RFQ-CO-115714-INTEG
ITM RECOVERY INCREMENT 1(ITM-RC1) – WORK PACKAGE (WP07)
SYSTEMS INTEGRATION AND CORE CAPABILITIES
BOOK II – PART IV

STATEMENT OF WORK (SOW)

CP 9C0150

PROJECT SERIAL: 2014/0IS03091-60 / 2020/0IS03301-00

VERSION: 1.0

Table of Contents

1. INTRODUCTION 6
1.1. Background 6
1.2. Purpose 7
1.3. WP07 High Level Scope 7
1.4. Statement of Work (SoW) Organisation 8
2. WORK PACKAGE IMPLEMENTATION 11
2.1. Phasing 11
2.2. Definition of Environments 14
2.3. Implementation Sites 14
2.4. Delivery Methodology 16
2.5. Milestones 19
3. REQUIREMENTS MANAGEMENT AND TRACEABILITY 22
3.1. High level ITM-RC1 Requirements 22
3.2. ITM-RC1 WP07 specific Requirements 22
4. DESIGN, IMPLEMENTATION AND INTEGRATION REQUIREMENTS 24
4.1. Introduction 24
4.2. Implementation Scope 24
4.3. Implementation principles 28
4.4. Generic Design and integration requirements for all Activity Groups 28
4.5. Critical Design Reviews 34
5. TRANSITION OF CAPABILITIES INTO OPERATIONS 36
5.1. Application Migration 36
6. SUPPORT TO PURCHASER ACTIVITIES 38
6.1. Supporting Mons AG1&AG2 Implementation 38
6.2. Supporting the Application Migration 39
6.3. Supporting the Enterprise SMC and Enterprise Cyber Security Integration 39
6.4. Supporting Purchaser Governance Meetings 39
6.5. Supporting the Integration with NATO Services 39
6.6. Supporting Purchaser Test and Acceptance Events 40
6.7. Early Life and O&M Support 40
6.8. Supporting Other Purchaser Activities 41
7. WORK PACKAGE MANAGEMENT 42
7.1. General Requirements 42
7.2. Implementation Methodology 42
7.3. Organisation 47
7.4. Work Package Management Processes 58
7.5. Project Management Communications 59
7.6. NATO Information Protection 64
7.7. Cyber Incident Reporting 64
8. CIS SECURITY ACCREDITATION 65
8.1. CIS Security Accreditation Requirements (NATO ON) 65
8.2. CIS Security Accreditation Requirements (Activity Group 1 and 2) 84
9. QUALITY ASSURANCE AND CONTROL 88
9.1. Definitions 88
9.2. Introduction 88
9.3. Roles and Responsibilities 88
9.4. Quality Management System (QMS) 90
9.5. Quality Assurance process 90
9.6. The Quality Assurance Plan (QAP) 91
9.7. Risks 91

9.8. Deficiencies 91
9.9. Support Tools 92
9.10. Certificates of Conformity 92

10. CONFIGURATION MANAGEMENT 93

10.1. General Requirements 93
10.2. Configuration Management Responsibility 93
10.3. Configuration Management Planning 94
10.4. Configuration Identification 94
10.5. Configuration Identification 96
10.6. Configuration Control 98
10.7. Configuration Status Accounting (CSA) 99
10.8. Configuration Verification and Audit 101

11. TEST AND ACCEPTANCE 104

11.1. Introduction 104
11.2. TV&V activities 104
11.3. Deliverables 112
11.4. Tools 118
11.5. TV&V Events and results 118
11.6. Test Defect Categorization 121

12. INTEGRATED PRODUCT SUPPORT (IPS) 124

12.1. Support Planning 124
12.2. Maintenance Support 124
12.3. Supply Support 125
12.4. Technical Manuals 128
12.5. Training 129

13. DOCUMENTATION MANAGEMENT 134

13.1. General Requirements 134
13.2. Project Management Documentation 137
13.3. Technical Documentation and Data 145

ANNEX A CIS PRINCIPLES AND MATURITY LEVELS 151

A.1. CIS Principles – Maturity Level per Activity Group 151

ANNEX B PURCHASER FURNISHED EQUIPMENT (PFE) AND PURCHASER FURNISHED INFORMATION (PFI) 155

B.1. Hardware 155
B.2. Virtualized Environment / NATO Public Cloud Services 156
B.3. Software Licenses 156
B.4. IT Equipment 156
B.5. List of PFE/PFI 158

ANNEX C CYBER SECURITY MONITORING IMPLEMENTATION 159

C.1. Introduction 159
C.2. NCSC Cyber Security Enclave Components Description 160
C.3. Specific Work to be carried out by the Contractor 163

ANNEX D REFERENCES AND APPLICABLE DOCUMENTS 174

D.1. References 174
D.2. Standardisation Agreements (STANAGS) .... **Error! Bookmark not defined.**
D.3. Allied Publications .... **Error! Bookmark not defined.**
D.4. Other NATO Documents 174
D.5. Non-NATO Standards 174
D.6. Security Documentation 174
D.7. NATO Security Accreditation Templates 175

List of Figures

Figure 1 - High-level Delivery Methodology 18
Figure 2 - ITM RC1 Requirements Landscape 22
Figure 3 - Incremental Development Process 44
Figure 4 - Roles and Responsibilities in the security accreditation process 66
Figure 5 - SAA approval of Security Accreditation Documentation 68
Figure 6 – IVV Documentation (Test Deliverables and products) 113
Figure 7 - Test Event timeline 114
Figure 8 - Product Quality Criteria 115
Figure 9 - Technical Documentation and Data 145
Figure 10 - CIS Principles Maturity Levels for Activity Groups (1/3) 152
Figure 11 - CIS Principles Maturity Levels for Activity Groups (2/3) 153
Figure 12 - CIS Principles Maturity Levels for Activity Groups (3/3) 154
Figure 13 - NCSC Cyber Security Monitoring Architecture 159
Figure 14 - Proposed ITM-R Enterprise Logging Architecture 163

List of Tables

Table 1 - Locations and Node Type per Activity Group and Spiral 16
Table 2 - Implementation Milestones per Activity Groups ..... **Error! Bookmark not defined.**
Table 3 - Milestones Achievement Criteria 21
Table 4 - Experience / Education substitution 48
Table 5 - Project Management Formal meetings 63
Table 6 - Security Accreditation Related Responsibilities 83
Table 7 - TV&V Phases 111
Table 8 - Definitions for Defect Categorization 122
Table 9 - Classification of defects based on severity 122
Table 10 - Priority Classes for Defect Classification 123
Table 11 - Defects Categories 123
Table 12 - Maturity level definitions 151
Table 13 – CIS Principles maturity level per Activity Group 151
Table 14 – PFE Hardware Baseline summary 155
Table 15 - PFE and PFI 158
Table 16- List of sites without an NCSC Cyber Security Enclave 163
Table 17 - Standard NCSC Enclave Equipment 165
Table 18 - Equipment to be installed at NATO HQ 165
Table 19 - Equipment to be delivered to the 3 signal battalion sites 166
Table 20 - Site to receive and FPC Upgrade 166
Table 21 - FPC Equipment to be installed at SJLSG HQ. 166
Table 22 – Network taps to be installed at DC locations. 167
Table 23 - NCDP Hosting Software 168

Table 24 - NCDP Virtual Machine Hosting Resources 168
Table 25 - Hosting Requirements for the Splunk virtual servers. 172

1. INTRODUCTION

1.1. Background

[0001] ITM Recovery Increment 1 (ITM-RC1) Work Package 07 (WP07): System Integration and Core Capabilities is an integral element of a larger effort within the scope of ITM-RC1 Project, and is responsible for the systems integration.

[0002] ITM-RC1 will enable the methods CIS services are provided to users across the NATO Enterprise by **modernizing, consolidating, and centralising** the infrastructure and service management, and by pooling and abstracting resources.

[0003] The objectives of the ITM-RC1 Project are to:

[0004] Create a flexible, agile, secure, resilient, and efficient NATO Communication and Information Systems (CIS) infrastructure that enables CIS Provider, the NATO Communications and Information (NCI) Agency, to provide the range of CIS services that are required by NATO Enterprise users.

