop	Project Website	7.2.
2.9.1.2	Orientation Workshop	Meeting	EDC + 4 weeks	NCIA	7.2.
2.9.2.	**System Requirements Analysis and Review**	**See Below**	**See Below**	**See Below**	**4.4. , 7.3.**
2.9.2.1	System Requirements Review (SRR)	NCIA	EDC + 2M	NCIA	4.4., 7.3
2.9.2.2	System Requirements Specifications Change Request	Project Website	EDC + 2M	Project Website	4.4., 7.3.
2.9.3.	**Design & Review**	**See Below**	**See Below**	**See Below**	**4.1. , 4.5., 5.5., 5.6., 7.4.**
2.9.3.1	Preliminary Design Review (PDR)	See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
2.9.3.1.1.	System Design Documentation Package (SDS, ICDs, Security Accreditation	Electronic	4 Weeks before PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4., 8.4
2.9.3.1.2.	Preliminary Design Review (PDR)	Meeting	EDC + 20w	NCIA	4.1., 7.4.
2.9.3.1.3.	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation	Electronic	2 Weeks after PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.9.3.2	Critical Design Review (CDR)	See Below	2 Weeks after PDR	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
2.9.3.2.1.	System Design Documentation Package (SDS, ICDs, Security Accreditation	Electronic	4 Weeks before CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.9.3.2.2.	Critical Design Review (CDR)	Meeting	PDR +1M	NCIA	7.4.
2.9.3.2.3.	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation	Electronic	2 Weeks after CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
2.9.4	**Extended SOA Platform (Wave 2)**		**As required**	**Project Website**	**6.9**
2.9.4.1	Interaction Services (Wave 2)	Electronic	As required	Project Website	6.9
2.9.4.2	Composition	Electronic	As required	Project Website	6.9
2.9.4.3	Registry and Repository Services	Electronic	As required	Project Website	6.9
2.9.4.4	Information Services	Electronic	As required	Project Website	6.9
2.9.4.5	SMC Services (in support of Wave 2)	Electronic	As required	Project Website	6.9
2.9.5	**Tests (during Product Baseline and before Operational Baseline)**	**See Below**	**See Below**	**See Below**	**5., 6., 8., 12., 14., G.4.**
2.9.5.1	System Tests Documentation Package to support tests	Electronic	3 Weeks before test start date	Project Website	8.3., G.4.
2.9.5.2	OEM Manuals to support tests	Electronic	3 Weeks before test start date	Project Website	5.2., 6.6., 6.8., 8.2., 14.6
2.9.5.3	Technical documentation to support tests	Electronic	3 Weeks before test start date	Project Website	5.2., 6.6., 6.8., 8.2., 14.6
2.9.5.4	TRR meeting and associated report	Meeting / Electronic	before test start date	NCIA, Project Website	8.2., 8.4
2.9.5.5	Baseline test campaigns	As required	start: EDC + 33 Weeks	Project Website	5.2., 6.6., 6.8., 8.2.
2.9.5.6	Updated System Tests Documentation Package as a result of test, in particular Test Report	Electronic	1 Week after test end date	Project Website	8.2., 8.3., 8.4., G.4.
2.9.5.7	Updated Product Baseline	As required	1 Week after test end date	Project Website & NCIA	8.2., 8.4., 12.2
2.9.5.8	FCA report	Electronic	1 Week after test test campaign end date	Project Website	8.2., 12.6
2.9.5.9	Status Test Review (STR) meeting and associated report	Meeting / Electronic	1 week after test campaign	NCIA, Project Website	8.4.
2.9.6	**Site Surveys for PSA sites**	**Meeting / Electronic**	**As required**	**NCIA, Project Website**	**3.1. , 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.**
2.9.7	**Engineering Documentation**	**Electronic**	**1 Week after baseline test campaign**	**NCIA, Project Website**	**5.4., 5.5, 5.6., 7., G.2**
Total Engineering					
2.10	**Implementation**				9
2.10.1.	**Implementation Plan**	**See below**	**See below**	**See below**	**4.2., 4.5., 5.3., 6.2., 6.4., 6.11., 9.2., 10.1., 13.2.**
2.10.1.1	Implementation Plan (final version)	Electronic	PSD+1 Month, and As required	Project Website	4.2., 4.5., 6.2., 6.4., 10.1., G.3.
2.10.1.2	Implementation Plan (annexes) - 1 per site	Electronic	8 Weeks before implementation at the site	Project Website	4.2., 4.5., 6.2., 6.4., 10.1., G.3.
2.10.2.	**Reference System Implementation**	**See Below**	**See Below**	**See Below**	**4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.**
2.10.2.1	Implementation Plan (initial version, covering Reference System implementation)	Electronic	4 Weeks before HW/SW shipment	Project Website	4.2., 4.5., 6.2., 6.4., 10.1., G.3.
2.10.2.2	Inventory / Material Data Sheet	Electronic	10 Days before shipment	Project Website	14.8., C.4.
2.10.2.3	Custom form 302 (if required)	Electronic	10 Days before shipment	Project Website	14.9.
2.10.2.4.	Recommended Tools and Test equipment List (RTTL)	Electronic	10 Days before shipment	Project Website	14.8.
2.10.2.5.	Software Distribution List (SWDL)	Electronic	10 Days before shipment	Project Website	14.8.
2.10.2.6.	Packing List (if applicable)	Electronic	shipment	shipment	14.9.
2.10.2.7.	Personnel Security Clearances (PSC)	Electronic	10 days before delivery	Project Website	6.5., 13.1
2.10.2.8.	Materials technical services and user services) and associated delivery, installation.	HW/SW	4 Weeks before test start date	NCIA	4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.10.2.9.	Special to Type Tools and Test Equipment; provision and installation (if required)	HW / SW / Labour; Testbed	4 Weeks before test start date	NCIA	4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.10.2.10.	As-built drawings/documentations	Electronic	Site installation (according to SIP)	Project Website	4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.10.2.11.	PCA report	Electronic	1 Week after test campaign end date	Project Website	4.7., 6.6., 7.1., 7.4., 8.2., 12.10., 14.8.
2.10.2.12.	Localised version of Security Operating Procedures (SecOPs)	Electronic	2 Weeks before test start date	Project Website	6.6., 10.1
2.10.2.13.	Localised version of Security Test and Verification Plan (STVP)	Electronic	2 Weeks before test start date	Project Website	6.6., 8.2., 10.1
2.10.2.14.	On-site training	Course; per site	As required to alien with the SIP	Sites	14.7.
2.10.2.15.	Site Installation and Activation checklist	Electronic	1 Week after PCA	Project Website	6.2., 6.4., 6.5., 6.6.
2.10.3	**Site Survey**	**Aligned with the SIP**		**Project Website**	**3.1. , 4.9., 5.6., 6.3., 6.6., 7.4., 7.6., 9.**
2.10.4.	**Implementation (PSA and FSA sites)**	**See Below**	**Aligned with the SIP**	**Project Website**	**3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.**
2.10.4.1.	Preparation for installation	Delivered "per site"	10 Days before shipment (Survey report - 1 mo before site installation)	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.4.1.1.	Site Verification Survey report (if required)	Delivered "per site"	1 Month before site installation	Project Website	6.3., 6.5.
2.10.4.1.2.	Inventory / Material Data Sheet (MDS)	Delivered "per site"	10 Days before shipment	Project Website	14.8.
2.10.4.1.3.	Custom form 302 (if required)	Delivered "per site"	10 Days before shipment	Project Website	14.9.
2.10.4.2	Integration & Tests	As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.4.3	Installation and activation (sites)	SW/meetings/electronic	Site installation (according to SIP)	See below	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.4.4	**Deployment**	**See below**	**1 Week after site activation, aligned with the SIP**	**Project Website**	**3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.**
2.10.4.4.1	Provision to PMIC lab	As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.4.4.2	Provision to PBN	As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.4.4.3	Provision to DN	As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
2.10.6.	**Baselines for Wave 2**	**See Below**	**See Below**	**Project Website**	**4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7., 8.5.1., 14.7.**
2.10.6.1.	Preliminary Design Review (PDR)	Meeting / Electronic	EDC+18M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.2.	Critical Design Review (CDR) - Initial Functional Baseline (FBL) Wave 2	Meeting / Electronic	EDC+19M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.3.	Functional Baseline Review (FBL)	Meeting / Electronic	CDR+1M, CDR+2M, CDR+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.4.	Allocated Baseline Review (ABL)	Meeting / Electronic	CDR+4M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.5.	Internal Release Candidate x.4 (IRCx4 alpha)	Electronic, site, website	CDR+4M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.6.	Production Baseline Review (PBL)	Meeting / Electronic	IRCx4+1M, IRCx4+2M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.7.	Internal Release Candidate x.5 (IRCx5 beta)	Electronic, site, website	IRCx4+3M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.8.	Release Candidate x.6 (RCx6 final)	Electronic, site, website	RCx5+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.9.	Operational Baseline Review (PBL)	Meeting / Electronic	RCx5+2M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.10.	Deployment Authorisation	NCIA	RCx5+2M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.11.	Partial System Acceptance (PSA) Wave 2	NCIA	OA+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.
2.10.6.12.	Final System Acceptance (FSA) Wave 2	NCIA	PSA+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9, 6.10, 6.11, 8.2.7, 8.5.1., 14.7.

CLIN Summary Instruction:
Bidders are to populate all yellow cells. Firm fixed prices need to be provided for every CLIN, with no omissions.

For the CLIN Summary Tab, Bidders have 2 options: A) Columns may be added to the right of the current table; three columns "Quantity", "Unit Price" and "Total Firm Fixed Price" would be added for each additional currency of the bid B) Bidders may duplicate the CLIN Summary tab for each currency bid.

Note any formulas existing in the cells are provided only to assist the bidder, and ultimately all calculations are the bidder's responsibility. As such, the contractor may alter any formulas necessary to provide an accurate, clear and traceable bid as required.

Important Note: The Total sum firm fixed price column in the CLIN Summary sheet should equal the grand total from the "Offer Summary" tab. These totals are also required to be traceable to the totals from the details tabs (Labour+Material+Travel+ODCs)=Grand Total= CLIN Summary Tab. The "Automatic Checks" tab provides a limited number of checks to help the bidder ensure the bid is accurate and traceable.

Total Implementation						
2.11	**System Testing and Acceptance**					6, 8,
2.11.1.	**Security Accreditation**		**See Below**	**See Below**		6.6, 7.4, 8.2.7, 8.5.1., 9.5., 10.
2.11.1.1	**Security Accreditation Documentation**		Paper, Electronic: 2 per site (1 for ON, 1 for PBN) + as needed for SSL Interconnection	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	6.6, 7.4, 8.2.7, 8.5.1., 9.5., 10., G.8.
2.11.1.2	**Software Approval**		**Electronic**	4 Weeks before test session and as required	**See Below**	7.4, 8.2
2.11.1.2.1.	Software Approval Documentation Package		Electronic	4 Weeks before test session	Project Website	6.6, 7.4, 8.2.7, 8.5.1., 9.5., 10.
2.11.1.2.2.	Support Software Security and Technical Tests		As required	As required	NCIA	6.6, 7.4, 8.2.7, 8.5.1., 9.5., 10.
2.11.1.2.3.	Support IV&V testing		As required	As required	NCIA	6.6, 7.4, 8.2.7, 8.5.1., 9.5., 10.
2.11.1.2.4	Updated Product Baseline		As required	As required	Project Website & NCIA	6.6, 7.4, 8.2.7, 8.5.1., 9.5., 10.
2.11.2.	**Acceptance Tests**		NCIA	As required	Project Website	5.2, 6.6, 6.8, 8.2.
Total System Acceptance						
2.12	**Integrated Logistics Support (ILS)**					3, 4, 5, 6, 7, 8, 9, 10.2, 12, 14, 16, G.
2.12.1.	**Integrated Logistics Support Plan (ILSP) +**		**Electronic**	4 weeks before CDR + as required	**Project Website**	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 16.
2.12.1.1	Maintenance and Support Concept		Electronic	with ILSP	Project Website	G.7, 8.
2.12.1.2	Logistic Support Analysis (in form of a report)		Electronic	4 week before CDR + as required	Project Website	16., 4
2.12.1.3	Safety Hazard definition and identification analysis		Electronic	4 week before CDR	Project Website	16.5
2.12.1.4	Documentation Business Rules		Electronic	with ILSP	Project Website	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 16
2.12.2.	**Technical Documentation**		**Electronic**	4 weeks before SBL and update as needed	Project Website + one per site	12.5., 12.6., 14.6.
2.12.2.1	Operation and user Manuals		Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
2.12.2.2	Maintenance Manuals (including admin and platform manuals)		Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
2.12.2.3	OEM Manuals for COTS		Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
2.12.2.4	On-line documentation (Embedded in the platform)		Electronic	Any SW release	embedded in the SW	14.6
2.12.3.	**Training**		**See below**	**See below**	**See below**	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 16.6., 14.7., 14.8., G.7.
2.12.3.1	Training Requirement Analysis (TRA) report (as part of site surveys)		Electronic	with site survey reports	Project Website	9.5, 14.7
2.12.3.2	Training Needs Analysis (TNA)		Electronic	2 weeks before SRD and update as needed	Project Website	4.5., 14.7
2.12.3.3	Training Program/Plan		Electronic	with ILSP	Project Website	4.5., 14.7., G.7.2.
2.12.3.4	Training Materials		Electronic	4 weeks before first training session	Project Website	8.5., 14.5., 14.7., 14.8., 14.10.
2.12.3.5.	Training Provisioning		On-site & Electronic	with ILSP	Website	14.7.
2.12.4.	**Configuration, Issues and Changes Management Package**		**See below**	**See below**	**See below**	14
2.12.4.1.	Configuration Item Management Database (CMDB)		Electronic	as required to align with the CMP	NCIA	4.9., 5.5., 8.3., 12.4., 12.11.,
2.12.4.2	Software Licenses Repository		Electronic	first version for PSA and updated version on FSA	Project Website	14 , 12.2.
2.12.4.3	Change Management Documentation Package (ECP, RFD, RFW)		Electronic	As required	Project Website	14., 8.4., 10.1., 12.6., 12.7.
2.12.4.4	Issues, Incidents, Risks and Problems Management Documentation Package		Electronic	As required	Project Website	114., 3.1., 3.4., 4.10., 5.2., 5.3., 5.5., 5.6., 8., 9.4., 10.2., 11.4., 11.7., 12.2.5., 14.6., G.2.
2.12.4.5	CSA (Configuration Status Accounting) Reports		Electronic	As required	Project Website	14., 5.6.1., 7.4.2., 12.8., 12.9
2.12.5.	**Warranty**		N/A	FSA	Equipment/software	6.12., 14.4., 14.6., 14.8, 14.10.
Total ILS						
2.13	**Software/Equipment**					
2.13.1.	**Software and licensing**		Electronic, CD/DVD/USB, website	when submitting IRC for review		3.1.2., 4.6., 4.9, 5.2, 6.4, 6.5, 6.8, 7., 8.2, 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1., 14.8., 14.9.4., 14.10.
Total Equipment/Software						
2.14	**Operations and Maintenance (OPTIONAL)**					9.4.1., 12.2.4., 14.
2.14.1.	**Initial Operational Support**		**See below**	from PSA + 1year	**See below**	14.3., 14.4.
2.14.1.1.	Governance activities		Labour	As required	Annex C	14.3., 14.4.
2.14.1.2.	System operations activities		Labour	As required	Annex C	14.3., 14.4.
2.14.1.3.	Maintenance and Help-Desk activities		Labour	As required	Annex C	14.3., 14.4.
2.14.1.4.	Non-production environment activities		Labour	As required	Annex C	14.3., 14.4.
2.14.1.5.	Updates to Service Catalogue for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.1.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.1.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and		Electronic	As required	Project Website	14.3., 14.4.
2.14.1.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.1.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.1.10.	Service Operation and Continuous Service improvement for Business Services and Support		As required	As required	NCIA	14.3., 14.4.
2.14.1.11.	Updates Interface to ITSM Tools - if required		HW/SW	As required	Annex C	14.3., 14.4.
2.14.1.12.	Service Performance Reports (SLA, KPIs, SLTs)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.1.13.	Service Support Reports (Service specific)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.1.14.	Service Performance Review		Meeting	As required	NCIA	14.3., 14.4.
2.14.1.15.	Service Performance Review Minutes		Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
2.14.2.	**Follow-on Support (Year 2)**		**See below**	**From PSA +1year to PSA + 2year**	**See below**	14.3., 14.4.
2.14.2.1.	Governance activities		Labour	As required	Annex C	14.3., 14.4.
2.14.2.2.	System operations activities		Labour	As required	Annex C	14.3., 14.4.
2.14.2.3.	Maintenance and Help-Desk activities		Labour	As required	Annex C	14.3., 14.4.
2.14.2.4.	Non-production environment activities		Labour	As required	Annex C	14.3., 14.4.
2.14.2.5.	Updates to Service Catalogue for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.2.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.2.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and		Electronic	As required	Project Website	14.3., 14.4.
2.14.2.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.2.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.2.10.	Service Operation and Continuous Service improvement for Business Services and Support		As required	As required	NCIA	14.3., 14.4.
2.14.2.11.	Updates Interface to ITSM Tools - if required		HW/SW	As required	Annex C	14.3., 14.4.
2.14.2.12.	Service Performance Reports (SLA, KPIs, SLTs)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.2.13.	Service Support Reports (Service specific)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.2.14.	Service Performance Review		Meeting	As required	NCIA	14.3., 14.4.
2.14.2.15.	Service Performance Review Minutes		Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
2.14.3.	**Follow-on Support (Year 3)**		**See below**	**From PSA + 2year to PSA + 3years**	**See below**	14.3., 14.4.
2.14.3.1.	Governance activities		Labour	As required	Annex C	14.3., 14.4.
2.14.3.2.	System operations activities		Labour	As required	Annex C	14.3., 14.4.
2.14.3.3.	Maintenance and Help-Desk activities		Labour	As required	Annex C	14.3., 14.4.
2.14.3.4.	Non-production environment activities		Labour	As required	Annex C	14.3., 14.4.
2.14.3.5.	Updates to Service Catalogue for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.3.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.3.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and		Electronic	As required	Project Website	14.3., 14.4.
2.14.3.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.3.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.3.10.	Service Operation and Continuous Service improvement for Business Services and Support		As required	As required	NCIA	14.3., 14.4.
2.14.3.11.	Updates Interface to ITSM Tools - if required		HW/SW	As required	Annex C	14.3., 14.4.
2.14.3.12.	Service Performance Reports (SLA, KPIs, SLTs)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.3.13.	Service Support Reports (Service specific)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.3.14.	Service Performance Review		Meeting	As required	NCIA	14.3., 14.4.
2.14.3.15.	Service Performance Review Minutes		Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
2.14.4.	**Follow-on Support (Year 4)**		**See below**	**From PSA + 3year to PSA + 4year**	**See below**	14.3., 14.4.
2.14.4.1.	Governance activities		Labour	As required	Annex C	14.3., 14.4.
2.14.4.2.	System operations activities		Labour	As required	Annex C	14.3., 14.4.
2.14.4.3.	Maintenance and Help-Desk activities		Labour	As required	Annex C	14.3., 14.4.
2.14.4.4.	Non-production environment activities		Labour	As required	Annex C	14.3., 14.4.
2.14.4.5.	Updates to Service Catalogue for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.4.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.4.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and		Electronic	As required	Project Website	14.3., 14.4.
2.14.4.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.4.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.4.10.	Service Operation and Continuous Service improvement for Business Services and Support		As required	As required	NCIA	14.3., 14.4.
2.14.4.11.	Updates Interface to ITSM Tools - if required		HW/SW	As required	Annex C	14.3., 14.4.
2.14.4.12.	Service Performance Reports (SLA, KPIs, SLTs)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.4.13.	Service Support Reports (Service specific)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.4.14.	Service Performance Review		Meeting	As required	NCIA	14.3., 14.4.
2.14.4.15.	Service Performance Review Minutes		Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
2.14.5.	**Follow-on Support (Year 5)**		**See below**	**From PSA + 4years to PSA + 5year**	**See below**	14.3., 14.4.
2.14.5.1.	Governance activities		Labour	As required	Annex C	14.3., 14.4.
2.14.5.2.	System operations activities		Labour	As required	Annex C	14.3., 14.4.
2.14.5.3.	Maintenance and Help-Desk activities		Labour	As required	Annex C	14.3., 14.4.
2.14.5.4.	Non-production environment activities		Labour	As required	Annex C	14.3., 14.4.
2.14.5.5.	Updates to Service Catalogue for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.5.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.5.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and		Electronic	As required	Project Website	14.3., 14.4.
2.14.5.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.5.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required		Electronic	As required	Project Website	14.3., 14.4.
2.14.5.10.	Service Operation and Continuous Service improvement for Business Services and Support		As required	As required	NCIA	14.3., 14.4.
2.14.5.11.	Updates Interface to ITSM Tools - if required		HW/SW	As required	Annex C	14.3., 14.4.
2.14.5.12.	Service Performance Reports (SLA, KPIs, SLTs)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.5.13.	Service Support Reports (Service specific)		Paper, Electronic	As required	Project Website	14.3., 14.4.
2.14.5.14.	Service Performance Review		Meeting	As required	NCIA	14.3., 14.4.
2.14.5.15.	Service Performance Review Minutes		Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
Total O&M						
Total - Work Package 2 Wave 2						

Work						
4.1	**Project Management**					
4.1.1.	**Project Management Plan(s) and Documents**		Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.4., 11.5, 11.6, 12.3, G.2., G.3
4.1.2.	**Project Status Report**		Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.3, 5.4., G.2.
4.1.3.	**Project Management Office**		Electronic	EDC + 4 Weeks	Project Website	5.5, 5.6, G.2.
Total Project Management						
4.2	**Engineering**					
4.2.1.	**Orientation Workshop**		**See Below**	**See Below**	**See Below**	7.2.
4.2.1.1	Orientation Workshop Documentation		Electronic	1 week before the workshop	Project Website	7.2.
4.2.1.2	Orientation Workshop		Meeting	EDC + 4 weeks	NCIA	7.2.
4.2.2.	**System Requirements Analysis (and Review)**		**See Below**	EDC + 2M	**See Below**	4.4., 7.3
4.2.2.1	System Requirements Review (SRR)		NCIA	EDC + 2M	NCIA	4.4., 7.3
4.2.2.2	System Requirements Specifications Change Request		Project Website	EDC + 2M	Project Website	4.4., 7.3
4.2.3.	**Design & Review (PDR and CDR)**		**See below**	See below	**See below**	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.1.	**Preliminary Design Review (PDR)**		**See below**	**See below**	**See below**	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.1.1	System Design Documentation Package (SDS, ICDs, Security Accreditation		Electronic	4 Weeks before PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.1.2	Preliminary Design Review (PDR)		Meeting	EDC + 20w	NCIA	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.1.3	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation		Electronic	2 Weeks after PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.2.	**Critical Design Review (CDR)**		**See below**	**See below**	**See below**	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.2.1	System Design Documentation Package (SDS, ICDs, Security Accreditation		Electronic	4 Weeks before CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.3.2.2	Critical Design Review (CDR)		Meeting	PDR +6M	NCIA	7.4.
4.2.3.2.3	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation		Electronic	2 Weeks after CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.2.4.	**Basic IdM Platform (Wave 1)**		**Electronic**	As required	Project Website	6.10.
4.2.4.1.	Identities Management		Electronic	As required	Project Website	6.10.
4.2.4.2.	Credential Management		Electronic	As required	Project Website	6.10.
4.2.4.3.	Authentication Management		Electronic	As required	Project Website	6.10.

ID	Description				Format	Timing	Destination	Reference
4.2.4.3.1	Authentication				Electronic	As required	Project Website	6.10.
4.2.4.3.2	Security Token Services				Electronic	As required	Project Website	6.10.
4.2.4.4.	Access Management				Electronic	As required	Project Website	6.10.
4.2.5	**Tests (during Product Baseline and before Operational Baseline)**				**See Below**	**See Below**	**See Below**	**5., 6., 8., 12., 14., G.4.**
4.2.5.1	System Tests Documentation Package to support tests				Electronic	3 Weeks before test start date	Project Website	8.1. G.4.
4.2.5.2	O&M Manuals to support tests				Electronic	3 Weeks before test start date	Project Website	5.2., 6.6., 6.8., 8.2., 14.6
4.2.5.3	Technical documentation to support tests				Electronic	3 Weeks before test start date	Project Website	5.2., 6.6., 6.8., 8.2., 14.6
4.2.5.4	TRR meeting and associated report				Meeting / Electronic	before test start date	NCIA, Project Website	8.2., 8.4
4.2.5.5	Baseline test campaigns				As required	start: EDC + 33 Weeks	Project Website	5.2., 6.6., 6.8., 8.2.
4.2.5.6	Updated System Tests Documentation Package as a result of test, in particular Test Report				Electronic	1 Week after test end date	Project Website	8.2., 8.3., 8.4., G.4.
4.2.5.7	Updated Product Baseline				As required	1 Week after test end date	Project Website & NCIA	8.2., 8.4., 12.2
4.2.5.8	FCA report				Electronic	1 Week after test test campaign end date	Project Website	8.2., 12.6.
4.2.5.9	Status Test Review (STR) meeting and associated report				Meeting / Electronic	1 week after test campaign	NCIA, Project Website	8.4.
4.2.6	**Engineering Documentation**				**Electronic**	**1 Week after baseline test campaign**	**NCIA, Project Website**	**5.4., 5.5, 5.6., 7., G.2**
Total Engineering								
4.3	**Implementation**							
4.3.1.	**Implementation Plan (PSA and FSA sites)**				see below	see below	see below	4.2., 4.5., 5.3., 6.2., 6.4., 6.11., 9.2., 10.1., 13.2.
4.3.1.1.	**Integration & Test**				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
4.3.1.2	**Installation and activation (sites)**				SW/meetings/electronic	Site installation (according to SIP)	See below	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
4.3.1.3.	**Deployment**				Electronic	1 Week after site activation, aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
4.3.1.3.1	Installation to FMIC lab				As required	1 Week after site activation, aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
4.3.1.3.2	Installation to PBN				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
4.3.1.3.3	Installation to ON				As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2., 8.2., 8.4., 8.5., 9.2., 9.3., 9.5., 10.
4.3.2.	**Baselines for Wave 1**				**See Below**	**See Below**	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.1.	System Requirements Review (SRR)				Meeting / Electronic	EDC+2M	Project Website	4.2.3., 6.1.2., 6.8 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.2.	Critical Design Review (CDR) - initial Functional Baseline (FBL)				Meeting / Electronic	EDC+2M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.3.	Functional Baseline Review (FBL)				Meeting / Electronic	CDR+1M, CDR+2M, CDR+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.4.	Allocated Baseline Review (ABL)				Meeting / Electronic	CDR+4M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.5.	Internal Release Candidate v.1 (IRCv1 alpha)				Electronic, site, website	CDR+4M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.6.	Production Baseline Review (PBL)				Meeting / Electronic	IRCv1+1M, IRCv1+2M, IRCv1+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.7.	Internal Release Candidate v.2 (IRCv2 beta)				Electronic, site, website	IRCv1+4M	Site, Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.8.	Release Candidate v.3 (RCv3 final)				Electronic, site, website	IRCv2+4M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.9.	Operational Baseline Review (PBL)				Meeting / Electronic	RCv3+1M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.10.	Deployment Authorisation				NCIA	RCv3+2M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.11.	Partial System Acceptance (PSA) Wave 1				NCIA	OA+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
4.3.2.12.	Final System Acceptance (FSA) Wave 1				NCIA	PSA+3M	Project Website	4.2.3., 6.1.2., 6.8, 6.9., 6.10., 6.11., 8.2.7., 14.7.
Total Implementation								
4.4	**System Testing and Acceptance**							6., 8.
4.4.1.	**Security Accreditation**				see below	see below	see below	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
4.4.1.1.	**Security Accreditation Documentation**				Paper, Electronic: 2 per site (1 for ON, 1 for PBN) + as needed for SSL Interception	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10., G.8.
4.4.1.2.	**Software Approval**				Electronic	4 Weeks before test session and as required	See Below	7.4., 8.2
4.4.1.2.1	Software Approval Documentation Package				Electronic	4 Weeks before test session	Project Website	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
4.4.1.2.2	Support Software Security and Technical Tests				As required	4 Weeks before test session	NCIA	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
4.4.1.2.3	Support IV&V testing				As required	As required	NCIA	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
4.4.1.2.4	Updated Product Baseline				As required	As required	Project Website & NCIA	6.6., 7.4., 8.2.7., 8.5.1., 9.5., 10.
4.4.2.	**Acceptance Tests**				NCIA	As required	Project Website & NCIA	5.2., 6.6., 6.8., 8.2.
Total System Acceptance								
4.5	**Integrated Logistics Support**							3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
4.5.1.	**Integrated Logistics Support Plan (ILSP)**				**Electronic**	4 weeks before CDR + as required	**Project Website**	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 14.
4.5.1.1.	Maintenance and Support Concept				Electronic	with ILSP	Project Website	6.7, 6.
4.5.1.2.	Logistic Support Analysis (in form of a report)				Electronic	4 week before CDR + as required	Project Website	14., 4
4.5.1.3.	Safety Hazard definition and identification analysis				Electronic	4 week before CDR	Project Website	14.5.
4.5.1.4.	Documentation Business Rules				Electronic	with ILSP	Project Website	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4, 8.2., 9.5., 14.
4.5.2.	**Technical Documentation**				**Electronic**	4 weeks before SBL and update as needed	Project Website + one per site	12.5., 12.6., 14.6.
4.5.2.1.	Operation and user Manuals				Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
4.5.2.2.	Maintenance Manuals (including admin and platform manuals)				Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6.
4.5.2.3.	O&M Manuals for COTS				Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6.
4.5.2.4.	On-line documentation (Embedded in the product)				Electronic	A/w SW release	embedded in the SW	14.6
4.5.3.	**Training**				**See below**	**See below**	**See below**	3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 16.6., 14.7., 14.8
4.5.3.1.	Training Requirement Analysis (TRA) report (as part of site surveys)				Electronic	with site survey reports	Project Website	6.5, 14.7
4.5.3.2.	Training Needs Analysis (TNA)				Electronic	2 weeks before SRD and update as needed	Project Website	4.5., 14.7
2.5.3.3.	Training Program/Plan				Electronic	with ILSP	Project Website	4.5., 14.7., G.7.2.
4.5.3.4.	Training Materials				Electronic	4 weeks before first training session	Project Website	8.5., 14.5, 14.7, 14.8., 14.10., G.7.
4.5.3.5.	Training Provisioning				On-site & Electronic	with ILSP	Website	14.7.
4.5.4.	**Configuration, Issues and Changes Management Package**				**See Below**	**See below**	**See below**	14
4.5.4.1.	Configuration Item Management Database (CMDB)				Electronic	as required to align with the CMP	NCIA	4.9., 5.5., 8.3., 12.4., 12.11.,
4.5.4.2.	Software Licenses Repository				Electronic	first version for PSA and updated version on FSA	Project Website	12.2., 14.
4.5.4.3.	Change Management Documentation Package (SCP, RFD, RFW)				Electronic	As required	Project Website	9.4., 10.1., 12.6., 12.7., 14.
4.5.4.4.	Issues, Incidents, Risks and Problems Management Documentation Package				Electronic	As required	Project Website	3.1., 3.4., 4.10., 5.2., 5.3., 5.5., 5.6., 8., 9.4., 10.2., 11.4., 11.7., 12.2.5., 14.6., G.2
4.5.4.5.	CSA Reports (Configuration Status Accounting)				Electronic	As required	Project Website	5.6.1., 7.4.2., 12.8., 12.9 14.
4.5.5.	**Warranty**				**N/A**	**FSA**	**Equipment/software**	6.12., 14.4., 14.6., 14.8., 14.10.
Total Support								
4.6	**Software/Equipment**							
4.6.1.	**Software and licensing IdM**				Electronic, CD/DVD/USB, website	when submitting IRC/RC for review		3.1.2., 4.6., 4.9., 5.2., 6.4., 6.5., 6.8., 7., 8.2., 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1., 14.8., 14.9.4., 14.10.
Total Equipment								
4.7	**Operations and Maintenance (OPTIONAL)**							9.4.1., 12.2.4., 14.
4.7.1.	**Initial Operational Support**				**See below**	**from PSA + 1year**	**See below**	**14.3., 14.4.**
4.7.1.1.	Governance activities				Labour	As required	Annex C	14.3., 14.4.
4.7.1.2.	System operations activities				Labour	As required	Annex C	14.3., 14.4.
4.7.1.3.	Maintenance and Help-Desk activities				Labour	As required	Annex C	14.3., 14.4.
4.7.1.4.	Non-production environment activities				Labour	As required	Annex C	14.3., 14.4.
4.7.1.5.	Updates to Service Catalogue for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.1.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.1.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and				Electronic	As required	Project Website	14.3., 14.4.
4.7.1.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.1.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.1.10.	Service Operation and Continuous Service Improvement for Business services and Support				As required	As required	NCIA	14.3., 14.4.
4.7.1.11.	Updates Interface to ITSM Tools - if required				HW/SW	As required	Annex C	14.3., 14.4.
4.7.1.12.	Service Performance Reports (SLA, KPIs, SLTs)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.1.13.	Service Support Reports (Service-specific)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.1.14.	Service Performance Review				Meeting	As required	NCIA	14.3., 14.4.
4.7.1.15.	Service Performance Review Minutes				Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.7.2.	**Follow-on Support (Year 2)**				**See below**	**From PSA +1year to PSA + 2year**	**See below**	**14.3., 14.4.**
4.7.2.1.	Governance activities				Labour	As required	Annex C	14.3., 14.4.
4.7.2.2.	System operations activities				Labour	As required	Annex C	14.3., 14.4.
4.7.2.3.	Maintenance and Help-Desk activities				Labour	As required	Annex C	14.3., 14.4.
4.7.2.4.	Non-production environment activities				Labour	As required	Annex C	14.3., 14.4.
4.7.2.5.	Updates to Service Catalogue for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.2.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.2.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and				Electronic	As required	Project Website	14.3., 14.4.
4.7.2.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.2.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.2.10.	Service Operation and Continuous Service Improvement for Business services and Support				As required	As required	NCIA	14.3., 14.4.
4.7.2.11.	Updates Interface to ITSM Tools - if required				HW/SW	As required	Annex C	14.3., 14.4.
4.7.2.12.	Service Performance Reports (SLA, KPIs, SLTs)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.2.13.	Service Support Reports (Service-specific)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.2.14.	Service Performance Review				Meeting	As required	NCIA	14.3., 14.4.
4.7.2.15.	Service Performance Review Minutes				Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.7.3.	**Follow-on Support (Year 3)**				**See below**	**From PSA + 2year to PSA + 3years**	**See below**	**14.3., 14.4.**
4.7.3.1.	Governance activities				Labour	As required	Annex C	14.3., 14.4.
4.7.3.2.	System operations activities				Labour	As required	Annex C	14.3., 14.4.
4.7.3.3.	Maintenance and Help-Desk activities				Labour	As required	Annex C	14.3., 14.4.
4.7.3.4.	Non-production environment activities				Labour	As required	Annex C	14.3., 14.4.
4.7.3.5.	Updates to Service Catalogue for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.3.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.3.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and				Electronic	As required	Project Website	14.3., 14.4.
4.7.3.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.3.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.3.10.	Service Operation and Continuous Service Improvement for Business services and Support				As required	As required	NCIA	14.3., 14.4.
4.7.3.11.	Updates Interface to ITSM Tools - if required				HW/SW	As required	Annex C	14.3., 14.4.
4.7.3.12.	Service Performance Reports (SLA, KPIs, SLTs)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.3.13.	Service Support Reports (Service-specific)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.3.14.	Service Performance Review				Meeting	As required	NCIA	14.3., 14.4.
4.7.3.15.	Service Performance Review Minutes				Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.7.4.	**Follow-on Support (Year 4)**				**See below**	**From PSA + 3year to PSA + 4year**	**See below**	**14.3., 14.4.**
4.7.4.1.	Governance activities				Labour	As required	Annex C	14.3., 14.4.
4.7.4.2.	System operations activities				Labour	As required	Annex C	14.3., 14.4.
4.7.4.3.	Maintenance and Help-Desk activities				Labour	As required	Annex C	14.3., 14.4.
4.7.4.4.	Non-production environment activities				Labour	As required	Annex C	14.3., 14.4.
4.7.4.5.	Updates to Service Catalogue for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.4.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.4.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and				Electronic	As required	Project Website	14.3., 14.4.
4.7.4.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.4.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.4.10.	Service Operation and Continuous Service Improvement for Business services and Support				As required	As required	NCIA	14.3., 14.4.
4.7.4.11.	Updates Interface to ITSM Tools - if required				HW/SW	As required	Annex C	14.3., 14.4.
4.7.4.12.	Service Performance Reports (SLA, KPIs, SLTs)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.4.13.	Service Support Reports (Service-specific)				Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.4.14.	Service Performance Review				Meeting	As required	NCIA	14.3., 14.4.
4.7.4.15.	Service Performance Review Minutes				Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.7.5.	**Follow-on Support (Year 5)**				**See below**	**From PSA + 4years to PSA + 5year**	**See below**	**14.3., 14.4.**
4.7.5.1.	Governance activities				Labour	As required	Annex C	14.3., 14.4.
4.7.5.2.	System operations activities				Labour	As required	Annex C	14.3., 14.4.
4.7.5.3.	Maintenance and Help-Desk activities				Labour	As required	Annex C	14.3., 14.4.
4.7.5.4.	Non-production environment activities				Labour	As required	Annex C	14.3., 14.4.
4.7.5.5.	Updates to Service Catalogue for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.5.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.5.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and				Electronic	As required	Project Website	14.3., 14.4.
4.7.5.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.
4.7.5.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required				Electronic	As required	Project Website	14.3., 14.4.