[0005] Enable the NCI Agency to provide effective and cost-efficient Infrastructure as a Service (IaaS), Enterprise Core Services (ECS) and Client Provisioning Services (CPS) that:

A. Support end-user business continuity and disaster recovery needs, as defined in the Availability and IT Continuity of Services Model, Chapter 5 of the Architecture Design Package (ADP);

B. Provide increased operational flexibility and agility in handling changing demands for infrastructure services;

C. Provide increased service availability and resiliency that meets user needs and Service Level Agreements (SLA);

D. Delivers improvements to the CIS security posture;

E. Deliver efficient service fulfilment, which is measured and reported, yielding:

E.1. optimized total cost of ownership;

E.2. low provisioning times throughout the service lifecycle;

F. Enable enterprise level reporting of IaaS performance indicators and metrics to ensure requirements are being met and costs are tracked;

G. Increase user productivity;

H. Is fully conformant to enterprise architecture;

I. Will be implemented adhering to enterprise level IT governance;

[0006] The transformation will change the service operation model:

A. from the ‘AS-IS’ highly decentralized environment, with each location possessing their own networks, server rooms, Service Management & Control (SMC) capabilities, Service Desk and capability experts servicing solely the local user community;

B. to the ‘TO-BE’ target of a centrally managed IT infrastructure, providing services on standardized infrastructure, utilising automated provisioning, operated by two (site redundant) centralised, Enterprise Service Operations Centres (ESOC).

[0007] The transformation will allow services to be delivered according to standard and measurable SLA, offering a higher quality, more flexible, resilient, and secure set of services at significantly lower costs to the user community.

[0008] The work to be accomplished by ITM-RC1 is structured in several WPs that have interdependencies with each other. These interdependencies are outlined throughout this Statement of Work (SoW) where relevant.

1.2. Purpose

[0009] The purpose of the present contract is to outline the services and products for the Contractor to plan, coordinate, schedule, procure, implement, integrate and test the defined core capabilities and systems integration for ITM RC-1.

[0010] This present contract is established as an Indefinite Quantity (IDIQ) Contract that will activate Task Orders for the specific scope of work to be contracted as the project progresses.

1.3. WP07 High Level Scope

[0011] ITM-RC1 WP07 will implement a Software Defined Data Centre (SDDC) private cloud capability on NATO's Operational Network (ON). WP07 will improve, modernize and enhance the ON's predecessor, the current Bi-Strategic Commands (Bi-SC) Automated Information System (AIS) CIS environment.

[0012] NATO's ON refers to the new IT environment delivering IT services up to NATO S*CR*T (NS) level across the NATO enterprise, replacing the current Automated Information Systems (AIS) environment. The ADP [Ref: ITM-RC1 ADP] is the primary record of the NATO ON architecture for the NATO's ITM-RC1 solution.

[0013] WP07 utilizes purchaser furnished equipment (PFE) and purchaser furnished information (PFI) to build the before mentioned SDDC private cloud capability.

[0014] WP07 will perform the following high level activities within the scope of this contract:

- A. Work Package Management
- B. Design, Implementation and Integration:
  - B.1. Providing and maintaining the design artefacts in accordance with the detailed requirements in Section 4 Design, Implementation and integration requirements, Section 13 Documentation Management and Appendix 1 Solution Requirements Specifications (SRS).
  - B.2. Implementation (i.e. to plan, prepare, install, configure, integrate, test, deploy and transition to operations) of the following capabilities in accordance with Appendix 1 SRS Activity Group requirements:
    - B.2.A IaaS capability for the NATO ON
    - B.2.B CPS capability for the NATO ON
    - B.2.C ECS capabilities for the NATO ON
    - B.2.D Cyber Security Services for the NATO ON
    - B.2.E SMC Services for the NATO ON
    - B.2.F Automation and Orchestration
  - B.3. Implementation (i.e. to plan, design, prepare, install, configure, integrate, test, deploy and transition to operations) of the Cyber Security Monitoring capabilities in specified sites in accordance with Annex C.
- C. Transition of Capabilities into Operations
- D. Support to Purchaser Activities on Level of Effort (LoE) basis for different technical areas:
  - D.1. Supporting Purchaser implementation in Mons
  - D.2. Supporting the Application Migration
  - D.3. Supporting Purchaser Governance Meetings (e.g. NSAB)
  - D.4. Supporting the Integration with NATO Services
  - D.5. Supporting Purchaser Test and Acceptance Events

D.6. Providing Early Life and O&M Support

D.7. Other Purchaser Activities

[0015] This WP07 integrates the IaaS, ECS and CPS capabilities with hardware, software and licenses provided as PFE, unless otherwise specified; Cyber Security (CS) and SMC services on the basis of Interface Design Descriptions (IDDs).

1.4. Statement of Work (SoW) Organisation

1.4.1. Conventions for Interpretation of the SoW

[0016] The SoW is structured with two main styles of content:

A. Texts with prefix numbering [####] represents information, which is provided as background, information, or as context.

B. Texts with prefix "SOW-####" and any following listed items (.A, .B, .C, etc.), provided in numbered paragraphs are statements of requirements that shall be met by the Contractor. The order of the SoW requirements is not intended to specify the order in which they shall be carried out unless explicitly stated. The SoW defines the activities that the Contractor's process shall cover, where the Contractor's implementation plans determine the timing of detailed Contractor activities.

[0017] Terminology conventions in this document:

E. The term "**the Purchaser**" means the NCI Agency or its authorized representative(s).

F. The term "**the Contractor**" means the selected bidder.

G. The word "**shall**" in the text expresses a mandatory requirement. Departure from such a task is not permissible without formal written agreement between the Contractor and the Purchaser.

H. The expression "**shall not**" means that the definition is an absolute prohibition of the specification.

I. The word "**must**" in the text is used for legislative or regulatory requirements (e.g., Health and Safety) with which both the Purchaser and the Contractor shall comply.

J. The word "**should**" in the text means something that is strongly encouraged but not mandatory.

K. The word "**will**" in the text expresses a provision or service by the Purchaser or an intention by the Purchaser in connection with a requirement of the Contractor. The Contractor is implicitly authorized to rely on such service or intention.

L. Requirements stating a technical capability to be "**supported**" shall be understood as a feature or capability that shall be inherently available within the design and the assets in its full extent, without restrictions; that feature or capability can be enabled and disabled at any time by the Purchaser.

M. Requirements stating a technical capability to be "**implemented**" shall be understood as a feature or capability that shall be available within the design and the assets in its full extent, without restrictions; that feature or capability shall be delivered activated and configured for use in the delivered system and tested for compliance.

N. Whenever requirements are stated herein to "**include**" a group of items, parameters, or other considerations, "**include**" means "**include but not limited to**".

[0018] Whenever reference is made to a document section, tasks, or paragraph, the reference includes all subordinate and referenced paragraphs.

[0019] This SoW invokes a variety of Standard NATO Standardisation Agreements (STANAG), Allied Quality Assurance Publications (AQAPs), and Military Standards (MIL-STD). While

these are NATO reference documents, there are national and international standards that are considered to be equivalent and are cited as such within these documents.

[0020] Where a national or international standard exists that is not specifically referenced in the STANAGs or MIL-STDs as being equivalent, the Purchaser may refuse Contractor's proposal to use these standards instead of the STANAGs and MIL-STDs. The original required standard shall prevail regardless if the Purchaser has approved the usage of such an equivalent standard or not. i.e. it shall be at the Contractor's risk to ensure full equivalence, including cross-standard interdependencies and will be fully responsible for possible negative consequences of using the equivalent standard over the standard stated in the SoW.

1.4.2. Document structure

[0021] This SoW, including Annexes and Appendices, defines the general requirements for services and supplies provided under this Contract. It has a section for each relevant area of activity or requirements.