#	Description			Media	Frequency/Timing	Destination	Reference
4.7.5.10.	Service Operation and Continuous Service Improvement for Business Services and Support			As required	As required	NCIA	14.3., 14.4.
4.7.5.11.	Updates Interface to ITSM Tools - if required			HW/SW	As required	Annex C	14.3., 14.4.
4.7.5.12.	Service Performance Reports (SLA, KPIs, SLTs)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.5.13.	Service Support Reports (Service specific)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.7.5.14.	Service Performance Review			Meeting	As required	NCIA	14.3., 14.4.
4.7.5.15.	Service Performance Review Minutes			Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
Total O&M							
Total - Work Package # Wave 1							
Work							
4.8	**Project Management**						
4.8.1.	Project Management Plan(s) and Documents			Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.4., 11.5, 11.6, 12.3, G.2., G.3
4.8.2.	Project Status Report			Electronic	EDC + 4 Weeks and as changes occur	Project Website	5.3, 5.4., G.2.
4.8.3.	Project Management Office			Electronic	EDC + 4 Weeks	Project Website	5.5, 5.6, G.3
Total Project Management							
4.9	**Engineering**						
4.9.1.	Orientation Workshop			See Below	See Below	See Below	7.2
4.9.1.1	Orientation Workshop Documentation			Electronic	1 week before the workshop	Project Website	7.2
4.9.1.2	Orientation Workshop			Meeting	EDC + 4 weeks	NCIA	7.2
4.9.2.	System Requirements Analysis (and Review)			See Below	See Below	See Below	4.4., 7.3
4.9.2.1	System Requirements Review (SRR)			Electronic	EDC + 2M	NCIA	4.4., 7.3
4.9.2.2	System Requirements Specifications Change Request			Project Website	EDC + 2M	Project Website	4.4., 7.3
4.9.3.	Design & Review (PDR and CDR)			See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.1.	Preliminary Design Review (PDR)			See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.1.1	System Design Documentation Package (SDS, ICDs, Security Accreditation)			Electronic	4 Weeks before PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.1.2	Preliminary Design Review (PDR)			Meeting	EDC + 20w	NCIA	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.1.3	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation)			Electronic	2 Weeks after PDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.2.	Critical Design Review (CDR)			See Below	See Below	See Below	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.2.1	System Design Documentation Package (SDS, ICDs, Security Accreditation)			Electronic	4 Weeks before CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.3.2.2	Critical Design Review (CDR)			Meeting	PDR +1M	NCIA	7.4.
4.9.3.2.3	Updated System Design Documentation Package (SDS, ICDs, Security Accreditation)			Electronic	2 Weeks after CDR	Project Website	4.1., 4.5., 5.5., 5.6., 7.4.
4.9.4	Extended IdM Platform (Wave 2)			Electronic	As required	Project Website	6.10.
4.9.4.1	Identity Federation			Electronic	As required	Project Website	6.10.
4.9.4.2	Allied Replication Hub			Electronic	As required	Project Website	6.10.
4.9.4.3	Federated Authentication			Electronic	As required	Project Website	6.10.
4.9.5	Tests (during Product Baseline and before Operational Baseline)			See Below	See Below	See Below	5., 6., 8., 12., 14., G.4.
4.9.5.1	System Tests Documentation Package to support tests			Electronic	3 Weeks before test start date	Project Website	8.1, G.4.
4.9.5.2	OEM Manuals to support tests			Electronic	3 Weeks before test start date	Project Website	5.2., 6.6., 6.8., 8.2., 14.6
4.9.5.3	Technical documentation to support tests			Electronic	3 Weeks before test start date	Project Website	5.2., 6.6., 6.8., 8.2., 14.6
4.9.5.4	TRR meeting and associated report			Meeting / Electronic	before test start date	NCIA, Project Website	8.2., 8.4
4.9.5.5	Baseline test campaigns			As required	start: EDC + 33 Weeks	Project Website	5.2., 6.6., 6.8., 8.2.
4.9.5.6	Updated System Tests Documentation Package as a result of test, in particular Test Report			Electronic	1 Week after test end date	Project Website	8.2., 8.3., 8.4., G.4.
4.9.5.7	Updated Product Baseline			As required	As required	Project Website & NCIA	8.2., 8.4., 12.2
4.9.5.8	FCA report			Electronic	1 Week after test test campaign end date	Project Website	8.2., 12.9.
4.9.5.9	Status Test Review (STR) meeting and associated report			Meeting / Electronic	1 week after test campaign	NCIA, Project Website	8.4.
4.9.6	Engineering Documentation			Electronic	1 Week after baseline test campaign	NCIA, Project Website	5.4., 5.5, 5.6., 7., G.2
Total Engineering							
4.10.	**Implementation**						6
4.10.1.	Implementation Plan (PSA and FSA sites)			see below	see below	see below	4.2., 4.5., 5.3., 6.2., 6.4., 6.11., 9.2., 10.1., 13.2.
4.10.1.1.	Integration & Test			As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2, 8.2, 8.4., 8.5., 9.2, 9.3., 9.5., 10.
4.10.1.2.	Installation and activation (sites)			SW/meetings/electronic	Site installation (according to SIP)	See below	3., 4., 5., 6., 7.2, 8.2, 8.4., 8.5., 9.2, 9.3., 9.5., 10.
4.10.1.3.	Deployment			Electronic	1 Week after site activation, aligned with the SIP	Project Website	3., 4., 5., 6., 7.2, 8.2, 8.4., 8.5., 9.2, 9.3., 9.5., 10.
4.10.1.3.1	Installation to PMIC lab			Electronic	1 Week after site activation, aligned with the SIP	Project Website	3., 4., 5., 6., 7.2, 8.2, 8.4., 8.5., 9.2, 9.3., 9.5., 10.
4.10.1.3.2	Installation to PBN			As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2, 8.2, 8.4., 8.5., 9.2, 9.3., 9.5., 10.
4.10.1.3.3	Installation to ON			As required	Aligned with the SIP	Project Website	3., 4., 5., 6., 7.2, 8.2, 8.4., 8.5., 9.2, 9.3., 9.5., 10.
4.10.3.	Baselines for Wave 2			See Below	See Below	See Below	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.1.	Preliminary Design Review (PDR)			Meeting / Electronic	EDC+18M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.2.	Critical Design Review (CDR) - initial Functional Baseline (FBL) Wave 2			Meeting / Electronic	EDC+19M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.3.	Functional Baseline Review (FBL)			Meeting / Electronic	CDR+1M. CDR+2M. CDR+3M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.4.	Allocated Baseline Review (ABL)			Meeting / Electronic	CDR+4M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.5.	Internal Release Candidate v.4 (IRCv4 alpha)			Electronic, site, website	CDR+4M	Site, Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.6.	Production Baseline Review (PBL)			Meeting / Electronic	IRCv4+1M. IRCv4+2M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.7.	Internal Release Candidate v.5 (IRCv5 beta)			Electronic, site, website	IRCv4+3M	Site, Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.8.	Release Candidate v.6 (RCv6 final)			Electronic, site, website	RCv5+3M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.9.	Operational Baseline Review (PBL)			Meeting / Electronic	RCv5+2M	Site, Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.10.	Deployment Authorisation			NCIA	RCv5+2M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.11.	Partial System Acceptance (PSA) Wave 2			NCIA	OA+3M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
4.10.3.12.	Final System Acceptance (FSA) Wave 2			NCIA	PSA+3M	Project Website	4.2.3., 6.12., 6.8, 6.9., 6.10., 6.11., 8.2.7, 8.5.1., 14.7.
Total Implementation							
4.11	**System Testing and Acceptance**			see below	see below	see below	6., 8.
4.11.1.	Security Accreditation			Paper, Electronic: 2 per site (1 for ON, 1 for PBN) + as needed for SSL Interception	4 Weeks before PDR + 4 Weeks before CDR + As required	Project Website	6.6., 7.4, 8.2.7, 8.5.1., 9.5., 10.
4.11.1.1.	Security Accreditation Documentation				4 Weeks before test session and as required	See Below	6.6., 7.4, 8.2.7, 8.5.1., 9.5., 10., G.8.
4.11.1.2.	Software Approval			Electronic	4 Weeks before test session and as required	See Below	7.4, 8.2
4.11.1.2.1	Software Approval Documentation Package			Electronic	4 Weeks before test session	Project Website	6.6., 7.4, 8.2.7, 8.5.1., 9.5., 10.
4.11.1.2.2	Support Software Security and Technical Tests			As required	As required	NCIA	6.6., 7.4, 8.2.7, 8.5.1., 9.5., 10.
4.11.1.2.3	Support IV&V testing			As required	As required	NCIA	6.6., 7.4, 8.2.7, 8.5.1., 9.5., 10.
4.11.1.2.4	Updated Product Baseline			As required	As required	Project Website & NCIA	6.6., 7.4, 8.2.7, 8.5.1., 9.5., 10.
4.11.2.	Acceptance Tests			NCIA	As required	Project Website & NCIA	5.2., 6.6., 8.4., 8.2.
Total System Acceptance							
4.12	**Integrated Logistics Support**						3., 4., 5., 6., 7., 8., 9., 10.2., 12., 14., B., G.
4.12.1.	Integrated Logistics Support Plan (ILSP)			Electronic	4 weeks before CDR + as required	Project Website	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4 8.2., 9.5., 14.
4.12.1.1.	Maintenance and Support Concept			Electronic	with ILSP	Project Website	6.7, 8.
4.12.1.2.	Logistic Support Analysis (in form of a report)			Electronic	4 week before CDR + as required	Project Website	14., 4
4.12.1.3.	Safety Hazard definition and identification analysis			Electronic	4 week before CDR	Project Website	14.5.
4.12.1.4.	Documentation Business Rules			Electronic	with ILSP	Project Website	3.1.2., 4.4., 4.5., 5.3., 5.6., 6.3., 6.4., 6.6., 7.2., 7.4 8.2., 9.5., 14.
4.12.2.	Technical Documentation			Electronic	4 weeks before SBL and update as needed	Project Website + one per site	12.5., 12.6., 14.6.
4.12.2.1.	Operation and user Manuals			Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6., G.7.
4.12.2.2.	Maintenance Manuals (including admin and platform manuals)			Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6
4.12.2.3.	OEM Manuals for COTS			Paper, Electronic	4 weeks before SBL and update as needed	Project Website + one per site	14.6
4.12.2.4.	On-line documentation (Embedded in the platform)			Any SW release	Any SW release	embedded in the SW	14.6
4.12.3.	Training			See below	See below	See below	3.1., 3.2, 4.5, 4.9, 6.1, 6.6, 8.5, 9.3, 9.5, 11.7, 12.2, 14.5, 14.6, 14.7, 14.8
4.12.3.1.	Training Requirement Analysis (TRA) report (as part of site surveys)			Electronic	with site survey reports	Project Website	9.5, 14.7
4.12.3.2.	Training Needs Analysis (TNA)			Electronic	2 weeks before SRO and update as needed	Project Website	4.5., 14.7
4.12.3.3.	Training Program/Plan			Electronic	with ILSP	Project Website	4.5., 14.7., G.7.2.
4.12.3.4.	Training Materials			Electronic	4 weeks before first training session	Project Website	8.5., 14.5, 14.7, 14.8, 14.10., G.7
4.12.3.5.	Training Provisioning			On-site & Electronic	with ILSP	Website	14.7.
4.12.4.	Configuration, Issues and Changes Management Package			See below	See below	See below	14
4.12.4.1.	Configuration Item Management Database (CMDB)			Electronic	as required to align with the CMP	NCIA	4.9., 5.5., 8.3., 12.4., 12.11.,
4.12.4.2.	Software License Repository			Electronic	first version for PSA and updated version on FSA	Project Website	12.3., 14.
4.12.4.3.	Change Management Documentation Package (ECP, RFD, RFW)			Electronic	As required	Project Website	9.4., 10.1., 12.6., 12.7., 14.
4.12.4.4.	Issues, Incidents, Risks and Problems Management Documentation Package			Electronic	As required	Project Website	3.1., 3.4., 4.10., 5.2., 5.3., 5.5., 5.6., 8., 8.4., 10.2., 11.4., 11.7., 12.2.5., 14.6., G.2
4.12.4.5.	CSA Reports (Configuration Status Accounting)			Electronic	As required	Project Website	5.6.1., 7.4.2., 12.8., 12.9, 14.
4.12.5.	Warranty			N/A	FSA	Equipment/software	6.12., 14.4., 14.6., 14.8., 14.10.
Total Support							
4.13	**Software/Equipment**						
4.13.1.	Software and licensing IdM			Electronic, CD/DVD/USB, website	when submitting IRC/RC for review		3.1.2., 4.6., 4.9., 5.2., 6.4., 6.5., 6.8., 7., 8.2., 8.3., 11.3., 11.6., 12., 13.4., 13.5., 14.6.1, 14.8., 14.9.4., 14.10.
Total Equipment							
4.14	**Operations and Maintenance (OPTIONAL)**						9.4.3., 12.2.4., 14.
4.14.1.	Initial Operational Support			See below	from PSA + 1year	See below	14.3., 14.4.
4.14.1.1.	Governance activities			Labour	As required	Annex C	14.3., 14.4.
4.14.1.2.	System operations activities			Labour	As required	Annex C	14.3., 14.4.
4.14.1.3.	Maintenance and Help-Desk activities			Labour	As required	Annex C	14.3., 14.4.
4.14.1.4.	Non-production environment activities			Labour	As required	Annex C	14.3., 14.4.
4.14.1.5.	Updates to Service Catalogue for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.1.6.	Updates to SLA / SLTs / KPIs for Business Services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.1.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and			Electronic	As required	Project Website	14.3., 14.4.
4.14.1.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.1.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.1.10.	Service Operation and Continuous Service Improvement for Business Services and Support			As required	As required	NCIA	14.3., 14.4.
4.14.1.11.	Updates Interface to ITSM Tools - if required			HW/SW	As required	Annex C	14.3., 14.4.
4.14.1.12.	Service Performance Reports (SLA, KPIs, SLTs)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.1.13.	Service Support Reports (Service specific)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.1.14.	Service Performance Review			Meeting	As required	NCIA	14.3., 14.4.
4.14.1.15.	Service Performance Review Minutes			Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.14.2.	Follow-on Support (Year 2)			See below	From PSA +1year to PSA + 2year	See below	14.3., 14.4.
4.14.2.1.	Governance activities			Labour	As required	Annex C	14.3., 14.4.
4.14.2.2.	System operations activities			Labour	As required	Annex C	14.3., 14.4.
4.14.2.3.	Maintenance and Help-Desk activities			Labour	As required	Annex C	14.3., 14.4.
4.14.2.4.	Non-production environment activities			Labour	As required	Annex C	14.3., 14.4.
4.14.2.5.	Updates to Service Catalogue for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.2.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.2.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and			Electronic	As required	Project Website	14.3., 14.4.
4.14.2.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.2.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.2.10.	Service Operation and Continuous Service Improvement for Business Services and Support			Electronic	As required	NCIA	14.3., 14.4.
4.14.2.11.	Updates Interface to ITSM Tools - if required			HW/SW	As required	Annex C	14.3., 14.4.
4.14.2.12.	Service Performance Reports (SLA, KPIs, SLTs)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.2.13.	Service Support Reports (Service specific)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.2.14.	Service Performance Review			Meeting	As required	NCIA	14.3., 14.4.
4.14.2.15.	Service Performance Review Minutes			Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.14.3.	Follow-on Support (Year 3)			See below	From PSA + 2year to PSA + 3years	See below	14.3., 14.4.
4.14.3.1.	Governance activities			Labour	As required	Annex C	14.3., 14.4.
4.14.3.2.	System operations activities			Labour	As required	Annex C	14.3., 14.4.
4.14.3.3.	Maintenance and Help-Desk activities			Labour	As required	Annex C	14.3., 14.4.
4.14.3.4.	Non-production environment activities			Labour	As required	Annex C	14.3., 14.4.
4.14.3.5.	Updates to Service Catalogue for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.3.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.3.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and			Electronic	As required	Project Website	14.3., 14.4.
4.14.3.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.

Item	Description			Media	Frequency	Destination	References
4.14.3.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.3.10.	Service Operation and Continuous Service improvement for Business Services and Support			As required	As required	NOA	14.3., 14.4.
4.14.3.11.	Updates Interface to ITSM Tools - if required			HW/SW	As required	Annex C	14.3., 14.4.
4.14.3.12.	Service Performance Reports (SLA, KPIs, SLTs)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.3.13.	Service Support Reports (Service specific)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.3.14.	Service Performance Review			Meeting	As required	NOA	14.3., 14.4.
4.14.3.15.	Service Performance Review Minutes			Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.14.4.	**Follow-on Support (Year 4)**			**See below**	**From FSA + 3year to FSA + 4year**	**See below**	**14.3., 14.4.**
4.14.4.1.	Governance activities			Labour	As required	Annex C	14.3., 14.4.
4.14.4.2.	System operations activities			Labour	As required	Annex C	14.3., 14.4.
4.14.4.3.	Maintenance and Help-Desk activities			Labour	As required	Annex C	14.3., 14.4.
4.14.4.4.	Non-production environment activities			Labour	As required	Annex C	14.3., 14.4.
4.14.4.5.	Updates to Service Catalogue for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.4.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.4.14.	Updates to Service Performance Monitoring and Reporting Plan for Business services and			Electronic	As required	Project Website	14.3., 14.4.
4.14.4.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.4.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.4.10.	Service Operation and Continuous Service improvement for Business Services and Support			As required	As required	NOA	14.3., 14.4.
4.14.4.11.	Updates Interface to ITSM Tools - if required			HW/SW	As required	Annex C	14.3., 14.4.
4.14.4.12.	Service Performance Reports (SLA, KPIs, SLTs)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.4.13.	Service Support Reports (Service-specific)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.4.14.	Service Performance Review			Meeting	As required	NOA	14.3., 14.4.
4.14.4.15.	Service Performance Review Minutes			Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
4.14.5.	**Follow-on Support (Year 5)**			**See below**	**From FSA + 4years to PSA + 5year**	**See below**	**14.3., 14.4.**
4.14.5.1.	Governance activities			Labour	As required	Annex C	14.3., 14.4.
4.14.5.2.	System operations activities			Labour	As required	Annex C	14.3., 14.4.
4.14.5.3.	Maintenance and Help-Desk activities			Labour	As required	Annex C	14.3., 14.4.
4.14.5.4.	Non-production environment activities			Labour	As required	Annex C	14.3., 14.4.
4.14.5.5.	Updates to Service Catalogue for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.5.6.	Updates to SLA / SLTs / KPIs for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.5.7.	Updates to Service Performance Monitoring and Reporting Plan for Business services and			Electronic	As required	Project Website	14.3., 14.4.
4.14.5.8.	Updates to Service Maintenance Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.5.9.	Update to Service IT-Continuity Plan for Business services and Support Services, if required			Electronic	As required	Project Website	14.3., 14.4.
4.14.5.10.	Service Operation and Continuous Service improvement for Business Services and Support			As required	As required	NOA	14.3., 14.4.
4.14.5.11.	Updates Interface to ITSM Tools - if required			HW/SW	As required	Annex C	14.3., 14.4.
4.14.5.12.	Service Performance Reports (SLA, KPIs, SLTs)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.5.13.	Service Support Reports (Service specific)			Paper, Electronic	As required	Project Website	14.3., 14.4.
4.14.5.14.	Service Performance Review			Meeting	As required	NOA	14.3., 14.4.
4.14.5.15.	Service Performance Review Minutes			Electronic	Meeting + 3 days	Project Website	14.3., 14.4.
Total O&M							

| **Total - Work Package 4 - Wave 2** | | | | | | | |

Work							
6.1	**Project Management**						**S., 6.11., G.**
6.1.1.	**Project Management Plan(s) and Documents**			Electronic	EDC + 4 Weeks and as changes occur	Project Website	S.4., 6.11., G.2.
6.1.2.	**Project Status Report**			Electronic	EDC + 4 Weeks and as changes occur	Project Website	S.3, 6.11., S.4., G.2.
6.1.3.	**Project Management Office**			Electronic	EDC + 4 Weeks	Project Website	S.5, 5.6, 6.11., G.2.
Total Project Management							

6.2	**Support**						
6.2.1.	**Training**						3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 6.11., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8
6.2.1.1.	Training Requirement Analysis (TRA/TRR) report (as part of site surveys)			Electronic	with site survey reports	Project Website	9.5, 6.11., 14.7
6.2.1.2.	Training Needs Analysis (TNA)			Electronic	2 weeks before SRD and update as needed	Project Website	4.5., 6.11., 14.7
6.5.1.3.	Training Program/Plan			Electronic	with ILSP	Project Website	4.5., 14.7., 6.11., G.7.2.
6.2.1.4.	Training Materials			Electronic	4 weeks before first training session	Project Website	6.11., 8.5., 14.5., 14.7., 14.8., 14.10.
6.2.2.	**Contractor Logistics Support**	325.0		Labour	As required	As required	6.11., 14
Total Support							

| **Total - Work Package 6 (Wave 1)** | | | | | | | |

Work							
6.3	**Project Management**						**S., 6.11., G.**
6.3.1.	**Project Management Plan(s) and Documents**			Electronic	EDC + 4 Weeks and as changes occur	Project Website	S.4., 6.11., G.2.
6.3.2.	**Project Status Report**			Electronic	EDC + 4 Weeks and as changes occur	Project Website	S.3, 6.11., S.4., G.2.
6.3.3.	**Project Management Office**			Electronic	EDC + 4 Weeks	Project Website	S.5, 5.6, 6.11., G.2.
Total Project Management							

6.4	**Support**						
6.4.1.	**Training**						3.1., 3.2., 4.5., 4.9., 6.1., 6.6., 6.11., 8.5., 9.3., 9.5., 11.7, 12.2., 14.5., 14.6., 14.7., 14.8
6.4.1.1.	Training Requirement Analysis (TRA/TRR) report (as part of site surveys)			Electronic	with site survey reports	Project Website	9.5, 6.11., 14.7
6.4.1.2.	Training Needs Analysis (TNA)			Electronic	2 weeks before SRD and update as needed	Project Website	4.5., 6.11., 14.7
6.4.1.3.	Training Program/Plan			Electronic	with ILSP	Project Website	4.5., 14.7., 6.11., G.7.2.
6.4.1.4.	Training Materials			Electronic	4 weeks before first training session	Project Website	6.11., 8.5., 14.5., 14.7., 14.8., 14.10.
6.4.2.	**Contractor Logistics Support**	300.0		Labour	As required	As required	6.11., 14
Total Support							

| **Total - Work Package 6 (Wave 2)** | | | | | | | |

Work							
7.1	**Project Management**						
7.1.1.	**Project Management Plan(s) and Documents**			Electronic	EDC + 4 Weeks and as changes occur	Project Website	S.4., 6.12., G.2.
7.1.2.	**Project Status Report**			Electronic	EDC + 4 Weeks and as changes occur	Project Website	S.3, 5.4., 6.12., G.2.
7.1.3.	**Project Management Office**			Electronic	EDC + 4 Weeks	Project Website	S.5, 5.6, 6.12., G.2.
Total Project Management							

7.2	**Support**						
7.2.1.	**Contractor Logistics Support**	300.0		Labour	no earlier than Wave 1 PSA	As required	6.12., 14
Total Support							

| **Total - Work Package 7** | | | | | | | |

As required
Course
Electronic
Form
Hardware
Labour
Meeting
Paper
Software
TBD

Each line of the table that contains effort is to be populated with the CLIN from the drop down menu that is associated with the effort. Note that all CLINS in the drop down list should be accounted for, and if there is no labour associated, please indicate include a line for that CLIN and indicate "No labour associated with this CLIN"

Bidder is to identify specific labour categories, including function. This may also include level as appropriate. For example: Senior Systems Engineer, Technician, Junior program analyst, etc

Each line is to be completed by the bidder with the applicable currency. Contractors may choose to enter multiple currencies in one sheet or duplicate the sheet for multiple currencies

This is a calculation of the profit for each line item (if applicable), and should be the sum of Unit cost*Quantity*Profit percentage for each year. **If the bidder did not apply profit,** any or all of these cells can be 0.

This is a calculation of the "fully burdened" cost for each labour category, which means the cost of all units including all profit and indirect rates associated with material (G/A, overhead, etc)

A) If the line of effort is performed by the bidder; indicate "No" in each line that is not subcontracted B) If the line of effort is subcontracted out to another company, indicate the company name in each line associated with their effort

Enter profit percentage for labour in yellow cell below

CLIN	Labour Category	Man-Days 2018	Man-Days 2019	Man-Days 2020	Labour rate 2018	Labour rate 2019	Labour rate 2020	Currency	Extended cost	Expat Allowance (ONLY if applicable)	Profit	Fully burdened cost	Subcontracted/ Name of Subcontractor		Profit	0%
		Number of Man-Days Year 1	Number of Man-Days Year 2	Number of Man-Days Year 3	Unit Cost per Man-Day Year 1	Unit Cost per Man-Day Year 2	Unit Cost per Man-Day Year 3									
CLIN X.1	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN X.2	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN X.3	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN X.4	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN X.5	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN X.6	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN X.7	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.1	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.2	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.3	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.4	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.5	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.6	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				
CLIN Y.7	Insert Labour category name here								-		-	-				
	Insert Labour category name here								-		-	-				

Labour table Instructions:
This detailed labour table is to be completed by the bidder with all columns populated, and shall be expanded to include as many rows as necessary to provide the detail requested, and any uncessary rows should be deleted (no blank entries). The bidder is required to identify for each item the CLIN it is associated with from the drop down menu. Each column should then be populated using the column-specific instructions in the first row. Bidder may not delete columns, or omit information from columns, but may add columns if neccessary, although it's not anticipated this will be needed.

Note any formulas existing in the cells are provided only to help the bidder, and ultimately all calculations are the bidder's responsibility. As such, the contractor may alter any formulas necessary to provide an accurate, clear and traceable bid as required.

Important Note: The Total sum of the "fully loaded" cost column should equal the grand total labour cost to include profit as well as all indirect rates (G&A/Overhead/etc.) associated with labour. These indirect cost rates must be included in the total firm fixed price on the appropriate detailed tab but are no longer required to be broken out seperately in the calculations at the bidding stage. However, the bidder is required to include the associated indirect costs in the totals of the detailed tab either A) in the base unit costs or B) shown seperately by expanding the table columns to show the additional costs due to these indirect rates (similar to the way profit is calulated). Option B is not required at the bidding stage but this detail will be requested from the winning bidder during pre-contract award discusions.

	Insert Labour category name here	-	-	-
	Insert Labour category name here	-	-	-
	Insert Labour category name here	-	-	-
	Insert Labour category name here	-	-	-
	Insert Labour category name here	-	-	-
	Insert Labour category name here	-	-	-
Total			-	

Each line of the table that contains effort is to be populated with the CLIN from the drop down menu that is associated with the effort. Note that all CLINS in the drop down list should be accounted for, and if there is no labour associated, please indicate include a line for that CLIN and indicate "No labour associated with this CLIN"

Bidder is to identify specific material that is to be procured as a part of the proposed solution. This includes specific hardware items, software licenses, etc.

Bidder is to provide a description of each item; this can be a model number, hardware configuation description, etc

Each line is to be completed by the bidder with the applicable currency. Contractors may choose to enter multiple currencies in one sheet or duplicate the sheet for multiple currencies

This is a calculation of the profit for each line item (if applicable), and should be Unit cost*Quantity*Profit percentage). **If the bidder did not apply profit,** any or all of these cells can be 0.

This is a calculation of the "fully burdened" cost for each item, which means the cost of all units including all profit and indirect rates associated with material (G/A, overhead, etc)

A) If the line of effort is performed by the bidder; indicate "No" in each line that is not subcontracted
B) If the line of effort is subcontracted out to another company, indicate the company name in each line associated with their effort

Enter profit percentage for material in yellow cell below

												Profit	0%

CLIN	Equipment Name	Item Description	Quantity 2018	Quantity 2019	Quantity 2020	Unit cost 2018	Unit cost 2019	Unit cost 2020	Currency	Extended cost	Profit	Fully burdened cost	Subcontracted/ Name of Subcontractor
CLIN X.1	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN X.2	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN X.3	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN X.4	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN X.5	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN X.6	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN X.7	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.1	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.2	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.3	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.4	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.5	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.6	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
CLIN Y.7	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	
	Insert Purchased Equipment name	Insert Item Description/Model number								-	-	-	

Insert Purchased Equipment name	Insert Item Description/Model number		-	-	-
Insert Purchased Equipment name	Insert Item Description/Model number		-	-	-
Insert Purchased Equipment name	Insert Item Description/Model number		-	-	-
Total					-

Each line of the table that contains effort is to be populated with the CLIN associated with the effort. Note that all CLINS in the "CLIN detail list" should be accounted for, and if there is no labour associated, please indicate include a line for that CLIN and indicate "No labour associated with this CLIN"

CLIN	Origin/Destination	Number of trips	Number of people	Number of Days per trip	Currency	Cost per roundtrip transportation	Per Diem	Total Cost
		Enter the number of trips	Enter the number of people for each trip	Enter the number of days per trip		Enter the cost per roundtrip transportation (Flight, train, etc)	Enter the per diem rate	Calculated the Total Travel Cost
CLIN X.1	Insert Origin/destination							-
CLIN X.2	Insert Origin/destination							-
CLIN X.3	Insert Origin/destination							-
CLIN X.4	Insert Origin/destination							
CLIN X.5	Insert Origin/destination							
CLIN X.6	Insert Origin/destination							
CLIN X.7	Insert Origin/destination							
CLIN Y.1	Insert Origin/destination							
CLIN Y.2	Insert Origin/destination							
CLIN Y.3	Insert Origin/destination							
CLIN Y.4	Insert Origin/destination							
CLIN Y.5	Insert Origin/destination							-
CLIN Y.6	Insert Origin/destination							
CLIN Y.7	Insert Origin/destination							
Total								-

Each line of the table that contains effort is to be populated with the CLIN associated with the effort. Note that all CLINS in the "CLIN detail list" should be accounted for, and if there is no labour associated, please indicate include a line for that CLIN and indicate "No labour associated with this CLIN"

Enter the name of the ODC item

Enter a description of the ODC item

Enter the currency

Enter the unit type

Enter the number of units

Enter the unit cost

Total ODC cost calculation

Enter year of expected ODC cost

CLIN	Item Name	Item Description	Currency	Unit Type (Man-Days, lot, etc)	Quantity	Unit cost	Total Cost	Year
CLIN X.1	Insert Other Direct Cost item						-	
CLIN X.2	Insert Other Direct Cost item						-	
CLIN X.3	Insert Other Direct Cost item						-	
CLIN X.4	Insert Other Direct Cost item						-	
CLIN X.5	Insert Other Direct Cost item						-	
CLIN X.6	Insert Other Direct Cost item						-	
CLIN X.7	Insert Other Direct Cost item						-	
CLIN Y.1	Insert Other Direct Cost item						-	
CLIN Y.2	Insert Other Direct Cost item						-	
CLIN Y.3	Insert Other Direct Cost item						-	
CLIN Y.4	Insert Other Direct Cost item						-	
CLIN Y.5	Insert Other Direct Cost item						-	
CLIN Y.6	Insert Other Direct Cost item						-	
CLIN Y.7	Insert Other Direct Cost item						-	
Total							-	

ODC table Instructions:
This detailed ODC table is to be completed by the bidder with all columns populated, and shall be expanded to include as many rows as necessary to provide the detail requested, and any uncessary rows should be deleted (no blank entries). The bidder is required to identify for each item the CLIN it is associated with from the drop down menu. Each column should then be populated using the column- specific instructions in the first row. Bidder may not delete columns, or omit information from columns, but may add columns if neccessary, although it's not anticipated this will be needed.

Note any formulas existing in the cells are provided only to help the bidder, and ultimately all calculations are the bidder's responsibility. As such, the contractor may alter any formulas necessary to provide an accurate, clear and traceable bid as required.

Important Note: The sum of the "Total cost" column on this tab should equal the grand total ODC cost to include any profit as well as all indirect rates (G&A/Overhead/etc.) associated with ODCs. These indirect cost rates must be included in the total firm fixed price on the appropriate detailed tab but are no longer required to be broken out seperately in the calculations at the bidding stage. However, the bidder is required to include the associated indirect costs in the totals of the detailed tab either A) in the base unit costs or B) shown seperately by expanding the table columns to show the additional costs due to these indirect rates as seperate columns. Option B is not required at the bidding stage but this detail will be requested from the winning bidder during pre-contract award discusions.

Example:

Name of Rate	Rate description	
General & Administrative		3%

Rate Name	Rate description	Percentage
Overhead		
Fringe		
G&A		
Material Handling		
Profit		
[Insert additional rates if needed]		

Instructions:

Although the rates in this tab do not need to be linked to calculations for purposes of the bid, it is required that bidders list any and all rates included in their bid to include (but not limited to): Overhead, Labour Fringe, Material handling, General &Administrative, profit, etc.

Reference Document	Reference ID (BI, SOW requirement, SRS requirement)	Desription	Bid Reference	Remarks	Compliance statement
BI	[BI – 2.11.1]	The Bidder shall furnish with its Bid a guarantee in an amount equal to Three Hundred Thousand EURO (€300,000) with a validity equal to that of the Bid as expressed in paragraph 2.10.1.			
BI	[BI – 2.11.1]	The Bid Guarantee shall be substantially similar to paragraph 7 Annex C			
BI	[BI – 2.11.5]	In the event that a Bid Guarantee is submitted directly by a banking institution, the Bidder shall furnish a copy of said document in the Bid Administration Package.			
BI	[BI – 3.1.1]	Bidders shall prepare and submit their Bid in accordance with the requirements and format set forth in this IFB.			
BI	[BI – 3.1.2]	3.1.2 Bidders shall prepare their bid in three (3) parts (a) Administrative Package Electronic: 1 scanned PDF copy sent via e-mail, with physical (nondigital) signatures (b) Technical Proposal (Part II): Electronic: 1 PDF copy sent via email (c) Price Proposal (Part III): Electronic: 1 Excel copy sent via email on the provided template(s)			
BI	[BI – 3.1.3]	3.1.3 Bidders shall not simply restate the IFB requirements.			
BI	[BI – 3.1.7]	Bidders shall deliver documentation in an electronic format which is best suited for review and maintenance by the Purchaser			
BI	[BI – 3.1.8]	Bids and all related documentation shall be submitted in the English language.			
BI	[BI – 3.1.9]	All documentation submitted as part of the Bid shall be classified no higher than "NATO UNCLASSIFIED".			
BI	[BI – 3.2.1]	The complete Bid shall consist of three distinct and separated parts each of which will be send as an individual electronic submission as described under 3.2			
BI	[BI – 3.2.2]	Part 1 is the Bid Administration Package shall be provided as a single PDF file, with scanned (non-digital) signatures.			
BI	[BI – 3.2.3]	Part 2 is the Technical Proposal consisting of three volumes as specified below. This shall be provided as a PDF files separately for each Volume			
BI	[BI – 3.2.3.1]	Volume 1 – Management and Risk with the Executive Summary with Technical Proposal Cross Reference Matrix and Management and Risk, and shall also include: a) Bidder Qualifications and Key Personnel; b) Project Milestone with delivery schedule; c) Initial Project Management Plan (PMP) and Work Breakdown Structure; d) Project Management Communication plan showing in particular: approach to status reporting, communications tool and web space; e) Initial Risk Management Plan with Risk Log.			
BI	[BI – 3.2.3.2]	Volume 2 – Engineering shall include (but not be limited to): a) Initial System Design Specifications (SDS); b) Initial Project Implementation Plan (PIP); c) Initial Security Risk Assessment (SRA) as a part of PIP; d) Initial Test Acceptance Plan (TAP).			
BI	[BI – 3.2.3.3]	Volume 3 – Supportability shall include (but not be limited to): a) Initial Itegrated Logistic Support Plan (ILSP); b) Initial Configuration Management Plan (CMP); c) Initial Quality Assurance Plan (QAP); d) Maintenance and Support Concept.			
BI	[BI – 3.2.4]	Part 3 is the Price Quotation shall be provided as a completed Excel file, using the Excel file provided in the IFB.			
BI	[BI – 3.3.1]	If the Bid Guarantee is sent to the Purchaser directly from the Bidder's bank, a letter, in lieu of the actual Guarantee, shall be included specifying the details of the transmittal and a copy of the Guarantee.			
BI	[BI – 3.3.2]	Bidders shall complete and return the IFB/ Bid Requirements Cross Reference Matrix (BRCM) (see instructions in paragraph 8 Annex D) covering the full Prospective Contract and Bidding Instructions where required			

BI	[BI – 3.3.3]	The Package shall include the Certificates set forth in paragraph 6 Annex B to these Bidding Instructions, signed in the original by an authorised representative of the Bidder.			
BI	[BI – 3.3.4]	Administrative package shall be contained on a single email submission.			
BI	[BI – 3.4.1]	The Bidders Technical Proposal shall be organised and submitted in three volumes			
BI	[BI – 3.4.2]	The Bidders shall assure Bid compliance with SoW and SRS requirements			
BI	[BI – 3.4.3]	Pages of each and every document shall be clearly readable and use a font no smaller than 12 point.			
BI	[BI – 3.4.5.1]	The Purchaser requires that all 'shall' statements from all sections SOW be addressed in this volume.			
BI	[BI – 3.4.5.3]	This volume shall also contain a Bid Requirements Cross Reference Matrix (BRCM)			
BI	[BI – 3.4.5.4.1]	Bidders shall provide an overview of the salient features of their technical Bid in the form of an executive summary.			
BI	[BI – 3.4.5.4.2]	Exwcutive Summary shall provide a general description of the major points contained in each of the required sections of the technical Bid. This summary shall not exceed 15 pages.			
BI	[BI – 3.4.5.4.3]	Bidders shall explicitly state in the Executive Summary of their Bid that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and services will comply with the requirements of the SOW.			
BI	[BI – 3.4.5.5.1]	Bidders shall compile a detailed Table of Contents which lists not only the section headings but also the major sub-sections, and topic headings of the Bid			
BI	[BI – 3.4.5.7.1]	The Bidder shall provide a section which describes the company structure and activities of the prime Contractor.			
BI	[BI – 3.4.5.7.1]	The country in which the prime contractor is registered shall be identified and the size and location(s) of the company headquarters and subsidiary branches described.			
BI	[BI – 3.4.5.7.1]	Within that structure the location and organizational unit of the office which will manage this contract shall be identified.			
BI	[BI – 3.4.5.7.1]	This section shall also describe the major activities of the company and how they are distributed across the organisation.			
BI	[BI – 3.4.5.7.2]	The Bid shall provide a description of the corporate capabilities of the Bidder			
BI	[BI – 3.4.5.7.2]	The Bidder shall provide evidence of relevant and recent experience in the design and implementation of projects similar to the SOA & IdM Platform project			
BI	[BI – 3.4.5.7.2]	The Bidder shall provide a section which describes how the experience and expertise of the prime contractor and all nominated sub-contractors will contribute to the successful execution of the contract.			
BI	[BI – 3.4.5.7.3]	The Bidder shall provide a section which identifies its major proposed sub-contractors for the Project			
BI	[BI – 3.4.5.7.3]	The Bidder shall identify the firm and the nation of origin and describe the contribution which the sub - contractor is expected to make to the execution of the project.			
BI	[BI – 3.4.5.7.3]	The Bidder shall also provide rationale for the selection of the sub-contractor and describe the added value the sub-contractor will bring to the execution of the project			
BI	[BI – 3.4.5.7.4]	Volume 1 shall provide a description of individual skills and experience in relation to the project of all project team members and Subject Matter Experts (SMEs) foreseen to support the project team			
BI	[BI – 3.4.5.7.4]	The description shall include how each individual expertise and experience will add value to the team.			
BI	[BI – 3.4.5.7.5]	Volume 1 shall provide the resumes / Curricula Vitae (CV) and supporting certification documentation (e.g. Prince 2 certificates) of each proposed Key Personnel that meet or exceed the requirements in SOW Section 13.			
BI	[BI – 3.4.5.7.6]	The Bidder, except CVs for all personnel nominated to fill Key Roles, shall also provide rationale to explain why each individual nominated for a Key Role has been proposed, having due regard for the requirements for each role expressed in the SOW			
BI	[BI – 3.4.5.7.7]	Bidder shall also present an overall organisational description for its team that makes clear how the team will function			
BI	[BI – 3.4.5.8.1]	Bidder shall submit initial versions of the following three (3) project management documents called for in the SOW, in a format based on that called for in Annex G of the SOW: a) the Project Management Plan (PMP), including the Work Breakdown Structure called for therein; b) the Risk Management Plan (RMP) with initial Risk Log; c) the Project Management Communications Plan (part of PMP).			
BI	[BI – 3.4.5.8.2]	The submitted documents shall include sufficient information to demonstrate the Bidder's understanding of the key challenges involved in the SOA & IdM Platform project			

BI	[BI – 3.4.5.8.3]	The Bidder shall demonstrate in the submitted initial three (3) plans how the Project Management Controls required under SOW Section 5 will be implemented during the life of the Contract			
BI	[BI – 3.4.5.8.3]	Bidder shall demonstrate that the Project Management Methodology proposed for the project is suitable to the successful execution of the project and shall further describe its approach to achievement of milestones, configuration management and quality assurance			
BI	[BI – 3.4.5.8.4]	The Bidder shall describe its approach to Project Management Communications and explain how requirements for Formal Meetings, Informal Meetings, Status Reports, Project Communications Tools and Project Web Space will be met			
BI	[BI – 3.4.5.9.1]	The Bidder shall provide a section which demonstrates its commitment to the achievement of project milestones as described in Section 4 of the SOW			
BI	[BI – 3.4.5.9.1]	This section shall address the two (2) Waves of the SOA & IdM Platform implementation and be consistent with the schedule information presented in the draft Project Implementation Plan			
BI	[BI – 3.4.5.10.1]	The Bidder shall submit an initial draft Risk Register describing a minimum of six (6) and a maximum of ten (10) most important risks to the successful completion of the project from its perspective			
BI	[BI – 3.4.5.10.2]	For each risk identified the Bidder shall state the perceived likelihood of the risk becoming a reality, the impact of risk manifesting itself and assess the severity of the impact should that come to pass			
BI	[BI – 3.4.5.10.3]	For each risk identified the Bidder shall describe its proposed mitigation of that risk in the event of it becoming a reality.			
BI	[BI – 3.4.5.10.4]	The Bidder shall describe how risks will be managed throughout the execution of the Contract in response to the requirements of SOW Sections 5 and 11.			
BI	[BI – 3.4.6.2.1]	The Bidder shall provide an initial System Design Specification (SDS), which describes its proposed technical solution and demonstrates its understanding of the requirements in Section 7 and Annex A of the SOW.			
BI	[BI – 3.4.6.2.2]	The Bid shall demonstrate a comprehensive understanding of all of the requirements of Section 7 and Annex A of the SOW and describe how every requirement is addressed in the Contractor's SOA & IdM Platform proposed solution			
BI	[BI – 3.4.6.2.3]	The Bid shall describe in the SDS how the following Architecture Principles (see Annex A, SRS, Section 2) have been treated			
BI	[BI – 3.4.6.2.4]	The Bid shall describe in the SDS the design solution proposed for the SOA & IdM Platform services			
BI	[BI – 3.4.6.2.7]	The Bid shall describe in the SDS how requirements for Continuity of Service, Disaster Recovery and Availability are met			
BI	[BI – 3.4.6.2.8]	The Bid shall comprehensively address all system requirements.			
BI	[BI – 3.4.6.2.9]	The Bidder shall describe how the Purchaser Furnished Information and As Is Information provided in Annex C of the SOW have been taken into account in the SDS included in the Bid.			
BI	[BI – 3.4.6.2.10]	The Bidder shall demonstrate that he has understood the design process imposed in the SOW by describing his support of the cycle of design reviews and approvals			
BI	[BI – 3.4.6.2.11]	The Bid must include an example of system design documentation which shows an understanding of the Design Deliverable requirements described in SOW Section 7 and Annex A. Such examples shall include already designed and working solution			
BI	[BI – 3.4.6.3.1]	The Bidder shall propose in his Bid initial Project Management Plan (PMP), which shall include Security Accreditation (SA) process (see Section SOW 10).			
BI	[BI – 3.4.6.3.2]	The Bid shall demonstrate the Bidder's clear and complete understanding of the Security Accreditation process described in SOW Section 10 and describe the role the Contractor will play in providing input to security documentation			
BI	[BI – 3.4.6.4.1]	The Bid shall include initial Security Risk Assessment (SRA) as described in SOW Sections 8 and 10			
BI	[BI – 3.4.6.4.2]	The Bidder shall demonstrate an understanding of the Security Measures described in SOW Section 10 and explain how they will feature in SOA & IdM Platform design and implementation			
BI	[BI – 3.4.6.5.1]	The Bid shall include initial Project Implementation Plan (PIP).			
BI	[BI – 3.4.6.5.2]	The Bidder shall provide a detailed account of how the implementation requirements in Section 6 of the SOW will be met.			