[0022] The following short summary provides an overview of what each section of the SoW, Annexes and Appendices contains:

1.4.2.1. SoW Main Body

A. **Section 1** Introduction: provides the background, vision, objectives and purpose of ITM project and high level scope of the WP07. It also provides a guideline of interpretation of the SoW and its sections

B. **Section 2** Work Package Implementation**:** covers the phasing approach of ITM-RC1 and WP07, definition of environments, list of implementation sites and delivery methodology for a generic understanding. It also includes the key milestones definitions with links to the delivery methodology.

C. **Section 3** Requirements Management and Traceability: describes the requirements management approach and landscape.

D. **Section** 4 Design, Implementation and integration requirements**:** contains general requirements pertaining how the design is to be undertaken and documented. It also covers overarching objectives and constraints and includes requirements for the design process and design deliverables, which have a direct link to Appendix 1 SRS and Section 13 Documentation .

E. **Section 5** Transition of capabilities into Operations**:** covers the requirements for 'release to operations', application migration, early life support and other support activities that will be required during the execution of this Contract.

F. **Section 6** Support to Purchaser Activities: describes the level of effort based support services that will be provided for Purchaser led activities during the implementation and O&M phase.

G. **Section 7** Work Package Management **:** contains management of the work package requirements, including Work Package Management Plan (WMP), Work Package Implementation Plan (WIP), Methodology, Organization, Work package Controls and Communication.

H. **Section 8** CIS Security Accreditation This section context includes ensuring that the ON conforms to NATO Security Policies and Directives and the ON-specific Security Accreditation Documentation Set.

I. **Section 9** Quality Assurance and Control: This section elaborates on process and set of procedures to ensure that a product or service adhere to defined set of quality criteria will meet specified requirements of the customer.

J. **Section 10** Configuration Management**:** This section outlines the process will enable the baselining and maintain of Configuration Items throughout the contract.

K. **Section 11** Test and Acceptance**:** contains requirements related to the planning and conduct of testing and acceptance procedures. There is a strong relationship to requirements in Section 5 (Implementation).

L. **Section 12** Integrated Product Support (IPS)**:** contains requirements for support planning and analysis, warranty, training, documentation and configuration management.

M. **Section 13** Documentation **:** summarises all of the requirements for documentation to be provided by the Contractor in all other sections of the SoW. It also contains additional requirements related to how the documents are to be formatted.

1.4.2.2. Sow Annexes

A. Annex A CIS Principles and Maturity Levels

B. Annex B Purchaser Furnished Equipment (PFE) and Purchaser Furnished Information (PFI)

C. Annex C Cyber Security Monitoring Implementation

D. Annex D References and Applicable documents

1.4.2.3. SoW Appendices

A. Appendix 1 : Solution Requirements Specifications (SRS)

B. Appendix 2 : Purchaser Furnished Information (PFI) Set

C. Appendix 3 : NATO Information Protection and Cyber Incident Reporting Requirements

D. Appendix 4: IDT Technical Interface Types

E. Appendix 5: Glossary of Abbreviations

F. Appendix 6: List of References and Applicable Documents

2. WORK PACKAGE IMPLEMENTATION

2.1. Phasing

[0023] ITM-RC1 is following a phased and parallel implementation approach dividing the activities into “Activity Groups” and locations in “Spirals” (e.g. the first 3 Activity Groups are executed in parallel for the sites in scope of Spiral 1.). Refer to Table 1 and **Error! Reference source not found.** below.

[0024] WP07 will follow this same phased and parallel implementation approach with “Activity Groups” and “Spirals”, as outlined in this Contract. Figure 1 - High-level Delivery Methodology depicts the high level scope of Work as outlined in this Contract.

[0025] The scope of work of this Contract will be implemented in ‘Task Order’ basis taking into account the Activity Group’s and the sites that will be implemented as per each Spiral.

2.1.1. Activity Group 1: Improve NS Bi-SC AIS

[0026] ITM-RC1 project focuses on delivering early benefits to the NCS through this phased implementation, by initially providing a standardized and aligned “SDDC ready[1]” infrastructure stack and software baseline, with central management and monitoring on hardware level, that can be re-used once the full SDDC private cloud will be implemented.

[0027] Implement infrastructure nodes in order to standardize and improve NS Bi-SC AIS focusing on delivering enhanced services which are a part of NATO ON foundation that will be augmented by Activity Group 4.

This Activity Group will reduce the need for further obsolescence mitigation activities for the current NS Bi-SC AIS infrastructure and provide central hardware management and an updated configuration management database (CMDB). This early benefit is delivered as part of an **Activity Group 1, namely ON Ready IaaS**.

[0028] This Activity Group executes the first step towards the target architecture and design of the NATO ON by implementing standardized IaaS nodes using defined building blocks (VSAN ready nodes, Spine/Leaf and OOB switches, Backup devices, Cisco ACI, Border Protection Devices) together with relevant orchestration and automation services as well as centralized management of the IaaS nodes.

2.1.2. Activity Group 2: End User Devices (Campus LAN and VDI)

[0029] An additional early benefit will be the improvement for the end-user interface by implementation and integration of new end-user devices using aligned and standardized client baselines for both thin and thick end-user devices, including the required back-end services for the desktop and application provisioning. This early benefit is delivered as part of **Activity Group 2, namely End User Devices (Campus LAN and VDI)** as part of NATO ON foundation which will be augmented by Activity Group 4.

[0030] Activity Group 2 deploys new Campus LAN service to the end users, new end user devices (to include an initial VDI (Virtual Desktop Infrastructure) capability for the sites which have this capability in scope) and the transition and migration for the end users who will receive the VDI end user devices.

[1] SDDC Ready: Hardware provided can be re-configured to be used in an SDDC configuration without the need to replace or modify the hardware.

2.1.3. Activity Group 3: Development of the new NATO ON multi-tenant private cloud

[0031] **Activity Group 3**, **namely ON DC Services**, aims to develop and validate the full ON SDDC Private Cloud solution, involving all aspects of people, processes and technology.

[0032] Activity Group 3 focuses on the implementation and configuration of the initial datacentre IaaS Nodes (starting with reduced capacity) to implement the NATO ON private cloud foundation.

[0033] This Activity Group will be executed as a Proof of Concept not connected to the NS. Once the Purchaser's requirements are proven to be met, and the solution has been accredited, there after the Contractor can start with Activity Group 4 implementation.

[0034] Activity Group 3 is the construction phase of the NATO ON and will be classified initially at the NATO UNCLASSIFIED (NU) / NATO RESTRICTED (NR) level and therefore leveraging the NU/NR NATO Communications Infrastructure (NCI), but isolated from any other production network. Successful completion of Activity Group 3 will be the prerequisite for start of the Activity Group 4.

[0035] Activity Group 3 aims to achieve the required maturity to establish the ON SDDC Private Cloud, involving all aspects of people, processes and technology.

2.1.4. Activity Group 4: Build out of the new NATO ON multi-tenant private cloud

[0036] **Activity Group 4, namely End-to-end (E2E) Services,** will integrate the full SDDC private cloud ON into production, merging with the products delivered by Activity Group 1 and 2.

[0037] Once Activity Group 3 has reached the required maturity to move into operations, Activity Group 4 includes all activities required to enable the NATO ON services on the NS network. Activity Group 4 also includes integration and/or transition of services and capabilities previously delivered in Activity group 1 and 2 in order to deliver the fully integrated NATO ON.

[0038] Depending on the required changes in Activity Group 4, the transition activities to bring sites with a baseline received at Activity Group 1 and 2 to the new target baseline may be significant.

2.1.5. Activity Group 5: Education, Training, Exercise and Evaluation (ETEE) Environments and VDIs

[0039] **Activity Group 5** will implement separate tenants for Education, Training, Exercise Evaluation (ETEE) on the NATO ON at two locations.

[0040] Under the ITM architecture there is next to the ON, a special purpose network in support of the ETEE Communities hosted in JWC Stavanger, Norway and JFTC Bydgoszcz, Poland.

[0041] The ETEE environments are in addition to the ON Enhance Node (EN), as described in Section 2.2, Infrastructure Nodes that shall be provided to these locations.

[0042] The ETEE environments in scope of WP07 are divided in 2 classifications:

A. ETEE@NS: This environment will have the ability to prepare and conduct NATO training and exercises over the ON. The ETEE@NS is a separate tenant that will consume the same management services from the Activity Group 3 and Activity Group 4.

B. ETEE@MS (MISSION S*CR*T): This environment is also referred to as the "NS Releasable To" Exercise environment when involved in a NATO led mission. This environment will have the ability to prepare and conduct NATO training and

exercises at MS classification level. This environment is physically isolated from the ON hence hardware between the ON and ETEE@MS cannot be shared. There is an existing BPD gateway between ON and ETEE@MS that allows for traffic for limited services. It is foreseen that a separate management environment is required for this.

[0043] Both environments make maximum use of VDI to support the training audiences.

[0044] The concept of operations for these environments is to frequently build up, deploy and teardown complete tenants in support of training and exercises, therefore the automation and orchestration is a key enabler.

2.2. Definition of Environments

SOW-0001 The Contractor shall provide the design, implementation and integration activities within the scope of this Contract at the following types of environments:

SOW-0001.A Datacentre (DC) Node: Key centralised location where the bulk of computing will take place, and from where functional application services (FAS) are centrally hosted for the enterprise.

SOW-0001.B Enhanced Node (EN): Location with enhanced computing capabilities in order to support FASs that will not be centralized for technical or other reasons.

SOW-0001.C Standard Node (SN): Location with limited amount of computing capabilities providing core services supporting user access.

SOW-0001.D Remote Nodes (RN): User location with a limited number of users, which will only contain client devices and campus LAN. Core services and FASs are provided from the DC locations. There will be no IaaS deployment in the Remote nodes.

SOW-0001.E ITM Reference Environments (IREEN): NATO ON Reference Environments operating both at NU and NS to support the life cycle management of the NATO ON services as further described in 4.2.6.

SOW-0001.F For solution requirements, the Contractor shall read ‘implement’ as ‘design, define, create, implement, configure, install, integrate, test and deploy to the relevant environments’. For efficiency, the requirements group these activities under ‘implement’ task.

2.3. Implementation Sites

SOW-0002 Table 1[2] below shows the sites, Spirals, and the Activity Group that they are affected by. In defining the site-specific parameters during implementation, the Contractor shall use the site specific data provided by the Purchaser.

Activity Group[3]	Spiral	Site ID	Site Name	Location	Node Type//Environment	VDI
1,2	1	BEL-CAS-01	Camp Casteau / SHAPE Barracks	Mons, Belgium	Infra Node ON EN User Node ON ESOC ON	Yes
4	4					
1,3	1	BEL-BRU-01	NATO HQ	Brussels, Belgium	Infra Node ON DC (including IREEN ON@NS)	No
4	4					
1,2,3	1	ITA-LAG-01	NATO Base/ Lago Patria	Naples, Italy	Infra Node ON DC User Node ON	Yes
4	4					
1,2,3	1	NLD-DEN-01	NCI Agency/ The Hague	The Hague, Netherlands[4]	Infra Node ON Reference (IREEN ON@NU)	No
4	4					
1,2	2	NLD-BRU-01	Hendrick Barracks	Brunssum, Netherlands	Infra Node ON EN User Node ON ESOC ON	No
4	4					
1,2	2	POL-BYD-01	Szubinska 3	Bydgoszcz, Poland	Infra Node ON EN	Yes

[2] Sites that will have the Cyber Security Monitoring implemented is described in Annex C.
[3] As part of the Activity Group 3 Proof of Concept, an interim EN infrastructure configuration will be utilized for testing purposes, which will be provided as PFE.
[4] The environment is aimed to be composed of on-premise infrastructure hardware and NATO Public Cloud Services (based on existing accredited NATO Software Factory services) operating at NU.

Activity Group[3]	Spiral	Site ID	Site Name	Location	Node Type//Environment	VDI
4	4				User Node ON Infra Node ON ETEE User Node ON ETEE	
5	5					
1,2	2	DEU-GEI-01	NATO Air Base Teveren Geilenkirchen	Geilenkirchen, Germany	Infra Node ON EN User Node ON	No
4	4					
1,2	2	TUR-IZM-01	General Vecihi Akin Garrison	Izmir, Türkiye	Infra Node ON EN User Node ON	No
4	4					
1,2	2	USA-NOR-01	NSA Hampton Roads, Suite 100	Norfolk, United States of America	Infra Node ON EN User Node ON	Yes
4	4					
1,2	2	GBR-NOR-01	Northwood HQ	Northwood, United Kingdom	Infra Node ON EN User Node ON	No
4	4					
1,2	2	DEU-RAM-01	Ramstein Air Base	Ramstein, Germany	Infra Node ON EN User Node ON	Yes
4	4					
1,2	2	ITA-LEN-01	Naval Air Station Sigonella	Sigonella, Italy	Infra Node ON EN User Node ON	No
4	4					
1,2	2	NOR-STA-01	Jatta Barracks	Stavanger, Norway	Infra Node ON EN User Node ON Infra Node ON ETEE User Node ON ETEE	Yes
4	4					
5	5					
1,2	2	DEU-ULM-01	Wilhelmsburg Barracks	Ulm, Germany	Infra Node ON EN User Node ON	Yes
4	4					
1,2	3	POL-BYD-02	Szubinska 105	Bydgoszcz, Poland	Infra Node ON SN User Node ON	No
4	4					
1,2	3	PRT-LIS-01	Avenida Tenente Martins	Lisbon, Portugal	Infra Node ON SN User Node ON	No
4	4					
1,2	3	ITA-POG-01	Poggio Renatico Air Base	Poggio Renatico, Italy	Infra Node ON SN User Node ON	No
4	4					
1,2	3	ESP-TOR-01	Torrejon Air Base	Torrejon, Spain	Infra Node ON SN User Node ON	No
4	4					
1,2	3	DEU-UED-01	Paulsberg Barracks	Uedem, Germany	Infra Node ON SN User Node ON	No
4	4					
1,2	3	ITA-GRA-01	Grazzanise Air Base	Grazzanise, Italy	Infra Node ON SN User Node ON	No
4	4					
1,2	3	DEU-WES-01	Schill Barracks	Wesel, Germany	Infra Node ON SN User Node ON	No
4	4					
2	3	GBR-BLA-01	Blandford Camp	Blandford, United Kingdom	User Node ON (RN)	No
4	4					
2	3	ROU-BUC-02	HQ Air Force Staff Barracks	Bucharest, Romania	User Node ON (RN)	No
4	4					
2	3	DNK-HAD-01	Haderslev Barracks	Haderslev, Denmark	User Node ON (RN)	No
4	4					

Activity Group[3]	Spiral	Site ID	Site Name	Location	Node Type//Environment	VDI
2	3	TUR-KON-01	Konya Air Base	Konya, Türkiye	User Node ON (RN)	No
4	4					
2	3	CZE-LIP-01	Hranicka Barracks	Lipnik nad Becvou, Czech Republic	User Node ON (RN)	No
4	4					
2	3	NOR-ORL-01	Main Air Station Orland	Oerland, Norway	User Node ON (RN)	No
4	4					
2	3	HRV-PLE-02	Marko Zivkovic Barracks	Pleso, Croatia	User Node ON (RN)	No
4	4					
2	3	GRC-PRE-01	Aktion National/Lefkada Airport	Preveza, Greece	User Node ON (RN)	No
4	4					
2	3	SVK-RUZ-01	Zarevuca Barracks	Ruzomberok, Slovakia	User Node ON (RN)	No
4	4					
2	3	BGR-GOR-01	Camp Gorna Malina	Gorna Malina, Bulgaria	User Node ON (RN)	No
4	4					
2	3	HUN-SZE-01	Zamolyi Barracks	Szekesfehervar, Hungary	User Node ON (RN)	No
4	4					
2	3	ITA-TRA-01	Airport Vincenzo Florio	Trapani, Italy	User Node ON (RN)	No
4	4					
2	3	LTU-VIL-04	Kairiukscio Barracks	Vilnius, Lithuania	User Node ON (RN)	No
4	4					

Table 1 - Locations and Node Type per Activity Group and Spiral

2.4. Delivery Methodology

SOW-0003 The Contractor shall deliver the products and services outlined in this Contract via Task Orders, which may be contracted for one or more of the following services in a series of Task Orders:

SOW-0003.A Design

SOW-0003.B Implementation – Agile Sprints

SOW-0003.C Implementation – Cyber Security Monitoring

SOW-0003.D Support to Purchaser Activities

SOW-0004 For ‘Design’ activities, the Contractor shall implement ‘Design Sprints’ and achieve the successful completion of Critical design Review(s) as described in Critical Design Reviews in Section 4.5.