BI	[BI – 3.4.6.5.4]	The Bidder shall assume that all elements of its design must be provided in full at the implementation stage and that no software or business processes exist on site in a reusable form.			
BI	[BI – 3.4.6.5.5]	The Bidder shall describe its approach to site surveys as mentioned in Section 9 of SOW, identify the issues to be checked on site and relate the site survey to the overall implementation effort in terms of timing and purpose.			
BI	[BI – 3.4.6.5.6]	The Bidder shall describe its Bid for the implementation of a SOA & IdM Platform Reference Environment.			
BI	[BI – 3.4.6.6.1]	The Bidder shall include a section in its Bid which takes a comprehensive approach to the testing and acceptance requirements in Section 8 of the SOW and describes how each requirement will be met.			
BI	[BI – 3.4.6.6.2]	The Bidder shall describe how the SOA & IdM Platform Reference Environment will be used to support testing activity.			
BI	[BI – 3.4.6.6.3]	The Bidder shall describe its Test Strategy and include in its Bid an initial draft Test and Acceptance Plan, in accordance with the template provided in Annex G of the SOW.			
BI	[BI – 3.4.6.6.4]	The test plan shall address how each of the defined requirements shall be tested, the acceptance criteria, the types of testing to be undertaken and the locations at which testing will occur.			
BI	[BI – 3.4.6.6.5]	The Bidder shall describe how testing will be conducted, the test documentation to be provided and how test results will be validated and recorded.			
BI	[BI – 3.4.6.6.6]	The Bidder shall describe how failures and off specifications will be dealt with during testing.			
BI	[BI – 3.4.6.6.7]	The Bidder shall demonstrate a comprehensive understanding of the acceptance procedures at site, wave and full system acceptance levels.			
BI	[BI – 3.4.6.6.8.1]	The Bid shall describe the test scenarios which will be developed to support service based testing and provide evidence that processes within services and activities within processes will be tested.			
BI	[BI – 3.4.6.6.8.1]	The Bid shall describe how test scenarios shall demonstrate that trained Users can exercise the processes successfully within the full range of services to be developed as part of the Contractor's design and within each service that processes for service design, service transition and service operation will all be tested			
BI	[BI – 3.4.6.7.1]	The Bid shall demonstrate a clear understanding of Purchaser Furnished Information, Equipment, Infrastructure and Services (PFE) and shall describe how the Bidder proposes to make use of PFE during the execution of the contract			
BI	[BI – 3.4.7.2.1]	The Bidder shall provide a detailed account of how the Integrated Logistics Support (ILS) requirements in Section 14 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Logistics Support Analysis (LSA) process and Reliability, Availability, Maintainability and Testability (RAMT) activities.			
BI	[BI – 3.4.7.2.2]	The Bidder shall include in its Bid a draft Integrated Support Plan which describes how the Bidder shall fulfil all ILS requirements during the life of the project. The Bidder shall describe its ILS organisation and responsibilities in relation to other disciplines in the project.			
BI	[BI – 3.4.7.2.3]	The Bidder shall describe its ILS procedures regarding how the Maintenance and support concept described in the ILS will be designed, implemented, demonstrated and delivered.			
BI	[BI – 3.4.7.2.4]	The Bidder shall demonstrate how the supply support and how the PHST (Packaging, Handling Storage and Transportation) activities are designed and integrated in the Maintenance and Support concept, also described in SOW Section 14 and Annex B.			
BI	[BI – 3.4.7.2.5]	The Bidder shall demonstrate how the Technical documentation and training are designed, implemented validated and delivered.			
BI	[BI – 3.4.7.2.6]	The Bidder shall include in the ILS Plan the CLS plan as described in the SOW (Section 14), which describes how the optional CLS contract will be managed and implemented.			
BI	[BI – 3.4.7.2.7]	The Bidder shall demonstrate that all ILS activities and milestones are integrated into the project's master schedule.			
BI	[BI – 3.4.7.2.8]	The Bidder shall include the draft ILS Plan how the required LSA support cases will be developed. The Bidder shall describe its approach to all the LSA required analysis. The Bidder shall explain how the LSA activities are integrated into the analysis, design and test activities of the project. The Bidder shall demonstrate that all LSA activities and milestones are integrated into the project's master schedule. The Bidder shall also demonstrate that its RAMT activities are consistent with the RAMT requirements in the System Requirements Specification.			
BI	[BI – 3.4.7.3.1]	The Bidder shall provide a detailed account of how the Configuration Management requirements in Section 12 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Configuration Management Process and Configuration Baseline management			

BI	[BI – 3.4.7.3.2]	The Bidder shall include in its Bid a draft Configuration Management Plan which describes how the Bidder shall fulfil all configuration Management requirements during the life of the project. The Bidder shall describe its configuration Management organisation and responsibilities in relation to other disciplines in the project. The Bidder shall describe its CM procedures regarding Configuration Item Identification and documentation; configuration Control; Engineering Change Process, configuration Status Accounting, Versioning and auditing. The Bidder shall demonstrate that all CM activities and milestones are integrated into the project's master schedule.			
BI	[BI – 3.4.7.4.1]	The Bidder shall provide a detailed account of how the Quality Assurance requirements in Section 11 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Quality Assurance Process management			
BI	[BI – 3.4.7.4.2]	The Bidder shall include in its Bid a draft Quality Assurance Plan which describes how the Bidder shall fulfil all QA requirements during the life of the project. The Bidder shall describe its configuration QA organisation and responsibilities in relation to other disciplines in the project. The Bidder shall describe its QA procedures related to the design, development, verification and qualification and of the support of the product. The Bidder shall demonstrate that all QA activities and milestones are integrated into the project's master schedule.			
BI	[BI – 3.4.7.5.1]	The Bidder shall provide a detailed account of how the Training requirements in Section 14.7 of the SOW will be met. In particular the Bid must demonstrate a clear understanding of the Training Process Management.			
BI	[BI – 3.4.7.5.2]	The Bidder shall include in its Bid a draft Training Plan which describes how the Bidder shall fulfil all Training requirements during the life of the project. The Bidder shall describe its configuration Training organisation and responsibilities in relation to other disciplines in the project. The Bidder shall provide some Training example from similar training programmes. The Bidder shall demonstrate that all Training activities and milestones are integrated into the project's master schedule.			
BI	[BI – 3.4.7.6.1]	The Bidder shall include in its Bid a draft Maintenance and Support Concept as described in SOW Section 14.3-14.4 and SOW Annex B.			
BI	[BI – 3.5.1-3.5.1.1]	The Price Quotations shall be submitted in electronic form and contain the following documentation and media: Annex A-1 (paragraph 5) "Bidding Sheets" and, as an Annex, the complete set of sheets contained in the electronic file "2-IFB-CO-14176-SOA-IDM -Bidding Sheets.xls" submitted as part of this IFB;			
BI	[BI – 3.5.2]	Bidders shall prepare their Price Quotation by completing the Bidding Sheets referred in paragraph 3.5.1.1 above, in accordance with the Bid Package Content instructions specified in paragraph 3.2.4.			
BI	[BI – 3.5.3]	The structure of the Bidding Sheets shall not be changed, other than as indicated elsewhere, nor should any quantity or item description in the Bidding Sheets. The currency(ies) of each Contract Line Item and sub-item shall be indicated by the Bidder. The prices provided shall be intended as the comprehensive total price offered for the fulfilment of all requirements as expressed in the IFB documentation including but not limited to those expressed in the SOW.			
BI	[BI – 3.5.3.1]	Bidders shall furnish Firm Fixed Prices for all required items in accordance with the format set forth in the Instructions for preparation of the Bidding Sheets.			
BI	[BI – 3.5.3.2]	Bidders shall furnish Firm Fixed Prices for the Work Packages of Wave 1 and the each Optional Work Package of Wave 2. Purchaser evaluation of the submitted Bids will be on the basis of the complete submission including administrative, price and technical components for the two (2) Waves.			
BI	[BI – 3.5.3.3]	Offered prices shall not be "conditional" in nature. Any comments supplied in the Bidding Sheets which are conditional in nature, relative to the offered prices, may result in a determination that the Bid is non-compliant.			
BI	[BI – 3.5.3.5]	Bidders shall quote in their own national currency. Bidders may also quote in other than their national currency if it can be demonstrated that the Bidder is expected to incur equivalent costs in that/those currency(ies)			
BI	[BI – 3.5.3.7]	Bidders shall therefore exclude from their price Bid all taxes, duties and customs charges from which the Purchaser is exempted by international agreement and are required to certify that they have done so through execution of the Certificate at 6.5			
BI	[BI – 3.5.3.8]	Unless otherwise specified in the instructions for the preparation of Bidding Sheets, all prices quoted in the Bid shall be on the basis that all deliverable items shall be delivered on the basis of Delivery Duty Paid (DDP) in accordance with the International Chamber of Commerce INCOTERMS.			
BI	[BI – 3.5.3.9]	The Bidder's attention is directed to the fact that Price Quotation shall contain no document and/or information other than the priced copies of the Bidding Sheets. Any other document will not be considered for evaluation.			
BI	[BI – 3.5.3.10]	All prices Bid shall be clearly traceable in the detailed Bidding Sheets.			

BI	[BI – 4.1.3]	The Purchaser shall not be responsible for locating or securing any information that is not identified in the Bid.			
BI	[BI – 4.1.4]	The Bidder shall furnish with its Bid all information requested by the Purchaser in Book 1, Section 3 Bid Preparation Instructions. Significant omissions and/or cursory submissions will result in a reduced Best Value Score and may result in a determination of non-compliance without recourse to further clarification			
BI	[BI – 4.1.4]	The information provided by the Bidder in its Bid shall be to a level of detail necessary for the Purchaser to fully comprehend exactly what the Bidder proposes to furnish as well as its approach and methodologies.			
BI	[BI – 4.1.5]	The Bidder is not permitted any cardinal alteration of the Bid regarding technical matters and shall not make any change to its price quotation at any time.			
BI	[BI – 4.3.1.1.1]	Bids received shall be reviewed for compliance with the mandatory Administrative requirements specified in paragraph 4.3.2. Bids not meeting all of the mandatory requirements may be determined to be non-compliant and not further considered in the evaluation or for award.			
BI	[BI – 4.3.1.1.2]	All Bid Bid Guarantees shall be reviewed for compliance with the mandatory Administrative requirements specified in paragraphs 4.3.2 and 2.11.			
BI	[BI – 4.3.2.5]	All Bid Bid Guarantees shall be reviewed for compliance with the mandatory Administrative requirements specified in paragraphs 2.11 and 4.3.2.1.			
BI	[BI – 4.3.4.1.1.1]	Total price offered in the price quotation of this Bid in Section 1 of the Bidding Sheets shall not exceed amounts, as described in 4.3.4.1.1.1			
BI	[BI – 4.3.4.1.2]	Bidders shall note that the total price stated in Section 1 of the Bidding Sheets shall not exceed the figure quoted in paragraph 4.2.5.1.2. for two Waves.			
BI	[BI – 5.1.2]	Bidders shall follow the specific instructions provided in each worksheet. Bidders shall insert information in all yellow cells.			
BI	[BI – 5.1.2]	The prices and quantities entered on the document shall reflect the total items required to meet the contractual requirements. The total price shall be indicated in the appropriate columns.			
BI	[BI – 5.1.2]	In preparing the Bidding Sheets, Bidders shall ensure that the prices of the Sub-items total the price of the major item of which they constitute a part.			
BI	[BI – 5.1.2]	Prices and detail of the traceability of application of the discount shall be clearly identified in the supporting detail sheets and applied at the unit price level.			
BI	[BI – 5.1.4.2]	Bidders shall fill in the Offer Summary sheet based on the information provided in the CLIN summary sheet.			
BI	[BI – 5.1.4.3]	Bidders shall fill in the CLIN summary sheet based on the information provided in the detailed Bidding sheets (CLIN Price Breakdown sheets).			
BI	[BI – 5.1.4.3]	The line items in the CLIN Summary Sheet shall be all INCLUSIVE of the price being Bid in order to fulfil the requirement for the line item in the CLIN Summary Sheet.			
BI	[BI – 5.1.4.3]	Bidders shall make sure that the total price indicated in the Detailed Bidding Sheets matches the price stated in the CLIN summary sheet for the same corresponding CLIN or sub-CLIN			
BI	[BI – 5.1.4.3]	Bidders shall make sure that they have filled all delivery dates in yellow and that these dates comply with the time limits specified in each worksheet and are in accordance with the dates proposed in the proposed Project Master Schedule (Book II, Part 4 – SOW, Sections 4, 5, 7, 8)			
BI	[BI – 5.1.5]	For each of the CLINs the Bidder shall use the separate Sheets as provided, adding additional sheets if multiple currencies are used. Change the currency in the header of the Sheets if necessary.			
BI	[BI – 5.1.5.1.1.c]	The Bidder shall provide a level of detail down the unique sellable item level (e.g. A server, a laptop, a printer)			
BI	[BI – 5.1.5.1.1.d]	The Bidder shall provide unit prices that shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance. Factors for overhead shall be applied in the MATERIAL LABOUR OVERHEAD section of the detailed Bidding sheet to the total cost of material.			
BI	[BI – 5.1.5.2]	Unit prices shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance			
BI	[BI – 5.1.5.2]	Factors for overhead shall be applied in the DIRECT LABOUR OVERHEAD section of the detailed Bidding sheet to the total cost of direct labour.			
BI	[BI – 5.1.5.3]	Unit prices shall be EXCLUSIVE of any applicable overhead, general and administrative costs, profit, costs associated to travel, per-diem and/or incidentals as well as Personnel Installation costs at the sites of performance			

BI	[BI – 5.1.5.3]	Factors for overhead shall be applied in the SUBCONTRACT LABOUR OVERHEAD section of the detailed Bidding sheet to the total cost of subcontract labour			
BI	[BI – 5.1.6]	Elements that are inherently only to Wave 1 or just Wave 2, the Bidder shall only fill in the CLIN summary for that element in the appropriate wave.			

Reference ID (BI, SOW requirement, SRS requirement)	Desription	Bid Reference	Remarks	Compliance statement
[SOW-1]	The Contractor SHALL be responsible for the totality of the implementation of the solution, which meets the requirements set forth in this Statement of Work (SoW), including but not limited to: overall design, integration, security accreditation and system engineering of the Service Oriented Architecture (SOA) & Identity Management (IdM) Platform throughout the Contract's Period of Performance.			
[SOW-2]	Through his responses to the requirements in this Statement of Work (SoW), the Contractor SHALL at all times ensure the integrity of the SOA & IdM Vision and strive to effect its achievement.			
[SOW-3]	The Contractor SHALL ensure during the execution of the contract that the purpose and functionality described in this SoW are completely addressed in the products and services provided.			
[SOW-4]	The Contractor SHALL observe the Project's priorities in their planning and execution of the work.			
[SOW-5]	The Contractor SHALL be aware and comply with the documents as referenced in ANNEX F and ANNEX G throughout the Contract.			
[SOW-6]	The Contractor SHALL provide all necessary resources to include services, personnel, materials, components, equipment, data and documentation needed to accomplish all the tasks described in the SoW, to meet all the requirements of the SoW (including annexes) and to fulfil all other Contract's provisions.			
[SOW-7]	The documents listed in SECTION 2: Applicable Documents may be revised over time. The Contractor SHALL always use the current version of each document.			
[SOW-8]	The Contractor SHALL be aware and comply with the above-mentioned documents throughout the duration of this Contract.			
[SOW-9]	The Contractor SHALL provide project management services.			
[SOW-10]	The Contractor SHALL provide systems engineering services to cover: requirements review, system design and system integration.			
[SOW-11]	The Contractor SHALL provide test services to prove the system Product Baseline (PBL) as meeting its requirements.			
[SOW-12]	The Contractor SHALL fully document the design, operation and maintenance of SOA & IdM Platform by providing the required manuals, operational procedures, supporting technical data, computer software and drawings required by the Contract.			
[SOW-13]	The Contractor SHALL conduct all necessary activities to support the Purchaser in achieving Security Accreditation at the Operational Network up to NATO SECRET (NS) and Protected Business Network (PBN - NATO RESTRICTED and PBN - NATO UNCLASSIFIED) levels.			
[SOW-14]	The Contractor SHALL co-ordinate with the Purchaser to ensure that the Site preparation activities are completed in accordance with the installation requirements of the delivered system.			
[SOW-15]	The Contractor SHALL procure and prepare the system components for delivery to the Sites specified in this Contract.			
[SOW-16]	The Contractor SHALL deliver the required software to the prepared Sites, and execute installation/deployment, on-site testing, training and activation.			
[SOW-17]	The Contractor SHALL provide support to application and service management integration and to pilot cases.			
[SOW-18]	The Contractor SHALL provide Integrated Logistics Support (ILS) services (see SECTION 14), including Training Services.			
[SOW-19]	The Contractor SHALL provide Operation and Maintenance (O&M) support with appropriate service management interfaces both at information (monitoring / reporting) and process (request / incident) level (see ANNEX B).			
[SOW-20]	The Contractor SHALL comply with all overarching requirements as described in the SoW (Testing process, Site Survey process, Quality Assurance and Control, Configuration Management).			
[SOW-21]	The Contractor SHALL deliver the analysis for Service Management interfaces between their Domain Service Management (the Contractor's) and the Enterprise Service Management (the Purchaser's), including but not limited to: Service Asset and Configuration Management, Event Management, Incident and Request escalation and delegation, raw or pre-processed data feed for service dashboarding and Service Level Agreement (SLA)/ Operational Level Agreement (OLA) reporting purposes.			

[SOW-22]	The Contractor SHALL actively contribute to the convergence between their Domain Service Management and the Enterprise Service Management and SHALL keep track of the SMC Target Architecture [NCIA SMC TA, 2018] development.			
[SOW-23]	As part of the project management activities, the Contractor SHALL maintain the necessary relationships with the above-mentioned projects, including other Purchaser's systems to be interfaced with SOA & IdM Platform and associated Contractors, as applicable: a. the Contractor SHALL attend, organise and conduct meetings as necessary; b. the Contractor SHALL be proactive in order to ensure the SOA & IdM Platform effectiveness when delivering services to the relying systems, including systems already implemented as well as ones planned for deployment; c. per Purchaser's request, the Contractor SHALL identify any documents, meeting minutes or any other information from these projects required to maintain an effective coordination process.			
[SOW-24]	The Contractor SHALL adhere to the Overall Project Schedule and split of Work Packages into two separate Waves.			
[SOW-25]	The Contractor SHALL reflect the Overall Project Schedule and split of Work Packages in all relevant Project Management Documentation (SECTION 5.4: Project Management Documentation).			
[SOW-26]	The Contractor SHALL integrate the Key milestones suggested schedule and delivery approach (see Table 2) in its Project Master Schedule, at a minimum by committing to deliver:			
[SOW-27]	The Contractor SHALL meet or exceed the dates mentioned in the above schedule. "Exceed" is understood as a situation where the Contractor has delivered earlier than the dates (i.e. EDC + 'x' months) mentioned in the above schedule, and the Purchaser has accepted the milestone accordingly.			
[SOW-28]	The Contractor SHALL implement SOA & IdM Platform at the following sites and networks described below in Table 3:			
[SOW-29]	The Contractor SHALL propose the implementation sequence of the sites in Project Implementation Plan in order to match the Purchaser's milestones.			
[SOW-30]	The Contractor SHALL host and conduct a System Design Review (SDR), as defined in SECTION 7: System Engineering and Integration, and the associated documentation SHALL be approved by the Purchaser.			
[SOW-31]	The Contractor SHALL host and conduct a System Design Review (SDR), as defined in SECTION 7: System Engineering and Integration, and the associated documentation SHALL be approved by the Purchaser.			
[SOW-32]	The Contractor SHALL achieve SBL every time the Contractor updates the Software Version and conducts a Sprint Test of this new Software Version.			
[SOW-33]	The Contractor SHALL perform necessary activities to satisfy criteria for meeting SBL as defined in SECTION 8.1 and SHALL submit the associated documentation for Purchaser approval.			
[SOW-34]	The Contractor SHALL achieve IRC and RC by successfully completing the Integration Test at Purchaser's Program Management and Integration Capability (PMIC) environment for the release.			
[SOW-35]	The Contractor SHALL have performed necessary activities and satisfied the criteria for meeting IRC and RC milestone as defined in SECTION 8: Testing and Acceptance, and the associated documentation SHALL have been approved by the Purchaser.			
[SOW-36]	Once IRC or RC is accepted and a Release is planned, the Contractor SHALL generate an updated Baseline as a result of IRC or RC, and SHALL install the updated SBL (System Baseline IRC/RCv.x) on the SOA & IdM Platform Reference System and integrate it within the appropriate IV&V Reference Environment.			
[SOW-37]	The achievement of the IRC and RC is subject to the Purchaser's approval. In particular, the Contractor SHALL note that any implementation activities on the IV&V environment MUST NOT start until the RC milestone is approved by the Purchaser.			
[SOW-38]	The Contractor SHALL have performed necessary activities and satisfied criteria for meeting DA as defined in SECTION 8: Testing and Acceptance and Request For Change (RFC) testing and the associated documentation SHALL have been approved by the Purchaser.			

[SOW-39]	The Contractor SHALL demonstrate that for the applicable Wave:
	a. all implementation activities have been executed at all the sites to be implemented under this contract, including, installation, testing and activation of all the SOA & IdM Platform components as described and defined in:
	  i. SECTION 4: Milestones;
	  ii. SECTION 6: System Implementation;
	  iii. SECTION 7: System Engineering and Integration;
	  iv. SECTION 8: Testing and Acceptance;
	  v. SECTION 11: Quality Assurance and Control;
	  vi. SECTION 14: Integrated Logistics Support (ILS).
	b. all SOA & IdM Platform functionality specified in this SoW has been successfully implemented;
	c. the Site Survey process has been completed as defined in SECTION 9: Site Surveys and the associated reports have been delivered for all the sites that form part of PSA scope (SECTIONs 8.2, 8.5 and 12.2.5).
	d. all agreed test cases have been executed, and all tests have a status "PASS" (see SECTION 8.3.5).
	e. all documentation has been deliverd as described in this SOW and in accordance to the templates provided in ANNEX G where applicable.
	f. the Configuration Management Database (CMDB) pertaining to this site has been delivered to the Purchaser.
	g. applicable Operational Acceptance Criteria (OAC) are met (see Operational Acceptance Criteria (OAC);
	h. centralised management and control of the SOA & IdM Platform has been fully implemented according to the requirements specified in this SoW.
	i. all required personnel has been trained according to SECTION 14.7: Training.
	j. the security requirements are satisfied in accordance to SECTION 10: Security.
	k. all activities have been executed required to have all SOA & IdM Platform software components on the AFPL, in accordance to SECTION 8.
	l. the OBL has been updated as described in 1.1 to reflect the actual PSA configuration (as built).			

[SOW-40]	The Contractor SHALL record any discrepancies discovered in achieving PSA on observation sheet(s) with a statement on their required resolution.			
[SOW-41]	All PSA milestone requirements (see Sect. 4.9), Site Activation and Site Acceptance milestone requirements (see Sect. 6.6.5), as well as Security Accreditation (Sect. 10.1) SHALL be met by the Contractor for all the sites to be implemented under this contract.			
[SOW-42]	The Contractor SHALL demonstrate that: a. all the identified deficiencies are either fixed or waived by the Purchaser; b. SOA & IdM Platform has been fully implemented across the entire NATO Enterprise and all requirements of this SoW are fully met.			
[SOW-43]	The Contractor SHALL deliver all deliverables and conducted all activities, as specified in this Contract.			
[SOW-44]	The Contractor SHALL close to the satisfaction of the Purchaser all outstanding issues, failures, and deficiencies.			
[SOW-45]	The Contractor SHALL at all times ensure that: a. adequate resources are applied to all activities undertaken under this Contract; b. the timely achievement of milestones is identified and met; c. the project status information is comprehensively reported to the Purchaser in a timely manner; d. Configuration Management baselines are established and maintained throughout the project lifecycle; e. all risks (Purchaser's and Contractor's risks) to project's achievement are identified and managed; f. professional standards of project activities and deliverables through the application of Quality Assurance techniques are applied; g. due account is taken of Purchaser Furnished Information (PFI), including Process Management Directives.			
[SOW-46]	The Contractor SHALL acknowledge email delivery and also answer to email communication received from NATO project team members (see SECTION 5.3) no later then the next business day.			
[SOW-47]	The Contractor SHOULD use a blended approach for Project Management as shown below in Figure 5.			

[SOW-48]	The Contractor SHOULD use PRINCE2 or an equivalent Project Management standard for the direction, governance and management activities for the entire project. If an equivalent Project Management standard is used, the Contractor SHALL prove that it at minimum meets all requirements stated in this section.			
[SOW-49]	The Contractor SHOULD follow Agile approach as preferred by the Purchaser or propose any other IT industry approach (e.g. for testing procedures) and provide results to the Purchaser as required.			
[SOW-50]	The Contractor SHOULD implement the Agile approach as described in this section for: a. the Product Creation process in Work Packages 2.1, 2.2, 4.1 and 4.2. b. the major testing activities, to include the System Integration Test and SAT.			
[SOW-51]	The Contractor SHALL define and describe its implementation of the required blended Project Management approach so that at minimum it shows a clear and consistent exchange of information between the Project team and minimal duplication of information and project management activities. For example: a. Project Master Schedule (Gantt chart) SHALL be used for higher level project planning and milestones tracking and SHALL be regularly fed by information from Product Delivery Reviews; b. Project Status Report (PSR) SHALL include inputs about delivery progress, issues and risks taken from Product Delivery Reviews and meeting.			
[SOW-52]	Although the Agile approach offers certain flexibility for the product delivery (e.g. prioritisation of features) within a Work Package, it MUST NOT by default tolerate deviations in the defined time, scope and cost within each authorised and initiated Work Package. If such deviations are forecasted, they SHALL be reviewed and approved according to the Configuration Management (CM) process (see SECTION 11: Quality Assurance and Control).			
[SOW-53]	The Contractor SHALL at minimum implement and conform to the Overall Project Organisation as structured in Figure 7: Project .			
[SOW-54]	The Contractor SHALL establish Product Delivery Teams which at least consist of the following roles: Team Manager, Technical Leader, Product Owner (Purchaser provided) and Test Director/QA Manager. One person can be a member of more than 1 Product Delivery Teams.			
[SOW-55]	The Contractor's Project Manager (CPM) SHALL frequently (at least once a week) liaise with Team Manager(s) to receive inputs from the Product Delivery and with the Purchaser Project Manager to provide inputs for overall Project Management and Direction, all of which SHALL be defined in the Project Communication plan (part of the Project Management Plan).			
[SOW-56]	The Purchaser is the official Product Owner (PO); however, the Contractor SHALL also ensure its SMEs are available to temporarily engage in the role of PO as needed. The Contractor's representative engaged in the role of PO will represent the Purchaser's interests within Product Delivery Teams and will work to enable:			
[SOW-57]	The Contractor SHALL identify all major Contractor's Organisational Units (OU) and any Sub-Contractors involved in the implementation of the SOA & IdM Platform and SHALL provide a description of the portion of the overall effort or list deliverable items for which they are responsible.			
[SOW-58]	The Contractor SHALL establish and maintain a Project Management Office (PMO) in Mons, Belgium area, to perform and manage all efforts necessary to discharge all his responsibilities under this Contract.			
[SOW-59]	The Contractor SHALL ensure the continuity of personnel assigned to work on this project.			
[SOW-60]	The Contractor's staff SHALL be identified as a key personnel, as listed in SECTION 13: Labour Categories			
[SOW-61]	The Contractor SHALL also provide all necessary manpower and resources to conduct and support the management and administration of operations in order to meet the objectives of the project, including taking all reasonable steps to ensure continuity of personnel assigned to work on this project.			
[SOW-62]	[SOW-62] All Contractors' Key Personnel SHALL be available throughout the performace of the Contract until the project's completion.			
[SOW-63]	The Contractor SHALL designate a Contractor's Project Manager (CPM), who will direct and co-ordinate the activities of the Contractor's project team.			
[SOW-64]	The Contractor's Project Manager SHALL be the Contractor's primary contact for the Purchaser's Project Manager and SHALL conduct all major project design, test and review meetings. See SECTION 13 for Labour Categories requirements.			

[SOW-65]	The Contractor SHALL designate a Senior Test Engineer to serve as a Test Director for all test activities conducted under this Contract. See SECTION 13 for Labour Categories requirements.			
[SOW-66]	The Contractor SHALL designate an Engineer to serve as a Quality Assurance Manager throughout the performance of the Contract until the project's completion.			
[SOW-67]	The Contractor's Quality Assurance (QA) Manager SHALL report to a separate manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.			
[SOW-68]	ILS, Change and Configuration Manager: The Contractor SHALL designate a Senior Engineer to serve as an ILS Manager throughout the performance of the Contract, including the O&M Phase (see SECTION 14: Integrated Logistics Support).			
[SOW-69]	The Contractor's team SHALL be available during Central European Time (CET) zone in business working hours: 8:30 - 17:30 Monday-Friday, when required.			
[SOW-70]	The Contractor SHALL deliver all Project Mananagement documentations as described in ANNEX G.			
[SOW-71]	The Contractor SHALL establish and maintain a PMP which describes how the Contractor will implement the totality of the Project as specified in this SoW.			
[SOW-72]	The Contractor's PMP SHALL cover all aspects of the project implementation including its management structure and project management processes, personnel roles and responsibilities, external dependencies necessary to provide the capability as required by this Contract.			
[SOW-73]	The Contractor's PMP SHALL be sufficiently detailed to ensure that the Purchaser is able to assess the Contractor's plans with insight into the Contractor's plans, capabilities and ability to satisfactorily implement the entire Project in conformance with the requirements as specified in this SoW.			
[SOW-74]	The Contractor SHALL propose PMP according to Annex G.2.1: Project Management Plan (PMP).			

[SOW-75]	The Contractor SHALL ensure that the PMP comprises at minimum of the following sections, as described in Annex G.2.1: Project Management Plan (PMP):
	a. an "Organisation" section describing the Contractor's organisation for this project according to the requirements in this SECTION 5. This section SHALL include:
	  i. an organisational chart showing the members of the Contractor's Project Team (including the members of the Contractor PMO);
	  ii. showing their respective responsibilities and authority;
	  iii. proposed Project Communication Plan;
	b. a "Project Planning" section describing the Contractor's processes supporting the development and maintenance of the Product Breakdown Structure (PBS), Product Flow Diagram (PFD) and Project Master Schedule (PMS) according to the requirements of:
	  i. SECTION 5: Project Management; and
	  ii. SECTION 11: Quality Assurance and Control;
	c. a "Risk management" section describing the Contractor's processes supporting Risk Management by the Contractor, according to the requirements of SECTION 5: Project Management;
	d. a "System Engineering" section describing the Contractor approach to these activities according to the requirements in SECTION 7: System Engineering and Integration;
	e. a ": System Implementation" section describing the Contractor approach to these activities according to the requirements in SECTION 6: System Implementation;
	f. an "Operation and Maintenance" section describing the Contractor approach to these activities according to the requirements in SECTION 14.3 Maintenance and Support concept;
	g. a "Testing" section describing the Contractor approach to these activities according to the requirements in SECTION 8: Testing and Acceptance.			

[SOW-76]	The Contractor's SOA & IdM Platform SDS (System Design Specification) SHALL be developed as per the detailed contents indicated in Annex G.2.1.			

[SOW-77]	The Contractor's PMP SHALL align with the SoW, but it MUST NOT be a simple 'cut & paste' from the relevant SoW sections. It SHALL demonstrate that the Contractor understands the work to be performed, applying industry best practices.			
[SOW-78]	The Contractor's PMP SHALL be provided to the Purchaser for acceptance.			
[SOW-79]	Acceptance of any deliverable provided by the Contractor to the Purchaser MUST NOT imply any waiver or any uni-sided interpretation of the original requirements as stated in the Contract. It remains the sole responsibility of the Contractor to unabridged fulfil all Contractual requirements and provide evidence of this to the Purchaser.			
[SOW-80]	The Contractor SHALL establish and maintain a PBS and a PFD.			
[SOW-81]	The Contractor's PBS SHALL identify the start and finish dates, duration, predecessors, successors and resource requirements for each task.			
[SOW-82]	The Contractor's PBS SHALL decompose all SOA & IdM Platform tasks to a level that exposes all project's risk factors and allows accurate estimation of each task's duration, resource requirements, inputs and outputs, and predecessors and successors.			
[SOW-83]	The Contractor's PBS SHALL identify all products and it SHALL distinguish between management products and specialist products.			
[SOW-84]	The Contractor's PBS SHALL include a hierarchical diagram of all the products (management products and specialist products), having at its topmost product the final product of the overall project, i.e. the SOA & IdM Platform System.			
[SOW-85]	The Contractor's PBS SHALL describe each product (management products and specialist products) including its quality requirements. The product descriptions SHALL address sufficient detail to permit management assessment of progress.			
[SOW-86]	The Contractor's PFD SHALL sequence all products in their logical order of creation.			
[SOW-87]	The Contractor's initial version of the PBS and PFD SHALL be provided to the Purchaser for acceptance.			
[SOW-88]	The Contractor's PMS SHALL correlate with the products defined in the PBS and sequentially ordered in the PFD.			
[SOW-89]	The Contractor's PMS SHALL: a. be provided in Microsoft Project format; b. identify the critical path for the overall project; c. identify the start and finish dates, duration, predecessors, constraints (as necessary) and the total slack of each task; d. identify key resources needed for each task completion; e. identify the main project milestones (see SECTION 4: Milestones) and intermediate milestones as required; f. identify the "physical" progress for each task; g. identify the applicable baseline and SHALL show progress against the baseline; h. minimise the use of constraints and absolute dates; i. provide network, milestone, Gantt and Tracking Gantt views; j. identify the main deliverables.			
[SOW-90]	The Contractor's PMS SHALL be provided to the Purchaser for acceptance.			
[SOW-91]	The Contractor's PBS, the PFD and the PMS SHALL be used as the primary framework for Contract planning and reporting to the Purchaser.			
[SOW-92]	The Contractor SHALL create and maintain a Product Backlog (PB) derived from the main PBS.			
[SOW-93]	The Contractor's PB SHALL contain a prioritised list of all required product features and SHOULD be used for planning and progress tracking of development activities within each time-boxed project effort.			
[SOW-94]	The Contractor's PB SHOULD also be used for the planning of iterative deployment of product features (releases) into test and production environments.			
[SOW-95]	The Contractor SHALL establish and maintain an RMP according to Annex G.2.2 Risk Management Plan (RMP), which SHALL describe how the Contractor will implement the Risk Management process.			

[SOW-96]	The Contractor's RMP SHALL at least describe: a. overall Risk Management approach; b. Key Risk Management processes; c. Key Risk Categories; d. Risk Prioritisation Matrix; e. Risk Management roles and responsibilities; f. Risk Log.			
[SOW-97]	The Contractor SHALL establish and maintain a Risk Management process for the project, and described it in the Risk Management Plan according to Annex G.2.2.			
[SOW-98]	The Contractor's Risk Management process SHALL at minimum enable and define identification of all types of risks, evaluation and prioritisation of each risk, definition of proposed response strategy, owner and actions and suggested monitor and control mechanisms.			
[SOW-99]	The Contractor SHALL rate risk based on its probability of occurrence and impact.			
[SOW-100]	The Contractor SHALL propose an appropriate response for each risk.			
[SOW-101]	If the Contractor and the Purchaser agree that the response to a risk is other than to accept it, the Contractor SHALL plan risk response tasks (having: start, finish, work required, resources to be used, result expected).			
[SOW-102]	The Contractor SHALL include in the Project Status Report (PSR) a chart that lists all active risks rated high on any factor and note any significant forecasted changes in these risks.			
[SOW-103]	The Contractor SHALL document, update and maintain status of all risks in the Risk Log where he SHALL record and track all project risks regardless of their status at every Project Review Meeting (PRM) and Design Review Meeting.			
[SOW-104]	The Contractor SHALL provide the Risk Log listing the risks, and indicating for each one the following information (but not limited to): a. Risk identifier: unique code to allow grouping of all information on this risk; b. Description: brief description of the risk; c. Risk category (e.g. management, technical, schedule, quality and cost risks); d. Impact: effect on the project if this risk were to occur; e. Probability: estimate of the likelihood of the risk occurring; f. Risk rating (High, Medium, Low); g. Proximity: how close in time is the risk likely to occur; h. Response strategy: avoidance, mitigation, acceptance, transference i. Response plan(s): what actions have been taken/will be taken to counter this risk; j. Owner: who has been appointed to keep an eye on this risk; k. Author: who submitted the risk; l. Date identified: when was the risk first identified; m. Date of last update: when was the status of this risk last checked; n. Status: e.g. closed, reducing, increasing, no change.			
[SOW-105]	The Contractor SHALL update Risk Log at minimum on a monthly basis as an input for the PSR (see SECTION 5.5.1) and provide to the Purchaser in an agreed format (e.g. Microsoft Excel).			
[SOW-106]	The Contractor SHALL add to the Risk Log additional risks identified by the Purchaser.			
[SOW-107]	The Contractor SHALL deliver the Risk Log to the Purchaser, throughout the duration of the Contract, and keep it up to date on the project portal.			
[SOW-108]	The Contractor SHALL establish and maintain a process for identifying, tracking, reviewing, reporting and resolving all project issues.			
[SOW-109]	The Contractor SHALL describe the Issue Management Process in the Configuration Management Plan (see SECTION 12.3).			

[SOW-110]	The Contractor SHALL develop and maintain an Issue Log where it SHALL record and track all project issues regardless of their status.				
[SOW-111]	The Contractor SHALL ensure that the Issue Log comprises the following information (but not limited to): a. Project Issue Number; b. Project Issue Type (Request for change, Off-specification, general issue such as a question or a statement of concern); c. Author; d. Date identified; e. Date of last update; f. Description; g. Action item/Decision; h. Responsible person (individual in charge of the action item); i. Suspense date (Suspense date for the action item); j. Priority; k. Status.				
[SOW-112]	The Contractor SHALL include the Issue Log in the configuration management process and keep it under configuration control and in the CMDB.				
[SOW-113]	The Contractor SHALL update Issue Log at minimum on a monthly basis as an input for the PSR (see section 5.5.1).				
[SOW-114]	The Contractor SHALL add to the Issue Log additional issues identified by the Purchaser.				
[SOW-115]	The Contractor SHALL deliver the Issue Log to the Purchaser, throughout the duration of the Contract, and keep it up to date on the project portal.				
[SOW-116]	All decisions taken during the project implementation lifecycle SHALL be tracked by the Contractor per project phase, together with evidence of options analysis when apply.				
[SOW-117]	First decisions SHALL be already available at CaW stage covering the Contractor's: a. design decisions, b. development decisions, c. tools and environment covered by the proposal; d. any possible proposed change before starting the project implementation.				
[SOW-118]	The Contractor's workflow SHALL allow for NCI Agency PM agreement with the decisions when proposed decisions are based on NCI Agency SME and stakeholders inputs.				
[SOW-119]	The Contractor's log SHALL also record design rationale, i.e. information capturing the reasoning of the designer that led to the system as designed, including design options, trade-offs considered, decision made and the justification of those decisions.				
[SOW-120]	The Contractor's log SHALL also record "architectural and implementation rationale" , i.e. information capturing the reasoning of the developer that led to the system as build, including implementation options, trade-offs considered, decision made and the justification of those decisions.				
[SOW-121]	[SOW-121] The Contractor's log SHALL also record "architectural and implementation rationale" , i.e. information capturing the reasoning of the developer that led to the system as build, including implementation options, trade-offs considered, decision made and the justification of those decisions				
[SOW-122]	A decision CANNOT and SHALL NOT overrule or modify: a. the Contract; b. the Statement of Work; c. the Product Scope as specified in the Contract; d. any part of an already accepted or baselined Workproduct.				
[SOW-123]	Any decision in a meeting to change any of the above artefacts SHALL be formalised by a Project Change through the Project Change Process.				

[SOW-124]	The Contractor SHALL ensure that requirements traceability to requirements changes, user histories, use cases, low level design - down to the application level (classes, packages and application) -, verification methods, test cases, test phases and test results are recorded and ready to be reported in the form of bi-directional requirements traceability matrixes and requirements verification matrix.			
[SOW-125]	A requirements baseline SHALL be created after each product release.			
[SOW-126]	The requirements baseline SHALL be provided to the purchaser as an export in DOORS format, for both of the SRS and the SoW.			
[SOW-127]	The Contractor SHALL keep the purchasers requirements ID for traceabiliy.			
[SOW-128]	The Contractor SHALL implement a CM process as referred to in NATO STANAG 4427, 2014 and [NATO ACMP-2000, 2017],[NATO ACMP 2009, 2017],[NATO ACMP-2100, 2017]to carry out the Configuration Management functions as described in this SoW (Configuration Item identification, configuration control, configuration status accounting, and configuration verification) and to perform Quality Assurance and Control.			
[SOW-129]	The Contractor SHALL provide, no later than the third working day of each month, a PSR.			
[SOW-130]	The Contractor's PSR SHALL at minimum summarise completed, ongoing, and upcoming activities, as well as attached updated PMS, and the status of any dependencies which affects or may affect the project.			
[SOW-131]	The Contractor SHALL ensure that the PSR summarises activities, including (but not limited to): a. Changes in key Contractor personnel; b. Summary of Contract activities during the preceding month, including the status of current and pending activities; c. Progress of work and schedule status, highlighting any changes since the preceding report; d. CSA report addressing all products in the Project Breakdown Structure; e. Issue Log; f. Change Requests status; g. Off-Specifications status; h. Risk Log; i. Test(s) conducted and results; j. Summary of any site surveys conducted; k. Plans for activities during the following reporting period; l. Provisional financial status and predicted expenditures.			
[SOW-132]	The Contractor SHALL issue answers to those comments within 1 week after their receipt. No comment received within that timeframe means that the Contractor agrees to the comments issued by the Purchaser.			
[SOW-133]	The Contractor SHALL schedule project meetings in the PIP.			
[SOW-134]	The Contractor SHALL produce a draft agenda for the Purchaser's approval at least one week before the meeting.			
[SOW-135]	The Contractor SHALL take meeting minutes, submit them in draft version to the Purchaser for approval within 2 (two) working days of the meeting. The minutes SHALL be submitted to an accelerated review cycle at Purchaser's discretion.			
[SOW-136]	The participants and mainly the Contractor's representatives SHALL NOT regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract nor as a vehicle to alter the design or configuration of equipment or systems. Any such changes SHALL only be made by authorised mechanisms as set forth in the Contract.			
[SOW-137]	All relevant documentation (even in draft format) SHALL be provided by the Contractor to the Purchaser no later than 2 (two) working days before the meeting.			
[SOW-138]	The Contractor's PM or his designated representative SHALL participate in all formal project meetings (kick-off meeting, PRMs and Design Review meetings).			
[SOW-139]	The Contractor SHALL participate in a project kick-off meeting that shall be held at the Purchaser's facility.			

[SOW-140]	The following provisions SHALL apply to Contractor, to all formal meetings to be held under the contract: a. the Contractor SHALL take meeting notes (capturing main points, decisions and action items) and submit them in draft version to the Purchaser for approval within three (3) working days after the meeting; b. the final version of the meeting notes SHALL be posted by the Contractor on the Project Website (see SECTION 5.5.3 below) within 3 (three) working days of receipt of Purchaser approval; c. the participants shall not regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract or as a vehicle to alter the design or configuration of equipment or systems. Any such changes shall only be made by agreement, amendment or by authorised mechanisms as set forth in the Contract; d. any documentation, even in draft format, that may be useful to the Purchaser in preparing for Design Review Meetings or PRMs and ensuring efficient discussions during the meetings shall be provided to the Purchaser no later than 10 (ten) working days before the meeting.			
[SOW-141]	The Contractor SHALL coordinate and hold PRMs with the Purchaser at least once a month throughout the Contract period of performance.			
[SOW-142]	The Contractor SHALL provide updated PSR not older than 5 (five) working days as a base document for the PRM as sent to all PRM participants at least 2 (two) business days in advance.			
[SOW-143]	At each PRM, the Contractor SHALL provide the status of all on-going tasks, the status of the Contract deliverables, identify any changes to the PMP, PMS, PIP, Integtated Logistics Support Plan (ILSP), Quality Assurance Plan (QAP), Issue Log, Change Requests document, Off-specifications document, baselines and Risk Log, and identify any problems.			
[SOW-144]	The Contractor SHALL address and discuss key project issues, risks and events with the Purchaser Project Manager promptly, and SHALL not postpone it until PRMs.			
[SOW-145]	The location of PRMs will vary and, when possible, and SHALL be scheduled by the Contractor in coordination with the Purchaser with other project meetings. Attendance in person is preferred but via video or telephone conference is acceptable when it can be arranged.			
[SOW-146]	The Contractor SHALL organize Product Delivery Meetings (PDM) in accordance with the chosen Agile framework.			
[SOW-147]	Contractor's PDMs SHALL at minimum cover the following activities: a. Product Delivery Planning meeting with frequency of minimum 1 (one) per month; b. Product Delivery Review meeting with frequency of minimum 1 (one) per month; c. Product Delivery Progress Meeting with frequency of minimum every 2 (two) working days.			
[SOW-148]	All Product Delivery Meetings SHALL be organized and run by the CPM, Team Manager or Tech Lead appointed by the Contractor.			
[SOW-149]	The Contractor SHALL record all outputs from all Product Delivery Meetings in a product delivery toolset chosen, implemented and hosted by the Contractor.			
[SOW-150]	The Contractor SHALL ensure Purchasers access to the abovementioned product delivery toolset.			
[SOW-151]	The Contractor SHALL report key outputs from PDMs such as delivery progress information (e.g. product backlog status, key test results, burndown / burnup charts) as well as key changes, issues and risks to the Contractor Project Manager who SHALL integrate that information in the PSR.			
[SOW-152]	The Contractor SHALL carry out ad-hoc project-level communication activities as needed to clarify project issues.			
[SOW-153]	The Purchaser and Contractor PM SHALL hold fortnightly contact from the Kick off meeting through the remaining contractual period. When unforeseen meetings are required the Contractor SHALL provide attendance within 3 (three) working days of the Purchaser request.			
[SOW-154]	The Purchaser and Contractor SHALL exchange contact telephone numbers and agree on conference call requirements (day and time) during the project kick-off meeting. The Contractor SHALL provide responses to Purchaser Emails on any subject within 1 (one) working day.			
[SOW-155]	Action Items from the conference calls SHALL be drafted by the Contractor and added to the SOA & IdM Platform Action Item List by the Contractor within 2 (two) days of the conference call.			
[SOW-156]	The Contractor's Project Manager SHALL provide inputs to and attend IPMT meetings as requested by the Purchaser Project Manager.			