SOW-0005 For implementation of the ‘Agile Sprints’, the Contractor shall follow a hybrid of agile and waterfall approach as listed below:

SOW-0005.A Agile approach for the design, implementation and integration of the Activity Group requirements (Appendix 1 SRS) including the relevant testing activities, update and release of the documentation

SOW-0005.B Waterfall approach for the Procurement, Security Audits, Training, Transition to Operations with relevant testing activities and Transition to Services with relevant testing activities

[0045] The Purchaser aims to cover approximately three agile implementation sprints for each task order, reserving the right to contract less or more sprints in a certain Task Order throughout the execution. Detailed requirements and explanations can be found in Section 7.2.

SOW-0006 For the implementation of the Cyber Security Monitoring requirements (Annex C), the Contractor shall follow the waterfall methodology for following activities:

- SOW-0006.A Procurement
- SOW-0006.B Design, Implementation and Integration
- SOW-0006.C Security Accreditation
- SOW-0006.D Transition to Operations with relevant testing activities
- SOW-0006.E Transition to Services with relevant testing activities
- SOW-0006.F Training

SOW-0007 Figure 1 - High-level Delivery Methodology describes the high level delivery and implementation methodology for the project.

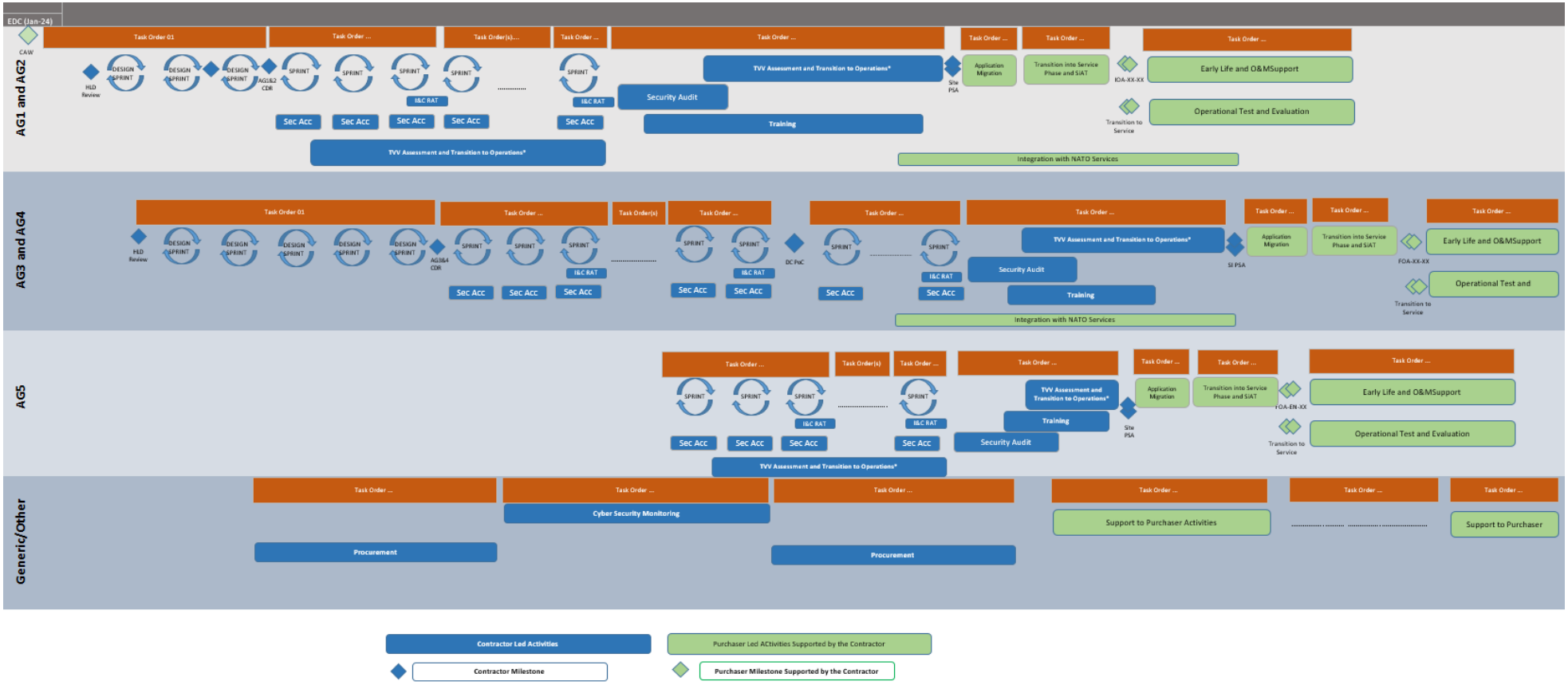

Figure 1 - High-level Delivery Methodology

2.5. Milestones

SOW-0008 The Purchaser has defined in Table 2 - Milestones Achievement Criteria a set of site implementation milestones, which shall be included in the Contractor's WIP as described in section 13.2.1.2 and will be tracked throughout project execution.

SOW-0009 To ensure completion of relevant milestones, the Contractor shall complete the implementation of all requirements in a given Activity Group within the number of estimated Sprints identified in Section 7.2.1.2 Execution of the Agile Process, via assigning adequate number of requirements in each Sprint.

SOW-0010 The Contractor shall ensure following criteria has been successfully satisfied with Purchaser approval for each element, as a prerequisite for the achievement of the relevant milestone:

Milestone	Applicability	Milestone Type	Milestone Achievement Criteria[5]
Critical Design Review (CDR)	• CDR - AG1 & AG2 • CDR - AG3 & AG4 & AG5	• Contractor Milestone	• Completion of the assessment and update of the High level Design (HLD) elements • Completion of creation of Low Level Design (LLD) elements • Completion of the CDR meetings • Purchaser acceptance of the design and documentation
Site PSA	• Site PSA – ENXX – AG1 • Site PSA – ENXX – AG2 • Site PSA – SNXX – AG1 • Site PSA – SNXX – AG2 • Site PSA – RNXX – AG1 • Site PSA – RNXX – AG2 • Site PSA – IREEN ON@NU • Site PSA – Cyber Security Monitoring – XX	• Contractor Milestone	• Completion of the implementation of relevant Activity Group SRS requirements as per the design OR Completion of the implementation of Cyber Security Monitoring requirements • Completion of Intermediate & Candidate Acceptance Tests • Completion of the Testing, Verification and Validation (TVV) Assessment Phase • Completion of inputs for security accreditation documentation and approvals • Completion of activities required for Security Audits and achievement of Interim Security Accreditation (ISA) • Completion of 'Transition to Operations' • Purchaser acceptance of the implemented system and documentation For IREEN ON@NU, • Completion of the implementation of relevant Activity Group SRS requirements for IREEN @NU • Completion of the development and implementation of the automation and orchestration capability (ready for further usage in implementation of Activity Group 1, 2, 3, 4 and 5 requirements) • Completion of Intermediate & Candidate Acceptance Tests • Completion of inputs for security accreditation documentation and approvals

[5] Security Audits and Interim Security Accreditation (ISA) will be performed if and when requested by the Security Accreditation Authority (SAA).

Milestone	Applicability	Milestone Type	Milestone Achievement Criteria[5]
			• Purchaser acceptance of 'Automation and Orchestration SW, tools and processes' are accepted by the Purchaser • Purchaser acceptance of the implemented system and documentation
(Site) IOA	• IOA – ENXX – AG1 • IOA – ENXX – AG2 • IOA – SNXX – AG1 • IOA – SNXX – AG2 • IOA – RNXX – AG1 • IOA – RNXX – AG2	• Purchaser Milestone supported by the Contractor	• Achievement of the relevant Site PSA • Completion of support for the Purchaser led Application Migration and User Transition • Completion of inputs for security accreditation documentation and approvals • Completion of activities required for Security Audits and achievement of Interim Security Accreditation (ISA) • Completion of support for the 'Transition into Service' and Site Acceptance Tests (SiAT) • 'Operational User' acceptance of the implemented system and documentation
Proof of Concept	• Proof of Concept - DC	• Contractor Milestone	• Completion of the implementation of relevant Activity Group 3 SRS requirements as per the design including IREEN ON@NS • Completion of Intermediate & Candidate Acceptance Tests • Completion of the Testing, Verification and Validation (TVV) • Assessment Phase • Completion of inputs for security accreditation documentation and approvals • Completion of activities required for Security Audits and achievement of Interim Security Accreditation (ISA) • Purchaser acceptance of the implemented system and documentation
System Integration (SI) PSA	• SI PSA – DC1 • SI PSA – DC2	• Contractor Milestone	• Achievement of Proof of Concept - DC • Completion of the implementation of relevant Activity Group 4 SRS requirements as per the design including IREEN ON@NS • Completion of Intermediate & Candidate Acceptance Tests • Completion of the Testing, Verification and Validation (TVV) • Assessment Phase • Completion of inputs for security accreditation documentation and approvals • Completion of activities required for Security Audits and achievement of Interim Security Accreditation (ISA) • Completion of 'Transition to Operations' • Purchaser acceptance of the implemented system and documentation
(Site) FOA	• FOA – ENXX – AG1 • FOA – ENXX – AG2 • FOA – SNXX – AG1	• Purchaser Milestone	• Achievement of the SI PSA and relevant Site IOA(s) • Completion of the implementation of relevant Activity Group 4 SRS requirements as per the design

Milestone	Applicability	Milestone Type	Milestone Achievement Criteria[5]
	• FOA – SNXX – AG2 • FOA – RNXX – AG1 • FOA – RNXX – AG2	supported by the Contractor	• Completion of support for the Purchaser led Application Migration and User Transition • Completion of inputs for security accreditation documentation and approvals • Completion of activities required for Security Audits and achievement of Interim Security Accreditation (ISA) • Completion of support for the 'Transition into Service' and Site Acceptance Tests (SiAT) • 'Operational User' acceptance of the implemented system and documentation
FSA	• FSA	• Purchaser Milestone supported by the Contractor	• Achievement of all FOAs for each site as well as the remediation of any deficiencies. • Completion of all deliverables (technical, documentation, training, support, accreditation, etc.) • 'Operational User' acceptance of the implemented system and documentation

Table 2 - Milestones Achievement Criteria

3. REQUIREMENTS MANAGEMENT AND TRACEABILITY

[0046] In this section, ITM-RC1 WP07 requirements management and traceability is detailed.

SOW-0011 The Contractor shall follow the ITM-RC1 project Requirements Management and Traceability approach [Ref: ITM-RC1 RMTA].

SOW-0012 The Contractor shall be responsible for maintaining the requirements artefacts and traceability relationships in the specified tools, as detailed in this section.

[0047] The ITM RC1 Requirements Landscape, applicable to the ITM-RC1 and WP07, is depicted in Figure 2:

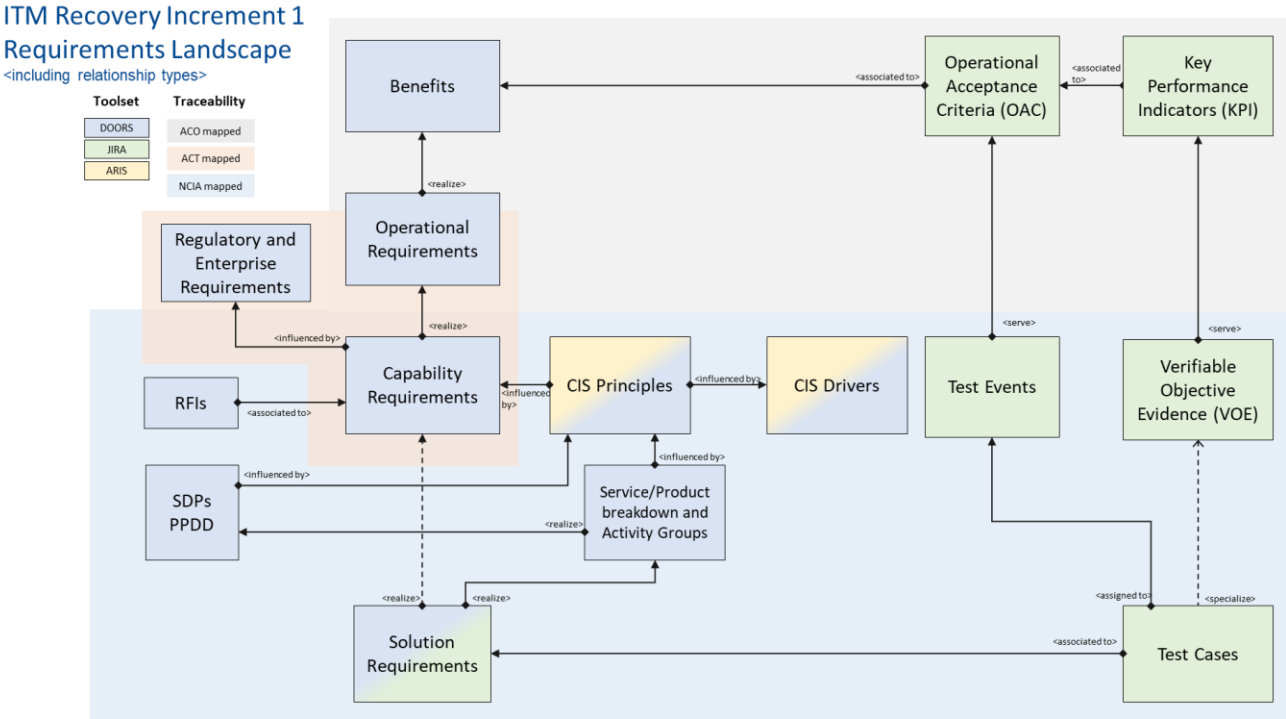

Figure 2 - ITM RC1 Requirements Landscape

3.1. High level ITM-RC1 Requirements

[0048] High level overall ITM RC1 Requirements are stated by the Commands in the form of Operational and Capability Requirements, supported by the SOR/MER 21 detailed requirements.

[0049] High level requirements and their traceability relationships are modelled and managed in the NCI Agency Requirements Repository (DOORS), as depicted in Figure 2. Extracts from these requirements artefacts in DOORS are available in Excel and Word formats.

3.2. ITM-RC1 WP07 Specific Requirements

SOW-0013 The Contractor shall design, implement and integrate the solution requirements stated in Appendix 1 SRS, which also includes system requirements specifications when applicable. The complete Solution Requirements initial baseline is documented in the NCI Agency Requirements Repository (DOORS).

SOW-0014 The Contractor shall maintain the Product Backlog and the traceability relationships between the Product Backlog items, throughout the project execution, documenting and updating the requirements as part of the Task Order and Sprint planning(s).

SOW-0015 The Contractor shall maintain traceability from the implemented baseline to all of the requirements of this SoW through the traceability matrix (see Section 11.3.5).

SOW-0016 The Contractor shall produce and maintain, throughout the project execution, the following Requirements Traceability Matrix (RTM) views:

SOW-0016.A In JIRA, Verification artefacts (i.e. Test Cases and Acceptance Criteria) linkage to the applicable Solution Requirements.