[SOW-157]	The Contractor SHALL use the project website provided by the Purchaser to maintain all NATO UNCLASSIFIED (NU) documents.			
[SOW-158]	The Contractor SHALL maintain on this website all unclassified documents, as soon as they are submitted in draft version to the Purchaser. This includes all project deliverables, presentation materials from all meetings, as well as the Contract SoW and SRS, and all applicable documents. More generally, the website SHALL include any document as deemed necessary by the Purchaser.			
[SOW-159]	The Project Website SHALL identify all relevant classified documents by title, unless a title itself is classified and SHALL state from where the classified document can be obtained.			
[SOW-160]	The Contractor SHALL submit all documentation in electronic format to the Purchaser for review and comments as applicable.			
[SOW-161]	The Contractor SHALL not provide any Contractual documentation in a partial or gradual manner.			
[SOW-162]	The Contractor SHALL ensure that any documentation delivered to the Purchaser has been properly reviewed according to Contractor's quality management process.			
[SOW-163]	The Contractor SHALL provide a first version of each deliverable for Purchaser review.			
[SOW-164]	The Contractor SHALL not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.			
[SOW-165]	The Contractor SHALL resubmit the document as a revised version (version 0.2) incorporating the Purchaser's comments within 2 (two) weeks after receipt.			
[SOW-166]	The Contractor SHALL provide an updated version of the document within two weeks of receipt of the Purchaser's comments on the revised version.			
[SOW-167]	The above cycle SHALL continue until the document reach a quality level acceptable by the Purchaser.			
[SOW-168]	If the document is included as part of the FBL, ABL or PBL, the Contractor SHALL remain responsible for updating the document as required in the course of the project (to correct errors, inconsistencies, omissions, etc. and to reflect changes in the system design, system implementation, support arrangements) as part of its Configuration Management tasks.			
[SOW-169]	The Contractor SHALL be able adapt the SOA & IdM Platform to accommodate abovementioned additional information.			
[SOW-170]	The Contractor per Purchaser request SHALL identify any documents, meeting minutes, or other information from these projects required to maintain an effective coordination process.			
[SOW-171]	The Contractor SHALL include into Project Communication Plan (part of PMP) activities clearly identifying his proactive approach with regards to the coordination with other related NATO projects.			
[SOW-172]	As a Project-level communication activity, the Contractor SHALL provide an SOA & IdM Platform Information Sheet of maximum 2 (two) pages providing an overview of the SOA & IdM Platform system, its functions, external interfaces and major components, and its projected installation schedule.			
[SOW-173]	The Contractor SHALL ensure that overall implementation at the sites of Technical Services respects the achievement of Milestones as described in SECTION 4.			
[SOW-174]	In accordance with this Statement of Work, during the implementation phase the Contractor SHALL implement at the capacity to support Wave 1 and Wave 2 as described in SECTION 4: Milestones and below in SECTION 6.8 - 6-12: a. all of the functionality required; b. the performance levels required; c. all of the interfaces required; d. all of the services required.			
[SOW-175]	[SOW-175] The Contractor SHALL implement System in two steps as described in para 3.2 Scope			
[SOW-176]	The Contractor SHALL ensure that the Purchaser's requirements for functionality, performance, interfaces and services are traceable from this SoW to the delivered product via the Contractor's accepted design.			
[SOW-177]	The Contractor SHALL maintain traceability from the implemented baseline to all of the requirements of this SoW and SRS through the Traceability Matrix and the Configuration Management Database.			

[SOW-178]	The Contractor SHALL ensure that the implementation activities are executed in the following steps: a. update and deliver the Project Implementation Plan (PIP) described below in Section 6.4; b. conduct Preparations for Installation activities described below in Section 6.5; c. conduct Site Installation and Activation described below in Section 6.6.			
[SOW-179]	The Contractor SHALL conduct site surveys, as described above, for all the sites related to the Site Activation and FSA milestones, and which are part of the contract (i.e. basic sites, and optional sites which have been activated under the contract).			
[SOW-180]	The Contractor SHALL follow the Site Surveys process for the target installation sites, as described in SECTION 9: Site Surveys.			
[SOW-181]	Before implementation begins at the sites designated in the contract the Contractor SHALL complete Site Surveys: a. for the target installation sites; b. for each site surveyed the Contractor SHALL present and provide to the Purchaser. c. the Site Survey Reports SHALL include a completed Site Survey Template.			
[SOW-182]	The provided Site Survey Template is an initial template. The Contractor SHALL be responsible to tailor the template to ensure all relevant information is captured to complete the implementation of the SOA & IdM Platform at the site.			
[SOW-183]	During the Site Survey the Contractor SHALL: a. identify and document Installation and migration schedules and constraints; b. identify and document any elements relevant to the implementation but not covered in this SoW.			
[SOW-184]	At the beginning of the Site Survey the Contractor SHALL provide a presentation to the local site personnel on the objectives and conduct of the site visit in the context of the overall SOA & IdM Platform project.			
[SOW-185]	At the end of the Site Survey the Contractor SHALL provide an out brief on the outcome of the site survey and identify actions and follow-on activities.			
[SOW-186]	The Contractor SHALL adjust the activities and deliverables to the results of the Site Surveys.			
[SOW-187]	The Contractor SHALL deliver the PIP that fully describes their PIP plan and activities.			
[SOW-188]	The Contractor SHALL include in the PIP a clear rationale for the logic and sequencing of all implementation activity which demonstrates how new capabilities and services will be introduced in an efficient and controlled manner with optimal use of resources and no loss of service to users.			

[SOW-189]	The Contractor SHALL submit to the Purchaser the Project Implementation Plan with the following information:
	a. the Contractor's approach to all system implementation tasks (including the sequence of activation of the sites to be implemented);
	b. the Contractor organisation and key personnel involved in system implementation;
	c. the overall schedule for implementation activities including site survey, site preparation, site installation and activation;
	d. the schedule of all planned outages of any kind in the sites;
	e. the detailed implementation sequence of Technical Services and User services considering and adapting to the ITM implementation sequence in order to minimise the impacts on both projects;
	f. the installation plan addressing:
	  i. a general installation plan showing how the gradual installation and activation of the SOA & IdM Platform will be carried out by the Contractor;
	  ii. the installation procedures, showing that those procedures will cause no or minimal disruption to the sites and to the User desktop applications;
	  iii. a site-specific design for each site;
	  iv. a detailed installation plan for each site;
	  v. site and system installation checklist;
	  vi. Site Activation checklist;
	  vii. an Allocation Matrix showing the allocation of each system CIs (nature and quantities) to each site, and the number of users and support staff for each site;
	  viii. any specific tools the Contractor intends to furnish and use during the site installation.
	g. the activation plan addressing:
	  i. the Site Activation activities;
	  ii. any post-activation tasks;
	  iii. the "back-out" procedures enabling deactivation and/or removal of all installed SOA & IdM Platform components and restoration of existing services without disruption of those services.
	h. the potential disruption/outage that the implementation activities might generate ensuring potential outages will be kept short (less than 3 hours in duration), planned (approved by the Purchaser at 48 hours in advance based on a Contractor-provided plan to restore functionality within 30 minutes), localised (limited to areas agreed to by the Purchaser) and, if			

[SOW-190]	The Contractor SHALL structure the PIP so that general implementation information is maintained in the body of the plan and site-specific details are kept as annexes.			
[SOW-191]	The Contractor SHALL provide the PIP for the Purchaser acceptance.			
[SOW-192]	In accordance to NATO policy [AC/317-D/71 (revised), 1996] the Contractor SHALL use Commercial-Off-The-Shelf (COTS) software in preference to the development of new software unless it evidently contains major disadvantages (e.g. cost effectiveness, negative impact on existing IT infrastructure, security, market stability, etc.) indicated by the Contractor.			
[SOW-193]	The Contractor SHALL integrate the system/application delivery and provisioning mechanism with Datacentre provided solution as specified in SRS.			
[SOW-194]	The Contractor SHALL include backup and restore testing (using ITM capability) as part of the test plans to confirm the functionality and performance.			
[SOW-195]	The Contractor SHALL include Remediation Plan section in the PIP.			
[SOW-196]	If the installation of any component of the SOA & IdM Platform is found to be interfering with the operation of other Purchaser's systems the Contractor's back-out plan SHALL be implemented by the Contractor.			
[SOW-197]	The Contrator's implementation of the back-out plan SHALL cause no loss or corruption of data in any of the existing systems.			

[SOW-198]	The installation and activation dates reflected in the PIP SHALL be co-ordinated by the Contractor with the Purchaser and the Site POCs to accommodate site-specific requirements, exercises, holiday periods, and other considerations. Any such dates and any revision of these dates SHALL be coordinated with the Purchaser and the relevant sites at least 4 (four) weeks before the start of the relevant activities.			
[SOW-199]	The Contractor SHALL provide each site POC, with a copy to the Purchaser Project Manager, with a draft list of software to be shipped, and a list of Contractor's personnel together with a copy of each person's personnel Security Clearance for those who will be involved in site installation and activation work.			
[SOW-200]	The Contractor SHALL monitor the progress of any required Site facilities preparations, and the progress of any required provision of input by the Purchaser and the Site, to ensure timeliness and quality of the preparatory work required from the Purchaser.			
[SOW-201]	The Contractor SHALL ensure that anything that may delay installation is brought to the attention of the Purchaser Project Manager promptly.			
[SOW-202]	The Contractor SHALL prepare and conduct a Site Verification Survey (see SECTION 9) no later than 2 months prior to installation activities at the site. The purpose of this Site Verification Survey is to verify that the information provided by the site is still valid, and to perform any necessary updates to the system implementation documentation. The actual visit of the sites subject to the Site Verification Survey is left to Contractor's appreciation.			
[SOW-203]	The Contractor SHALL submit the updated PIP for the Purchaser's acceptance immediately after the Site Verification Survey and no later than 2 weeks before the Site installation and obtain the Purchaser approval of the PIP before planned start date.			
[SOW-204]	The Contractor SHALL perform site installation of any SOA & IdM Platform elements, including establishment of network connectivity between all required components.			
[SOW-205]	The Contractor SHALL perform site activation.			
[SOW-206]	The Contractor SHALL execute all activities related to security accreditation.			
[SOW-207]	The Contractor SHALL execute system configuration audit.			
[SOW-208]	The Contractor SHALL deliver all documentation associated to site installation and activation.			
[SOW-209]	The Contractor SHALL produce a Site Activation Plan in coordination with the Purchaser.			
[SOW-210]	The Contractor SHALL deliver the SOA & IdM Platform Reference system to the Purchaser before the Reference Test.			
[SOW-211]	The Contractor SHALL provide the toolset to the reference environments to allow future Services to be designed, built, unit tested, integrated and approved.			
[SOW-212]	The Contractor SHALL provide pre-configured templates including required tools, services, processes and repositories to the reference environments.			
[SOW-213]	The Contractor SHALL provide the toolset for the reference environment to support different development and testing methodologies, in particular for remote (non-NATO staff) development: a. external remote connection to the NATO dev/test environment b. NATO dev/test environment connection to external environment (i.e.: Contractor premises) c. downloading of a copy of the environment as a virtual machine (VM).			
[SOW-214]	The Contractor SHALL provide the toolset to the reference environments to support: a. Functional Service testing b. Data driven service testing c. Performance testing d. Service load testing			
[SOW-215]	The Contractor SHALL coordinate the start date of the planned installation no later than 3 (three) weeks before that start date.			
[SOW-216]	Throughout all Site installation activities the Contractor SHALL hold a daily meeting with the site POC to agree on the work to be conducted during the day.			

[SOW-217]	Although the Purchaser will provide the facilities in which the SOA & IdM Platform will be installed and the external systems to which it will be interfaced, the Contractor SHALL be responsible for timely and complete delivery and installation of all relevant supplies.			
[SOW-218]	If required for the Implementation, the Contractor SHALL solve all integration and interface problems that may occur during the SOA & IdM Platform installation.			
[SOW-219]	The Contractor SHALL provide and install all miscellaneous equipment (for example shelves, mounting brackets, power filters, signal filters, cables, installation kits) to enable the connection of SOA & IdM Platform elements to the existing infrastructure at a site.			
[SOW-220]	The Contractor SHALL ensure that all the necessary miscellaneous equipment come out from the site survey so it could be quantified and monitored.			
[SOW-221]	The Contractor SHALL deliver the SOA & IdM Platform in accordance with: a. the agreed PIP; b. the agreed design and SRS; c. site specific implementation details.			
[SOW-222]	The Contractor SHALL deliver the SOA & IdM Platform to sites in line with details in SECTION 14: Integrated Logistics Support.			
[SOW-223]	The Contractor SHALL perform site acceptance activities locally at the site.			
[SOW-224]	The Contractor SHALL ensure that none of the site activation activities have any impact on any operational elements of the SOA & IdM Platform, nor on the NATO Staff Users' desktop applications, except for some authorised potential and limited outages.			
[SOW-225]	The Contractor SHALL conduct the SAT as per the process detailed in SECTION 8: Testing and Acceptance.			
[SOW-226]	The Contractor SHALL produce a test report after the successful completion of SAT. The Purchaser shall approve the SAT Test Report for each site.			
[SOW-227]	The Contractor SHALL ensure that SAT on the operational sites demonstrate that the system installed provides the Contractual functionality and performance level, including all interfaces with all internal and external systems, including administration requirements, and is ready for operational use.			
[SOW-228]	The Contractor SHALL carry out the SAT for a maximum of one week at each site, exclusive of any preparation time.			
[SOW-229]	The Contractor SHALL support the Purchaser in obtaining Security Accreditation with the activities and deliverables as specified in SECTION 10: Security.			
[SOW-230]	For each of the sites where a component of the SOA & IdM Platform system is to be installed, the Contractor SHALL modify the approved generic Security Operating Procedures (SecOPs) to meet the requirements of the local site.			
[SOW-231]	The Contractor SHALL deliver and present the localised version of the SOA & IdM Platform SecOPs to the local Security Accreditation Authority for approval.			
[SOW-232]	The Contractor SHALL take into account any comments from the reviewers and Local Security Accreditation Authority and SHALL update the document as many times as necessary in order to gain Local Security Accreditation Authority approval of the SOA & IdM Platform localised SecOPs for the site.			
[SOW-233]	For each of the sites where a component of the SOA & IdM Platform system is to be installed, the Contractor SHALL modify the approved generic STVP to meet the requirements of the local site.			
[SOW-234]	The Contractor SHALL deliver and present the localised version of the STVP to the local security accreditation authority for approval.			
[SOW-235]	The Contractor SHALL take into account any comments from the reviewers and Local Security Accreditation Authority and SHALL update the document as many times as necessary in order to gain Local Security Accreditation Authority approval of the SOA & IdM Platform localised STVP for the site.			
[SOW-236]	The Contractor SHALL support the NCI Agency in the execution of the STVP.			
[SOW-237]	The Contractor SHALL update the documentation delivered at the sites to accommodate any site-specific changes and/or configurations.			

[SOW-238]	Upon completion of site implementation work, the Contractor SHALL provide the Purchaser with a copy of the site installation and activation checklist and resolve any discrepancies identified.			
[SOW-239]	The Contractor SHALL keep the documentation under configuration control, as per SECTION 12.11: Configuration Identification and Documentation.			
[SOW-240]	The Contractor SHALL deliver training documentation and execute the required training, as described in SECTION 14.7: Training.			
[SOW-241]	The Contractor SHALL design and document all the required Support Service as required in the SECTION 14: Integrated Logistics Support, and in compliance with the support concept depicted in ANNEX B: Maintenance and Support Concept (After PSA).			

[SOW-242]	The Contractor SHALL provide following components of WP 2.1 during Wave 1:
	a. Integration Services:
	  i. Messaging Infrastructure;
	  ii. Mediation;
	b. SMC Services;
	c. Platform Hosting Services.			

[SOW-243]	The Contractor SHALL provide following components of WP 2.2 during Wave 2: a. Integration Services: i. Composition; b. Registry and Repository Services; c. Information Services; d. SMC Services (in support of Wave 2).			
[SOW-244]	The Contractor under Wave 1 (Basic IdM Platform Implementation) SHALL provide following components on both ON and PBN environment (including Enhanced nodes if required) in corresponding reference facilities and in the integration and testing facility, enabling the following capabilities: a. Identities Management; b. Credential Management; c. Authentication Management: iv. Authentication; v. Security Token Services; d. Access Management.			
[SOW-245]	The Contractor under Wave 2 (Extended IdM Platform Implementation) SHALL provide following components on both ON and PBN environment (and also on Enhanced nodes if required) in corresponding reference facilities and in the integration and testing facility: a. Identity Federation; b. Allied Replication Hub; c. Federated Authentication.			
[SOW-246]	The Contrator SHALL provide: a. Project management Plan; b. Project Status Report; c. PMO.			
[SOW-247]	The Contractor SHALL provide Training according to Section 14.7 and SHALL deliver: a. Training Requirements Analysis and Report (TRA/TRR); b. Training Needs Amalysis (TNA); c. Training Program/Plan; d. Training Materials.			
[SOW-248]	The Contractor SHALL provide the Implementation Plan for Work Packages 6 (as described below).			

[SOW-249]	The Contractor SHALL provide support to the Functional Service 3rd party contractor, in: a. consultancy (for support of other Sole Source Contractor); b. integration			
[SOW-250]	The Contractor SHALL deliver: a. requirements for installation of other FSs on SOA platform and integration and connection to the IdM Platform; b. documentation for connection and integration of other FSs as described above; c. lessons learned.			
[SOW-251]	The Contractor SHALL provide a not-to-exceed level of effort of 625 (six hundred twenty five) man-days over a 2 (two) years period. This support will be provided to a number of projects, with: a. approximately 4 (four) man-days/week for the SOA platform; b. approximately 2 (two) man-day/week for the IdM platform.			
[SOW-252]	The Contractor SHALL start Work Packages 6 (6.1 and 6.2) during Work Packages 5 and propose to the Purchaser the exact start date, including the following: a. the Contractor SHALL ensure, that Work Package 6.1 (Wave 1) is finished before or together with WP5 PSA; b. the Contractor SHALL ensure, that Work Package 6.2 (Wave 2) is finished before or together with WP5 FSA.			
[SOW-253]	The Contrator SHALL provide: a. Project Management Plan; b. Project Status Report; c. PMO.			
[SOW-254]	The Contractor SHALL provide a not-to-exceed level of effort of 300 (three hundred) man-days over a 2 (two) years period. This support will be provided to a number of projects, with: a. approximately 2 (two) man-days/week for the SOA platform; b. approximately 1 (one) man-day/week for the IdM platform.			
[SOW-255]	The Contractor SHALL meet the requirements listed in SECTION 5: Project Management.			
[SOW-256]	The Contractor SHALL meet the Engineering requirements listed in SECTION 7: System Engineering and Integration.			
[SOW-257]	The Contractor SHALL meet the requirements listed in SECTION 8: Testing and Acceptance.			
[SOW-258]	The Contractor SHALL meet the requirements listed in SECTION 6: System Implementation.			
[SOW-259]	The Contractor SHALL meet the requirements listed in SECTION 14: Integrated Logistics Support.			
[SOW-260]	The Contractor SHALL meet the requirements listed in SECTION 14.3 Maintenance and Support concept and ANNEX B: Maintenance and Support Concept (After PSA).			
[SOW-261]	The Contractor SHALL develop the SOA & IdM Platform System Design Specification based on an analysis of the Purchaser's requirements.			
[SOW-262]	The Contractor SHALL integrate all necessary components to establish the SOA & IdM Platform SBL, and plan and execute a series of tests to confirm that this baseline meets its requirements.			
[SOW-263]	The Contractor SHALL perform the activities described in this section considering that the SOA & IdM Platform will support a wide variety of NATO activities and systems (e.g. Core Services, Functional Services (FS)).			
[SOW-264]	The Contractor SHALL be responsible for integration of the SOA & IdM Platform System. This means both the integration of the various hardware and software products that constitute the SOA & IdM Platform System and the integration of the SOA & IdM Platform System with other NATO systems.			
[SOW-265]	The Contractor SHALL make use of "testbeds" to perform this integration and more generally to conduct tests, in particular: a. tests related to "Software Approval" SHALL be conducted on the SOA & IdM Platform Reference System, at the Purchaser premises, (see SECTION 0); b. the baseline tests SHALL be conducted on the SOA & IdM Platform Reference System, at Purchaser premises.			
[SOW-266]	The Contractor SHALL deliver and activate the SOA & IdM Platform Reference System as required in this section for the Reference System.			

[SOW-267]	The Contractor SHALL integrate the SOA & IdM Platform Reference System with the appropriate IV&V Reference Environment.			
[SOW-268]	The Contractor SHALL conduct a workshop (at a Purchaser-provided facility) to orient the SOA & IdM Platform Administrators and other stakeholders (Contractor proposes Purchaser decision) on the overall system design and capabilities. As part of this workshop, the Contractor SHALL: a. deliver overview briefings on the anticipated SOA & IdM Platform system, and lead question and answer sessions with the attendees; b. provide information about the anticipated SOA & IdM Platform System Implementation; c. provide information about how the System Design fully meets the requirements specified in this SoW and SRS; d. provide an overall description of the external interfaces; e. provide an overall description of the ILS concept and strategy; f. provide an overall description of Configuration Management and Quality concept and strategy.			
[SOW-269]	The Contractor SHALL review the SRS (see ANNEX A) and all applicable documents, meet and communicate with NATO SMEs as necessary, and present its findings in terms of proposed changes to the SRS based on system cost, schedule, or performance impacts.			
[SOW-270]	The Contractor SHALL also identify any inconsistencies within the requirements. Any inconsistencies not identified by the requirements review will not be accepted later as the basis for a change with cost impact.			
[SOW-271]	[SOW-271] The Contractor SHALL host and conduct a SRR to present and discuss its findings and proposed changes to the requirement baseline for the design and integration of the SOA & IdM Platform. The purpose of this review is to agree upon the requirement baseline for the design and integration of the SOA & IdM Platform system			
[SOW-272]	Upon completion of the SRR, the Contractor SHALL identify any proposed changes to SRS in the form of one or more Change Requests. These Change Requests SHALL be addressed according to the processes implemented by the Contractor to meet the requirements of SECTION 12.6: Engineering Change Proposals.			
[SOW-273]	The Contractor SHALL ensure that Change Request documentation includes: a. list of all Change Requests processed since the start of the project, in a tabular form, indicating for each of them the date it was created and the current status; b. all Change Requests processed since the start of the project.			
[SOW-274]	The Contractor SHALL use the updated FBL as the basis for the SOA & IdM Platform system design and subsequent activities.			

[SOW-275]	The Contractor SHALL provide the following information with each off-specification report:
	a. off-specification identification;
	b. date identified;
	c. description of the Off-specification;
	d. related requirement;
	e. related test (if the Off-specification was raised further to a test failure);
	f. severity (Major or Minor):
	  i. Major: an off-specification categorised as Major SHALL be corrected by the Contractor (at no cost to the Purchaser) before the deployment;
	  ii. Minor: an off-specification categorised as Minor SHALL be corrected by the Contractor (at no cost to the Purchaser) as soon as practicable and as part of this Contract;
	g. Configuration Items (CIs) affected;
	h. action taken;
	i. Fault Resolution status:
	  i. Conceded = the Purchaser's decision is to leave the off-specification not resolved;
	  ii. Open = the Off-specification is identified and work is in progress to resolve it;
	  iii. Resolved = remedial action has been taken by the Contractor and demonstrated through tests conducted by the Contractor without official witnessing by the Purchaser;
	  iv. Closed = the resolution was formally demonstrated to the Purchaser.
	j. comments.			

[SOW-276]	The Contractor SHALL submit to the Purchaser off-specification document which includes: a. list of all Off-specification Reports processed since the start of the project, in tabular form, indicating for each of them the date it was created and the current status; b. all Off-specification Reports processed since the start of the project.			
[SOW-277]	The Contractor SHALL consider two-steps architecture: a. in first step design the Architecture for two datacenters working in asynchronous mode: Lago Patria (JFC Naples) and Mons (SHAPE); b. in second step design the Architecture for three datacentres: Brussels (NNHQ) and Mons (SHAPE) working in synchronous mode and Lago Patria (JFC Naples) working in asynchronous mode with Mons (SHAPE) and Brussels (NNHQ) with preliminary delivery date for datacenter in Brussels (NNHQ), in October of 2020.			
[SOW-278]	The Contractor SHALL conduct the necessary Design Activities and develop its own complete design of the SOA & IdM Platform at the Preliminary and Critical levels, including all interfaces to other systems to meet the SRS.			
[SOW-279]	The Contractor SHALL keep the system design documentation package (including security accreditation documentation) up to date throughout project execution, in particular as a result from the site surveys and/or in order to obtain the security accreditation.			
[SOW-280]	The Contractor's SOA & IdM Platform System Design SHALL cover all sites identified for this project.			
[SOW-281]	The Contractor's SOA & IdM Platform architecture SHALL be designed so that it can be reused for other security classification levels (in any case, the system will be installed and operated at System High mode of operation).			
[SOW-282]	The Contractor's SOA & IdM Platform system SHALL be built to a modular design that allows future extension and enhancements.			

[SOW-283]	The Contractor SHALL establish, deliver and maintain the SOA & IdM Platform System Design Documentation Package, comprising of: a. the Project Implementation Plan (PIP); b. the System Design Specification, the Interface Control Document; c. the Security Accreditation Documentation Package; d. the Requirements Traceability Matrix (RTM); e. Project Master Test Plan (PMTP); f. Integrated Logistic Support (ILS) Plan; g. Training Needs Analysis (TNA).			
[SOW-284]	The Contractor's SDS SHALL describe the SOA & IdM Platform System to a level of detail that is sufficient for the Purchaser to be able to understand how the requirements in the SRS and the security requirements (see ANNEX A) SHALL be implemented and Functional and non-Functional Requirements (see SRS) SHALL be addressed.			
[SOW-285]	Based on the CDR, the Contractor SHALL provide the specification and quantity of the Virtual Machines required to operate the SOA & IdM Platform for each Wave.			
[SOW-286]	Based on the CDR, the Contractor SHALL provide the specification and quantity of the Enterprise Software (Operating System, Database System) required to operate the SOA & IdM Platform for each Wave.			
[SOW-287]	At CDR, the Contractor SHALL provide the Purchaser with the schedule clearly identifying when required Virtual Machines and Enterprise Software, to be provided by the Purchaser, as required.			

[SOW-288]	The Contractor SHALL include the following information in the SDS document (but not limited to):
	a. System architecture
	  i. The following Operational and Systems Views, as defined in the NATO Architecture Framework (NAF, [NAC AC/322-D92007)0048, 2017]):
	    1. NATO Operational View (NOV)-1 High-Level Operational Concept Diagram;
	    2. NATO System View (NSV)-1 Systems Interface Description (Composition);
	    3. NSV-1 System Interface Description (Intra System);
	    4. NSV-1 System Interface Description (Inter System);
	    5. NSV-2, Systems Communications Description – this includes: NSV-2a: System Port Specification;
	    6. NSV-4 System Functionality.
	  ii. The (minimum) information in the NAF views the Contractor SHALL supply is defined in the Table 4 below.
	  iii. The NAF views SHALL be produced and provided in the format of the NCI Agency approved architecture tools (Software AG Aris IT Architect, IBM System Architect or Troux Architect). If not, the Contractor SHALL ensure the exchange format SHALL be approved by the Purchaser upfront.
	  iii. Physical layout and operation principles of the SOA & IdM Platform in the deployment sites (including the site of the SOA & IdM Platform Reference System), including as a minimum:
	7. identification of where the components will be installed, of how users (NATO Staff Users) will make use of the provided functionality, of how support staff (SOA & IdM Platform Administrators will operate the system. This SHALL cover in particular how the SOA & IdM Platform components SHALL integrate into the storage and backup solutions existing at the implementation sites.
	  i. Results of the network simulation, showing the integration with the underlying network infrastructure, the mitigation of potential impact of the available bandwidth and of any latency;
	  ii. Replication, synchronisation and browsing protocols and flows;
	  iii. Proposed topology for the system;
	  iv. Routing, Transport, and connectivity to SOA & IdM Platform components;
	  v. Administration model design (Administrative groups and permissions, administrative roles, trust relationships between separate domains);
	  vi. Schema;			

[SOW-289]	The Contractor SHALL ensure that: a. each direct interface between the SOA & IdM Platform and other systems (e.g. NEDS) is documented in a specific annex of the ICD; b. each interface between the SOA & IdM Platform and SOA & IdM Platform in another security domain is documented in a specific annex of the ICD; c. each interface between the SOA & IdM Platform and other systems is documented in a specific annex of the ICD; d. each interface between the SOA & IdM Platform subordinate or superior SOA & IdM Platform components is documented in a specific annex of the ICD; e. each interface between the SOA & IdM Platform and end-entity users and devices is documented in a specific annex of the ICD; f. the ICD includes detailed description of the interfaces between the SOA & IdM Platform and NEDS, including any "configuration settings" and agreements to enable synchronisation between SOA & IdM Platform and NEDS; g. where work was conducted by the Contractor under this Contract to document the design of any system to be interfaced to the SOA & IdM Platform, the results of that work is included in the relevant annex of the ICD.			
[SOW-290]	The Contractor SHALL develop ICD in accordance with [NTEMP-1] and contain the following information: a. A list of the applicable technical standards b. A catalogue of the services and interfaces exposed by the Platform c. A detailed description of the interfaces, including diagrams, Data Elements, data formats, Performance values, communication protocols, security settings, etc. d. Descriptions of Data Elements e. units of measure required for the Data Element, such as seconds, meters, kilohertz, etc. f. limit/range of values required for the data element (for constants provide the actual value) g. accuracy required for the Data Element h. precision or resolution required for the Data Element in terms of significant digits, i. frequency at which the Data Element is calculated or refreshed, such as 10 KHz or 50 msec j. legality checks performed on the Data Element k. data type, such as integer, ASCII, fixed, real, enumerated, etc. l. data representation/format m. priority of the Data Element n. Service Descriptors, identifying the services endpoints, a detailed description of the service operations and service parameters o. All related Artefacts such as WSDL, schema files and descriptors p. Message descriptions q. Interface priority r. Communications protocol			
[SOW-291]	The Contractor SHALL ensure that the Security Accreditation Documentation Package comprises all documentation mentioned in SECTION 10.1.3.			
[SOW-292]	The Contractor SHALL develop and maintain a RTM as required below.			

[SOW-293]	The Contractor SHALL ensure that the RTM includes the following information (but is not limited to): a. the requirements stated in the SRS and SSRS; b. the detailed contents of the SDS in terms of SDS statements and lowest-level Cis; c. for each requirement, two-way traceability between the requirement and the design feature that implements the requirement; d. for each requirement, identification of any Off-specifications associated with the requirement; e. for each requirement already successfully verified or tested: identification of the test(s) or test waiver(s) on the basis of which the requirement was demonstrated; f. for each requirement not yet successfully tested: identification of the test(s) or test waiver(s) that are intended to demonstrate the requirement; identification of the associated problem report; g. the requirement coverage status by the RTM date with a clear identification of what is the requirement status (met, not met, not yet verified) and if the verification has been witnessed by NCI Agency as part of an acceptance test activity.			
[SOW-294]	The Contractor SHALL ensure that RTM will maintain raceability to Use Histories/ Use cases, Change Requests and their approval status.			
[SOW-295]	As part of the Configuration Management activities, and like any other management product or specialist product, the Contractor SHALL update the System Design Documentation Package to reflect changes, at least at each of the following major milestones: a new design review, the start of a test phase, the completion of each tests activities, the start of the deployment, PSA, FSA.			
[SOW-296]	The Contractor's RTM SHALL provide the basis for scope and change management.			
[SOW-297]	The Contractor SHALL ensure, that in the RTM maintains full traceability between the functional, the allocated and the product baselines, so that the Purchaser can verify their compliance throughout the Contract, including time and place of tested environment, test result and linked test cases and deficiencies.			
[SOW-298]	The Contractor SHALL ensure that RTM is kept up to date in order to reflect any changes during the implementation of the project, in a timely manner (i.e., within one (1) week of change occurring).			
[SOW-299]	The Contractor SHALL provide the RTM in a format compatible with the current version of Microsoft Excel.			
[SOW-300]	The Contractor SHALL post RTM to the Project's Documentation portal.			
[SOW-301]	The Contractor's RTM SHALL be generated automatically from information managed by means of requirements/test management tools.			
[SOW-302]	The Contractor SHALL ensure that In order to maintain clear consistency throughout all documents in the System Design Documentation Package, any update of any of the documents comprised in the System Design Documentation Package SHALL result in re-delivery of a new version of the complete System Design Documentation Package.			
[SOW-303]	The Disaster Recovery Plan & Procedures and the Backup Plan & Procedures prepared by the Contractor SHALL address the best practices developed by the vendors of the system components (hardware and software), including security best practices.			
[SOW-304]	The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL address all possible scenarios and corresponding actions, including security.			
[SOW-305]	The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL align with the site-specific Disaster Recovery Plan & Procedures.			
[SOW-306]	The Backup Plan & Procedures prepared by the Contractor SHALL align with the site-specific Backup Plan & Procedures.			
[SOW-307]	As a minimum, the Disaster Recovery Plan & Procedures prepared by the Contractor SHALL address the following scenarios: a. recovering the entire SOA & IdM Platform; b. transferring of a SOA & IdM Platform service from one platform to another.			
[SOW-308]	The Disaster Recovery Plans & Procedures prepared by the Contractor SHALL clearly distinguish between service restoration and data restoration, and SHALL include a disaster recovery kit.			

[SOW-309]	The Contractor SHALL deliver the disaster recovery kit which SHALL contain distribution media for all software (including versions, upgrades/updates, patches and hot-fixes) to restore an SOA & IdM Platform Element from "bare metal", in accordance with site-specific Disaster Recovery plans.			
[SOW-310]	The Contractor SHALL deliver the disaster recovery kit that includes a full, customised, installation plan that covers all steps (including OS installation) to build and configure each of the SOA & IdM Platform components.			
[SOW-311]	The Contractor SHALL deliver the disaster recovery kit that includes a list of all passwords, community strings, etc. required, with the exception of the information that is retained by the Purchaser as stipulated in the Contract.			
[SOW-312]	The Contractor SHALL ensure that Volume Shadow copy service is used to optimise the backup/recovery process where appropriate.			
[SOW-313]	The Contractor SHALL ensure that disaster recovery procedures are included in the Technical Manuals and SHALL be a dedicated section of it.			
[SOW-314]	The Contractor SHALL ensure that disaster recovery Kit is analysed in terms of ILS resources and all the necessary resources and support needed for disaster recovery is produced as required in the SECTION 14: Integrated Logistics Support of this document.			
[SOW-315]	The Contractor SHALL review the SOA & IdM Platform System Requirements Specification (SRS) and all other applicable documents: a. liaise with NATO subject matter experts as necessary; b. prepare its recommendations in terms of proposed changes to the SRS; c. The Contractor MAY propose changes to the SRS, in order to resolve inconsistencies and/or make improvements; such proposals SHALL be considered by the Purchaser through the Configuration Control Board (CCB) process after Systems Requirements Review (SRR) Meetings.			
[SOW-316]	The Contractor SHALL justify any proposed changes to the requirements together with the expected system cost, schedule, performance and supportability impacts.			
[SOW-317]	The Contractor SHALL identify any inconsistencies within the requirements or that which are in conflict (e.g., with design constraints). Any inconsistencies not identified by the requirements review WILL NOT be accepted later by the Purchaser as the basis for a change with cost impact.			
[SOW-318]	The Contractor's SRS SHALL be the Purchaser provided SRS with approved changes and, as required, extended with additional details supporting the approved scope.			
[SOW-319]	The Contractor's proposed changes to the SRS SHALL be delivered five (5) days prior to SRR.			
[SOW-320]	The Contractor SHALL use the DOORS (IBM) requirements management tool for management of the SRS and project requirements.			
[SOW-321]	The Contractor SHALL organise and conduct SRR to present its proposed changes for the design and integration of the SOA & IdM Platform.			
[SOW-322]	The Contractor SHALL provide items listed below in , above:			
[SOW-323]	The Contractor's SRR SHALL be considered completed when the Purchaser and the Contractor have agreed to all necessary changes to the SRS and when the changes will be implemented accordingly, such that the SRS is sufficient to begin or continue with the design and implementation work.			
[SOW-324]	The Contractor SHALL update the Change Proposal documentation, as defined in SECTION 12.6: Engineering Change Proposals.			
[SOW-325]	The duration of the review cycle for the SOA & IdM Platform System Design Documentation Package SHALL not exceed 4 (four) weeks.			
[SOW-326]	Purchaser review and acceptance of the System Design Documentation Package SHALL not imply Purchaser acceptance of the SOA & IdM Platform Design. The Contractor SHALL prove the design through the regime of testing set forth in the Contract and the Contractor SHALL be responsible in the event that the system proves deficient in meeting the Contractual requirements.			

[SOW-327]	The Contractor SHALL conduct System Design Reviews (Preliminary Design Review (PDR) and Critical Design Review (CDR)) to present the SOA & IdM Platform Design Documentation Package and evidence that all other engineering documents and tools and data is ready to proceed with the development/customization and testing stage. The Contractor SHALL include the following areas in the Design Review: a. SOA & IdM Platform overall system architecture and interactions; b. system functionality, modularity and interfaces, breakdown into lowest-level Configuration Items (see SECTION 12.4 for Configuration Item Identification and Documentation); c. off-the-shelf products to be used in the system: the Contractor SHALL identify the intended product and version, and note if any additional elements (such as macros or plug-ins) are required; d. interfaces with other relevant systems (in particular with NEDS); e. system security design: Presentation of the Risk Assessment Methodology that the Contractor intends to use for the Project, Results of the Risk Analysis, Definition and implementation of the Security measures to counter the risks identified in the Security Risk Assessment. This presentation SHALL be done as a separate item; f. sequence and scope of system tests of the ABL and any requirements for Purchaser support and participation; g. any change request or off-specification; h. any changes to the PBS and PFD; i. any changes to the PMS; j. cost considerations; k. risk assessment of proposed changes and an update of the Risk Log and Issue Log; l. Requirements Traceability Matrix (RTM).			
[SOW-328]	The Contractor SHALL provide a Design Review Report.			
[SOW-329]	The Contractor SHALL update the Design Documentation Package as per the result of the Design Review.			
[SOW-330]	The Contractor SHALL provide all the ILS engineering activities and analysis integrated in the System Design as requested in Section 14.3 and in Section 14.4 and as described in the Integrated Logistic Support Plan.			
[SOW-331]	The Contractor SHALL support the AFPL-associated process and tests as defined in SECTION 8: Testing and Acceptance.			
[SOW-332]	As part of this work package, the Contractor SHALL conduct site surveys at all the sites related to the PSA milestone (see SECTION 3: Scope and SECTION 4: Milestones).			
[SOW-333]	The Contractor SHALL re-deliver any changed documentation.			
[SOW-334]	The Contractor SHALL design and document all the Support, Operation and Maintenance services for SOA & IdM Platform in complete integration with the System platform, as required in the Integrated Logistics Support (SECTION 14) and ANNEX B: Maintenance and Support Concept (After PSA).			
[SOW-335]	The Contractor SHALL perform all the testing & acceptance activities according to the best market practices, as identified and referred to by the Contractor, unless specific testing process requirements and/or definitions are given in this Contract. Should the Contractor deviate from the requirements set forth in this section, it is the Contractor's responsibility to demonstrate the benefit of such approach to the Purchaser.			
[SOW-336]	The contractor SHALL define test automation strategy in PMTP.			
[SOW-337]	The Contractor SHALL plan and undertake a comprehensive set of test steps which will be described in the Project Master Test Plan (PMTP).			
[SOW-338]	The Contractor SHALL conduct Quality-Based Testing (QBT) for each Release prior to any deployment activity.			
[SOW-339]	The Contractor SHALL ensure that QBT demonstrates compliance of the installed, configured and integrated environment based on criteria described in detail in ANNEX A, SRS, SECTION 4 Non-functional Requirements			
[SOW-340]	The Contractor SHALL develop test cases for each type of quality criteria and ensure full test coverage.			

[SOW-341]	The Contractor SHALL provide the following information for each Test Case: a. its objective, by clearly identifying the SRS, SRA, and SSRS requirements (subset of the Requirements Traceability Matrix) intended to be demonstrated by the test procedure; b. the SOA & IdM Platform CIs and facilities and test equipment involved; c. any pre-conditions which SHALL be satisfied prior to application of the test; d. any post-condition which SHALL be satisfied after execution of the test; e. a block diagram showing the proposed method of meeting the test requirements; f. the data to be collected; g. the sequence of testing steps in the procedure, to a level of detail that enables full understanding by the Purchaser of the purpose and effect of each test step; h. the expected outcome; i. the means of measurement and/or assessment for the test.			
[SOW-342]	The Contractor SHALL obtain the Purchaser approval for test cases prior to their execution.			
[SOW-343]	The contractor SHALL define test scenarios that will demonstrate that the SOA & IdM Platform can be used by the pilot application chosen under WP6.			
[SOW-344]	The Contractor's test scenarios SHALL include elements of the three pillars: people, processes and technology.			
[SOW-345]	All Contractor's test cases and scenarios SHALL be approved prior to their execution by the Purchaser.			
[SOW-346]	The Contractor SHALL demonstrate through testing the integration of the system (SMC toolset, as described in ANNEX A, ANNEX C and ANNEX F), with processes and with trained users.			
[SOW-347]	The Contractor's Testing approach SHALL comprise of test phases and milestones described in this section.			
[SOW-348]	The Contractor's Testing SHALL be performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.			
[SOW-349]	The Contractor SHALL conduct engineering Tests during each sprint at the Contractor's environment, consisting of Unit and Component Test, Component Integration Test and system test.			
[SOW-350]	During the Sprint Planning session, the Contractor SHALL: a. identify functional and non-functional requirements of the system that will be develop during the sprint phase; b. define testable User Stories; c. create test cases for user stories; d. participate in project risk analysis; e. plan Test for the release; f. estimate test effort; g. support test automation.			
[SOW-351]	During each Sprint the Contractor SHALL: a. integrate and execute automated and manual tests; b. report the test status to the project team; c. update test cases when new scenarios arise.			
[SOW-352]	The Contractor SHALL deliver Test Reports according to paragraph 8.4.2.			
[SOW-353]	After three sprints, the Contractor SHALL perform a set of System Integration Tests and code quality check on the Purchaser's environment.			
[SOW-354]	Per the Purchaser request the Contractor SHALL submit code for inspection.			
[SOW-355]	To achieve the IRC and RC milestone, the Contractor SHALL: a. execute all agreed test cases; b. correct and re-tested all failures with severity "Critical" or "Major" c. create an agreed action plan for failures with severity "Moderate", "Minor" and "Cosmetic".			
[SOW-356]	The Contractor SHALL show that the plan is suitable and effective in ensuring a smooth activation and avoiding any loss of existing SOA & IdM Platform functionality while maintaining service availability and performance as stated in the Contractual requirements;			

[SOW-357]	The Contractor SHALL deliver the following documentation: a. Installation and activation plans (see SECTION 6). b. SHALL show that the plan is suitable and effective in ensuring a smooth activation and avoiding any loss of existing SOA & IdM Platform functionality while maintaining service availability and performance as stated in the Contractual requirements; c. updated documentation, including the ILSP; d. Original Equipment Manufacturer (OEM) Manuals, the Custom Manuals, and the System Tests Documentation Package in support of the Release Acceptance Tests; e. Disaster Recovery Plan & Procedures; f. Backup Plan & Procedures.			
[SOW-358]	The Contractor SHALL make sure that the SOA & IdM Platform Reference System environment used to conduct Release Acceptance Tests and Software Approval Tests is representative of the actual operational environment, including (but not limited to): a. design and configuration; b. performance; c. security settings; d. software versions.			
[SOW-359]	The Contractor SHALL schedule a period of 6 weeks for the Reference Test phase in the PMTP.			
[SOW-360]	The Contractor SHALL identify any limitations due to the Reference environment regarding its representatively of the actual operational environment, including (but not limited to): a. design and configuration; b. performance; c. security settings; d. software versions.			
[SOW-361]	For each version, the Contractor SHALL verify and validate any new features of the SOA & IdM Platform or Reference Environment that requires a configuration alignment with the Production Environment.			
[SOW-362]	The Contractor SHALL execute any regression tests as required by the Purchaser.			
[SOW-363]	The Contractor SHALL provide a DCIS Test Plan for Purchaser's review and approval.			
[SOW-364]	The Contractor SHALL prepare the DCIS Test Cases, Test Procedures and Test Steps based on Purchaser provided scenarios and submitted these to the Purchaser for their review and approval.			
[SOW-365]	The Contractor SHALL carry out the DCIS test at the Contractor's facility on a test environment that is representative for the deployed environment.			
[SOW-366]	The Contractor SHALL execute the DCIS Test, which will be witnessed by the Purchaser and Purchaser designated Quality Representative(s).			
[SOW-367]	The Contractor SHALL reference the DCIS test case and steps to a requirement with a pass and fail.			
[SOW-368]	The Contractor SHALL record all DCIS test cases and test step results based on the agreed pass/fail criteria and incident categorization, and in case of a fail document the reason of failure.			
[SOW-369]	For successful completion of the DCIS Test, the Contractor SHALL: a. Execute all the agreed test cases; b. Correct and re-test all failures with severity "Critical" or "Major" c. Create an agreed action plan for failures with severity "Minor" and "Cosmetic".			
[SOW-370]	The Contractor SHALL support the Purchaser's RFC test, which consists of a: a. Independent Verification and Validation; b. preliminary User Acceptance Test (UAT); c. cybersecurity testing.			
[SOW-371]	The Contractor SHALL provide fifteen days (15 days) of support to the Purchaser in preparing a RFC to meet the requirements of the Purchaser's Change Evaluation process.			

[SOW-372]	The Contractor's RFC Evaluation SHALL include security testing.			
[SOW-373]	The Contractor SHALL support the Functional Configuration Audit (FCA) as described in SECTION 12.9.			
[SOW-374]	The Contractor SHALL execute any regression tests on the updated PBL as required by the Purchaser.			
[SOW-375]	The Contractor SHALL support any Software Approval tests on the updated PBL as required by the Purchaser, in order to achieve the incorporation of SOA & IdM Platform on the AFPL.			
[SOW-376]	These potential additional tests SHALL be performed by the Contractor to the Purchaser's satisfaction before DA milestone can be accepted by the Purchaser.			
[SOW-377]	DA and Software Approval Tests SHALL NOT start before the Design Documentation Package is accepted by the Purchaser.			
[SOW-378]	The Contractor SHALL complete the Software Approval process for all the software products part of the solution provided by the Contractor, and obtain the Change Advisory Board approval.			
[SOW-379]	The Contractor SHALL obtain Purchaser approval for ILSP as defined in SECTION 14.			
[SOW-380]	The Contractor SHALL provide a tool and a procedure to ensure that the Reference Environment is kept up to date and in line with the Production Environment.			
[SOW-381]	The Contractor SHALL support Independent Verification and Validation (IV&V) conducted by the NCI Agency.			
[SOW-382]	The Contractor SHALL supply the items listed in (see: 12.2.5 Operational Baseline (OBL)) for inclusion in the NCI Agency Release Package			
[SOW-383]	The Contractor SHALL provide and maintain SIVP, if required. The SIVP shall consist of a set of software scripts and/or security tests (in addition to the STVP) to confirm the correct installation and configuration of the system and/or components, in compliance with the Security Documentation Package.			
[SOW-384]	The Contractor SHALL use test cases automation to the maximum extent.			
[SOW-385]	The Contractor SHALL start the UAT phase after the Purchaser has reviewed, approved and signed-off the PSA and Project Test Plan.			
[SOW-386]	The Contractor SHALL prepare the UAT Plan and UAT Specification in accordance with the Project Test Plan.			
[SOW-387]	The Contractor SHALL plan to perform regression testing at the end of the User Tests.			
[SOW-388]	The Contractor's regression tests SHALL be conducted using 100% automated test cases.			
[SOW-389]	The Contractor SHALL specify sufficient test cases at the UAT phase to enable the Purchaser and users designated by the Purchaser to determine whether the SOA & IdM Platform satisfies user needs, requirements, and business processes.			
[SOW-390]	The Contractor SHALL specify use cases, user scenarios and business processes to exercise all user roles for SOA & IdM Platform.			
[SOW-391]	The Contractor SHALL specify test cases to exercise the functions of SOA & IdM Platform by means of use cases, user scenarios and business processes in a representative test environment.			
[SOW-392]	The Contractor SHALL specify test cases to exercise the interactions of SOA & IdM Platform with other systems by means of use cases, user scenarios and business processes.			
[SOW-393]	The Contractor SHALL provide the UAT Plan to the Purchaser at least three weeks before the Test Readiness Review (TRR) meeting.			
[SOW-394]	The Contractor SHALL provide the UAT Specification to the Purchaser at least two weeks before the TRR meeting.			
[SOW-395]	The Contractor SHALL prepare the test data and test environment in accordance with the UAT Plan and UAT Specification.			

[SOW-396]	The Contractor SHALL review test readiness prior to execution of User Acceptance tests. The review of test readiness SHALL confirm, as a minimum, that: a. the conditions for exit from the System Test and Integration Test have been met; b. the UAT Plan and UAT Specification are completed and have been approved by the Purchaser; c. the test environment and test data are ready; d. the UAT Specification has been validated; e. the Contractor has provided sufficient training in the use of SOA & IdM Platform to Purchaser and users designated by the Purchaser; f. the Purchaser and users designated by the Purchaser are available to attend the UATs.			
[SOW-397]	After successful completion of the review of test readiness, the Contractor SHALL execute User Acceptance tests in accordance with the UAT Specification and record the test execution in Test Logs and Test Defect Reports.			
[SOW-398]	The Contractor's QA Manager SHALL review and sign-off all completed User Acceptance test cases and submit for the Purchaser approval.			
[SOW-399]	The Contractor SHALL prepare periodic (preferably monthly) test reports of UATs.			
[SOW-400]	The Contractor SHALL update the Requirements Traceability Matrix to provide traceability from tests completed to contracted requirements and provide the updated Matrix to the Purchaser in soft copy format.			
[SOW-401]	The Contractor SHALL facilitate and support fifteen (15) days of user testing by the Purchaser and users designated by the Purchaser.			
[SOW-402]	The Contractor SHALL record and assess any anomalies identified during user testing, and include it in UAT Report.			
[SOW-403]	The Contractor SHALL prepare a complete build including source and object code, version description document (including issues and workarounds), including deployment and installation instructions.			
[SOW-404]	The Contractor SHALL prepare a UAT Report on completion of User Acceptance testing.			
[SOW-405]	The Contractor SHALL ensure that security testing, including verification of compliance with NATO CIS security regulations, is planned as an integral part of the test process.			
[SOW-406]	The Contractor SHALL exit the UAT phase after it has met the following conditions: a. all UATs have been completed; b. user testing by Purchaser personnel has been completed; c. regression testing has been completed; d. there are no uncorrected system defects with Critical or Major severity; e. actions to resolve all open items have been agreed; f. the UAT Report has been reviewed and signed off by the Contractor and the Purchaser; g. a complete SOA & IdM Platform build (Release Package) is available.			
[SOW-407]	The Contractor SHALL execute all agreed test cases (including security test cases) and all failures with severity "Critical", "Major" or "Moderate" SHALL be corrected and re-tested OK, and an action plan SHALL be agreed for failures with severity "Minor" and "Cosmetic".			
[SOW-408]	The Contractor's System implementation activities in operational environment SHALL not start until the DA milestone is approved by the Purchaser.			
[SOW-409]	The Contractor SHALL perform for each Release that will be published in operational environment a SAT on the Purchaser's operational environment at a limited number of sites, where Release will be implemented. This typically will be after completion of an SOA and IdM Platform Wave (see also SECTION 6.8: Work Packages Introduction for Wave 1 and Wave 2 and ANNEX C).			
[SOW-410]	The Contractor's System Acceptance Test SHALL enable checking compliance with relevant SRS requirements, System Design Documentation Package (including Security Accreditation Documentation Package), and all applicable documents.			

[SOW-411]	As part of Preliminary System Acceptance Test the Contractor SHALL: a. demonstrate that all components of the SOA & IdM Platform have been integrated (including other systems, like NEDS) to meet all the SOA & IdM Platform requirements of the SRS as well as all security requirements specified in the SOA & IdM Platform Security Accreditation Documentation; b. demonstrate that the SOA & IdM Platform meets all of the interface requirements of the SOA & IdM Platform SRS and the SOA & IdM Platform Security Accreditation Documentation package; c. demonstrate the STVP for the SOA & IdM Platform.			
[SOW-412]	The Contractor SHALL support any Software Approval tests on the updated product baseline as required by the Purchaser, tests in order to achieve the listing of SOA & IdM Platform on the AFPL.			
[SOW-413]	Above mentioned potential additional tests SHALL be performed by the Contractor to the Purchaser's satisfaction before DA milestone can be accepted by the Purchaser.			
[SOW-414]	The Contractor SHALL NOT start DA and Software Approval Tests before the Design Documentation Package is accepted by the Purchaser.			
[SOW-415]	The Contractor SHALL conduct the DA, and in compliance with the overall System Testing Process (see SECTION 8: Testing and Acceptance).			
[SOW-416]	The Contractor SHALL successfully conduct Software Approval Tests as defined in SECTION 8.2, and in compliance with the overall System Testing Process detailed in SECTION 10.			
[SOW-417]	The Contractor SHALL successfully implement the SOA & IdM Platform Reference System with all its components as defined in SECTION 6.6.2, in compliance with the processes described in SECTION 7: System Engineering and Integration.			
[SOW-418]	The Contractor SHALL complete the Software Approval process for all the software products part of the solution provided by the Contractor and the CAB has given its approval.			
[SOW-419]	The Contractor SHALL deliver the ILSP as defined in SECTION 14: ILS, and the ILSP SHALL have been approved by the Purchaser.			
[SOW-420]	The Contractor SHALL complete the delivery of Allocated and Product Baselines (ABL and PBL) as defined in SECTION 12: Configuration Management.			
[SOW-421]	The Contractor SHALL develop a SAT Plan, which SHALL be approved by the Purchaser.			
[SOW-422]	After getting the authorisation to deploy the Contractor SHALL execute SAT at every Site (if required) during the implementation.			
[SOW-423]	The Contractor's SAT SHALL be arranged, so that the Purchaser can witness Test at each deployment location.			
[SOW-424]	The Contractor SHALL conduct the DA, and in compliance with the overall Testing Process.			
[SOW-425]	The Contractor SHALL successfully conduct Software Approval Tests as defined in SECTION 8: Testing and Acceptance, and in compliance with the overall System Testing Process.			
[SOW-426]	The Contractor SHALL successfully implement the SOA & IdM Platform with all its components as defined in SECTION 6.6.2 Reference System Installation and SECTION 7: System Engineering and Integration, in compliance with the processes described in SECTION 7: System Engineering and Integration.			
[SOW-427]	The Contractor SHALL develop and deliver the STDP and keep it up to date, as the supporting documentation for each test session.			

[SOW-428]	The Contractor SHALL ensure that STDP comprises the following documents:
	a. the Test and Acceptance Plan (TAP);
	b. the STVP;
	c. SIVP;
	d. any submitted test Waivers (together with supporting material);
	e. the System Version Definition Document (SVDD);
	f. the description of the Test Bed with complete list of Configuration Items (CI):
	  i. hardware and software documentation;
	  ii. services installed;
	  iii. all configuration information;
	g. the test procedures;
	h. the test reports (with issues);
	i. the RTM updated with test related information;
	j. the results of any dry-runs performed by the Contractor as a preparation for the upcoming test session.			

[SOW-429]	The Contractor MAY propose to combine any complementary (i.e. non-overlapping) test documentation package (e.g., the STDP might be complementary to the SAT Packages).			
[SOW-430]	The Contractor SHALL design, develop, execute and maintain the SOA & IdM Platform test cases. The test cases SHALL be described and/or referenced in each Sprint Test phase.			
[SOW-431]	The Contractor SHALL format the test cases such that these can be handed over to the Purchaser in a format that is compatible with the Purchasers Tools (TestRail).			
[SOW-432]	The Contractor SHALL use a Test Management System accessible by the Purchaser.			
[SOW-433]	The Contractor SHALL propose which test should be automated with automated verification conditions. If the automated test will not be performed, the Contractor SHALL justify to the Purchaser lack of automation and obtain its approval.			
[SOW-434]	The Contractor SHALL provide and maintain the TAP.			
[SOW-435]	Within the TAP, the Contractor SHALL define his overall concept of testing and accepting of the SOA & IdM Platform deliverables, and SHALL ensure that above is in line with SAT, SBT, QBT and other testing requirements.			
[SOW-436]	The Contractor SHALL propose a testing process which should use automated testing to the maximum applicable extent.			
[SOW-437]	The Contract SHALL estimate the target automation level and provide explanation on what and why cannot be automated.			
[SOW-438]	In the TAP, the Contractor SHALL define a set of test activities to verify each deliverable's compliance with the contractual requirements, to demonstrate its operational suitability and to evaluate its performance to establish benchmarks for future enhancements and capture above in RTM.			
[SOW-439]	In the TAP, the Contractor SHALL provide the schedule for the provision of the TAP deliverables and detail the conduct of testing (test suites, test scripts, conduct of tests, test reports, etc.).			
[SOW-440]	In the TAP, the Contractor SHALL indicate which requirements from the RTM are being addressed in each test to be executed.			
[SOW-441]	In the TAP, the Contractor SHALL detail which tests are to be conducted during the specific test stage.			
[SOW-442]	The Contractor SHALL ensure that the SVDD includes the following: a. list of differences between this and the previous System version including documentation; b. list of capabilities of this System version; c. guidelines on how to install this System version; d. breakdown of the system into CIs and provision of accurate identification information for every CI, in accordance to the CMDB (see SECTION 12.4).			
[SOW-443]	The Contractor SHALL ensure that the TAP is issued to the Purchaser at least one (1) month before the delivery of the Test Suites and Test Scripts.			

[SOW-444]	The Contractor SHALL provide Test Suites and Test Scripts to the Purchaser at least one (1) month before the planned start of testing.			
[SOW-445]	The Contractor SHALL ensure that Test Acceptance Criteria provide clear evidence that the SoW requirements are fully met.			
[SOW-446]	The Contractor SHALL take Purchaser's comments into account as part of the update of the Test Suites prior to their execution.			
[SOW-447]	The Contractor SHALL formally organise testing once the Test Suites and Test Scripts have been approved by the Purchaser.			
[SOW-448]	The Contractor SHALL ensure that Testing Process verifies that the quality parameters listed in SRS section 4 Non-functional Requirements.			
[SOW-449]	The Contractor SHALL have the overall responsibility for meeting the SOA & IdM Platform testing requirements and conducting all related activities (except for the tests executed by NCI Agency staff and/or other Purchaser's Contractors). This includes the development of all tests and associated documentation required under this Contract, the conduct of all testing and the evaluation and documentation of the tests results.			
[SOW-450]	The Contractor SHALL use a common and verified Test Management System in coordination with the Purchaser, create TAP and SHALL provide the outputs of the Test Management System as required.			
[SOW-451]	The Contractor SHALL ensure that Testing is performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.			
[SOW-452]	The Contractor's RTM SHALL demonstrate that the RTM is implemented as requested in Section 7.4.2.2.3 Requirements Traceability Matrix (RTM).			
[SOW-453]	The Contractor SHALL record the results for each test called for in the Test Plan in a Test Log (also known as Test Execution Log).			
[SOW-454]	The Contractor SHALL summarise the evaluation process in the Test Report and submit for acceptance by the Purchaser.			
[SOW-455]	The Contractor's Test Report SHALL indicate the result of the Test Cases execution.			
[SOW-456]	The Contractor SHALL provide the following information with test report: a. reference to Test Case/Suite; b. date when the test was run; c. test result ("Pass", "Fail", "Not run"); if "Fail", identification of the associated problem report; d. any annotations by the Purchaser's representative; e. comments; f. contractor representative signature (Test Suite); g. purchaser representative signature; h. identification of the PBL under test; i. identification of the data set used to conduct the test session; j. description of the system under test and of the configuration of the testbed.			
[SOW-457]	The Contractor SHALL submit Test Report cover sheet which clearly shows how many tests passed, failed, or were not run.			
[SOW-458]	Where the Purchaser or his representative has witnessed the testing, the Contractor SHALL make appropriate annotations on each page of the test results to ensure that the test report is a true record of test activities and results as witnessed by the Purchaser, and the whole test report SHALL be signed by the Contractor representative and by the Purchaser representative on completion of that testing.			
[SOW-459]	Each original Contractor's test report plus one copy SHALL be distributed to the Purchaser for acceptance within 10 (ten) working days after the completion of the test.			
[SOW-460]	Upon completion of the test session, the Contractor SHALL provide the updated version of the STDP and a System Test Session Report.			
[SOW-461]	The Contractor SHALL provide a Test Progress Report.			

[SOW-462]	The start of any test session SHALL be subject to the Purchaser approval. All entry criteria SHALL be reviewed during a TRR meeting to be held before the test session starts.			
[SOW-463]	The end of any test session SHALL be subject to the Purchaser approval. All exit criteria SHALL be reviewed during a Status Test Review (STR) meeting to be held after the execution of a test session.			
[SOW-464]	Should a failure occur during testing, a failure report SHALL be raised by the Contractor and a preliminary investigation SHALL be immediately carried out in order to classify the failure according to its severity and its priority following the definitions in Table 8: Definitions for Defect .			
[SOW-465]	According to their severity, failures SHALL be classified as one of the following in Table 9: Classification of defects based on severity:			
[SOW-466]	The Contractor SHALL ensure, that according to their priority, failures are classified as one of the following in Table 10: Priority Classes for Defect Classification:			
[SOW-467]	Throughout any test session the Contractor SHALL organise and conduct Tests Status Meetings with the Purchaser as listed in Table 11: Test Status Meetings below:			
[SOW-468]	The Contractor MAY request a Test Waiver, if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts.			
[SOW-469]	The Contractor SHALL request a Waiver on any subset of the above principles by providing sufficient arguments, which state the benefits for the Purchaser. If the Purchaser grants the waiver, the Contractor SHALL execute the Testing in accordance with the Waiver.			
[SOW-470]	The Contractor SHALL certify that the Test Environment to be implemented is identical to that which was originally used for testing of components being in scope of a Waiver, or advise the Purchaser of design changes which affect form, fit or function.			
[SOW-471]	The Contractor SHALL record and log all Waiver requests along with their resolution.			
[SOW-472]	The Contractor SHALL take the following actions into account in their activities and deliverables to meet the criteria identified in the OAC:			
[SOW-473]	The Contractor SHALL respect below requirements for every site survey.			
[SOW-474]	For each site survey, the Contractor SHALL conduct site survey preparatory work, visit each site subject to site survey, survey relevant facilities, interview site personnel, and collect data to support project activities.			
[SOW-475]	The Contractor SHALL ensure coherence between site survey results and project documentation (e.g. System Design Documentation Package, PIP) at any time. The Contractor SHALL update project documentation accordingly.			
[SOW-476]	The Contractor SHALL prepare a SSWB of checklists, fill-in forms, installation sketches, contact information, installation specifications, and site data to be collected by the Contractor during the site survey, and any other documentation required to perform site surveys.			
[SOW-477]	The Contractor's SSWB SHALL be available for Purchaser review and comment before the first site survey, and SHALL be maintained and updated as necessary during the site survey process.			
[SOW-478]	Upon acceptance of the SSWB by the Purchaser, the Contractor SHALL distribute the Site Survey Workbook to the Site(s) for preparation of the Site Surveys. This approach will enable a better preparation by the sites.			
[SOW-479]	The Contractor's site survey(s) and installation sequence and dates reflected in the Project Implementation Plan SHALL be co-ordinated by the Contractor with the Purchaser and the Site POCs to accommodate site-specific requirements, exercises, holiday periods, and other considerations.			
[SOW-480]	The Contractor's Introductory Briefing SHALL be an introduction to the SOA & IdM Platform project outlining the system requirements, describing the system functionalities, the sites to be implemented, the project timelines, the goals and objectives and agenda of the Site Survey process, and the notional implementation identified for the surveyed site and to be refined through the Site Surveys activities.			
[SOW-481]	The Contractor's Introductory Briefing SHALL NOT assume other than basic knowledge of the project by the site personnel.			

[SOW-482]	During the Site Surveys activities the Contractor SHALL determine the necessary installation preparations and support arrangements and collect all system implementation-relevant information. This SHALL include: a. identification of the relevant for SOA & IdM Platform Administrators, Operators, and more generally all POCs; b. identification of existing business processes (for both physical access control and logical access control), and how those processes will integrate with SOA & IdM Platform. c. analysis of the training needs (see also para 14.7 Training); d. identification of any input (item of equipment, documentation, information) or work required from the Purchaser and from the Site with indication of suspense date; e. identification of the facilities where the SOA & IdM Platform will have to be installed, together with each facility's zone level (see [NAC AC/322-N(2014)0158-ADD3, 2015]); f. identification of any potential TEMPEST-related requirement for the SOA & IdM Platform equipment (see [NAC AC/322-N(2014)0158-ADD3, 2015]); g. list of all system CIs (nature and quantities) to be installed in the site; h. update of the user list; i. identification of the tools, policies and procedures in use at Purchaser facilities, in order to determine the integration requirements with the ITSM tools.			
[SOW-483]	The Contractor SHALL determine if site-specific equipment is required at a location as part of any Site Survey performed under this Contract.			
[SOW-484]	If site-specific equipment is required, the Contractor SHALL issue an Engineering Change Proposal (ECP).			
[SOW-485]	In the ECP, the Contractor SHALL identify any requirements of the SOA & IdM Platform System Design Specification it believes will not be met due to differences between the site-specific equipment and the standard baseline.			
[SOW-486]	If these exceptions to the SOA & IdM Platform System Design Specification are accepted by the Purchaser and incorporated into the Contract as formal amendments, the Contractor is not required to demonstrate, as part of its Site Activation work, that the associated System Design Specification requirement has been met. In such a case, the Contractor SHALL update the System Design Specification to reflect site-specific situations.			
[SOW-487]	The Contractor SHALL identify all facilities support, including modifications or additions, required. After coordination with the Purchaser, this notification SHALL be in the form of a letter to the site POC, with a copy to the Purchaser, accompanied by engineering drawings, checklists, or any other supporting information. Facilities support issues that represent Medium or High risk items SHALL be reflected in the Risk Log.			
[SOW-488]	The Contractor SHALL produce and deliver a Site Survey Report for each site, detailing its findings from the site survey, identifying all required Purchaser and Contractor actions and follow-on activities, to prepare for, conduct, or support SOA & IdM Platform installation and activation, and identifying the type of training courses required and the number of Purchaser staff to be trained for each course.			
[SOW-489]	The Contractor's Site Survey Reports SHALL be provided within one week after the respective Site Survey is completed.			

[SOW-490]	At minimum, the Site Survey Report SHALL include:
	a. Installation & Activation:
	  i. Stakeholders communication;
	  ii. System installation requirements;
	  iii. Schedule of installation activities;
	b. Training requirements;
	c. Logistics:
	  i. available system location & and space;
	  ii. technical infrastructure;
	  iii. delivery details;
	d. Local Security Accreditation Authority documentation:
	  i. Contact Details of security responsibilities;
	  ii. Interconnection details;
	  iii. Network diagrams;
	e. Register for all findings that require modification of the site infrastructure or change of the agreed implementation scope. For each of the changes the Contractor SHALL produce a formal change proposal;
	f. For each out of scope item that requires either technical support or procurement activity, the Contractor SHALL offer a proposal to the Purchaser with his recommended solution;
	g. Site diagram that SHALL be used as the basis for the "As Built" Documentation and used in the installation of the site.			

[SOW-491]	After all site survey the Contractor SHALL organise whole sites survey out-brief.			
[SOW-492]	The Contractor SHALL be responsible to follow, implement and conform to the Pre-Accreditation Activities, and the Accreditation Process as defined and documented in [NAC AC/35-D/2005-REV3, 2015] and in SOA and IdM Platform SAP [NCIA NSAP SOA & IdM, 2017]in order to obtain the required security accreditation statement(s) for the SOA & IdM Platform during each phase of the SOA & IdM Platform project.			
[SOW-493]	The Contractor SHALL be required to carry out and meet the terms of the Security Accreditation Authority to perform any Post-Accreditation activities, such as periodic re-assessments of the security risks and periodic inspections up to the time of handover of the SOA & IdM Platform to the CIS Provider.			
[SOW-494]	The Contractor SHALL obtain Approval for Testing (AfT) and (Interim) Security Accreditation ((I)SA) statements which are necessary during the stages of the implementation, tests and trials of the SOA & IdM Platform project. Achieving ISA does not diminish the requirement for the Contractor to obtain the full Security Accreditation statement.			
[SOW-495]	The Contractor SHALL carry out the necessary work as well as to implement the advice, instructions and changes provided by the Security Accreditation Authority and local Security Accreditation Authorities.			
[SOW-496]	The Contractor SHALL produce security accreditation documentation and/or provide inputs to documents in support of the SOA & IdM Platform security accreditation, as detailed in Table 13, below.			
[SOW-497]	The Contractor SHALL produce all security accreditation documentation or inputs to documents using security document templates and/or generic documents provided by the Purchaser. These will be provided after the CAW.			

[SOW-498]	The documentation to be developed to support the SOA & IdM Platform security accreditation process is listed below.The following subsections describe these documents in detail. The documentation set is described in SOA and IdM Platform SAP [NCIA NSAP SOA & IdM, 2017] and includes:
	a. Communication Information System (CIS) description that includes the Security Mechanisms (SMs)
	b. Security Accreditation Plan (SAP);
	c. Security Risk Assessment (SRA) Reports (separate for ON and PBN);
	d. Delta System-specific Security Requirement Statement (SSRS) (dSSRS) (separate for ON and PBN);
	e. Security Operating Procedures (SecOPs); generic SecOPs will be providedby the Purchaser after CAW;
	f. Security Test and Verification Plans (STVP) (separate for ON and PBN);
	g. Security Test and Verification Report (STVR) template;
	h. Site-specific documentation:
	  i. Annex to delta SSRS (if required by the Local Security Accreditation Authority);
	  ii. System Interconnection Security Requirements Statement (SISRS; if required by the Local Security Accreditation Authority);
	  iii. Local SecOPs (if required by the Local Security Accreditation Authority);
	  iv. Local STVP (if required by the Local Security Accreditation Authority); and
	  v. Test Report (mandated for each site).			

[SOW-499]	The Contractor SHALL be responsible to implement the activities described in the SAP as approved by the Security Accreditation Authority.			
[SOW-500]	The Contractor SHALL update the initial CIS description document based on the CIS description template [NTEMP-3] provided by the Purchaser, maintain the CIS description during the project, including all relevant information taken from the System Design Documentation Package as required to understand the content of the CIS description document.			
[SOW-501]	The Contractor SHALL conduct SRA, separate for ON and PBN, and develop the SRA Reports in accordance with Guidelines for Security Risk Risk Management of Communication and Information Systems (CIS) [NAC AC/35-D/1017 –REV3, 2017]. These Reports SHALL address risks specific for SOA and IdM Platform not covered in the formal SRAs for ITM (conducted by the Purchaser) and risks related to modern CIS technologies.			
[SOW-502]	The Contractor SHALL use the NATO template "SRA Report (PILAR) Template" [NTEMP-4] to document the results of the SRAs.			
[SOW-503]	The Contractor SHALL identify areas of the SOA & IdM Platform requiring safeguards and countermeasures to comply with NATO Security Policy and supporting directives. The decision on specific security mechanisms will be based on evidence and results produced by the Security Risk Assessment.			
[SOW-504]	The Contractor SHALL consider any change to be within the technical and financial scope of this Contract whenever the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components; no ECP shall be generated.			
[SOW-505]	The Contractor SHALL raise an ECP whenever the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand.			
[SOW-506]	The Contractor SHALL produce a dSSRS to include the minimum levels of security deemed necessary in addition to the security measures in Automated Information Systems for the NATO SECRET, NATO RESTRICTED and NATO UNCLASSIFIED environments, provided by IT Modernization, in order to counter the risks identified in the SOA & IdM Platform SRAs.			
[SOW-507]	The Contractor SHALL produce the SOA & IdM Platform dSSRS using the NATO dSSRS Template [NTEMP-5] and following the guidance on SRS development [Ref. NAC AC/35-D/1015-REV3, 2012].			
[SOW-508]	The Contractor SHALL ensure that each security requirement in the dSSRS has a unique identifier which is cross-referenced to the security mechanism addressing the requirement.			

[SOW-509]	The Contractor SHALL determine whether each security mechanism is mandatory or recommended. Note: final decision which security mechanisms is mandatory belongs to the CIS Operational Authority (CISOA) and the SAA.			
[SOW-510]	The Contractor SHALL produce the Security Architecture according to the guidelines stated in the appropriate CIS Security Reference Baselines (NATO SECRET CIS Security Reference Baseline [NS CIS Security Reference Baseline, 2017] for ON; NR Reference Baseline for PBN provided in the [ITM NR AIS CSRS]) and per the guidance received by the NATO IT and Security Architect.			
[SOW-511]	The Contractor SHALL produce the Security Operating Procedures (SecOPs) for the SOA & IdM Platform system according to the guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for CIS [NAC AC/35-D/1014 –REV3, 2012], using either, if available, the ITM SecOPs or otherwise the Generic NS AIS SecOPs [2014].			
[SOW-512]	The Contractor SHALL produce the STVPs for the SOA & IdM Platform, separate for ON and PBN, using the NATO template for either, if available, ITM or otherwise the NS AIS [NTEMP-8], defining the complete sequence of steps to be followed to prove that the security mechanisms designed into the SOA & IdM Platform enforce the security requirements identified in the SOA & IdM Platform SRAs.			
[SOW-513]	The Contractor SHALL ensure every security test is cross-referenced to the corresponding security requirement from dSSRSs as well as to the tested security mechanisms.			
[SOW-514]	The Contractor SHALL ensure all security mechanisms of the SOA & IdM Platform are planned for testing.			
[SOW-515]	The Contractor SHALL generate a Security Test and Verification Report, containing results of all security tests specified in the STVP, using the Security Test and Verification Report template [NTEMP-6].			
[SOW-516]	The Contractor SHALL ensure security test identifiers are preserved in the Report as defined in the STVP.			
[SOW-517]	The Contractor SHALL produce SOA & IdM Platform SISRS for each of the interconnections between security domains served by SOA & IdM Platform, using the NATO SISRS template [NTEMP-7].			
[SOW-518]	The Contractor SHALL ensure documents or inputs are delivered within 1 month of Design acceptance.			
[SOW-519]	The Contractor SHALL ensure implementation plans are flexible to take account of the time required for accreditation.			
[SOW-520]	The Contractor SHALL produce Security Documentation under the close supervision and guidance of Purchaser's specialists.			
[SOW-521]	The Contractor SHALL submit Security Documentation to the Purchaser for review before submission to Security Accreditation Authority for approval.			
[SOW-522]	The Contractor SHALL take into account any comments from the reviewers and Security Accreditation Authority and shall update Security Documentation as many times as necessary in order to gain Security Accreditation Authority approval.			
[SOW-523]	[SOW-523] The Contractor SHALL undertake the work identified in the column 'Contractor Responsibility' in Table 13 below			
[SOW-524]	The Contractor SHALL identify Security Mechanism (SM) to be implemented by the SOA & IdM Platform, based on: a. the outcome of the SRA; and b. the Purchaser-developed SM Baselines for the PBN and ON networks (Ref. [NS CIS Security Reference Baseline, 2017], [ITM NR AIS CSRS, 2017]). The NATO CIS Security Reference Baseline(s) will be provided to the Contractor after the CAW.			
[SOW-525]	During design stage the Contractor SHALL apply SRA-recommended security measures in the design, utilizing the NATO CIS Security Reference Baselines ([ITM NR AIS CSRS, 2013], [NS CIS Security Reference Baseline, 2017]).			

[SOW-526]	The Contractor, in the SOA & IdM Platform design, SHALL include implementation of the required Security Mechanisms and provide full traceability of high level security measures requirements down to the implementation level, testing phases, and project lifecycle, utilizing the following documents. a. NATO SECRET CIS Security Reference Baseline [NS CIS Security Reference Baseline, 2017] for NATO SECRET environment; b. Community Security Requirement Statement (CSRS) for NATO RESTRICTED Automated Information System provided by IT Modernization [ITM NR AIS CSRS, 2013]; c. Community Security Requirement Statement (CSRS) for NATO RESTRICTED Automated Information System provided by IT Modernization [ITM NR AIS CSRS, 2013]; d. System Description template [NTEMP-3]; e. Delta System Security Requirements Statement (dSSRS) template [NTEMP-5]; f. Secure AIS STVP Template [NTEMP-8]; and g. Security Test and Verification Report template.			
[SOW-527]	The Contractor SHALL maintain an end-to-end traceability of the required security measures throughout the project, in order to provide assurance that security does support the business requirements and objectives and it is rightly sized to the scope of the project and the solution(s) developed and implemented.			
[SOW-528]	The Contractor SHALL include any additional security measures resulting from the follow-on risk assessments as part of the end-to-end traceability.			
[SOW-529]	The Contractor SHALL design the SOA & IdM Platform security mechanisms to integrate with the existing NATO wide IA Services capability as defined in SRS.			
[SOW-530]	The Contractor SHALL implement the security mechanisms, approved by the Purchaser after coordination with the Security Accreditation Authority, as a part of the SOA & IdM Platform design and security accreditation work and SHALL produce the associated documentation.			
[SOW-531]	The Contractor SHALL establish, execute, and maintain an effective Quality Management process throughout the Contract lifetime. It SHALL be based on [AQAP-2110, 2016], which incorporates by reference ISO 9001 directive.			
[SOW-532]	The Quality Assurance (QA) implemented by the Contractor SHALL apply to all hardware, software (including firmware) and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract. This includes non-deliverable test and support hardware and software.			
[SOW-533]	The Contractor SHALL be responsible for the control of quality of all deliverables and associated Contractual products throughout the life-cycle of the Contract.			
[SOW-534]	The Contractor's QA Process SHALL ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.			
[SOW-535]	The Contractor's QA Process SHALL be described in the QA Plan as outlined below. The process is subject to approval by the Purchaser, or its delegated representative(s), whenever it does not meet the Quality Assurance requirements.			
[SOW-536]	The Contractor's overall QA Process SHALL adhere to the provisions of [AQAP-2110, 2016].			
[SOW-537]	The Contractor SHALL use its own Quality Manual as a reference in the Quality Assurance Process.			
[SOW-538]	The Contractor's Quality Manual SHALL outline the quality focus and the objectives in the Contractor's organisation.			
[SOW-539]	The Contractor SHALL demonstrate, with the Quality Assurance process, that the processes set up for design, develop, produce and maintain the product will assure the product will meet all the requirements.			
[SOW-540]	If sub-contracted quality resources are used, the Contractor's Quality Management Process SHALL describe the controls and processes in place for monitoring the sub-Contractor's work against agreed timelines and levels of quality.			
[SOW-541]	The Contractor SHALL assure that all the test and procedure used to demonstrate the requirements will be monitored and controlled under the QA process.			
[SOW-542]	Unless when invoked in this contract, the Contractor (or his Supplier) SHALL determine the test methods required and perform the tests to demonstrate conformity with the corresponding requirements at appropriate stages up to and including the final product			

[SOW-543]	The Contractor SHALL on request provide the Purchaser with a copy of any subcontracts or orders for products related to the contract.			
[SOW-544]	The Contractor SHALL notify Purchaser if a subcontract or order has been identified as constituting or involving risk.			
[SOW-545]	The Contractor SHALL documented all the identified risks in accordance with SECTION 5.4.6: Risk Management Plan and [AQAP-2110, 2016].			
[SOW-546]	The Contractor SHALL flow down the applicable contractual requirements to Sub-suppliers by referencing the stated contractual requirement, including relevant AQAP(s).			
[SOW-547]	The Contractor SHALL be responsible of ensure that the procedures and processes required to fulfil contract requirements are fully implemented at the Sub-supplier's facilities.			
[SOW-548]	The Contractor SHALL periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser POC.			
[SOW-549]	The Contractor SHALL ensure that all contractual requirements, including NATO supplements, are included in internal audits.			
[SOW-550]	The Contractor SHALL inform the Government Quality Assurance Representative (GQAR) and/or Purchaser of deficiencies identified during internal audit unless otherwise agreed between the GQAR and/or the Purchaser and the Contractor.			
[SOW-551]	The Contractor and Sub-contractor SHALL provide objective evidence, that risks are considered during planning, including but not limited to Risk Identification, Risk analysis, Risk Control and Risk Mitigation.			
[SOW-552]	The Contractor SHALL start planning with risk identification during contract review and updated thereafter in a timely manner. The Purchaser reserve the right to reject QPs, Risk Plans and their revisions.			
[SOW-553]	The Contractor SHALL implement a quality/product assurance risk log/action track system, which identifies all the major/minor non conformity raised during the life cycle of the product.			
[SOW-554]	The contractor SHALL demonstrate that all the non-conformities are solved before the product acceptance.			
[SOW-555]	The Contractor SHALL establish and implement a Corrective Action System to ensure prompt detection, documentation and correction of problems and deficiencies (non-conformities).			
[SOW-556]	The Corrective Action System SHALL track all reported and recorded problems and deficiencies until their closure and clearance.			
[SOW-557]	The Contractor SHALL notify the Purchaser of proposed action, resulting from Review Output that will affect compliance with contractual requirements.			
[SOW-558]	The Contractor's Review outputs SHALL, where action item(s) are identified, specify the responsible person/function and due date of the action item(s).			
[SOW-559]	The Contractor SHALL issue and implement documented procedures which identify, control and segregate all non-conforming products. Documented procedures for the disposition of non-conforming product are subject to approval by the Purchaser when it can be shown that they do not provide the necessary controls.			
[SOW-560]	The Contractor SHALL notify the Purchaser of non-conformities and corrective actions required, unless otherwise agreed with the Purchaser.			
[SOW-561]	When the Contractor establishes that a subcontractor or a Government Furnished Equipment (GFE) product is unsuitable for its intended use, he SHALL immediately report to and coordinate with the Purchaser the remedial actions to be taken.			
[SOW-562]	The Contractor SHALL ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.			
[SOW-563]	The Contractor SHALL document the Corrective Action System in the QA Plan.			
[SOW-564]	The Contractor SHALL deliver all the Certificate of Conformity (CoC) for products, COTS SW (including firmware) and hardware released by the COTS Vendors unless otherwise instructed.			
[SOW-565]	The CoCs delivered by the Contractor SHALL be part of the acceptance data package of the product.			
[SOW-566]	The Contractor SHALL provide a QAP to the Purchaser in accordance with the requirements of AQAP-2105, Edition 2 and the above mentioned AQAPs, and as amended herein.			

[SOW-567]	The Contractor's QAP SHALL be submitted to the Purchaser for review.			
[SOW-568]	The Contractor's QAP SHALL distinguish between the Quality Assurance process and Quality Control Process and plan, manage and resource both.			
[SOW-569]	The Contractor's QAP SHALL be structured as a living document subject to revision/update, as required.			
[SOW-570]	The Contractor's QAP SHALL reference or document and explain the Contractor's QA procedures for analysis, software support, development, design, production, installation, configuration management, control of Purchaser furnished property, documentation, records, programming standards and coding conventions, library controls, reviews and audits, testing, corrective action and certification as specifically related to this project.			
[SOW-571]	The Contractor's QAP SHALL be compatible and consistent with all other plans, specifications, standards, documents and schedules, which are utilised under this Contract.			
[SOW-572]	All Contractor procedures referenced in the QA Plan SHALL either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.			
[SOW-573]	The QA Plan and all related QA procedures shall be subject to Purchaser QAR approval.			
[SOW-574]	The Contractor's personnel comprising the QA organisation SHALL have sufficient responsibility, authority, organisational freedom and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective action.			
[SOW-575]	The Contractor's Personnel performing Quality Assurance functions SHALL have specific documented definitions of their assigned duties.			
[SOW-576]	The Contractor's QA personnel performing QA functions MUST NOT be the same personnel responsible for performing other tasks that are reviewed by QA.			
[SOW-577]	The Contractor's QA Manager Role SHALL provide the Purchaser with all required by this SoW documentation and technical data.			
[SOW-578]	The Contractor's QA personnel SHALL participate in the early planning and development stages to ensure that attributes of good quality for life-cycle procurement are specified in plans, standards, specifications and documentation.			
[SOW-579]	After establishment of attributes, controls and procedures, Contractor QA personnel SHALL ensure that all elements of the QA Process are properly executed, including inspections, tests, analysis, reviews and audits.			
[SOW-580]	The Contractor's QA personnel SHALL be designated as the Contractor's QA Management Representative and point of contact for interface with and resolution of quality matters raised by the NCI Agency or his delegated National Quality Assurance Representative (NQAR) and identified in the Quality Assurance Plan.			
[SOW-581]	The Contractor SHALL ensure that Quality Management personnel have the required qualifications, knowledge, skills, ability, practical experience and training for working with, and in accordance with the applicable NATO AQAP's and ISO standards.			
[SOW-582]	The Contractor SHALL ensure that Quality Management Personnel are of sufficient number and have sufficient resources to adequately and effectively monitor and control the QA Process.			
[SOW-583]	The Contractor SHALL notify the Purchaser if a sub-supplied product is rejected or repaired which has been identified as involving risk or supplied by a Sub-contractor whose selection or subsequent performance has been identified as involving risk.			
[SOW-584]	The Contractor's Configuration Management (CM) process SHALL enable the baselining of Configuration Items (CIs) into the FBL, ABL, PBL and OBL as defined in this section of the SoW and the maintenance of these baselines throughout the duration of the Contract.			
[SOW-585]	The Contractor SHALL ensure that an effective CM organisation is established to implement and manage the Configuration Management processes throughout the duration of this Contract.			