SOW-0016.B In DOORS, Design artefacts linkage to the applicable Solution Requirements (e.g. update links after changes in the SDPs, or build the links to the related Solution Requirements once a new Design artefact has been created).

SOW-0017 The Purchaser will provide the Contractor with the NR classified laptop(s), otherwise called REACH, as PFE including DOORS and JIRA for requirements management and traceability activities.

SOW-0018 The Contractor shall provide extracts of the RTM views in the original file format and MS Excel compatible formats.

SOW-0019 The Contractor shall follow the requirements related to RTM in accordance with Section11.3.5.

4. DESIGN, IMPLEMENTATION AND INTEGRATION REQUIREMENTS

4.1. Introduction

[0050] This section describes the Contractor's design task and integration activities in more detail in terms of the objectives to be attained, the constraints to be observed, the process to be followed and the deliverables to be produced.

[0051] The implementation approach outlines “Activity Groups” and associates the breakdown of the ON capabilities that shall be achieved, allowing development and implementation activities to be separated in manageable increments.

[0052] The Activity Groups have as goal to improve the expected level of service maturity at a site. CIS Principles with maturity and implementation are defined in Annex A.

SOW-0020 Maturity levels shall be used as a target to the expected maturity levels to be delivered.

[0053] Generic requirements which apply to site implementation activity at all sites regardless of designation as ESOC, DC, EN, SN or RN is described in Section 4.

SOW-0021 The Contractor shall take these generic requirements into account during the implementation of each Agile Sprint for the design, implementation and integration of the selected set of Appendix 1 SRS requirements.

SOW-0022 The Contractor shall design, implement and integrate all the applicable technical interfaces in each Sprint, in accordance with the selected set of Appendix 1 SRS requirements from the Product Backlog.

SOW-0023 The Contractor shall design, implement and integrate the Cyber Security Monitoring in accordance with the requirements specified in Annex C.

4.2. Implementation Scope

[0054] This section summarizes the overall implementation scope of the deliverables by the Contractor.

SOW-0024 In accordance with this SoW, during the Implementation the Contractor shall:

- SOW-0024.A Review the requirements, and update the HLD/LLD design as necessary
- SOW-0024.B Implement all of the functionality required;
- SOW-0024.C Implement the performance levels required;
- SOW-0024.D Implement all of the interfaces required;
- SOW-0024.E Implement all of the services required.
- SOW-0024.F Perform all the tests described in Section 11 to confirm the completeness that solution meets planned requirements.
- SOW-0024.G Provide all relevant security accreditation inputs.
- SOW-0024.H Update all the relevant documentation and data in frequent intervals

SOW-0025 Based upon the approved design documentation and the provided PFE/PFI (Hardware/Software licences), the Contractor shall execute system implementation and integration of the IaaS, ECS and CPS capabilities and integrate these with the Enterprise Cyber Security Services and Enterprise SMC services to establish both the NATO ON operating at NS and the reference environment IREEN ON@NU operating at NU.

SOW-0026 The Contractor shall maintain Change Control, Release and Configuration Management (CI, Service tree, Service) for the deliverables of WP07 throughout the life of the project. This shall include the PFE if any changes made directly by the Contractor in agreement with the Purchaser.

SOW-0027 The Contractor shall define and establish DevOps lifecycles (tools, process) and use automation and orchestration to implement and deliver the system in scope of the contract. This capability (technology, people/roles, process) will be transitioned to the Purchaser for continued service delivery.

SOW-0028 The Contractor shall cooperate with the Purchaser team(s) and third parties as directed by the Purchaser as necessary for the implementation activities.

4.2.1. IaaS

SOW-0029 The Contractor shall plan, prepare, install, configure, integrate, test and transition into operations, all the required elements to successfully implement the IaaS capability, for which specific hardware, software and licenses6 will be provided by the Purchaser as PFE. The infrastructure services shall include:

SOW-0029.A Infrastructure Cyber Security Services;

SOW-0029.B Infrastructure Domain SMC Services;

SOW-0029.C Infrastructure Processing Services;

SOW-0029.D Infrastructure Storage Services;

SOW-0029.E Infrastructure Archive Storage Services;

SOW-0029.F Backup and Recovery Services;

SOW-0029.G Infrastructure Networking Services.

[0055] Further requirements for IaaS are detailed in Appendix 1 SRS and the IaaS SDP [Ref: ITM-RC1 SDP IAAS].

4.2.2. CPS

SOW-0030 The Contractor shall plan, prepare, install, configure, integrate, test and transition into operations, all the required elements to successfully implement **CPS**, for which specific hardware, software and licenses[6] will be provided by the Purchaser as PFE. The CPS shall include the following services:

SOW-0030.A Desktop Provisioning Services;

SOW-0030.B Application Provisioning Services;

SOW-0030.C User Profile Services;

SOW-0030.D Client Provisioning Domain SMC Services

SOW-0030.E Print and Scan Services;

SOW-0030.F Campus LAN Services.

SOW-0030.G Client Provisioning Cyber Security Services

[0056] Further requirements for CPS are detailed in Appendix1 SRS and the CPS SDP [Ref: ITM-RC1 SDP CPS].

4.2.3. ECS

SOW-0031 The Contractor shall plan, prepare, install, configure, integrate, test and transition into operations, all the required elements to successfully implement **ECS**, for which specific hardware, software and licenses will be provided by the Purchaser as PFE. The ECS shall include the following services:

SOW-0031.A Directory Services;

SOW-0031.B Email Messaging Services;

SOW-0031.C Portal Services;

SOW-0031.D Unified Communication Services;

SOW-0031.E Database Platform Services.

SOW-0031.F Core Services Cyber Security Services

SOW-0031.G Core Services Domain SMC Services

[0057] Further requirements for ECS are detailed in Appendix1 SRS and the ECS SDP [Ref: ITM-RC1 SDP ECS].

4.2.4. Cyber Security Services

SOW-0032 The Contractor shall plan, prepare, install, configure, integrate, test and transition into operations, all the required elements to successfully implement **CS** Services. The Cyber Security services shall include the following services:

SOW-0032.A Cyber Security Monitoring;

SOW-0032.B Privileged Access Management;

SOW-0032.C Enterprise Logging;

SOW-0032.D Data Diode

SOW-0032.E User and Device Credentials.

SOW-0032.F Gateway to External CIS

[0058] Further requirements for Cyber Security Services are detailed in Appendix 1 SRS and Annex C Cyber Security Monitoring.

4.2.5. SMC Services

SOW-0033 The Contractor shall plan, prepare, install, configure, integrate, test and transition into operations, all the required elements to successfully implement the **SMC** Services.

SOW-0034 The Contractor shall implement domain and element SMC for IaaS, CPS and ECS.

SOW-0035 The Contractor shall integrate the Domain SMC services with the following Enterprise SMC services:

SOW-0035.A Enterprise SMC Request Management Services;

SOW-0035.B Enterprise CI Discovery and CMDB Services;

SOW-0035.C Enterprise SMC Access Management Services;

SOW-0035.D Enterprise Monitoring and Management Services;

SOW-0035.E Enterprise Orchestration and Automation Services;

SOW-0035.F Electronic DML Services.

SOW-0036 The Contractor shall refer to the SMC SDP [Ref: ITM-RC1 SDP SMC] for the technical service topology and HLD of the SMC components.

[0059] Further requirements for SMC are detailed in Appendix 1 SRS and the SMC SDP [Ref: ITM-RC1 SDP SMC].

SOW-0037 The Contractor shall provide additional support to WP11 Enterprise SMC for any services provided, as required throughout the project lifecycle, Level of Effort (LoE) basis.

4.2.6. Data Diode as a Service (DDaaS)

SOW-0038 The Contractor shall design and implement the Data Diode as a Service in order to support one way data transfers, between lower classification networks (NU/NR) to NS, required for ECS, CPS, IaaS, SMC, Cyber Security services.

SOW-0039 The Contractor shall transition existing Data Diode information transfer for ECS, CPS, IaaS, Cyber Security to the new Data Diode Service.