[SOW-586]	The Contractor SHALL create and maintain 4 (four) Configuration Baselines, as follows (see Figure 12). a. Functional Baseline (FBL or "as-required"); b. Allocated Baseline (ABL, or "as-designed"); c. Product Baseline (PBL, or "as-built"); d. Operational Baseline (OBL, or "as-delivered", or "as-deployed").			
[SOW-587]	Under the CM process the Contractor SHALL maintain and update all project CIs as requested by changes within the project or external to the project throughout the duration of the Contract;			
[SOW-588]	The Contractor SHALL ensure that there is full traceability through all baselines back to the functional baseline.			
[SOW-589]	The Contractor's developed baselines SHALL be encapsulated and maintained by the Contractor in a database established by the Contractor as specified under Configuration Management Tools.			
[SOW-590]	The Contractor's developed FBL SHALL be derived from the SOA & IdM Platform SRS and SHALL be established at the successful completion of the SRR with the approved updated SRS.			
[SOW-591]	The Contractor's design in the ABL SHALL meet the functional and non-functional requirements allocated in the FBL.			
[SOW-592]	The Contractor's ABL set of documents and Artefacts SHALL contain (but is not limited to) the following documents: a. Software Design Specification; b. the Test Specification; c. Requirment Traceability Matrix (RTM).			
[SOW-593]	The Contractor's ABL SHALL be established at the successful completion of the SDR.			
[SOW-594]	The Contractor's PBL SHALL meet the functional and non-functional requirements allocated in the FBL and the design of the ABL.			
[SOW-595]	The Contractor's developed PBL for SOA & IdM Platform SHALL be established after successful completion of the RC and DA Review(s). It reflects the "as-built" configuration of the system.			
[SOW-596]	The Contractor's PBL products SHALL be distinguished in documentation, software, hardware/equipment and services.			
[SOW-597]	The Contractor's software products of the PBL SHALL contain the following: (off-the-shelf) software media, (off-the-self) software license(s).			
[SOW-598]	The Contractor's (supporting) documentation products of the PBL SHALL contain: a. PBL (as-built) drawings, b. off-the-shelf OEM manuals, c. FBL (as-required) documentation, d. ABL (as-designed) documentation, e. Operations and Maintenance support documentation, f. Inventory documentation, g. Training documentation, h. Quality assurance documentation, i. Security documentation, j. Configuration Management documentation, k. Warranty documentation and Traceability Matrix.			
[SOW-599]	The Contractor SHALL include the System Design Specifications (SDS including the Requirements Traceability Matrix), the Test Plan, and any other documentation deemed appropriate by the Contractor, in accordance with provisions of IEEE 12207, to ensure that requirements are reflected in the system during development and integration can be demonstrated through a comprehensive set of tests and can be delivered in the form of the PBL.			
[SOW-600]	The Contractor's developed OBL SHALL be initially established after successful completion of the PSA and then finally established after successful completion of FSA. It reflects the "as-deployed" ("as-delivered") configuration of the system			

[SOW-601]	The Contractor's OBL SHALL contain: all delivered Software Configuration Item (SWCI), including COTS; b. all delivered Hardware Configuration Item (HWCI), if any; c. Computer Software Configuration Item (CSCI); d. all the Documentation that comprise the system and any subsequent releases and SHALL reflects the "as-deployed" configuration of the system.			
[SOW-602]	SOA-IdM Platform baselines SHALL be given by a Contractor a major release number and a minor release number comprising an X.X notation. Some of the releases will be defined beforehand and numbering system can be summarised as per following example: a. SOA-IDM RCv3.0.0 is the OBL at First PSA; b. SOA-IDM RCv3.0.1 is 3.0.0 with minor modifications as applied until Next PSA; c. SOA-IDM RCv3.1.0 is the OBL at Next PSA; d. SOA-IDM RCv3.1.1 is 3.1.0 with minor modifications as applied until Next PSA (or last – FSA); e. for Wave 2 – similar: SOA-IDM RCv7.0.0 is the OBL at First PSA.			
[SOW-603]	The Contractor SHALL include in the PBL and/or OBL release package the following elements, as a minimum all items described below in Table 14:			
[SOW-604]	The Contractor SHALL provide a CMP tailored to the requirements of the proposed technical solution.			
[SOW-605]	The Contractor's CMP SHALL be structured as a living document subject to revisions and updates, as required.			
[SOW-606]	The Contractor SHALL place the CMP under configuration control prior to its implementation and for the life of the Contract.			
[SOW-607]	In producing the Contractor's CMP, the Contractor SHALL define the organisation and procedures used to configuration manage the functional and physical characteristics of CIs, including interfaces and configuration identification documents.			
[SOW-608]	The Contractor SHALL ensure that all required elements of CM are applied in such a manner as to provide a comprehensive CM process.			
[SOW-609]	The Contractor's CMP SHALL be compatible and consistent with all other plans, specifications, standards, documents and schedules.			
[SOW-610]	The Contractor SHALL propose in the CMP detailed configuration control procedures.			
[SOW-611]	All Contractor and Purchaser activities and milestones related to CM SHALL be identified and included in the PMS of the PMP.			
[SOW-612]	The CMP SHALL address all disciplines within this section and SHALL as a minimum include the following sections: a. Introduction; b. Organisation; c. Configuration Identification and Documentation; d. Configuration Control; e. Configuration Status accounting; f. Configuration Audits; g. Configuration Management tools/Interface management.			
[SOW-613]	The Contractor SHALL divide the products and specialist products into CIs (Configuration Items).			
[SOW-614]	The Contractor's CI structure SHALL show the relationships between the lower level baselines and CIs.			
[SOW-615]	The Contractor SHALL propose appropriate CIs in the CMP including an explanation of the rational and criteria used in the selection process, based on the criteria for selection of CIs as detailed in [NATO ACMP 2009, 2017].			
[SOW-616]	The Contractor's CIs SHALL be chosen in a way to assure visibility and ease of management throughout the development effort and the support to the OBL after acceptance.			
[SOW-617]	All Contractor's COTS, adapted, and developed software SHALL be designated as CIs.			
[SOW-618]	Where Contractor's COTS product can be installed in a modular fashion, the description of the CI, the Contractor SHALL unambiguously identify the complete list of installed components.			

[SOW-619]	The Contractor SHALL designate all complete hardware elements as CIs (if any).			
[SOW-620]	The Contractor SHALL create or use a COTS software to maintain the CMDB that persists the Configuration Items (CIs) attributes, (inter-) relationships and Configuration Baselines.			
[SOW-621]	The Contractor SHALL ensure that the Configuration Baselines and CIs are persistently stored, maintained and managed in the CMDB.			
[SOW-622]	The Contractor SHALL keep the CMDB consistent and updated.			
[SOW-623]	The Contractor's CMDB SHALL be compliant with the Purchaser's ITSM Tools.			
[SOW-624]	The Contractor's CMDB SHALL provide the ability to trace higher and subordinate CIs using CI identifiers or other CI attributes.			
[SOW-625]	The level of granularity for the Contractor's Configuration Item selection SHALL reach at minimum: a. Line Replaceable Units (LRUs) - Hardware CIs,(if any); b. Software Assets and/or Firmware/Software CIs; c. Documentation delivered under this Contract - Documentation CIs; d. The Hardware CI attributes SHALL include, but is not limited to, the Material Datasheet information,(Optional); e. The Software CI attributes SHALL include, but is not limited to, the STANAG 4427, 2014 definitions; f. Any Documentation CI that is not linked to a Software CI or Hardware CI (optional) SHALL include, but is not limited to, the Contract SSS attributes.			
[SOW-626]	The Contractor SHALL be responsible for issuing in a timely manner, as required by this SoW, all approved changes and revisions to the functional, development and product baseline documents included in the Contract. This includes changes originated both by the Contractor and the Purchaser.			
[SOW-627]	Where a change affects more than one document, or affects documents previously approved and delivered, the Contractor SHALL ensure that the change is properly reflected in all baseline documents affected by that change.			
[SOW-628]	All design changes SHALL be appropriately reflected in the technical documentation by the issue of appropriate changes or revisions and SHALL be provided to the Purchaser.			
[SOW-629]	The Contractor SHALL be fully responsible for the Configuration Control of all baselines and CIs in accordance with [NATO ACMP 2009, 2017].			
[SOW-630]	The Contractor SHALL define the responsibilities and procedures used within the Contractor's organisation for configuration control of established CI, and for processing changes to these CI.			
[SOW-631]	The Contractor SHALL define the Configuration Baseline Change procedures and SHALL submit Notice of Revision or Request for Deviations and Wavers when required and approved by the Purchaser.			
[SOW-632]	Changes to the Contractor's developed baselined CIs SHALL be processed as either Class I or Class II ECPs as defined in [NATO ACMP 2009, 2017] and the change request requirements specified in SECTION 7.3.2.			
[SOW-633]	The Contractor SHALL use the configuration control procedures specified in the CMP for the preparation, submission for approval implementation and handling of ECPs to baselined CIs.			
[SOW-634]	When submitting ECPs, the Contractor SHALL assign a priority rating of Emergency, Urgent or Routine Extensions to the target times for processing.			
[SOW-635]	Class I ECPs SHALL have to be mutually agreed upon by the Contractor and Purchaser.			
[SOW-636]	The Contractor SHALL propose in the CMP an ECP format based on the requirements in [NATO ACMP 2009, 2017].			
[SOW-637]	The Contractor SHALL use the configuration control procedures specified in the CMP for the preparation, submission for approval implementation and handling of ECPs to baseline CIs.			
[SOW-638]	Extensions to the target times for processing Class I ECPs SHALL be mutually agreed upon by the Contractor and Purchaser.			
[SOW-639]	Prior to implementation, all Class II ECPs SHALL be submitted by the Contractor to the Purchaser for review and classification concurrence.			
[SOW-640]	If the Purchaser's representative does not concur in the classification, Class I ECP procedures SHALL be applied by the Contractor and the ECP and then formally submitted to the Purchaser for approval or rejection.			

[SOW-641]	The Contractor SHALL appropriately reflect in the technical documentation all design changes by the issue of appropriate changes or revisions.			
[SOW-642]	Any Engineering Change Proposal SHALL include, as a minimum, the following information: a. Reference Number; b. requirement affected (using the outline numbering of the core SoW, or of Annex A and B); c. nature of change; d. rationale for the change; e. impact of change; f. description of how the change will be reflected in the delivered system's cost, schedule, and/or performance. This description SHALL include any trade-offs that SHALL be considered; g. status; h. priority.			
[SOW-643]	If required, the Contractor SHALL prepare, handle, and submit for Purchaser's approval, RFDs and RFWs as defined in [NATO ACMP 2009, 2017]			
[SOW-644]	The Contractor SHALL propose in the CMP a RFD/RFW format based on the requirements in [NATO ACMP 2009, 2017]			
[SOW-645]	The Contractor SHALL be aware that permanent departures from a baseline SHALL be accomplished by ECP action rather than by RFD.			
[SOW-646]	The Contractor SHALL be fully responsible for the CSA for all CIs in accordance with [NATO ACMP 2009, 2017]			
[SOW-647]	The Contractor SHALL propose the format of CSA report his CMP for Purchaser's approval.			
[SOW-648]	The Contractor SHALL deliver CSA reports to the Purchaser both as part of management and specialist products in this contract and also as standalone documents at the Purchaser's request.			
[SOW-649]	At the end of the Contract, the Contractor SHALL deliver a set of final CSA reports for each CI or set of CI's in both hard copy and in electronic media.			
[SOW-650]	Upon request from the Purchaser, the Contractor SHALL support configuration audits to demonstrate that the actual status of all Cis matches the authorised state of CIs as registered in the CSA reports.			
[SOW-651]	The Contractor SHALL support the FCA and Physical Configuration Audit (PCA) by providing the required Baseline Documentation and answering questions from the Purchaser's Auditor.			
[SOW-652]	The Contractor SHALL draft a Configuration Audit Report for the FCA and PCA that summarises the results for the Purchaser's approval.			
[SOW-653]	The Contractor SHALL solve any deficiencies found during the Configuration Management Audits within the agreed timeframe and update the baseline accordingly.			
[SOW-654]	The initial version of the Contractor's ABL, and PBL SHALL be provided to the Purchaser for acceptance.			
[SOW-655]	Upon Purchaser Acceptance, ABL and PBL SHALL be placed by the Contractor under the control of the CCB.			
[SOW-656]	The Contractor SHALL keep the contents of the ABL and PBL under Configuration Control to reflect the progress of the project activities.			
[SOW-657]	The Contractor's version control/configuration management automated tool SHALL include the capabilities for baselines management, source code control versioning, configuration item identification, change request management, deficiency reporting management, and configuration status accounting.			
[SOW-658]	The Contractor SHALL provide the Purchaser read-only access to the version control/configuration management automated tool, including source code of the baseline.			
[SOW-659]	The Contractor SHALL provide these tools as part of the SOA & IdM Platform Reference System to enable life-cycle configuration management.			
[SOW-660]	The Contractor SHALL establish a Configuration Identification System.			
[SOW-661]	The Contractor's configuration Identification System SHALL identify all documents necessary to provide a full technical description of the characteristics of the Hardware and Software Configuration Items (CIs) that require control at the time each baseline is established.			
[SOW-662]	The Contractor's configuration Identification System SHALL include the relevant deliverables in the contract.			

[SOW-663]	The Contractor's CI structure SHALL be a tree structure with the system being the top level CI.			
[SOW-664]	Detailed proposals for the documents that will comprise the above baselines SHALL be included in the CMP for approval by the Purchaser.			
[SOW-665]	At the end of the contract, the Contractor SHALL deliver the baseline documentation in a format which complies with section 14.6.12: Publication Criteria			
[SOW-666]	As part of the CMDB, as specified under Configuration Management Tools, the Contractor SHALL transfer to CMDB a copy of the current version of all baselines to the Purchaser at contract completion.			
[SOW-667]	All Contractor's SOA & IdM Platform project key personnel SHALL demonstrate spoken and written fluency in English language, at a minimum of 4343 as defined in [STANAG 6001, 2014].			
[SOW-668]	All Contractor's SOA & IdM Platform project key personnel SHALL have a current NATO SECRET security clearance and maintain it throughout the lifecycle of the Contract.			
[SOW-669]	All Contractor's SOA & IdM Platform personnel who need System Administrator privileges or access when working on NATO SECRET systems SHALL hold NATO CTS (Cosmic Top Secret) clearance and maintain it throughout the lifecycle of the Contract.			
[SOW-670]	All Contractor's SOA & IdM Platform project key personnel SHALL present references of successful project delivery and description of roles, responsibilities, activities executed, and SHALL include reachable points of contact for above.			
[SOW-671]	The Contractor's SOA & IdM Platform PM SHALL meet educational requirements: a. have an university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, equivalent to a Master's, supported by relevant certificates/diplomas; exceptionally, extensive relevant experience may be considered if the above qualifications are not met; b. have current Project Management certification (Information Technology Infrastructure Library (ITIL) Foundation, Prince2 Practitioner or Project Management Institute (PMI) Project Management Professional (PMP), or equivalent); c. SHOULD HOLD relevant Agile Practitioner Certificate.			
[SOW-672]	The Contractor's SOA & IdM Platform PM SHALL meet experience requirements: a. have at least ten (10) years of experience as an Information and Communication Technology (ICT) project manager; b. have at least five (5) years of experience as the project manager for an effort of similar scope to the SOA & IdM Platform project; c. have preferably including the application of a formal project management methodology such as PRINCE2 or Agile. d. experience SHALL include, as the project manager, the successful delivery of at least one similar project involving PaaS implementation, migration of applications, integration of the capabilities under one centralised service management and control system in an environment where security was a significant concern. The experience SHALL be supported by project references, points of contact, and description of role/responsibilities/activities executed.			
[SOW-673]	The Contractor's SOA & IdM Platform PM SHALL: a. be responsible for: i. project management; ii. performance and completion of tasks and deliveries; b. establish and monitor project plans and schedules and has full authority to allocate resources to insure that the established and agreed upon plans and schedules are met; c. manage costs, technical work, project risks, quality, and corporate performance; d. manage the development of designs and prototypes, test and acceptance criteria, and implementation plans; e. establish and maintain contact with Purchaser, subcontractors, and project team members; f. provide administrative oversight, handles Contractual matters and serves as a liaison between the Purchaser and corporate management; g. ensure that all activities conform to the terms and conditions of the Contract.			
[SOW-674]	The Contractor's SOA & IdM Platform TL/SSE SHALL have university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/diplomas.			

[SOW-675]	The Contractor's SOA & IdM Platform TL/SSE SHALL have current ITIL Foundation and Service Design certificates.			
[SOW-676]	The Contractor's SOA & IdM Platform TL/SSE SHALL meet experience requirements: a. have at least seven (7) years in engineering positions associated with the review, design, development, evaluation, planning and operation PaaS components, subsystems, or systems for government or commercial use (e.g., middleware, Service Oriented Architecture, Network Access/Admission Control, IdM); b. have at least 5 years of the experience which SHALL be related to the architecture, design and implementation of system/platform similar to SOA & IdM Platform project; c. have a minimum of one (1) years' experience in undertaking ICT QA activities; d. have knowledge and experience with QA standards (either AQAP or ISO), processes for integration and testing; e. have a minimum of three (3) years of experience as a team leader or project manager to ensure the technical management oversight of a: SOA platform designer, IdM Platform designer, Infosec/Compusec designer, communications engineer and systems integrator; which SHALL be supported by project references, points of contact, and technical description of the role, responsibilities and activities; f. have an ITILv3 Intermediate certification (ITIL Service Operation and/or ITIL Service Transition).			
[SOW-677]	The Contractor's SOA & IdM Platform TL/SSE SHALL: a. plan and co-ordinate engineering activities to meet SRS requirements; b. perform complex engineering tasks and multiple tasks simultaneously; c. direct and co-ordinate all activities necessary to complete a major, complex engineering program or multiple smaller tasks or programs; d. perform advanced engineering research, hardware or software development; e. supervise the work of a design, integration, test, and implementation team; f. analyse architectural options for performance and manageability; g. recommend design changes/enhancements for improved system performance; h. provide comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance; i. be competent in technical disciplines as applied to government and commercial information and communications systems.			
[SOW-678]	The Contractor's SOA & IdM Platform Test Director and/or Test Engineer SHALL NOT perform any other duties within the SOA & IdM Platform project.			
[SOW-679]	The Contractor's SOA & IdM Platform TD/TE SHALL have university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/diplomas.			
[SOW-680]	The Contractor's SOA & IdM Platform TD/TE SHALL meet experience requirements: a. have integration and testing engineering skills with five (5) years of experience as part of projects at least equivalent to SOA & IdM Platform, supported by project reference and description of role, responsibilities and activities; b. have demonstration of practical experience in planning, conducting and assessing integration and testing activities in support of projects for at least equivalent to SOA & IdM Platform for at least two (2) years, supported by project references and description of role, responsibilities and activities; c. have at least ten (10) years of experience in the planning and execution of testing information systems, defence systems, and large scale C2 systems.			
[SOW-681]	The Contractor's SOA & IdM Platform TD/TE SHALL: a. be responsible for directing test planning, design and tools selection; b. establish guidelines for test procedures and reports; c. co-ordinate with Purchaser on test support requirements and manage Contractor test resources.			
[SOW-682]	The Contractor's SOA & IdM Platform QA Manager SHALL NOT perform any other duties within the SOA & IdM Platform project.			

[SOW-683]	The Contractor's SOA & IdM Platform QA Manager SHALL have university Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/diplomas.			
[SOW-684]	The Contractor's SOA & IdM Platform QA Manager SHALL meet experience requirements: a. have at least seven (7) years working with quality control methods and tools, b. have at least four (4) years supporting system development and test projects.			
[SOW-685]	The Contractor's SOA & IdM Platform QA Manager SHALL: a. establish and maintain process for evaluating software, hardware, and associated documentation; b. determine the resources required for Quality Control; c. maintain the level of quality throughout the system life cycle; d. prepare and guide the development of system Quality Assurance plans; e. develop project Quality Assurance plan; f. guide development and implement quality standards; g. review hardware, software, and documentation; h. prepare and guide formal and informal reviews to determine quality; i. examine and evaluate design, integration, and test processes and recommend enhancements and modifications; j. conduct formal and informal reviews at predetermined points throughout the system life cycle; k. audit subcontractors, suppliers and outsource companies to ensure that appropriate standard practices are applied; l. be competent in technical disciplines as applied to government and commercial information and communications systems.			
[SOW-686]	The Contractor SHALL use the [AIA/ASD SX000i, 2016] specification as guidance when establishing and conducting the ILS Process, in accordance with the requirements of the contract.			
[SOW-687]	The Contractor SHALL provide and maintain an Integrated Logistic Support Plan, tailored to the Project Program phases.			
[SOW-688]	The Contractor SHALL develop the ILSP in accordance with the requirements described in this section.			
[SOW-689]	The Contractor SHALL ensure compatibility between the ILS management documentation and the System Management Plan by providing the ILS relevant inputs for the System Management Plan			
[SOW-690]	The Contractor SHALL detail in the ILSP how Integrated Logistics Support will be designed, managed, procured and provided throughout the system lifetime.			
[SOW-691]	The Contractor's initial version of the ILSP SHALL be provided to the Purchaser for acceptance.			
[SOW-692]	The Contractor SHALL maintain and update the ILSP as required to reflect changes in the PBLs, in the SoW, or in support arrangements for any SOA & IdM Platform CIs.			
[SOW-693]	As an Annex of the ILSP and in accordance with ANNEX B, the Contractor SHALL develop and maintain the SOA & IdM Platform Maintenance and Support Concept that defines the maintenance and support environment, constraints, locations, procedures, artefacts, organisation and personnel skills to maintain the Delivered Baselines of the platform.			
[SOW-694]	The Contractor's Maintenance and Support Concept SHALL refer to the functional and non-functional Requirements of the SOA & IdM Platform.			
[SOW-695]	The Contractor's Maintenance and Support Concept SHALL define the Maintenance and Support tasks at any level of support and at any level of maintenance.			
[SOW-696]	The Contractor's Maintenance and Support Concept SHALL define the Delivered Baselines maintenance and supply flow amongst the various NATO locations, organisations, groups, and people.			
[SOW-697]	The Contractor's Maintenance and Support Concept SHALL define and describe the Maintenance and Support process interfaces to the other processes.			
[SOW-698]	The Contractor SHALL define the 2nd and 3rd Level Support process interfaces to the other processes, including the existing NCI Agency's Service Desk (1st Level of Support).			
[SOW-699]	The Contractor's Support process interface definition SHALL include the input and output information, its structure, the communication path, POCs, the time constraints for sending and receiving information, and quality criteria to evaluate the integrity of the interface.			

[SOW-700]	At each Support and Maintenance Level, the Contractor's Support Concept SHALL describe the support environment, constraints, locations, procedures, artefacts, organisation and personnel.			
[SOW-701]	The Contractor's procedural description SHALL include objective(s), triggering event(s), input(s), output(s), task(s), roles and responsibilities using a Responsible, Accountable, Consulted, Informed (RACI) matrix, constraints, exceptional case(s), and tool(s) support.			
[SOW-702]	The Contractor's SOA & IdM Platform ILSP SHALL be based on the established Support Concept, approved by the Purchaser.			
[SOW-703]	As part of the Maintenance and Support Concept, the Contractor SHALL implement the Supply Support Plan.			
[SOW-704]	The Contractor's Supply Support Plan SHALL: a. define the Supply Support requirements; b. describe the procedures for the provisioning, procurement, and acquiring of spare/repair parts, inventories, and consumable material for PBL and the OBL during the system lifetime.			
[SOW-705]	The Contractor SHALL conduct a Logistics Support Analysis (LSA) Process, tailored to support the specific scope of the System operation activities.			

[SOW-706]	The Contractor's LSA SHALL include, as a minimum:
	a. Reliability, Availability, Maintainability and Testability (RAMT) responsibility, analysis and procedure :
	  i. the RAMT analysis SHALL clearly capture and display the RAMT characteristics of each main platform component, aggregated up to the level of sub-system, and subsequently the entire system;
	  ii. the RAMT analysis SHALL be used to calculate and predict intrinsic availability and operational availability, as defined in SRS, for each type of subsystem, each type of node and each type of end-to-end connection;
	  iii. the Contractor SHALL ensure that the first issue of RAMT analysis is performed and delivered before SDR and accepted at SDR.
	b. planning of the identification of operation and Service Management and Control (SM&C) tasks;
	c. planning of a Task Analysis for operation tasks, SM&C tasks, corrective maintenance tasks and preventive maintenance tasks;
	d. Allocation of each Operational and Maintenance task to the correct Level of Support/Maintenance (Level of Repair Analysis (LoRA));
	e. Planning and execution of the Operation and Maintenance Procedures Verification Test;
	f. Total Cost of Ownership Analysis, which SHALL include the warranty cost and all the operational costs and all the maintenance cost for ALL the support and Maintenance levels for at least 5 years after FSA;
	g. Warranty Management and Obsolescence Analysis and Management.			

[SOW-707]	The Contractor SHALL develop and maintain the necessary Support Cases in which all LSA activities SHALL be documented. The Support Case SHALL include: a. Reliability, Availability, Maintainability and Testability (RAMT)results and calculation; b. the complete data set of the Task Analysis, including listings of all operation tasks, SM&C tasks, corrective maintenance tasks and preventive maintenance tasks; c. The results of the Disaster Recovery Logistic Analysis; d. The results from the Operation and Maintenance Procedures Verification Test; e. The Total Cost of Ownership Analysis results; f. The Obsolescence Analysis results.			
[SOW-708]	The Contractor's Support Case SHALL demonstrate that all LSA and RAMT requirements have been met, with correct data used and results achieved in all calculations and models.			
[SOW-709]	The Support Case SHALL provide rationale and justifications for all data and formulas used in any of the calculations and models.			
[SOW-710]	The Contractor's design of the system SHALL include sufficient redundancy and other RAMT measures to ensure the requirements in this Contract are achieved and attained at an optimal TCO, minimising preventive maintenance, manpower requirement and usage of special-to-type tools and test equipment.			

[SOW-711]	Such measures taken to ensure fulfilment of RAMT requirements and optimisation of TCO SHALL be documented by the Contractor in the Support Case.			
[SOW-712]	The Contractor SHALL use the MIL-STD-882E as guideline to eliminate or mitigate risks associated with both Functional Safety and Health & Safety hazards			
[SOW-713]	The Contractor SHALL perform a System Hazard Analysis, ensure that any potential hazards to people or the environment will be identified and that associated risks are clearly documented and mitigated and/or eliminated.			
[SOW-714]	The Contractor SHALL document the result of the hazard analysis as an annex of the ILSP.			
[SOW-715]	The Contractor SHALL develop and maintain the list of all operation tasks, SM&C (Service Management and Control) tasks, administrative tasks, corrective maintenance tasks and preventive maintenance tasks, to be used as a starting point for the task analysis.			
[SOW-716]	The Contractor SHALL perform and deliver the first issue of Operation and Maintenance Task Analysis before SDR and accepted at SDR.			
[SOW-717]	The Contractor's analysis SHALL contain also the list of procedures needed to configure the platform for mission and/or exercise environment.			
[SOW-718]	The Contractor's operation tasks SHALL be identified through analysis of the functional and no functional requirements of the new system taking into account mission scenarios and conditions under which the system will be operated.			
[SOW-719]	The Contractor's analysis SHALL examine each system function allocated to personnel and determine what operator tasks are involved in the performance of each system function			
[SOW-720]	The Contractor's SM&C tasks SHALL be identified through analysis of all functions related to customer support and service management and control and analysis SHALL examine each customer support function and service management and control function allocated to personnel and determine what SM&C tasks are involved in the operation and maintenance of the system.			
[SOW-721]	For each task, the Contractor SHALL determine the properties and physical resources required to execute the task. For that purpose, each task SHALL be analysed to identify and capture: a. the support level to be assigned; b. location/ facility involved; c. personnel skills required; d. task duration and frequency, reusing Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) data available; e. manpower required.			
[SOW-722]	For each task, the Contractor SHALL perform a cost calculation based on the properties and physical resource requirements of each task.			
[SOW-723]	The Contractor's cost calculation SHALL provide an estimated annual cost for each task.			
[SOW-724]	The Contractor's data and results of the Task Analysis SHALL be used as input to the development of technical publication (all manuals at any level of maintenance) and the development of training material to the maximum extent possible			
[SOW-725]	All the technical Documentation SHALL be kept updated by the Contractor and under configuration control for the entire life cycle of the system.			
[SOW-726]	The above information contained in each technical documentation SHALL be coherent with the operational configuration (i.e. OBL) deployed.			
[SOW-727]	The Contractor's technical documentation SHALL be developed as follows: a. on line technical publication SHALL be accessible using the platform; b. off line technical publication SHALL be accessible without using the platform.			

[SOW-728]	Technical documentation SHALL consist (as a minimum) of:
	a. Technical Manuals:
	  i. training documentation (off line documentation);
	  ii. Operation and User Manuals (off line documentation);
	  iii. Maintenance Manual (including administration manuals) (off line documentation);
	  iv. OEM (for COTS product) (Off line documentation);
	  v. Quick user guide (on line documentation);
	  vi. Release Notes (On line documentation);
	  vii. Read me file (On line documentation);
	  viii. On line Help (On line documentation);
	  ix. Frequently Asked Question (FAQ; On line documentation);
	b. other project documentation as required in this SoW.			

[SOW-729]	All the activities, milestones and actors associated with the development of technical documentation SHALL be described in the Contractor's ILSP.			
[SOW-730]	All the off line technical documentation SHALL be provided by the Contractor in electronic form.			
[SOW-731]	The Platform developed by the Contractor SHALL make all relevant documentation accessible on line.			
[SOW-732]	The Contractor SHALL provide all the technical documentation in British English language.			
[SOW-733]	The Contractor SHALL maintain lowest level possible for Classification of the Technical documentation. The security classification of any on line Contractor's documentation SHALL not be higher than NATO UNCLASSIFIED.			
[SOW-734]	All Contractor's documents, however short, SHALL identify the complete name and version identifier of the software they refer to, originator, date of production, the type of document, and configuration management information of the document itself.			
[SOW-735]	All Contractor's documents SHALL contain a list of those CIs (title and version identifier) that the document or parts thereof refers to.			
[SOW-736]	The Contractor SHALL submit all final and accepted versions of documentation deliverables in Portable Document Format (PDF), with an Object Character Recognition (OCR) capability format or in Microsoft Office Professional (MsWord) compatible format.			
[SOW-737]	The Contractor SHALL submit documentation, intended for review by the Purchaser, with each modification identified through the change tracking feature or otherwise marked			
[SOW-738]	The Contractor's developed manuals SHALL supplement the off-the-shelf OEM documentation the Contactor SHALL provide with the SOA & IdM Platform system			
[SOW-739]	The Contractor SHALL capture and document lessons learned during the System development and the System Installation.			
[SOW-740]	The Contractor SHALL develop, provide and maintain the System Operation Manual (SOM)			
[SOW-741]	The Contractor's developed Operation Manual SHALL describe the complete system by the explanation of functional blocks and Configuration Items			
[SOW-742]	The Contractor's developed Operation Manual SHALL define the in-depth, step-by-step procedure how to operate the system and how to perform Level 1 maintenance tasks			
[SOW-743]	The Contractor's developed SOM SHALL include all the Standard Procedures in order to safely operate and use the platform.			
[SOW-744]	The operation described in the Contractor's developed Manual SHALL be an outcome of the Operation and maintenance Task Analysis as described in SECTION 14.5.2			

[SOW-745]	The Contractor SHALL include each and any procedure as a minimum the following information: a. location/ facility involved (if the operation is performed remotely, it has to be specified); b. personnel skills required; c. task duration and frequency, reusing MTBF and MTTR data available; d. manpower required; e. tools and special tools required (if any); f. the steps needed to perform the operation.			
[SOW-746]	The Contractor SHALL develop, provide and maintain the System Maintenance and Administration Manual.			
[SOW-747]	The Contractor's Maintenance Manual SHALL: a. contain all the possible Scheduled and Unscheduled Maintenance Procedure and all the possible Administration Procedures as requested in SECTION 14.5.2; the Contractor SHALL ensure that all Configuration Items and all items required for maintenance are included in this full product breakdown list; b. define the in-depth, step-by-step procedure how to perform the 1st, 2nd and 3rd level corrective and preventive maintenance tasks and SM&C tasks; c. contain a full product breakdown list.			
[SOW-748]	The Contractor's manual SHALL include an annex with troubleshooting information. The troubleshooting annex SHALL provide a break-down on actions to solve a full range of (potential) problems or provide workarounds (Problem Management).			
[SOW-749]	The Contractor's manual SHALL contain all the possible configuration information and settings.			
[SOW-750]	The Contractor's Maintenance Manual SHALL also include all information, illustrations, and procedures required for the installation, configuration, provisioning, testing, repairing, replacing and troubleshooting of an item CI.			
[SOW-751]	The Contractor's manual SHALL contain all the possible information on the use and the locations of the log files			
[SOW-752]	Each and any procedure in the Contractor's manual SHALL include as a minimum the following information: a. the support level to be assigned; b. location/ facility involved (if the operation is performed remotely, it has to be specified); c. personnel skills required; d. task duration and frequency (if applicable), reusing MTBF and MTTR data available; e. manpower required; f. tools and special tools required (if any); g. the steps needed to perform the procedure.			
[SOW-753]	The Contractor's Maintenance and Administration Manual SHALL include an annex with database management information.			

[SOW-754]	The Contractor's database management annex SHALL describe as minimum:
	a. a break-down from the user interface (fields and actions) down to the effected database tables, triggers and stored procedures;
	b. the Platform Logical Data Model in full detail;
	c. the Platform Physical Data Model, where the following items SHALL be described:
	  i. triggers;
	  ii. foreign keys;
	  iii. tables and columns;
	  iv. stored procedures and parameters.			

[SOW-755]	The Contractor SHALL be responsible to keep the OEM COTS manual under configuration control and to assure that all the O&M COTS Manuals will be always coherent with the Operation configuration (i.e. OBL) deployed.			
[SOW-756]	The Contractor SHALL assure that all the possible information needed to configure, operate, manage and maintain the COTS product will be in the User Manual and in the Maintenance Manual if they are no in the COTS O&M manuals.			
[SOW-757]	The Contractor's Platform SHALL be equipped with a Quick User Guide.			
[SOW-758]	The Contractor's Quick User guide SHALL describe the frequently used user functions in a short format.			

[SOW-759]	The Contractor's Quick User guide SHALL be integrated in the "help on line" publication.			
[SOW-760]	Each Contractor's Platform release SHALL be equipped with a Release Notes file which SHALL include: a. the change log describing the difference in functionality with the previous release; b. known issues of the current release.			
[SOW-761]	The Contractor's Platform SHALL be equipped with 'Read Me' files for specific components.			
[SOW-762]	The Contractor's Platform Read Me files SHALL at minimum contain: a. minimal system requirements necessary to run the specific Platform part; b. the functional changes since the latest release; c. the solved errors; d. known errors; e. contact information for problem reporting.			
[SOW-763]	All the Other Project Documentation required SHALL respect the general requirement about publication in this SoW, and therefore SECTION 14.6.1, 14.6.12, and 14.6.13 as a minimum.			
[SOW-764]	The Contractor SHALL prepare and submit for approval a set of business rules which explain the harmonisation criteria of all the technical documentation in terms of fonts, numbering, bullet points and all the publication rules to be used for the complete set of documentation. The business rules will be applicable for both Paper and electronic publication.			
[SOW-765]	The Contractor's Manuals SHALL be printable if required and therefore the page format SHALL be A4, printable in loose-leaf form, and possible to be presented bound in stiff backed covers with 4-ringed binders which permit the removal and insertion of individual pages and drawings.			
[SOW-766]	The Contractor SHALL ensure that each page contains the appropriate NATO classification of the manual at the top and bottom of each page and at the top and bottom of each drawing.			
[SOW-767]	The Contractor SHALL ensure that each drawing contains the security classification in the identification block of the drawing.			
[SOW-768]	The Contractor SHALL ensure that all drawings and schematic diagrams are of the same length (not width) as other pages of the manuals.			
[SOW-769]	The Contractor SHALL ensure that electronic copies of the documentation composed and compiled by the Contractor if not delivered via Project Portal SHALL be delivered in PDF compatible or Microsoft compatible format (doc, .docx, .xls, .xlsx, .ppt, .pptx, .mpp, or other Microsoft compatible) on Universal Serial Bus (USB) memory stick.			
[SOW-770]	The Contractor SHALL ensure that OEM Manuals SHALL be delivered in the format specified above, if available. If not available in this format, one of the other common use formats will be accepted. If the commercial documentation is not available on USB memory sick, another form of electronic media is acceptable with the prior authorisation of the Purchaser PM.			
[SOW-771]	The Contractor SHALL ensure that the physical support of the electronic, optical, soft or hard copies SHALL display the highest level of the classification of its contents.			
[SOW-772]	The Contractor SHALL ensure that the Header and/or Title of the directory structure of the documentation provided in soft or hard copies SHALL bear a reminder of the highest classification level of its contents at the top and the bottom of every document page.			
[SOW-773]	The Contractor SHALL ensure that unclassified documentation is separated from classified documentation and provided on separate media (e.g. USB memory stick, Compact Disc (CD)-Read-Only-Memory (ROM) or Digital Versatile Disc (DVD)-ROM.			
[SOW-774]	The Contractor SHALL be the responsible authority for the issue, control, and distribution of amendments to delivered documentation in the format provided for the associated equipment or system until expiration of the warranty period.			
[SOW-775]	The Contractor SHALL test and validate the procedures and resources described in the technical manuals.			
[SOW-776]	Not later than two (2) months prior to the delivery of the SOA & IdM Platform fit at the first location, the Contractor SHALL submit a copy of the draft to the Purchaser for review.			
[SOW-777]	Any resulting recommended changes, corrections and/or additions submitted by the Purchaser SHALL be incorporated by the Contractor in the final version.			

[SOW-778]	The Contractor SHALL provide the final versions of each Technical Publication, in the requisite number of copies within four (4) weeks of FSA.			
[SOW-779]	Until the expiration of the warranty, the Contractor SHALL remain responsible for any changes to the manuals required as a result of any omission or inaccuracy discovered in use or, whenever changes/modifications in equipment or spare parts are made under the Contractor's responsibility.			
[SOW-780]	The Contractor SHALL deliver two copies on CD-ROM of the SOA & IdM Platform Operations Manuals for each of the sites, plus two copies for the NCI Agency.			
[SOW-781]	In addition to the "Manual Issuing schedule", the Contractor SHALL update all Manuals as needed throughout this contract.			
[SOW-782]	The Contractor SHALL provide SOA & IdM Platform training, including both classroom and E-learning/ Computer Based Training (CBT), for the Purchaser and users designated by the Purchaser.			
[SOW-783]	The Contractor SHALL provide training for the SOA & IdM Platform support staff through development and implementation of a Training Process.			
[SOW-784]	All the activities, milestones and actors associated with the Training of the SOA & IdM platform SHALL be guided by the Contractor's Training Plan.			
[SOW-785]	The Contractor SHALL be able to design, develop, deliver and perform the following type of training: a. Classroom Training; b. On-site Training (with E-Learning/CBT Capabilities, when applicable); c. On the Job Training (including self-study training); d. Train-the-trainer training.			
[SOW-786]	As part of the system implementation the Contractor SHALL provide on-site training to all support staff designated by the Site POC and on all tasks required to operate and maintain and recover the SOA & IdM Platform system.			
[SOW-787]	As part of the training process the Contractor SHALL provide "Train the Trainer" courses for a minimum of 10 instructors designated by the Purchaser.			
[SOW-788]	The Contractor SHALL provide all other facilities, services and equipment (including servers and workstations for students and teachers, network equipment, all required SW, etc....) necessary to carry out the On-Site Training activities.			
[SOW-789]	The Contractor SHALL identify the prerequisite of the personnel for training participation as part of the training needs analysis.			
[SOW-790]	The Contractor's Reference and Testing Facility staff SHALL be trained to operate the Reference and Testing Facility, through attending a short, informal, on-site training course, prepared, organised and led by the Contractor.			
[SOW-791]	The Contractor's training SHALL be provided for both Waves of the project.			
[SOW-792]	The Contractor's Training Materials SHALL include training on the Transition from the Platform Wave 1 to the next Platform increment (Wave 2) (when it's realised) and how to install, configure and maintain the Modified or new Platform capability, including COTS components.			
[SOW-793]	The Training Process and Procedures SHALL be based on the results of the TNA to be performed by the Contractor.			
[SOW-794]	The Contractor SHALL conduct a TNA in accordance with the [BiSC D-075-007, 2015]. The TNA SHALL include: a. a Target Audience Analysis; b. a Performance Gap Analysis; c. a Difficulty, Importance and Frequency (DIF) Analysis; d. a Training Delivery Options Analysis.			
[SOW-795]	The Contractor's TNA SHALL be based on the tasks resulting from Task Analysis carried out as part of the LSA Process and on the possible gaps highlighted during the site surveys (so called Target Audience Analysis)			
[SOW-796]	The Contractor's Training Needs Analysis SHALL consider all assigned staff roles involved in SOA & IdM Platform operation, administration, maintenance and support at all levels			
[SOW-797]	The Contractor's TNA SHALL include the transition training requirement from the Wave 1 to Wave 2.			

[SOW-798]	The Contractor SHALL deliver a TNA Report that captures the results of the TNA. The TNA report SHALL include the following: a. a description of the TNA approach and activities; b. an account of the operation, support, corrective and preventive maintenance tasks considered in the TNA; c. the results of the Target Audience Analysis, the Performance Gap Analysis the DIF Analysis and the Training Options Analysis; d. the final list of Performance Objectives in the form of Table 2 of Annex H of BiSCD 75-7, 2015; e. the final list of Learning Objectives in accordance with Annex G of BiSCD 75-7, 2015; f. one or more Course Control Document II – Course Proposals in accordance with Annex L of [BiSCD 75-7, 2015] as summaries of the proposed E&IT solutions.			
[SOW-799]	The Contractor SHALL develop and provide SOA and IdM Platform Training Plan.			
[SOW-800]	The Contractor's Training Plan SHALL describe how it will meet the Training requirements found after the TNA for initial and follow-on training.			
[SOW-801]	The Contractor's training plan SHALL describe the quality management process for training.			
[SOW-802]	The Contractor's Training Plan SHALL address all stages of training development, delivery, and support covered under this Contract.			
[SOW-803]	The Contractor's Training Plan SHALL describe in a coherent way how training will be designed, developed, delivered, and maintained throughout the life of the SOA & IdM Platform.			
[SOW-804]	The Contractor's Training Plan SHALL include training design documentation using the Course Control Document III – Programme of Classes template provided in [BiSC D 75-7 2015] Annex R-4.			
[SOW-805]	The Contractor SHALL describe in this plan the approach to training, milestones, resource requirements, management structure, interrelationships and other tasks related for training development.			
[SOW-806]	The Contractor's Training Plan SHALL describe the training documentation for each course including but not limited to the syllabuses, schedules, course prerequisites (both for attendees and physical resources), evaluations and instructors.			
[SOW-807]	The Contractor SHALL recommend in this plan the mode(s) of training (e.g. formal classroom, individual computer-based, on-the-job, commercial or a combination) and the rationale for those recommendations for each type of training (User , Administrator, etc.).			
[SOW-808]	The Contractor's training plan SHALL describe the transition training process to manage the change of training from the transition of the platform from Wave 1 to Wave 2.			
[SOW-809]	The Training Plan SHALL describe the support to be provided (manpower, services and material).			
[SOW-810]	The Contractor SHALL provide all the appropriate training documentation to support the Purchaser Personnel to test, operate and maintain the SOA & IdM Platform System and its support equipment.			
[SOW-811]	The following Platform Training Material SHALL be generated by the Contractor: a. Training Syllabus; b. Student Manual; c. Instructor Guide and Material; d. Learning Guide; e. Quick Reference card; f. upon completion - a Training Certificate; g. course evaluation feedback form.			
[SOW-812]	The Contractor's Training documentation SHALL conform to the standards outlined in the training section of the SoW and SRS.			
[SOW-813]	The Contractor's training materials for the SOA & IdM Platform-specific courses SHALL provide all the information required to conduct the courses and maintain the training materials.			
[SOW-814]	The Contractor's materials SHALL follow an existing instructional methodology that links training objectives with course structure, instructional techniques, course content, and assessment tools			

[SOW-815]	For the development of training material, the Contractor SHALL reuse existing COTS documentation and manuals to the maximum extent possible.			
[SOW-816]	All course content SHALL be referenced by the Contractor to commercial or Contractor-developed documentation - preferably user or technical manuals - that describe the subject matter and that are available on-site to students after course completion.			
[SOW-817]	The hands-on exercises included in the Contractor's Training Process SHALL incorporate all SOA & IdM Platform implementation activities at a site.			
[SOW-818]	The Contractor SHALL ensure that the SOA & IdM Platform Training Materials are all provided in the UK English language. It can be assumed that all Purchasers personnel selected to attend the courses will meet the minimum Standardised Language Proficiency (SLP) of 3232 in English as specified in STANAG 6001.			
[SOW-819]	The Contractor's Training presentation materials SHALL include all slides or other information to be presented by the instructor during the course.			
[SOW-820]	The Contractor's Platform Training Course (i.e., NATO End Users, Administrators, Solution Architects and Developers)) SHALL include a Training Syllabus containing the following elements: a. course title; b. course description; c. learning objectives, as identified in the Training Needs Analysis and confirmed in the Training Plan; d. entry profile; e. concepts, Functions and Features presented in the course; f. instructional methodologies to be employed in the delivery of the course; g. in-class assignments or laboratories; h. evaluation tools; i. performance standards.			
[SOW-821]	The Contractor SHALL develop and provide a Student Handbook for each course, with necessary information on all lesson objectives and contents, guidance for all learning activities and cross-references to assist the students in achieving the course objectives.			
[SOW-822]	The Contractor's Student Manuals SHALL take into account results from the DIF analysis and SHALL enable students to perform their major tasks.			

[SOW-823]	The Contractor's System Administrator Training SHALL provide as a minimum the following training on the platform:
	a. how to install, configure and maintain the Platform capability, including COTS components;
	b. how to maintain the Platform and how to use the logging and performance counters provided by the Platform which, as minimum, SHALL include:
	v. all the configuration settings for the Platform modules, services and components;
	  i. how to configure the logging and uses of performance counters;
	  ii. where to find the log files;
	  iii. the different categories of logging;
	  iv. the different performance counter categories;
	c. how to trouble shooting the system, including actions to solve a full range of (potential) problems or provide workarounds;
	d. how to manage database information, including database tables, triggers and stored procedures;
	e. how perform back-up and restore procedures.			

[SOW-824]	The Contractor SHALL provide an Instructor's Guide for each training course.			
[SOW-825]	The Contractor's Instructor's Guide SHALL contain all necessary information to prepare and conduct lessons and to evaluate students, including exercises, quizzes, and examinations and their corresponding answer sheets and SHALL also provide notes to instructors to assist in conducting the lecture or exercise.			
[SOW-826]	Presentation materials SHALL be provided in Microsoft PowerPoint.			

[SOW-827]	The Contractor's Platform Instructor Guide SHALL detail the sequence of course instruction, providing references to the applicable training presentation materials, assignments and laboratories, evaluation tools and answer keys, Student Manual, and the Platform on-line help function. The Instructor Guide SHALL also include: a. materials for in-class assignments and laboratories; b. sample evaluation tools and answer keys; c. Training System installation and configuration procedures.			
[SOW-828]	The Contractor SHALL propose student's assessment and evaluation methodology to the Purchaser as part of the Training Plan.			
[SOW-829]	The Contractor's Training Assessment methodology SHALL be based on [BiSC D 75-7 2015] sections 7-6 and 7-7 for assessment approaches and instruments and include: a. examination methodologies and certification; b. minimum score to achieve for successfully passing the course; c. course(s) to be done to get the certification for each role; d. description of Role's certification process.			
[SOW-830]	The Contractor SHALL ensure that each student is instructed at the end of each course (or use of a CBT) to complete and return the course evaluation feedback form, provided as part of the training course or CBT/E-Learning product.			
[SOW-831]	The Contractor SHALL consolidate and forward student feedback to the Purchaser following each training course in the form of a Training Evaluation Report. The report SHALL also recommend changes and improvements to the training plan based on the consolidated student feedback. The report SHALL also address student attendance, problems encountered and actions taken to resolve the problems.			
[SOW-832]	The Contractor SHALL revise/ refine and reissue course material and CBT/E-Learning products to reflect the consolidated student feedback and proposed improvements in the training evaluation report.			
[SOW-833]	The Contractor SHALL produce Training Certificates for each training session and student.			
[SOW-834]	The certificates SHALL be delivered not later than two weeks following the completion of the training.			
[SOW-835]	The Contractor SHALL provide all the appropriate training documentation to support the Purchaser Personnel to perform the trainings using the NCIA Learning management system			
[SOW-836]	All Contractor's e-learning training material SHALL be prepared in compliance with the Sharable Content Object Reference Model (SCORM) edition 2004. Preferably any e-learning material should be deliverable on the NATO Advanced Distributed Learning (ADL) platform.			
[SOW-837]	The Contractor's CBT/E-Learning material SHALL complement the SOA & IdM Platform classroom training and online help capabilities by defining and explaining key concepts and terminology of the operational processes incorporated into SOA & IdM Platform features and functions.			
[SOW-838]	The Contractor's CBT/E-Learning Package SHALL allow modifications by the Purchaser to reflect changes in the training concept and/or content without any additional cost to NATO.			
[SOW-839]	The Contractor SHALL provide the Purchaser's ILS POC with a System Inventory in electronic Microsoft Excel format at least ten (10) working days before the first delivery of equipment.			
[SOW-840]	The Contractor's System Inventory is site-specific and SHALL include, in separate chapters, all items furnished under this Contract, as follows: a. all support equipment – i.e. all tools, test equipment, etc. (where applicable); b. all Purchaser Furnished Equipment (PFE); (where applicable); c. all documentation, such as manuals, handbooks and drawings; d. all training materials.			
[SOW-841]	The Contractor SHALL deliver a complete Material Datasheet (MDS) per Site. The MDS template will be available to the contractor upon request.			

[SOW-842]	All equipment delivered by the Contractor SHALL be labelled with the true manufacturer's name, part number and serial number to ensure proper and quick identification, as they are procured, stored, and issued. Nameplates in the English language with non-erasable letters/ numbers, giving the true manufacturer part number (including modification state), serial number (including revision level), NCI Agency contract number, date of manufacture, manufacturer's name and address and principal characteristics, where appropriate SHALL be provided by the Contractor.			
[SOW-843]	All equipment labels delivered by the Contractor SHALL contain a machine-readable code (e.g. barcode) compliant with [STANAG 4329] and [AAP-44(A)] and in accordance with the NATO coding schema, which will be provided by the Purchaser at the request of the Contractor.			
[SOW-844]	The Contractor's labels SHALL enable positive identification of assemblies and modules upon removal for maintenance purposes and to prevent loss of utilisation of items that have been separated from their original packages or containers.			
[SOW-845]	Whenever practicable, the Contractor label SHALL be located in such a manner as to allow it to be visible after installation.			
[SOW-846]	Marking SHALL be capable of withstanding the same environment tests required of the part and any other tests specified for the label itself.			
[SOW-847]	When possible, the Contractor SHALL ensure that letters, numerals, and other characters are of such a size as to be clearly legible.			
[SOW-848]	All the plates SHALL be properly attached by the Contractor in a prominent position on each major assembly to enable reading and control with easy access when installed.			
[SOW-849]	The Contractor SHALL provide a detailed Software Distribution List (SWDL), which SHALL detail comprehensively all CSCIs and associated software, firmware or feature/performance licenses provided under this Contract. The SWDL SHALL include, the following data elements: a. CSCI identification number; b. nomenclature; c. version number; d. license key (if applicable); e. license renewal date (if applicable); f. warranty expiration date; g. date of distribution; h. distribution location (geographically); i. distribution target (server).			
[SOW-850]	The Contractor SHALL make sure that all licenses are registered with the NCI Agency as end-user.			
[SOW-851]	The Contractor SHALL deliver a fully detailed and priced Recommended Tools and Test equipment List (RTTL), covering the "Standard" Tools and Test Equipment.			
[SOW-852]	The Contractor SHALL provide "Special to Type" tools and/or test equipment if required, in particular on the Reference System and/or on the Testbed.			
[SOW-853]	The Contractor SHALL, for the purpose of transportation, package, crate, or otherwise prepare items in accordance with the best commercial practices for the types of supplies involved, giving due consideration to shipping and other hazards associated with the transportation of consignments overseas.			

[SOW-854]	Packing lists SHALL accompany each shipment, which SHALL include the following:
	 a. the Purchaser's Contract Number;
	 b. the NATO project number;
	 c. names and addresses of the Contractor and the Purchaser;
	 d. names and addresses of the Carrier, Consignor and Consignee (if different from Contractor or Purchaser);
	 e. final destination address and POC;
	 f. method of spriorhipment;
	 g. for each item shipped:
	   i. CLIN number as per the SSS;
	   ii. nomenclature;
	   iii. part number;
	   iv. serial number;
	   v. quantity;
	 h. for each box, pallet and container:
	   i. box/pallet/container identification number;
	   ii. number of boxes/pallets/containers;
	   iii. weight;
	   iv. dimensions.			

[SOW-855]	The Contractor SHALL fasten two copies of the packing lists in a weather-proof, sealed envelope on the outside of each box, palette and/ or container, and additionally one packing list SHALL be put inside each container/box.			
[SOW-856]	The Contractor SHALL be responsible for all handling and storage of equipment, packages, boxes and containers during the project.			
[SOW-857]	The Contractor SHALL also be responsible for organising and operating any handling equipment and storage facilities required.			
[SOW-858]	Unless clearly specified otherwise, the Contractor SHALL be responsible for transportation of all equipment furnished under this Contract from its site in a NATO nation to its respective implementation destination.			
[SOW-859]	The Contractor SHALL be responsible for any insurance covering these shipments.			
[SOW-860]	The Contractor SHALL be responsible for customs clearance of all shipments into the destination countries. It is the Contractor's responsibility to take into account delays at customs. He SHALL therefore consider eventual delays and arrange for shipment in time. Under no circumstances can the Purchaser be held responsible for delays incurred, even when utilising Purchaser provided Customs Form 302			
[SOW-861]	Ten (10) working days before each shipment of supplies, the Contractor SHALL provide the Purchaser with a Notice of Shipment comprising the following details: a. Shipment Date; b. Purchaser Contract Number; c. CLIN; d. Consignor's and Consignee's name and address; e. Number of Packages/Containers; f. Gross weight; g. Final/Partial Shipment; h. Mode of Shipment (e.g. road…); i. Number of 302 Forms used.			
[SOW-862]	The Contractor SHALL ship all required software, documentation, and installation or testing tools to the locations designated by the Purchaser.			
[SOW-863]	The Contractor SHALL be responsible for resolving any loss incurred in shipping.			

[SOW-864]	The Contractor SHALL warrant that all equipment and software furnished under this Contract and all installation work performed under this Contract conform to the requirements and is free of any defect in material, code or workmanship for a period starting at date of each Wave PSA to date of PSA plus one (1) year.			
[SOW-865]	The Contractor SHALL fix/repair/replace all items received as per his internal procedures with the highest priority allocated.			
[SOW-866]	If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any supplies, the Contractor SHALL coordinate with the Purchaser and promptly correct the defect.			
[SOW-867]	Defective magnetic, solid state and electronic media storage devices (e.g. USB memory sticks, CD-ROMs, DVD-ROM's, solid state storage drives, hard drives) SHALL remain NATO property, at no additional cost, and not be returned to the Contractor when being replaced.			
[SOW-868]	Any such defective storage devices SHALL be replaced by the Contractor with new storage devices at no additional cost to the Purchaser.			
[SOW-869]	The Contractor SHALL be responsible for the provision of any alternative or superseding items, should the original part be no longer available, ensuring compliance with the original design provided by this Contract.			
[SOW-870]	During the warranty period, the Contractor SHALL be responsible for supplying all COTS hardware and software upgrades and updates.			
[SOW-871]	The availability of COTS hardware and software upgrades and updates SHALL be made known to the Purchaser and, if proposed for introduction by the Contractor for whatever reason, including any corrective action for an identified fault, SHALL always be subject to Purchaser approval.			
[SOW-872]	The Contractor SHALL not be responsible for the correction of defects in Purchaser furnished property, except for defects in installation, unless the Contractor performs, or is obligated to perform, any modifications or other work on such property. In the event described above, the Contractor SHALL be responsible for correction of defects that result from the modifications or other work.			
[SOW-873]	The Contractor SHALL provide CLS services in accordance with the requirements of this section for a period of five (5) years.			
[SOW-874]	The contractor SHALL integrate the Wave 2 CLS with Wave 1 CLS if the purchaser will activate Wave 2 CLS.			
[SOW-875]	The CLS services for 3rd and 4th Support and Maintenance levels SHALL be provided off-site from the Contractor's premises.			
[SOW-876]	The Contractor SHALL integrate Warranty with the CLS services.			
[SOW-877]	The contractor SHALL provide a CLS Plan as part of the ILSP, which explains in detail how the contractor fulfils all the CLS requirements in the contract and how the CLS services will be integrated with the Purchaser Operations.			
[SOW-878]	During the CLS period, the Contractor SHALL provide software and hardware support at all levels of support and at all levels of maintenance as described in ANNEX B.			
[SOW-879]	During the CLS period, as part of obsolescence management, the Contractor SHALL be responsible for the management, provision and implementation of any alternative or superseding hardware and software items should the original item be no longer available or no longer supported, ensuring compliance with the original design provided by this Contract.			
[SOW-880]	The availability of and need for superseding items SHALL be made known to the Purchaser and, if proposed for introduction by the Contractor for whatever reason, including any corrective action for an identified fault, shall always be subject to Purchaser approval.			
[SOW-881]	Defect magnetic and electronic media storage devices (i.e. CD-ROM's, DVD's, USB sticks, solid state drives, hard drives) SHALL remain NATO property and shall not be returned to the Contractor when being replaced under CLS arrangements			
[SOW-882]	The Contractor SHALL ensure that all software procured under the Contract have software licenses valid for the duration of the contracted CLS.			
[SOW-883]	The contractor SHALL renew Software licenses when required and for a duration sufficient to cover the contracted CLS period.			

[SOW-884]	The Contractor SHALL implement and document processes to record all events relating to the security of the SOA&IdM Capability, in a forn of audit logs.			
[SOW-885]	The Contractor SHALL implement and document an input for NCIRC in support on-line security monitoring and management of NATO's CIS infrastructure, off-line analysis of incidents, and incident handling. The SOA&IdM input for NCIRC SHALL include event logs related to the SOA internal operations as well as to the Identity and Access Management (IAM) processes where SOA&IdM platform capability is utilized.			
[SOW-886]	The Contractor SHALL provide a monthly CLS Performance Report during the contract CLS period which includes, as a minimum, the following: a. actual measurements of the performance and quality figures defined in the SRS; b. details of all failures and warranty cases that have occurred during the reporting period; c. applied changes to the product baseline; and d. expended resources.			
[SOW-887]	For the purpose of monitoring and reporting, the Contractor SHALL maintain a configuration management database (CMDB) and a known error database (KEDB) for the duration of the contracted CLS.			
[SOW-888]	If the actual achieved performance and quality figures of SOA & IdM Platform does not (or no longer) satisfy the Performance and Quality figures requirements in this Contract then the Contractor shall modify the design and implementation of the platform to fulfil the requirements in this Contract.			
[SOW-889]	The CMDB and KEDB SHALL be provided to the Purchaser at the end of the contracted CLS period in a non-proprietary, electronic format.			
[SOW-890]	The Contractor SHALL update and re-issue any documentation (including training material) delivered under this Contract each time a change is implemented resulting from the CLS arrangements and requirements in this Contract.			
[SOW-891]	During the CLS period, the Contractor SHALL provide an Annual Recurrent Training Programme, which consist of: a. one SOA&IdM training course for NCIA designated staff (Operators, Maintainers, train the trainers); b. an updated Computer-Based Training package, in accordance with the requirements of Section 14.7			
[SOW-892]	The Contractor's training courses SHALL accommodate a maximum number of five (5) students per course and take place at Purchaser specified NATO locations and at Purchaser specified dates.			
[SOW-893]	The Contractor SHALL provide dedicated Engineering and integration support to a purhcaser's selected projects to enable migration of the functional service to SOA and IdM platform delivered under this Contract.			
[SOW-894]	The contractor SHALL integrate the Engineering and Integration activities in the CLS 3rd level of support activities, if it is activated by the Purchaser.			
[SOW-895]	The Contractor SHALL be responsible for the removal of the items from the installation facilities as required, and SHALL work with local site personnel to ensure the controlled removal and disposal.			

Reference Document	Reference ID *(BI, SOW requirement, SRS requirement)*	Desription	Bid Reference	Remarks	Compliance statement
SOW Annex-A SRS	SRS-1960	The Platform SHALL be compliant with [NAC ADatP-34(G)-REV1, 2013] base standards and profiles for information exchange			
	SRS-1959	The Platform SHALL be compliant with [NAC ADatP-34(G)-REV1, 2013] base standards and profiles for XML implementation.			
	SRS-1962	The Platform SHALL comply with the standards referenced in section 2.1 "Technical Standards" in Annex F of the Statement of Work.			
	SRS-4231	Any variations from the Technical Standards SHALL be approved by the Purchaser.			
	SRS-2000	The Platform SHALL comply with the standards referenced in section 2.2 "Quality Standards" in Annex F of the Statement of Work.			
	SRS-4232	Any variations from the Quality Standards SHALL be approved by the Purchaser.			
	SRS-2002	The Platform SHALL comply with the standards referenced in section 2.3 "Programming Standards" in Annex F of the Statement of Work.			
	SRS-4233	Any variations from the Programming Standards SHALL be approved by the Purchaser.			
	SRS-280	The Platform SHALL support Multi-tenancy in terms of isolation of the software Components (services, applications) by providing Middleware services for each individual tenant (Users).			
	SRS-293	The Platform SHALL implement mechanisms that enable the provision of new services from existing services by: composing them providing proxies by using data and protocol transformations.			
	SRS-3180	The Platform SHALL enable the processing of messages, including data extraction from the messages.			
	SRS-4234	The Platform SHALL enable data aggregation from different services and service providers.			
	SRS-295	The Platform SHALL provide a library of built-in Mediation patterns to be used for the provision of new services including, at least, the patterns officially known as "Enterprise Integration Patterns" [Hohpe and Woolf, 2012]: Integration Styles Messaging Systems Messaging Channels Message Construction Simple Messaging Message Routing Message Transformation Composed Messaging Messaging Endpoints System Management patterns			
	SRS-454	The Platform SHALL support multiple Web Service communication protocols to include REST and SOAP.			
	SRS-3655	The Platform SHALL support data exchange via XML and JSON.			
	SRS-2161	The Platform SHALL support a variety of messaging styles (also known as MEP) at a minimum: Request-Response (further specified in section 3.1.1.1) Publish-Subscribe, (further specified in section 3.1.1.2) Solicit Response (reverse of Request-Response) Fire and Forget (one-way messages) Store and Forward Broadcast Streaming			
	SRS-2187	The Platform SHALL support the following delivery modes: Synchronous messaging Asynchronous messaging Long running messaging.			

	SRS-4220	The Platform SHALL be able to prioritise messages in order to ensure that high priority requests take precedence over lower-priority ones.			
	SRS-2162	The Platform SHALL be able to add messages and retrieve messages from a Message Queue through a standard interface.			
	SRS-2160	The Platform SHALL support communication through a variety of transport standards, formats and protocols and their secure versions, at a minimum: TCP/IP UDP/IP HTTP SMTP FTP SOAP			
	SRS-400	The Platform SHALL enable management of its endpoints, executable both by the operator via GUI or via service definition file processing, allowing for the following operations: Associate an information source with an endpoint Associate an information sink with an endpoint Support the dynamic creation of endpoints Support the dynamic modification of endpoints Support the dynamic removal of endpoints			
	SRS-4245	The platform SHALL be able to support a variety of service definition standards, at a minimum: WSDL 1.1 WSDL 2.0 WADL			
	SRS-406	The Platform SHALL provide the means to logically connect two endpoints for the purpose of establishing information flow from the producer to the consumer.			
	SRS-4246	The Platform SHALL provide tools to define, manage (i.e., start, stop, suspend, resume), optimize and debug services and information flows between information providers and consumers, and intermediate operations.			
	SRS-3978	The Platform SHALL be able to perform the following operations on information as it flows between the consumer and producer: Augmentation Filtering Modification Combination Deletion			
	SRS-4247	The Platform SHALL be able to execute background, periodic or user requested tasks for: data ingestion data notifications/generation data processing			
	SRS-2174	The Platform Services SHALL use the Hypertext Transfer Protocol (HTTP; see [IETF RFC 2616, 1999]) as a transport mechanism to exchange messages.			
	SRS-2175	The Platform Services SHALL employ the Uniform Resource Identifiers (URI; see Ref. [IETF RFC 3986, 2005]) to identify resources.			
	SRS-2177	The Platform Web Services using the REST Style when invoking other Web Services SHALL comply with the technical specifications as defined in the SIP for REST Messaging (see [NCIA AI 06.02.07, 2015]).			
	SRS-2178	The Platform Web Services using the SOAP Style when invoking other Web Services SHALL comply with the technical specifications as defined in the SIP for SOAP Messaging (see [NCIA AI 06.02.06, 2015]).			
	SRS-2182	The Publish-Subscribe interfaces SHALL comply with the technical specifications as defined in the SIP for Publish-Subscribe Services (see [NCIA AI 06.02.08, 2015], [NCIA AI 06.02.09, 2015], and [NCIA AI 06.02.10, 2015]).			
	SRS-2226	The Platform SHALL be able to act as a Message Broker propagating Notifications from Publishers to Consumers.			
	SRS-428	The Platform SHALL provide the means to disseminate information to multiple Consumers.			
	SRS-2202	The Platform SHALL expose a Consumer interface to receive Notifications from Publishers.			

	SRS-2203	The Platform SHALL publish Notifications to the interface exposed by subscribed Consumers.			
	SRS-426	The Platform SHALL allow producers to publish messages.			
	SRS-430	The Platform SHALL allow Consumers to modify and cancel existing Subscriptions.			
	SRS-2207	The Platform SHALL allow Subscribers to subscribe to a subset of information products matching a specific filter (e.g. Topic).			
	SRS-2205	The Platform SHALL expose the Subscription Manager interface to which a Consumer can be subscribed.			
	SRS-397	The Platform SHALL provide the means for Consumers to receive information according to operationally defined Topics.			
	SRS-395	The Platform SHALL provide the means to manage the Topics supported, including: Organise a Topic hierarchy Create a Topic Move a Topic within the hierarchy Remove a Topic Manage Topic Filters			
	SRS-2184	The Platform SHALL provide a Notification Cache which complies with the technical specifications as defined in [NCIA AI 06.02.11, 2015].			
	SRS-2126	The Platform SHALL provide the means for a producer to submit messages to the message queues.			
	SRS-441	The Platform SHALL provide the means for a consumer to retrieve (and remove) messages from the message queue(s).			
	SRS-440	The Platform SHALL provide the means to create, modify and delete message queues.			
	SRS-2165	The Platform SHALL be able to route messages to the intended service provider.			
	SRS-432	The Platform SHALL be able to route messages correctly based on the address.			
	SRS-433	The Platform SHALL be able route messages based on message Metadata (e.g., addressee) or message content.			
	SRS-434	The Platform SHALL support message delivery to a single consumer.			
	SRS-435	The Platform SHALL support message delivery to multiple consumers.			
	SRS-3188	The Platform SHALL support guaranteed delivery of messages.			
	SRS-284	The Platform SHALL be able to provide a single point of access to services.			
	SRS-437	The Platform SHALL provide the means to proxy request messages from a consumer to an Information Provider.			
	SRS-438	The Platform SHALL provide the means to proxy response messages from an Information Provider to a consumer.			
	SRS-3187	The Platform Message Cache SHALL store frequently called data and make it available for reuse, based on configurable parameters.			
	SRS-4229	The Platform Message Cache SHALL be configurable to include as a minimum the replacement method, cache heap space, number of entries, and size of object.			
	SRS-447	The Platform Message Cache SHALL provide the means for a requester to receive responses stored by the Message Cache.			
	SRS-444	The Platform SHALL provide the means for an authorised requester to clear a Message Cache.			
	SRS-445	The Platform SHALL allow for automatic clearing of the Message Cache based on the size, number and expiry time of messages.			
	SRS-178	The Platform SHALL be able to take data in the format or protocol used by an information producer and transform the data into another format or protocol, according to a predefined set of extensible rules, that can be understood by the intended Information Consumer.			
	SRS-175	The Platform SHALL provide the means to expose a transformation as a service.			
	SRS-176	The Platform SHALL provide the means to make use of a transformation service.			
	SRS-177	The Platform SHALL provide the means to activate and deactivate a transformation service.			
	SRS-2128	The Platform SHALL provide the means to convert data from one value into another, compatible value.			
	SRS-3189	The Platform SHALL be able to transform data formats independently from their representation; at a minimum, supported representations include binary, MTF, XML, JSON, and plain (unformatted) text.			
	SRS-2218	The Platform SHALL allow for Extensible Stylesheet Language Transformations (XSLT), when mediating between different XML data formats.			
	SRS-4236	The Platform SHALL retrieve all stylesheet based transformations from the Metadata Registry and Repository.			
	SRS-2219	Each XSLT Stylesheet SHALL be created as a separate Artefact, and not embedded in the implementation of the service.			
	SRS-2221	The Platform services using XSLT Stylesheets for Mediation SHALL comply with the XSLT-Based Mediation SIP Proposal (see [NCIA TR/2012/SPW008423/23, 2012]).			

	SRS-3192	The Platform services SHALL be able to run data transformations using externally provided: XSLT Executables Transformation Services.			
	SRS-2164	The Platform will be able to transform between transport protocol formats and format versions according to predefined rules.			
	SRS-3197	The Platform SHALL be able to adapt between different Message Exchange Patterns.			
	SRS-511	The Platform SHALL provide functionality to compose existing services.			
	SRS-512	The Platform SHALL provide functionality to propagate and coordinate interactions between services being composed.			
	SRS-513	The Platform SHALL provide functionality to correlate messages that are exchanged between composed services.			
	SRS-514	The Platform SHALL provide functionality to monitor the state of the active Compositions.			
	SRS-3198	The Platform SHALL be able to support Choreography modelling.			
	SRS-2223	The Platform SHALL be able to compose services following the Business Process Execution Language (BPEL, [OASIS WS-BPEL V2.0, 2007]) specification.			
	SRS-4250	The Platform SHALL be able validate a BPEL file, and all supporting needed schemas and descriptors.			
	SRS-2224	The Platform SHALL be able to compose services BPEL Composition SIP Proposal (see [NCIA TR/2012/SPW008423/20, 2012]).			
	SRS-516	The Platform SHALL be able to compose multiple individual services into a single business-process represented by an Orchestration.			
	SRS-517	The Platform SHALL be able to expose an Orchestration (i.e. composed process) as a service with an exposed interface.			
	SRS-519	The Platform SHALL be able to support as a minimum the following process control flow constructs: Sequence Parallel execution Process joins Loops Conditional execution Action synchronisation Asynchronous eventing			
	SRS-521	The Platform SHALL provide functionality to execute multiple Orchestration instances.			
	SRS-524	The Platform SHALL be able to create Orchestration instances and manage their execution, including start/stop/suspend/resume.			
	SRS-525	The Platform Orchestration SHALL coordinate Sub-services calls and process data produced by Sub-services.			
	SRS-527	The Platform Orchestration SHALL support multiple versions of the same process definition running in parallel.			
	SRS-528	The Platform SHALL provide mechanism to handle Orchestration execution Faults.			
	SRS-529	The Platform SHALL maintain state of Orchestrations being executed.			
	SRS-3858	The Platform Orchestration Services SHALL support long running processes.			
	SRS-530	The Platform Orchestration Services SHALL support temporal suspension of long running processes to secondary memory (aka dehydration).			
	SRS-3678	The Platform SHALL allow a Service Provider to register a web service at both runtime and design time, with at least the following Metadata (e.g., description, keywords) information: service end-point URL service name service description service contract keywords point of contact details			
	SRS-3677	The Platform SHALL allow a Consumer to discover published services using the service metadata as filters via a programmatic service interface and via user accessible GUI.			
	SRS-373	The Platform SHALL return sufficient information to the requesting service to bind with it at run-time.			
	SRS-2113	The Platform SHALL provide functionality to identify and register separate service instances that can provide identical results.			

	SRS-285	The Platform SHALL maintain a managed list of internal and external services as a Service Catalogue, accessible by Service Consumers.			
	SRS-3680	The Service Catalogue SHOULD be complemented with information from the Platform SMC services (see Section 3.3) on the status, Availability, usage and other operational information of registered web services.			
	SRS-3681	The Platform SHALL provide a web-based GUI for the Users to visualise, manage and search for services and their corresponding information.			
	SRS-3682	The Platform SHALL provide a UDDI v.3 compliant Interface for the GUI and the web services interaction with the Service Registry Component.			
	SRS-3770	The Platform SHALL comply with the Service Discovery SIP Proposal (see Ref. [NC3A RD-3185, 2011]).			
	SRS-4118	The Platform SHALL implement an API Management Capability to enable lifecycle management (including versioning) of APIs, adequate documentation of interfaces, and implementation of the Identity and Security Services to protect access to the API.			
	SRS-4033	For each API Component the Platform SHALL fully document the interface, including: Mechanisms for securely invoking the API Available methods and functionality Available information elements, including Attributes and enumeration values Error handling			
	SRS-2533	The Platform SHALL allow authorised Components and systems to access the API supporting the Platform Capability.			
	SRS-4063	The Platform SHALL expose an API using open standards or widely accepted industry standards.			
	SRS-3202	The Platform SHALL expose a service API to be used as interface by other services and Users (through a GUI) interface to provide access to the Metadata Registry and Repository functionality.			
	SRS-3200	The Platform SHALL provide the ability to register, make available, update, and delete Artefacts, Artefact Collections, and associated Metadata.			
	SRS-4095	The Platform SHALL provide the ability to update Metadata of multiple Artefacts simultaneously (i.e. bulk operation).			
	SRS-4070	The Platform SHALL support registration, search, update, and deletion of Artefacts, including: XML schema WSDL supporting documentation (like PDF) with design or usage information.			
	SRS-488	The Platform SHALL provide the ability to control at a User level, read, write, edit and delete access to Artefacts, Artefact Collections, and Metadata.			
	SRS-4084	The Platform SHALL be able to extract Artefact Metadata from: the Artefact itself a separate metadata-document (XML Artefact).			
	SRS-3309	On registration of an Artefact the Platform SHALL provide the ability to also register referenced Artefacts, including XML schema and WSDL.			
	SRS-492	The Platform SHALL be able to differentiate between different object types based on Artefact content (e.g. WSDL, OWL, RDF, XML schema)			
	SRS-4237	The Platform SHALL be able to to manage XSLTs.			
	SRS-4248	The Platform SHALL be able to validate uploaded XSLT against XML schemas.			
	SRS-3310	The Platform SHALL be able to validate an Artefact, based on syntax and availability of referenced Artefacts, and depending on: the Artefact type the operation an Artefact is involved in.			
	SRS-493	The Platform SHALL provide the ability to search, list and retrieve Artefacts, including different versions, using a filter on the Artefact content and/or on the Artefact Metadata.			
	SRS-3311	The Platform SHALL provide filtered search on contents of XML Artefacts using XPath and/or XQuery.			
	SRS-4071	The Platform SHALL be able to store and manage different versions of an Artefact, Artefact Collection and associated Metadata.			
	SRS-489	The Platform SHALL provide the ability to create and manage workflows with customisable life-cycle statuses for Artefacts and Artefact Collections.			
	SRS-3305	The Platform SHALL provide functionalities to assign a workflow to Artefacts and to Artefact Collections.			

	SRS-3306	The Platform SHALL assign a default workflow to Artefacts and Artefact Collections based on the Artefact type or the Artefact Collection(s) to which it belongs, if no specific workflow is provided.			
	SRS-4085	The Platform SHALL be able to inform Users and services about changes to an Artefact or Artefact Collection.			
	SRS-4086	The Platform SHALL be able to inform subscribed Users about Artefact or Artefact Collection changes via: e-mail GUI.			
	SRS-3308	In order to be notified about Artefact and/or Artefact Collection changes, the Platform SHALL provide the ability to: subscribe and unsubscribe view and manage Subscriptions select Notification delivery preferences			
	SRS-3314	The Platform SHALL provide the ability to reference and retrieve specific versions of an Artefact via an accessible unique and non-editable URL.			
	SRS-4096	The Platform SHALL provide the ability to search and list Artefacts together with the Artefact Metadata, and export the result as a structured document (for example as XML document).			
	SRS-485	The Platform SHOULD support federated searches using open standards for federated or aggregated search, in order to allow searching of other Metadata Registry and Repositories.			
	SRS-3315	The Platform SHALL provide functionality to reference to Artefacts from other Metadata Registry and Repositories.			
	SRS-3312	In case of an XML Artefact the Platform SHALL provide functionality to retrieve and export: XML Artefacts together with referenced XML Artefacts called out by import or include statements specific Artefact fragments (XML fragments) using XPath end XQuery.			
	SRS-4094	The Platform SHALL be able to create, view, search and manage associations between Artefacts, which can be both dependent or independent of the Artefact version. Examples of an associations between Artefacts are "is superseded by", "refers to", "is derived from".			
	SRS-3981	The Platform SHALL deliver the necessary interfaces to exchange information in both directions with the Enterprise SMC Capability, with the necessary flexibility to present the data in accordance with evolving enterprise level data structures and vocabularies.			
	SRS-238	The Platform SHALL provide Capabilities to define, deploy, manage and enforce quality of service and Service Level Agreements (SLAs) for individual services and service groups.			
	SRS-239	The Platform SHALL be able to define, deploy and manage SLA parameters for whole end-to-end processes.			
	SRS-274	The Platform SHALL provide the Capability to manage the full life-cycle of services, from provisioning to controlling to decommissioning, including versioning.			
	SRS-2417	The Platform SHALL support remote deplyment of all the Platform Components and updates using Microsoft System Center Configuration Manager.			
	SRS-4252	The Platform SHALL support configuration reporting of Platform Components using Microsoft System Center Configuration Manager.			
	SRS-2419	The Platform SHALL support collection and reporting of asset inventory metrics for all the Platform Components using Microsoft System Center Configuration Manager, including: Memory Operating System Peripherals Services Login tracking Software existence and usage Licensing			
	SRS-3571	The Platform SHALL re-use the Enterprise SMC Configuration Management Component (BMC IT Service Management Atrium (ITSM) CMDB) to track Platform assets and their configuration information when possible, and be compatible with it when re-use is not possible.			
	SRS-244	The Platform SHALL provide the capability to search for Platform assets based on available Metadata information.			
	SRS-3546	The Platform SHALL provide a dashboard with an overall view of the Platform inventory items.			
	SRS-3588	The Platform SHALL integrate with the Event Management system that will be provided by the Enterprise SMC Capability.			

	SRS-3556	The Platform SHALL collect Events generated from all Platform Components and forward them to the Enterprise Event Management System.			
	SRS-3555	The Platform SHALL provide a toolset which allows Authorised Users to define, filter, correlate and group Events according to their context, criticality, source and impacts.			
	SRS-3557	The Platform SHALL provide a toolset to configure policy and rule based Event filtering, and to automate Alert triggering capabilities.			
	SRS-291	The Platform SHALL provide functionality to generate Alerts associated with SOA services to include: breach of Performance or Capacity thresholds stalled processes unauthorised access to services SLA parameters can't be met specific mechanisms to enforce SLAs were activated (e.g., throttling)			
	SRS-251	The Platform SHALL be able to generate SLA compliance reports Error/exception reports operational and historical reports on Events overall Performance trends service usage reports other customizable reports based on captured metrics which can be filtered and sorted based on various criteria			
	SRS-2118	The Platform SHALL monitor the status and quality of service, (including Availability, Performance, and utilisation) of the Platform infrastructure, the underlying Web Hosting Services and the services hosted on the Platform.			
	SRS-381	The Platform SHALL provide functionality for real time monitoring of services against expected KPI, SLA, or other configurable metric thresholds.			
	SRS-3563	The Platform SHALL report on usage patterns over daily, monthly and variable periods.			
	SRS-2896	The Platform SHALL automatically detect degraded Performance.			
	SRS-3562	The Platform SHALL provide customizable dashboards for monitoring selected statistics and metrics for Platform, Web Hosting, and hosted services.			
	SRS-288	The Platform SHALL provide the Capability to monitor access attempts to Platform services.			
	SRS-382	The Platform SHALL provide functionality to monitor composed and/or orchestrated services, as well as to drill down to monitor individual services of a Composition and/or Orchestration.			
	SRS-383	The Platform SHALL provide functionality to monitor service Faults and exceptions.			
	SRS-252	The Platform SHALL be able to collect and present the statistics on service utilisation broken down by User/tenant.			
	SRS-390	The Platform SHALL aggregate collected statistics for a given User/tenant or group of Users/tenants over specified periods of time.			
	SRS-4249	The Platform SHALL be able to use statistics on service utilisation for Metering, billing and other purposes.			
	SRS-392	The Platform SHALL make collected and aggregated statistics available for retrieval.			
	SRS-2197	The Platform SHALL track and monitor the message routing for service invocation and responses.			
	SRS-241	The Platform SHALL provide the functionality to diagnose faulty message flows and identify improvements to prevent disruption of transactions.			
	SRS-3578	The Platform SHALL be able to automatically manage services by defining, configuring and triggering automated actions when certain Alerts (triggers) are received.			
	SRS-3565	The Platform SHALL accept triggers from Alerting, Monitoring, and Message Tracking Services.			
	SRS-367	The Platform SHALL be able to automatically execute as a minimum the following actions: service call prioritisation selective routing based on configurable criteria service throttling			
	SRS-449	The Platform SHALL provide the functionality to provision, manage and decommission hosted services.			
	SRS-3701	The Platform SHALL provide a Web Interface for Users for automated provision of Platform services, including of pre-configured templates.			
	SRS-3702	The Platform SHALL allow for development of an approval workflow to support the provisioning of the Platform services.			

	SRS-3607	The Platform SHALL provide an operational environment which supports Scalability of deployed software (Services), featuring as a minimum load balancing and failover.			
	SRS-3602	The Platform SHALL provide the following environments as pre-configured templates for various development environments, specifically: LAMP to include Ruby, PHP and Python frameworks with Apache HTTP Service .NET Framework applications on IIS SharePoint 2013/2016 Java Application Framework on Apache Tomcat The exact configuration of the templates will be finalised during the design review phase.			
	SRS-3603	Development Platform environments SHALL be able to make use of Platform provided services via their service interfaces, independent of their run-time environment.			
	SRS-3614	The Platform SHALL allow an Authorised User to configure basic features of the hosted environments, to include as a minimum CPU, RAM and Storage parameters.			
	SRS-3385	The Platform SHALL make the semantics and structure of information products available using the Web Ontology Language (OWL).			
	SRS-3386	The Platform SHALL support the retrieval and manipulation of Resource Description Framework (RDF) data based on SPARQL Protocol and RDF Query Language (SPARQL) interface recommendations.			
	SRS-3387	The Platform will be compatible with Information Discovery Services SIP Proposal (see Ref. [NC3A RD-3297, 2011]).			
	SRS-267	The Platform SHALL implement mechanisms to expose data from data sources and data stores as web services.			
	SRS-465	The Platform SHALL provide functionality for mapping or identifying synonymous information products (i.e.information products in different Information Catalogues providing the same information content). It will leave the information products intact and creates only the linkages between products.			
	SRS-3407	The Platform SHALL be able to validate and enforce data quality rules			
	SRS-480	The Platform SHALL provide the means to define an aggregation of two or more data sources			
	SRS-479	The Platform SHALL provide the means to expose the integrated information as a new information source.			
	SRS-3511	The Platform SHALL manage the data hierarchies, groupings, relationships such as parent-child relationships, and relationships between data.			
	SRS-3413	The Platform SHALL provide the ability to query and search for information products.			
	SRS-464	The Platform SHALL provide functionality for a search across multiple information sources.			
	SRS-327	The Platform SHALL provide the mechanisms to collect, filter, prioritise and order the search results coming from the different search sources into a single result set.			
	SRS-461	The Platform SHALL provide functionality to group information products based on their content.			
	SRS-458	The Platform SHALL provide the means to create and maintain Information Catalogues.			
	SRS-459	The Platform SHALL provide the means to uniquely identify information products associated with a catalogue.			
	SRS-460	The Platform SHALL provide the means to specify the Metadata associated with an information product.			
	SRS-462	The Platform SHALL provide the means to search Information Catalogues for a specific information product.			
	SRS-463	The Platform SHALL provide details to the Consumer on how to obtain discovered information products, which can also encompass a referral to the full information product could be available through another service (i.e. via or service endpoint reference).			
	SRS-322	The Platform SHALL allow to enrich and annotate information.			
	SRS-504	The Platform SHALL provide functionality to create, update, delete and store annotations associated with existing information objects			
	SRS-505	The Platform SHALL maintain Metadata on the annotations, including but not limited to: who created it when was it created what is the history of the annotation			
	SRS-506	The Platform SHALL provide functionality to retrieve annotations for individual information objects.			
	SRS-507	The Platform SHALL provide functionality to retrieve annotations based on User defined search criteria.			
	SRS-3623	The Platform SHALL provide an authoring environment and User interface that allows for the management of Business Rules.			
	SRS-510	The Platform SHALL provide the Capability to create, modify, store, delete, version and retrieve Business Rules.			
	SRS-3627	The Platform SHALL support the archiving of rules that are no longer used in production.			

	SRS-509	The Platform SHALL provide the Capability to evaluate and validate Business Rules against expected behaviour and results.			
	SRS-3853	The Platform SHALL provide the Capability to monitor and record Business Rules execution.			
	SRS-3630	The Platform SHALL enable Business Rule designers to test/execute rules and rulesets, and allow for running simulations using pre-loaded data.			
	SRS-3631	The Platform SHALL notify Business Rule designers when conflicting Business Rules are written.			
	SRS-3636	The Platform SHALL support intelligent code completion to assist in Business Rule authoring.			
	SRS-3637	The Platform SHALL support contextual display (e.g., colour) of Business Rules to assist in human interpretation of the Business Rules.			
	SRS-3638	The Platform SHALL enable rules to be developed using commercial Office tools (e.g., Microsoft Excel, Word).			
	SRS-3646	The Platform SHALL provide a runtime environment (Business Rules Engine) that allows applications to invoke Business Rules.			
	SRS-3647	The Platform SHALL accept Business Rules in natural language.			
	SRS-3648	The Platform SHALL accept Business Rules in rule tables.			
	SRS-3666	The Platform SHALL allow Business Rules to be time bound such that new rules can be authored and put into production and not take effect until a specific date and time.			
	SRS-3649	The Platform SHALL allow Business Rules to be time bound such that existing rules can be deprecated at a specific date and time.			
	SRS-3650	The Platform SHALL support full forward and backward chaining.			
	SRS-3652	The Platform SHALL enable Business Rules to be maintained separately from application code.			
	SRS-3657	The Platform Business Rules Engine SHALL support batch processing of data.			
	SRS-3658	The Platform Business Rules Engine SHALL support online transaction processing of data.			
	SRS-3854	The Platform SHALL enable to export Business Rules as [OASIS WS-BPEL V2.0, 2007] and/or [OMG BPMN V2.0.2, 2013] for processes and workflow rules.			
	SRS-3711	The Platform SHALL provide a framework for IAM Capability at the NATO Enterprise level, consisting of coherent solutions and processes, fully integrated with existing Capabilities such as NEDS.			
	SRS-3715	The Platform SHALL leverage NEDS mechanisms for affiliation, data processing, and data exchange with the NATO Physical and Logical Access Control system(s).			
	SRS-3340	The Platform SHALL comply with the technical specifications as defined in the SIP for Security Services (see Ref. [NCIA AI 06.02.01, 2015]).			
	SRS-3343	The Platform SHALL comply with the technical specifications as defined in the SIP for REST Security Services (see Ref. [NCIA AI 06.02.02, 2015]).			
	SRS-3341	The Platform SHALL comply with the technical specifications as defined in the SIP for Security Token Services (see Ref. [NCIA AI 06.02.03, 2015])			
	SRS-3342	The Platform SHALL comply with the technical specifications as defined in the SIP for Policy Enforcement Point (see Ref. [NCIA AI 06.02.04, 2015]), and the technical specifications as defined in the SIP for REST Security Services (see Ref. [NCIA AI 06.02.02, 2015]).			
	SRS-3348	The Platform SHALL comply with the technical specifications as defined in the SIP for Enterprise Directory Services (see Ref. [NCIA AI 06.02.05, 2015]).			
	SRS-608	The Platform SHALL monitor and manage the lifecycle of Enterprise Identity for the NATO Enterprise.			
	SRS-2977	The Platform SHALL allow Authorised Users (i.e. the Platform Administrator) to manage (create, update, delete) the Platform User Accounts, Credentials (e.g., password), details, and manage general access Privileges of individual User Accounts.			
	SRS-584	The Platform SHALL allow for the definition and maintenance of the lifecycle state Attribute for Enterprise Identities (e.g., unknown, established, active, suspended, archived).			
	SRS-601	The Platform SHALL allow the definition, enforcement and compliancy verification of policies for creation and maintenance of Identity Attributes.			

	SRS-3722	The Platform SHALL use NEDS as the broker of identity data from Authoritative Data Source for different types of entities as follows: people organisational Entities facilities Roles groups devices software policy			
	SRS-619	The Platform SHALL use NEDS to enable searching the Identity Repository based on any Identity Attribute.			
	SRS-359	The Platform SHALL provide the Capability to define, establish and manage technical Trust between Federated Identity Service Providers.			
	SRS-570	The Platform SHALL support sharing of Identity data with external trusted partners by providing a dedicated instance of a repository.			
	SRS-4223	The Platform SHALL provide an LDAP over TLS (LDAPS) interface for NATO and partners to push and pull information.			
	SRS-4224	The Platform SHALL use the [CCEB ACP133D, 2014] schema.			
	SRS-2996	The Platform SHALL manage credential details (e.g., login and password, PKI certificate), enabling authentication for Users that cannot be authenticated through Active Directory			
	SRS-3028	The Platform SHALL allow an access control component to require Authentication for access to a specific resource.			
	SRS-356	The Platform SHALL support as a minimum the following Authentication mechanisms: basic (Username, password) Authentication open standards-based Claims-based Authentication, to include SAML for SOAP/WS-Security OAuth for REST OpenID Connect WS-Federation forms-based Authentication to the Identity Service Provider PKI certificates-based Authentication to the Identity Service Provider Kerberos multi-factor (multi-credential) Entity Authentication			
	SRS-4069	The Platform SHALL allow configuring unauthenticated access to a resource.			
	SRS-3048	All Platform Authentication controls (including libraries that call external Authentication services) SHALL have a centralised implementation, used for all resources.			
	SRS-3038	All Authentication controls SHALL be enforced on the server side.			
	SRS-2976	The Platform SHALL uniquely Identify and Authenticate Users.			
	SRS-355	The Platform SHALL allow Authentication of a User to an application (Relying Party).			
	SRS-187	The Platform SHALL enable sharing of Identity data among multiple relying parties as a part of an authenticated Entity session, implementing Single Sign-On (SSO) across the Platform for one or more services.			
	SRS-338	The Platform SHALL allow the Entity to leave the current Authentication session (log out), including Logging out from multiple applications, services or resources in one step			
	SRS-227	The Platform SHALL support different methods of User Authentication depending on Authentication policies and required level of Authentication assurance.			
	SRS-3744	The Platform SHALL support web-based Authentication in Federations by: Providing federated Identities for the authenticated NATO-affiliated Entities Validating and accepting federated Identities from NATO-trusted partners Using federated Identities in Authorisation processes.			

	SRS-3437	The Platform SHALL be able to establish a Trust relationship between Federated Identity service providers in order to authenticate Users from other domains, by: using a Security Token issued by a trusted Federated Identity Provider mapping Attributes from a federated Identity Service Provider to other Attributes according to predefined rules reissuing a Security Token that is trusted internally containing the appropriate Attribute values			
	SRS-361	The Platform SHALL expose an Identity Service Provider interface to its service providers (e.g., enterprise applications) supporting multiple Authentication protocols, as specified in SRS-356.			
	SRS-362	The Platform SHALL expose a Service Provider interface able to consume Identity Information provided by external Identity Service Providers after successful User Authentication.			
	SRS-364	The Platform SHALL mediate between Claims-based Authentication protocols (see SRS-356) used by external Federated Identity Service Providers and the identity providers configured in the Platform.			
	SRS-363	The Platform SHALL enable a User to authenticate through a chain of trusted Identity Service Providers in order to get access to the protected resources made available to the User within an established Federation.			
	SRS-331	The Platform SHALL provide a token-based security mechanism.			
	SRS-3447	The Platform SHALL ensure that the Security Token Service on the Platform is configured to support the open standards-based Claims-based Authentication by default as its Authentication methods for all Relying Parties.			
	SRS-186	The Platform SHALL be able to issue a new Security Token, including new proof information, based on the Credential provided/proven in the request.			
	SRS-188	The Platform SHALL be able to renew a previously issued token when expiration is presented (and possibly proven) and return a token with new expiration information.			
	SRS-3442	The Platform SHALL allow an exchange of tokens to take place between the requestor and the Relying Party that passes on the Identity, Context and all necessary information a Relying Party needs to grant access.			
	SRS-183	The Platform SHALL allow Authorised Users to configure which Assertions are issued to individual Relying Parties within each Security Token.			
	SRS-184	The Platform SHALL be able to configure other aspects of token-issuance, such as the lifetime of the token and which certificates are used.			
	SRS-3503	The Platform SHALL support both SAML 2.0 and OAuth 2.0 token types.			
	SRS-3444	The Platform SHALL hide internal Security Token Service instances from Entities in domains beyond the NATO Enterprise.			
	SRS-3445	The Platform SHALL provide dedicated Security Token Services for Entities from domains beyond the NATO Enterprise.			
	SRS-3448	The Platform SHALL be able to configure the Security Token Service for enabling a one-way Trust with other Security Token Services.			
	SRS-3438	The Platform SHALL perform required Identity token transformations (Attribute mappings) between tokens obtained from external Identity Service Providers and provided to local Service Providers.			
	SRS-2121	The Platform SHALL allow the Security Token Service in the domain of the service provider to place further constraints on the abilities and Privileges of consuming services and Users from the federated Consumer domain.			
	SRS-345	The Platform SHALL ensure that the Security Token Service can be configured to limit issuance of Security Tokens for acceptance by a particular Relying Party or a particular group of Relying Parties.			
	SRS-3066	The Platform SHALL ensure that Users can only access functions or services for which they possess specific Authorisation.			
	SRS-3067	The Platform SHALL ensure that Users SHALL only access URLs for which they possess specific Authorisation.			
	SRS-3068	The Platform SHALL ensure that Users SHALL only access information for which they possess specific Authorisation.			
	SRS-2133	The Platform SHALL allow an Authorised User to retrieve access rights bound to the Enterprise Identity of an Entity.			
	SRS-223	The Platform SHALL support usage of different access control modes, best suited for a given resource, including: Discretionary Access Control (DAC) Role-Based Access Control (RBAC) Attribute-Based Access Control (ABAC) Context-Aware Access Control			

	SRS-4011	The Platform SHALL allow for ABAC according to the following guidelines: Authorisation decisions to be based on composable, machine-readable policies. Authorisation decisions to be based on Attributes of the following: Actor; Resource; Action; Environment; Others, by configuration. Attributes to be retrieved from known repositories, when they are not included in the request. Obligations on the PEP to be returned with the Authorisation decision.			
	SRS-2992	The Platform SHALL allow for RBAC according to the following guidelines: Users are associated with User Roles and also with organisations. User Roles determine the functions and types of objects available to the User. organisations determine the data available for use by the available functions. a User has permission on a particular data item only if the User has an authorised Role and is a member of that organisation.			
	SRS-3099	The Platform Access Control function SHALL deny access by default			
	SRS-3077	All Platform Authorisation controls (including libraries that call external Authorisation services) SHALL have a centralised implementation enforced on the server side, used for all resources.			
	SRS-232	The Platform SHALL allow an Authorised User to define and enforce various overall access management policies (e.g., governing creation and maintenance of Privilege and entitlement Attributes, required Authentication levels, required Event collection levels, etc.)			
	SRS-193	The Platform SHALL allow an Authorised User to configure the location (e.g., URI) of the policy store.			
	SRS-194	The Platform SHALL allow an Authorised User to configure the location (e.g., URI) of the Attribute store.			
	SRS-2980	The Platform SHALL lock User access after a configurable number of unsuccessful Authentication attempts.			
	SRS-3757	The Platform SHALL enforce Authorisation decisions for requests to protected resources.			
	SRS-190	The Platform SHALL apply required security mechanisms to the responses returned from protected services (signing, encryption).			
	SRS-191	The Platform SHALL validate the security elements of the incoming message, including message encryption and signature, validity of the Security Token, and that the Security Token is from a trusted issuer.			
	SRS-3460	The Platform provided PEP instances SHALL as a minimum support .NET framework and Java Runtime Environment.			
	SRS-3756	The Platform SHALL provide Authorisation (Policy Decision Point) functionality to evaluate Authorisation decisions based on access policies associated with requested resource, authenticated requestor Identity Information and other data required by access policies.			
	SRS-3458	The Platform SHALL allow external Policy Decision Points to be called for evaluation security policies associated with protected services.			
	SRS-196	The Platform SHALL return any further obligations that are required in order for the requester to access the service provider.			
	SRS-198	The Platform SHALL retrieve any further Attributes from the appropriate Attribute store that are required by the policy in order to make a decision.			
	SRS-199	The Platform SHALL apply required security mechanisms to access requests (signing, encryption).			
	SRS-3424	The Platform SHALL provide Access Policy Administration functionality to create, disseminate, modify, manage, and maintain hierarchical rule sets to control digital resource management, utilisation, and protection in a standard policy exchange format.			
	SRS-221	The Platform SHALL allow an Authorised User to evaluate (test) access control policies for any combination of resource, Identity and other access decision factors.			
	SRS-235	The Platform SHALL provide tools to support verification (testing) of access management data compliancy with overall access management policies			
	SRS-205	The Platform SHALL provide the means to store and administer access control policies via one or more policy store repositories.			
	SRS-3752	The Platform SHALL provide organisational Role Management functionality to include Role modelling, manual and automated Role assignment, and a routine/scheduled Role validation.			

	SRS-2994	The Platform SHALL allow two or more Users to have the same Roles within the Platform simultaneously.			
	SRS-3716	The Platform SHALL provide a toolset for Authorised Users to model IAM business processes, including actions such as approvals, notifications, initiation of Identity and access data processing requests.			
	SRS-3717	The Platform SHALL provide automation of the modelled IAM business processes through the ability to execute conditional sequences of (sub)-processes and tasks, arranged in a form of workflows.			
	SRS-4105	The Platform SHALL support triggering IAM tasks on demand, scheduled, and/or as part of complex workflows.			
	SRS-631	The Platform SHALL support testing mode of workflows for simulation and validation of newly defined/updated workflows before execution in the production environment.			
	SRS-618	The Platform SHALL use a data retrieval mechanism to support filling out forms for IAM workflows.			
	SRS-533	The Platform SHALL define transition workflows between lifecycle states of Enterprise Identities (e.g. Enrolment, activation, maintenance (update), adjustment, suspension, reactivation, deletion, archiving, and restoring).			
	SRS-4106	The Platform SHALL define workflows related to on-boarding processes, including pre-arrival and at arrival activities.			
	SRS-4108	The Platform SHALL define workflows related to Identity Information update requests, including modification of User Privileges when the Identity data update implies it (e.g., change of the assignment in the organizational structure).			
	SRS-4107	The Platform SHALL define workflows related to off-boarding processes, including deactivation and archiving of the Enterprise Identity for an employee who has left the organization, deactivation of corresponding User accounts, cards, Credentials, Privileges, etc.			
	SRS-3738	The Platform SHALL define workflows related to NPKI certificate request processes, including integration with the on-boarding processes.			
	SRS-4109	The Platform SHALL define workflows related to Pass (Token) (re-)issue request processes, including integration with the on-boarding processes.			
	SRS-4110	The Platform SHALL define workflows related to Personal Identification Number (PIN) Reset Request.			
	SRS-592	The Platform SHALL allow authorised Users to display and report the status of all executed IAM business processes.			
	SRS-3713	The Platform SHALL provide a self-service Capability, with a secure Web interface, for Authorised Users to initiate execution of the defined IAM business processes, including filling out and submitting the required pre-defined electronic forms.			
	SRS-3714	The Platform SHALL provide a self-service Capability, with a secure Web interface, for enabling authenticated Users to trigger requests to maintain their own personnel information and to perform certain routine Identity lifecycle maintenance tasks (e.g., update their personal contact information), including a change validation process before any data is updated within the system and synchronised.			
	SRS-4191	The Platform SHALL meet at a minimum the throughput levels defined for the individual services in Table 2.			
	SRS-4192	The Platform SHALL not exceed the latency defined for the individual services in Table 2.			
	SRS-4169	The Platform SHALL be able to support a throughput increase of 10% every year with no degradation of the maximum latency.			
	SRS-3264	The Platform SHALL be able to handle any or all of its designed Platform services when the maximum number of concurrent Users are using the platform, without any Fault/Error or timeout, for at least 99.5% of its Operational time.			
	SRS-3265	The Platform shall be able to handle all Platform services concurrently, using the defined information product for each of them, without any Fault/Error or timeout, for at least 99.5% of its Operational time.			
	SRS-3266	The Platform SHALL be able to handle any or all of its designed Platform services with the maximum amount of allowed data, without any Fault/Error or timeout, for at least 99.5% of its Operational time.			
	SRS-4016	Platform services SHALL meet the minimum required throughput defined in Table 2, for at least 99.5% of its Operational time.			
	SRS-4175	None of the Platform services SHALL ever drop below the maximum throughput value defined Table 2 by more than 10%.			
	SRS-3270	Each of the Platform services SHALL be able to answer any request within the required time limits defined in Table 2, for at least 99.5% of its Operational time.			
	SRS-4176	None of the Platform services SHALL ever exceed the maximum time limits value defined in Table 2 by more than 10%.			
	SRS-3291	The Platform SHALL exhibit a Mean-Time-Between-Failure (MTBF) characteristic, for each service level, in alignment with ITM of at least the number of operational hours as defined in Table 5.			
	SRS-2425	The Platform SHALL have an Inherent Availability for each service level of at least the percentages defined in Table 6.			

	SRS-2447	The Platform SHALL be able to queue requests to an unavailable Service and deliver them when the Service becomes available again.			
	SRS-3302	For 99% of the possible Faults/Errors in any of the Platform services, the system SHALL be able to recover the service or switch to an alternative service, in no more than the amount of Recovery Time defined in Table 7, without loss of data.			
	SRS-2463	The Platform SHALL resume/retry services, in case of Failure due to high latency/timeout/loss of network connectivity, without loss of data.			
	SRS-2464	The Platform SHALL continue to function within and between the remaining nodes following the loss of one or more connected Organisational Nodes operating within the Platform implementation architecture using the ON WAN or PBN WAN.			
	SRS-3806	In the event a service is interrupted because of a Fault/Error, the Platform SHALL be able to restore the data in no more than the duration of Recovery Point specified in Table 7, at least 99.9% of the faults.			
	SRS-3810	When the Platform is installed in any different environment (deployed, exercise, etc.), 100% of critical (Level 1) services and at least 90% of non-critical (Level 2 and Level 3) services SHALL run without any Faults/Errors, at least 99.5% of the time.			
	SRS-4170	The Platform SHALL not present any Fault/Error after any Scalability process, for at least 99.5% of its Operational time.			
	SRS-2400	The Platform SHALL provide a MTTR in accordance with the times defined in Table 8.			
	SRS-3294	The MaxTTR for the Platform SHALL not exceed the times defined in Table 8 for a single maintenance action.			
	SRS-2401	The Platform SHALL provide a RPO in case of Disaster Recovery in accordance with the times defined in Table 8.			
	SRS-3286	When a maintenance action is required on a software Component of the Platform, this action SHALL not cause any possible Fault/Error in other Components of the system, at least 99.9% of the time.			
	SRS-4068	The Platform SHALL allow individual Platform services to be deployed separately, without the need to install the full Platform software.			
	SRS-3287	The Platform SHALL be able to detect at least 99.5% of the possible problem which can occur, notifying the User or Administrator with a general message.			
	SRS-3288	The Platform SHALL be able to isolate 85% of the possible problem which can occur, notifying the User or Administrator with a specific message which identifies the Error/Fault which has occurred.			
	SRS-4263	90% of the software Components of the Platform shall be bservable, using automatic test procedures.			
	SRS-4264	80% of the software Components of the Platform shall be controllable, using automatic test procedures.			
	SRS-3003	The Platform SHALL be able to generate and retain logs (audit records) for System Events, associated with individual User Identities, to include: system start-up (including re-starts) and shutdown log-on (including failed log-on attempts) and log-off of individual Users changes to permissions and Privileges of Users and groups changes to security relevant system management information (including audit functions) start-up and shutdown of the audit function any access to security data deletion, creation or alteration of the security audit records changes to system date and time unsuccessful attempts to access system-level resources			
	SRS-4021	The Platform SHALL be able to generate and retain logs (audit records) for Service Events, associated with individual User Identities, to include: Successful or unsuccessful requests to and responses from services Successful or unsuccessful authorization (access control) decisions Service startup or shutdown Configuration changes to services Message delivery and non-delivery			

	SRS-376	The Platform SHALL be able to log all messages, including whole messages or Attributes to include: Message time-stamp Message source and target address URL requested Service requested Operation requested Request size Unique request id (extracted from the message or automatically generated by the SOA Logging Services)			
	SRS-3098	The Platform logs SHALL include: Event type Time stamp from a reliable source Severity level of the Event, if applicable Service(s) involved in the Event, if applicable The Identity of the User that caused the Event (if applicable) Status of the Event A description of the Event			
	SRS-248	The Platform SHALL be able to export logging information to the format agreed with the Purchaser.			
	SRS-4022	The Platform SHALL allow Authorised Users to enable, configure verbosity of, and disable the various types of logging.			
	SRS-3005	The Platform SHALL protect the Audit Logs from unauthorised modification or deletion.			
	SRS-3173	The Platform SHALL not log data that could assist an attacker, including and personal information.			
	SRS-3010	The Platform SHALL retain Audit Logs for a configurable period of time, the period being configurable by Authorised Users.			
	SRS-4023	The Platform SHALL allow Authorised Users to configure the maximum permitted size of the Audit Logs.			
	SRS-3013	The Platform SHALL raise an alarm via the Service Management and Control system when the Audit Logs reach an Authorised User configurable percentage of its maximum permitted size.			
	SRS-4024	The Platform SHALL provide a log analysis and reporting tool, which will allow Authorised Users to browse, search and report on Audit Logs, based on combinations of search criteria across all fields in the log record format supported by this system.			
	SRS-3009	The Platform SHALL enable the archiving of logging that is no longer actively used to a separate data storage device for long-term retention.			
	SRS-2122	The Platform SHALL use available session information to allow an Entity to access another resource without the need for another Authentication.			
	SRS-4046	A session management mechanism to protect session IDs SHALL be used after a successful Authentication.			
	SRS-4119	A session management mechanism related security context SHALL be maintained until the session expires.			
	SRS-4047	Any change in the security context SHALL require re-Authentication.			
	SRS-4048	The Platform SHALL allow Authorised Users to set a "timeout" period which SHALL automatically log-out any sessions which have been inactive for that period of time.			
	SRS-4049	Authorised Users SHALL be able to enable and disable the session timeout feature.			
	SRS-3060	Session IDs SHALL be generated using a cryptographically secure (pseudo)random number generator and they SHALL be at least 128 bits long.			
	SRS-3063	The application SHALL not permit duplicate concurrent authenticated User sessions originating from different machines or IP addresses.			
	SRS-3128	If HTTPS is required, the web application SHALL make use of HTTP Strict Transport Security (HSTS; previously called STS) to enforce HTTPS connections.			
	SRS-2978	The Platform SHALL apply password policy which will enforce individuals to select a password that is at least a configurable (by Authorised Users) minimum number of characters long, comprising a configurable mix of uppercase, lowercase, numerics and symbols.			
	SRS-4030	The Platform SHALL force passwords to be changed at intervals configurable by Authorised Users.			
	SRS-2979	The Platform SHALL deny the re-use of a configurable (by Authorised Users) number of previous passwords.			

	SRS-4031	The Platform passwords SHALL be stored, encrypted, as NATO SECRET information in an approved location with controlled and recorded access			
	SRS-3029	Password fields SHALL not echo the User's password when it is entered, and password fields (or the forms that contain them) have autocomplete disabled.			
	SRS-3000	The Platform SHALL provide help texts to support the login process together with links to recover lost password and login details.			
	SRS-3045	Forgotten password and other recovery paths SHALL send a time-limited activation token or use two factor proofs			
	SRS-3032	Forgot password functionality and other recovery paths SHALL do not send the existing or new passwords in clear text to the User.			
	SRS-3034	No default passwords SHALL be used, for any Platform Components.			
	SRS-4032	Passwords SHALL never be hard-coded in any source code or executable, not even in an encrypted/hashed form.			
	SRS-3046	Shared knowledge questions/answers (so called "secret" questions and answers) SHALL not be used.			
	SRS-3109	The Platform SHALL never cache data identified by the Purchaser as sensitive. and SHALL be cleared (invalidated) on logout and/or when the session expires and/or on re-Authentication.			
	SRS-4239	The Platform SHALL clear (invalidate) data identified by the Purchaser as sensitive on logout and/or when the session expires and/or on re-Authentication.			
	SRS-3107	The Platform SHALL send to the server data identified by the Purchaser as sensitive in the HTTP message body (i.e., URL parameters are never used to send sensitive data).			
	SRS-3111	The Integrity of interpreted code, libraries, executables, Audit Logs, and configuration files SHALL be verified using checksums or hashes.			
	SRS-2962	The Platform SHALL maintain referential Integrity between entities across data sets.			
	SRS-2983	The Platform SHALL protect User Credentials in transit.			
	SRS-2989	The Platform SHALL protect the User's entire login transaction and session via SSL or similar technologies.			
	SRS-3179	All cryptographic functions SHALL be implemented on the server side.			
	SRS-2960	If a file is being generated or exported in a format that does not use headers/footers, the Platform SHALL include a Security Classification into an appropriate part of the file so that it is clearly visible to the User.			
	SRS-2990	The Platform SHALL allow the User (with the same user-id) to access the same information and functionality from any workstation on the NS WAN (i.e., 'roving user' functionality).			
	SRS-3171	The Platform SHALL enforce: a trust path to be built from a trusted CA to each Transport Layer Security (TLS) server certificate, as well as each server certificate to match the Fully Qualified Domain Name of the server, and each server certificate to be valid.			
	SRS-3115	The Platform SHALL enforce TLS to be used for all connections, internal (e.g., backend) or external, that involve data or functions identified by the Purchaser as sensitive.			
	SRS-3116	The Platform SHALL enforce backend TLS connection Failures to be logged.			
	SRS-3119	The Platform SHALL enforce failed TLS connections to not fall back to an insecure connection.			
	SRS-3120	The Platform shall enforce certificate paths to be built and verified for all client certificates using configured Trust anchors and revocation information.			
	SRS-3121	The Platform SHALL use a single standard TLS implementation that is configured to operate in a mode of operation approved by the Purchaser.			
	SRS-3122	The Platform SHALL enforce specific character encodings to be defined for all TLS connections (e.g., UTF-8).			

	SRS-2509	For each specified interface (i.e., inputs and outputs to the Platform), the Platform SHALL be equipped with an Interface Control Document (ICD) describing the interface provided in a format proposed by the Contractor and accepted by the Purchaser. The content SHALL include, where applicable, the following information: A list of the applicable technical standards A catalogue of the services and interfaces exposed by the Platform A detailed description of the interfaces, including diagrams, Data Elements, data formats, Performance values, communication protocols, security settings, etc. Descriptions of Data Elements units of measure required for the Data Element, such as seconds, meters, kilohertz, etc. limit/range of values required for the data element (for constants provide the actual value) accuracy required for the Data Element precision or resolution required for the Data Element in terms of significant digits, frequency at which the Data Element is calculated or refreshed, such as 10 KHz or 50 msec legality checks performed on the Data Element data type, such as integer, ASCII, fixed, real, enumerated, etc. data representation/format priority of the Data Element Service Descriptors, identifying the services endpoints, a detailed description of the service operations and service parameters All related Artefacts such as WSDL, schema files and descriptors Message descriptions Interface priority Communications protocol			
	SRS-2519	The Platform SHALL provide adequate documentation for the content and meaning of the file formats it produces or accepts. An adequate definition is one that enables a programmer or User to understand the meaning of the data and determine whether it is suitable for its intended use.			
	SRS-4230	The Platform SHALL supply a definition for every element, Attribute, and enumeration value defined in the file format.			
	SRS-2522	As a design rule, direct database access in the Platform SHOULD be avoided.			
	SRS-4009	The Contractor SHALL ensure that the Platform supports traversal of firewalls and gateways through the use of well-known proxy protocols or encapsulation of cryptographic protocols over http/https.			
	SRS-2624	The Platform SHALL support Interoperability with instant messaging based on the Extensible Messaging and Presence Protocol (XMPP).			
	SRS-2625	The Platform SHALL conform to the fundamental features and security mechanisms of instant messaging as described in the Service Interface Profile for Basic Collaboration Services (AI 06.02.12).			
	SRS-2628	The Platform SHALL interface with the Bi-SC AIS E-mail Services based on MS Exchange.			
	SRS-2629	The Platform SHALL comply with Bi-SC AIS E-mail services and protocols			
	SRS-2630	E-mail messages produced by the Platform to be provided to the Bi-SC AIS E-mail Services SHALL comply with the formats used in the Bi-SC AIS (e.g., classification header).			
	SRS-2652	The Platform SHALL be able to interface with the NATO Information Portal using the SharePoint 2013 APIs.			
	SRS-2658	All data disseminated to a different Security Domain SHALL contain approved NATO security labels and adhere to NATO labelling standards.			
	SRS-2555	The Platform SHALL exchange information with IEG-C to cross from NATO Secret to Mission Secret Security domains.			
	SRS-2678	The Platform SHALL integrate with the Bi-SC AIS Directory Services Active Directory.			
	SRS-2680	If the Platform requires an Active Directory schema change, these schema extensions SHALL be documented and submitted for approval to the Purchaser during the Design Stage.			
	SRS-2681	The Platform SHALL be compatible with Active Directory services and protocols.			
	SRS-2684	The Platform SHALL support integration with Windows File and Print Services (including publishing and lookup through Active Directory).			
	SRS-2685	The Platform SHALL support integration with Windows built-in services (e.g., Domain Name System (DNS), Internet Information Services, RUP, Terminal Server).			
	SRS-2686	The Platform SHALL support integration with Windows Security Services.			

	SRS-2687	The Platform SHALL support integration with Active Directory-supported security access control (e.g., ACL, security groups) to Operating System resources.			
	SRS-2688	The Platform SHALL be able to operate with the latest security settings from the NATO Information Assurance Technical Centre (NIATC) without change.			
	SRS-2702	The Platform will be able to run with NATO Standard Malware Detection Services and anti-virus software.			
	SRS-2703	The Platform SHALL work correctly and not adversely impact other applications when Bi-SC AIS standard Anti-Virus software is applied.			
	SRS-3619	The supplied software SHALL be compatible with the NATO Anti-Virus management centre and approved by the Purchaser.			
	SRS-2563	The Platform MAY use Generic Security Services Application Program Interface as the application programming interface for accessing security services.			
	SRS-2564	The Platform security application program interface SHALL be compliant with [IETF RFC 2078, 1997].			
	SRS-2565	The Platform primary security services (access control, Confidentiality, Integrity, Authentication, and Non-repudiation) SHALL use X.509.			
	SRS-2566	The Platform X.509 support to primary security services SHALL be compliant with NPKI.			
	SRS-3493	The Platform SHALL be required to be able to run on the Deployable CIS platform.			
	SRS-2921	The Platform SHALL be deployed depending on the type of Deployable CIS node. A single Deployable CIS node SHALL vary between the full suite, a selection of Platform service or no Platform Services.			
	SRS-2888	The Platform SHALL not bear additional licences and charges for deployment of the Platform Product if used in a NATO context (exercise, mission, static and deployable commands, NRF).			
	SRS-4255	The Platform SHALL be able to continue service locally if a WAN connection is disrupted.			
	SRS-4257	The Platform SHALL be able to resume services to other nodes if a WAN connection is restored after a disruption.			
	SRS-4256	The Platform SHALL be able to provide services to other nodes if interconnections are over degraded networks.			
	SRS-2898	Each deployable Platform instance SHALL have the Capability to be operated by local administration and management, so that if a node is isolated from the central support, local administration and management can be executed.			
	SRS-2899	The Platform preparation for deployment and movement SHALL not take more than 5 days from receiving the Notice to Move until the equipment is packed up ready to move.			
	SRS-2915	The Platform data resynchronisation in deployment after long periods off-net SHALL resolve consistency conflicts.			
	SRS-2916	The Platform SHALL implement data compression that guarantees an efficient use of network bandwidth.			
	SRS-2917	The Platform SHALL implement incremental database synchronisation communication protocol that guarantees an efficient use of network bandwidth.			
	SRS-2918	The Platform SHALL not encrypt WAN data exchange.			
	SRS-2924	The backend deployment for NATO locations SHALL be done using the NATO Infrastructure (Processing, Storage, Networking) Services.			
	SRS-2925	The Platform SHALL be deployable in both MS Hyper-V and VMWare virtualised environments.			
	SRS-2611	The Platform SHALL operate with other Bi-SC AIS FSs in the same environment without causing an Error condition in itself or in other systems.			
	SRS-1720	The Platform SHALL be compliant with the standards given in the section "Applicable Standards". Any proposed deviation SHALL be approved by the Purchaser.			
	SRS-4104	The Platform SHALL be designed and implemented based on the Platform Principles as described in section 2.1.1.			
	SRS-1722	The proposed software architecture, development environment, middleware system and the separation of Components (Human Machine Interface, Business and Data) for the Platform SHALL be documented and explained in detail.			
	SRS-1724	The Platform services SHALL comply with the C3 Classification Taxonomy [NC3B AC/322-N(2016)0021-AS1, 2016], and applicable Service Interface Profiles.			
	SRS-1726	The Platform design process SHALL balance design implementation with cost for implementation and support to minimise life cycle cost. The Platform design SHALL take into account the technical, support and cost impacts for NATO.			
	SRS-2404	The Platform SHALL be composed of discrete Components such that a change to one Component has minimal impact on other Components.			
	SRS-1728	The Platform User functionality SHALL be browser-based, except as specifically waived by the Purchaser.			
	SRS-4138	The Platform SHOULD not use plug-ins and runtime environments (e.g. Flash plug-in, Silverlight). The use of Hypertext Mark-up Language (HTML) 5 and AJAX is strongly recommended.			
	SRS-1746	The Platform SHALL use standard internet addressing, Universal Resource Locator and Universal Resource Identifier.			

	SRS-1731	The Platform SHALL be based on COTS in its architecture in place of dedicated solutions when the functionalities of a COTS matches the requirements for a Service with no or minimal adaptation.			
	SRS-1732	All functionalities provided by the COTS used for the Platform SHALL be available and not shielded nor masqueraded by an additional layer.			
	SRS-1733	The Platform adaptations SHALL be delivered as additional Services, owned by NATO, that complement the COTS native functionalities.			
	SRS-1750	The Platform SHALL comply with the standards and language specifications described below. Any variations from the languages or specifications SHALL be agreed with the Purchaser: C# [ISO/IEC 23270:2003] Java SE Version 9 [JSR 379] .NET C++ [ISO/IEC 14882] Common Language Infrastructure (CLI) [ISO/IEC 23271:2003 and ISO/IEC 23272:2003] JavaScript [ECMA 262] HTML [ISO/IEC 15445, 2000]			
	SRS-1752	The Platform SHALL not use DCOM, COM, ActiveX and/or COM+ unless specifically authorised in advance by the Purchaser.			
	SRS-1757	A convention SHALL be adopted and applied consistently across all code Artefacts for each programming language employed.			
	SRS-1758	Source code Artefacts delivered for the Platform SHALL be written using Standard English (e.g., for Classes, Methods, Variables etc.).			
	SRS-4120	Industry coding best practices SHALL be used for Platform source code Artefacts.			
	SRS-1761	Source code delivered for the Platform, including customisation code for COTS products and modifications to Free Open Source Software (FOSS) products but not to existing COTS/FOSS source code, SHALL be documented with in-line comments using standard English. Commercial best practices SHALL be used in the level of commenting.			
	SRS-1762	Comments for the source code of the Platform SHALL be used to clarify intent of the code and SHALL be provided for: Each class definition explaining the purpose of the class Each member function explaining what the function does Each member variable explaining what the variable means Each type definition (enums) explaining what the type represents			
	SRS-1764	Comments for the source code of the Platform SHALL be able to be extracted and formatted to augment technical documentation.			
	SRS-1766	All usage of the Windows Registry by the Platform applications SHALL be fully documented, and requires approval by the Purchaser not later than the Design Stage.			
	SRS-4253	The Platform SHALL provide a Web-based toolset to configure the Platform services.			
	SRS-4254	The Platform toolset SHALL be able to graphically display and configure service parameters.			
	SRS-4064	In case the Platform provided toolset makes use of an API to interact with a service, the tool SHALL be able to make use of all API features and Performance.			
	SRS-4251	In case the Platform provided toolset makes use of an API to interact with a service, the tool SHALL be designed to allow for future GUI enhancement or replacement.			
	SRS-2739	The Platform visual design SHALL follow the recommendations and guidelines stated in the following Documents: NATO Visual Identity Guidelines [NATO Visual Identity Guidelines, 2016] NCIA Visual Identity Guidelines [NCIA Visual Identity Guidelines, 2013]			
	SRS-2740	The Platform SHALL follow the recommendations and guidelines of the Human Machine Interface (HMI) Style Guide for C4ISR Rich Applications [NCIA HMI Style Guide, 2015] regarding to windows and layouts, User interactions, User support and feedback, common User interface Components design, visual design and text use.			
	SRS-2742	The Platform icons included in the designed solution SHALL be compliant with the ISO 18152 standard series.			
	SRS-2743	The Platform SHALL be compliant with the ISO 9241 standard series for software usability.			
	SRS-1769	FOSS Components in the Platform SHALL comply with the NATO strategy on the use of Open Source Software in NATO systems.			
	SRS-1770	Any Platform Components based on free and open source software SHALL be provided with the source code for the FOSS.			

	SRS-1771	Use of a FOSS Component SHALL not limit the deployment or use of the Platform in any way and SHALL not require the release of code developed for the Platform.			
	SRS-3676	The general requirements for technical documentation developed in the SOW SHALL also apply to the on line documentation.			
	SRS-1777	The Platform on-line User documentation and help system SHALL be compliant with standards identified under section "Applicable Standards".			
	SRS-1779	The Platform SHALL adhere to the 'Microsoft standard User interface' methods for accessing on-line documentation resources.			
	SRS-1826	The Platform SHALL support on-line help describing all functionality of the Platform Capability.			
	SRS-1827	The Platform on-line help SHALL translate every use case and usage scenario into a browsing sequence.			
	SRS-4240	The Platform SHALL structure every browsing sequence according to the User workflow.			
	SRS-1828	The Platform on-line help SHALL describe each Platform function, the interrelationships between and the logical sequence of functions.			
	SRS-1829	The Platform on-line help SHALL explain all menu items, dialog windows, data entry and query fields implemented in the Platform Product Baseline.			
	SRS-1830	The Platform on-line help SHALL include a glossary providing definitions of all terms and acronyms implemented in the Platform Product Baseline.			
	SRS-1831	All definitions in the Platform glossary SHALL be available in roll-over, pop-up windows linked to every appearance in on-line help of the corresponding term or acronym.			
	SRS-1832	In the Platform, each dialogue, menu item, toolbar item, function, field or button (each item on the screen) SHALL have an on-line help option. This SHALL be clearly visible, but not intrusive.			
	SRS-1833	The Platform on-line help function SHALL provide meaningful advice and hints to Users appropriate to the actions they are trying to take.			
	SRS-1834	The Platform on-line help SHALL be concise, compact and clear to the User.			
	SRS-1835	The on-line help SHALL include snapshots of the Platform screens, windows, and dialogue boxes. The snapshots SHALL be provided in a suitable lightweight format (e.g., Graphics Interchange Format (GIF), PNG) approved by the Purchaser.			
	SRS-1836	Pictures in the Platform on-line help showing more than five GUI elements/controls SHALL have a clickable image map describing each element.			
	SRS-1837	If the Platform on-line help subject requires a large picture that does not fit on a normal page, a reduced copy SHALL be additionally included on the Help page that will expand to its full size on User request.			
	SRS-1838	The Platform on-line help SHALL be context-sensitive (i.e., based on a specific point in the state of the software and providing help for the situation that is associated with that state on action being performed).			
	SRS-1839	All context-sensitive GUI elements in the on-line help SHALL be linked to the relevant User Manual subjects.			
	SRS-1840	In the Platform, all source code elements SHALL be configured to link the GUI elements to their context-sensitive subjects.			
	SRS-1841	The Platform SHALL contain help functions that provide access to interactive training sessions to guide Users through procedures and functions.			
	SRS-1842	The Platform on-line help SHALL be given by a small pop-up screen or infotip screen. This screen SHALL appear quickly and be very easy to hide, for instance clicking anywhere within it.			
	SRS-1843	The Platform on-line help SHALL open a dedicated web page when the User request access to the full content of the on-line help. The on-line help SHALL not be preventing the User to perform on the Platform GUI.			
	SRS-1844	The Platform SHALL allow the User to hide the on-line help screen just by clicking anywhere else, or there SHALL be another single action hiding mechanism.			
	SRS-1846	The Platform on-line help SHALL be organised in the following two sections: Contents, providing access to all help pages and organised in a logical manner by subject or procedure Index, providing Users with both the ability to search for keywords in all Help pages and retrieve a list of those pages in which those keywords appear and the ability to select and trigger such a query from a list of all keywords.			
	SRS-1847	The Platform SHALL be able to display search query results for finding help items in the online help in a list. The Platform SHALL display the help item when the User selects a query result in this list.			
	SRS-1849	The on-line help shall be available as a web site and includes all project-related source elements and graphics. The web site shall be available as a stand-alone web site to be installed and used on a stand-alone computer if required.			

	SRS-1851	The Platform SHALL provide a list of Frequently Asked Questions(FAQ). FAQs SHALL be available to support the NCIA Help Desk and other support organisations.			
	SRS-1852	The Platform SHALL allow the User to display the Platform FAQ.			
	SRS-1853	The Platform SHALL allow the User to search the Platform FAQ			
	SRS-1854	The Platform SHALL allow the Platform User or the Platform Administrator to ask questions to the NCIA Help Desk in electronic form by using the Platform FAQ.			
	SRS-1855	The Platform SHALL allow Authorised Users to update the contents of the FAQ.			
	SRS-1937	The Platform SHALL be able to run on NATO-provided infrastructure including virtual servers and operational workstations.			
	SRS-1942	The infrastructure requirements of a service or application SHALL not be designed and deployed with a "per service, per application" approach but SHALL be covered through a harmonised "infrastructure services" approach applicable to all services and applications making use of the infrastructure services.			
	SRS-4125	The Platform SHALL be compatible with the x86-64 architecture (32-64 bit applications).			
	SRS-4126	The server-side of the Platform SHALL be compatible with the NATO desktop baseline including: Microsoft Windows Server; Red Hat Enterprise Linux; or Solaris.			
	SRS-4128	The client-side of the Platform SHALL be compatible with the NATO desktop baseline including: MS Windows Operating system; MS Office Professional Plus; MS Internet Explorer; MS Silverlight; Adobe Acrobat Reader; Java Virtual Machine; Email security classification Labelling client; McAfee Anti-Virus and Data Loss Prevention (DLP) agent; NCIRC desktop Host-based Intrusion Detection System (HIDS) and Forensics analysis based agents; VPN client for PBN mobile client devices; and Disk encryption for PBN mobile client devices.			
	SRS-4139	The Platform SHALL support multiple browsers, including as a minimum: MS browser, and Firefox.			
	SRS-4130	The Platform SHALL support the IPv6 protocol.			
	SRS-4131	The Platform SHALL support either: MS IIS, or Tomcat.			
	SRS-4132	The Platform's server deployment package (virtual appliance or installation package) SHALL be compatible with both: Microsoft Hyper-V, and VMWare ESXi hypervisor.			
	SRS-4133	The software installation package of the Platform SHALL be compatible with either: Windows Installer program, Redhat RPM, or Solaris Image Packaging System (IPS).			
	SRS-4134	The Platform software SHALL not have any hard coded: URL, DNS or IP Address settings. UNC, File Path, Drive Letter or similar storage location settings.			
	SRS-1949	All URL, DNS, IP Addressing and similar network settings SHALL be parametric, configurable, and possible to automate for unattended installation, backup, recovery.			
	SRS-4135	The Platform SHALL not have any direct dependency on the physical parameters of the storage environment (such as disk type, connection type, SAN topology, SAN protocol).			
	SRS-4141	The Platform SHALL be able to adapt immediately to changes in resource Capacity due to changing priorities (e.g. shrinking RAM).			

	SRS-4151	The Platform SHALL be able to automatically add a new instance without shutting down.			
	SRS-4150	All infrastructure states for the Platform environment SHALL be automatically recreatable from templates that describe how the instances need to be configured and updated with data.			
	SRS-4142	The Platform SHOULD be resource consumption aware to minimise consumption of CPU, memory, network input/output (I/O) and storage I/O.			
	SRS-4145	The Platform SHALL allow for geographic distribution of its instances across multiple ITM nodes.			
	SRS-4146	The Platform SHALL allow for global load balancing between Datacentres, in order to scale and support increasing volumes.			
	SRS-4147	The Platform SHALL support an active/active design local to a datacentre and across datacentre nodes (with replication of session and states for stateful Components). In this case both locations are running simultaneously, handling different Users and ready to fail over to each other should it become necessary.			
	SRS-4148	The Platform SHALL be able to perform full and incremental backups (i.e. snapshots) of data and software without impacting system Availability and Performance.			
	SRS-4158	The Platform SHALL be able to backup of both complete repositories as well as selected information element.			
	SRS-4157	The Platform SHALL allow for backups of full or selected data to occur automatically at a configurable frequency.			
	SRS-4156	The Platform SHALL make use of offload-host VM backup for backup jobs that create large I/O load and can impact the correct functioning of the production system for more than 5 minutes.			
	SRS-4155	The Platform SHALL use offline indexing of image backups for those systems that need to be indexed at the file level.			
	SRS-4154	The Platform SHALL use agentless image-based backups with incremental-forever using Changed Block Tracking (CBT).			
	SRS-4153	The Platform SHALL provide mechanisms to restore software and data lost since last backup.			
	SRS-4152	The Platform SHALL allow for selection of the backup files and the elements to restore.			
	SRS-4149	The Platform SHALL be able to archive both a complete repository as well as selected information elements (e.g. objects, records, documents).			
	SRS-4160	Archived data is searchable/readable and the Platform SHALL provide mechanisms for restoring it to a specified repository as required.			
	SRS-4159	The Platform SHALL allow an Authorised User to recover an archive, or parts of archive, by overwriting or appending.			

Provided/Detailed
Partial
Deviation proposed
Not Detailed

BI
SOW
SRS
SOW Annex B
SOW Annex C