SOW-0040 The Contractor shall transition existing Data Diode information transfer required to support reference environments, including NATO Software Factory (NSF) aspects used as part of the reference environment further described in 4.2.7.

SOW-0041 The Contractor shall support the transition of Functional Services to the new Data Diode Service.

SOW-0042 The Contractor shall design, implement and configure the Border Protection Devices (BPD) for data diode as a service as described in the IaaS SDP [Ref: ITM-RC1 SDP IAAS].

[0060] In order to continuously monitor the security compliance posture of the NATO ON CIS, IAAS SDP [Ref: ITM-RC1 SDP IAAS] includes compliance dashboards to be deployed and used as part of the design objective.

[0061] Further requirements for DDaaS are detailed in Appendix 1 SRS.

4.2.7. IREEN

[0062] The Purchaser will have one reference environment established operating at NS (IREEN ON@NS) and one reference environment operating at NU (IREEN ON@NU).

[0063] The intent of the Purchaser is to utilize the IREEN environments for formal Verification and Validation (V&V) process and as part of DevOps Continuous Deployment lifecycles:

A. IREEN ON@NU: Reference environment of the NATO ON operating at NU. IREEN ON@NU is composed of on-premise infrastructure hardware and NATO Public Cloud Services, based on NATO Software Factory, operating at NU. It is used to develop and test the automation and orchestration.

A.1. The NATO Public Cloud Services are based on the NATO Software Factory (NSF) [0278], which is NCI Agency 'Development and Integration Environment', in order to develop and test software based components and is currently accredited at NU.

A.2. On-premise Hardware are to be leveraged for developing and testing the automated deployment and change management of hardware related components.

B. IREEN ON@NS: Pre-production tenant, allows a release to be deployed on an environment that is not production, but integrated with production in order to maximize similarity, and minimize the risk of a failed release. This is used as the last step before release in operation.

[0064] The hardware with the associated infrastructure licenses (excluding automation and orchestration tools described in 4.4.4) for IREEN and therefore NATO Public Cloud Services will be provided to the Contractor as PFE.

SOW-0043 The Contractor shall establish IREEN ON@NU and IREEN ON@NS environments to support the development and implementation of automation and orchestration and the associated CD/CI pipelines.

SOW-0044 The Contractor shall use the product release processes/procedures and technology environment, from the very first deployment until FOA.

[0065] Further requirements for IREEN are detailed in Appendix 1 SRS and PPDD.

4.3. Implementation principles

4.3.1. General Implementation Principles (GIP)

SOW-0045 The Contractor shall follow the General Implementation Principles (GIP) intended for any new implementation of systems and services:

SOW-0045.A [GIP-1] Bring value as early as possible by focusing on an incremental implementation (small set of working capabilities as opposed to many unusable capabilities);

SOW-0045.B [GIP-2] Prioritize security baselines/hardening for both configurations and procedures.

SOW-0045.C [GIP-3] Automate testing and verifications, to improve confidence that changes are not affecting negatively operational services, and to provide automated compliance reports;

4.3.2. Infrastructure Implementation Principles (IIP)

SOW-0046 The Contractor shall follow the Infrastructure Implementation Principles (IIP) intending to optimise the implementation and lifecycle management of services:

SOW-0046.A [IIP-1] Leverage the provisioning and managing the IT Infrastructure using code through resource pooling, software-defined intelligence and unified API's, commonly referred to in industry as "Infrastructure as a Code";

SOW-0046.B [IIP-2] Every change shall be under automated version control;

SOW-0046.C [IIP-3] Allow for the execution of small and frequent changes over big and complex changes;

SOW-0046.D [IIP-4] Automate deployments to allow reuse, rebuild and automated service fulfilment;

SOW-0046.E [IIP-5] Verify and validate possible changes of the production environment via the reference environment.

4.3.3. Infrastructure Implementation Constraints (IIC)

SOW-0047 The Contractor shall take into account the Infrastructure Implementation Constraints (IIC) which are applicable to NATO and affect any integration or implementation planning.

SOW-0047.A [IIC-1] Security accreditation procedures and timeline shall be taken into account in order to define the implementation phases;

SOW-0047.B [IIC-2] Implementation approach shall be flexible to adapt to potential non-readiness of physical facilities and their associated elements (e.g. security controls, manpower etc.) at some sites;

SOW-0047.C [IIC-3] The infrastructure services to be implemented depends on existing operational services and the implementation approach shall avoid operational disruptions.

4.4. Generic Design and integration requirements for all Activity Groups

4.4.1. Design documentation and sources

[0066] The Purchaser is providing the Contractor with the PPDD, describing extensively the target design, including how systems and components should be implemented and integrated. The Purchaser will provide the latest version of PPDD at EDC.

SOW-0048 The Contractor shall make use of the existing PPDD, and update it as needed in order to successfully implement and integrate the systems to delivers the IaaS, CPS, ECS and SMC systems and services.

[0067] The implementation will be performed in Activity Groups as described in paragraph 2.1.

SOW-0049 The Contractor shall include all the interfaces towards IaaS, ECS, CPS, Cyber Security, Enterprise SMC, and other NATO Services, a list of required interfaces are included in the IDT [Ref: ITM-RC1 IDT]. The interface type shall be detailed in an Interface Definition Documents (IDDs) and each interface instance shall be documented in an Interface Control Documents (ICDs). The template for ICDs will be provided by the Purchaser at EDC.

[0068] The Design and Implementation requirements for each Activity Group are listed in the paragraphs below and Appendix 1 SRS, the sites per Activity Group and spiral are listed in Table 1. The overall schedule per Activity Group and spiral is listed in **Error! Reference source not found.**.

SOW-0050 The Contractor shall ensure and demonstrate that the delivered systems and capabilities are compliant with the System Requirement Specifications (SRS) and the updated (and approved by the Purchaser) detailed design and as-built documentation.

4.4.2. Technical Interfaces

SOW-0051 The Contractor shall implement interfaces as part of its System Integration role, as detailed in Section 5. The interface types with the related activities for the Contractor are as follows:

SOW-0051.A **Type A** interfaces: Between two services delivered by the Contractor. The Contractor shall deliver the ICDs and IDDs. The Contractor shall define, implement, integrate and test the interface.

SOW-0051.B **Type B** interfaces: Between a service delivered by the Contractor and a service delivered through another WP.
The Contractor shall deliver the ICDs and IDDs. The Contractor shall define, implement, integrate and test the interface in cooperation with the other Work Package teams.

SOW-0051.C **Type C** interfaces: Between a service delivered by the Contractor and a legacy (AIS) service.
The Contractor shall deliver the ICDs and IDDs. The Contractor shall define, implement, integrate and test with the Purchaser's existing services interfaces.

SOW-0052 The Contractor shall design, implement and test all interfaces of type A, B and C that are listed in the PFI Interface Definition Table (IDT) [Ref: ITM-RC1 IDT] and in Appendix 4 for IaaS, ECS, CPS, SMC, CS, and others.

[0069] The Purchaser will provide the following IDD's to constitute an example for the template, scope and level of details covered:

A. IDD-Data Diode as a Service

B. IDD-DLP Discovery

SOW-0053 The Contractor shall document the interfaces implemented in ICD provided by the Contractor as part of the as built documentation.

[0070] The following interface types identified in the IDT are out of scope for the WP07 Contractor :

A. **Type D** interfaces: Between services delivered by other WPs. Purchaser will manage these interfaces using the inputs from different Contractors.

B. **Type E** interfaces: Between a service delivered by other WPs and an existing Purchaser service. Purchaser will manage these interfaces using the inputs from different Contractors.

4.4.3. The use of PFE Hardware baseline

SOW-0054 The Purchaser will provide the hardware for the DC, EN, SN and IREEN as PFE on which the Contractor shall build the IaaS solution. In order to maintain a complete and relevant configuration baseline, the Contractor shall include the HW specifications in its configuration baseline for LLD and make recommendations on required baseline adaptations throughout the lifetime of the project.

SOW-0055 The Purchaser will provide the initial rack layout and cabling documentation. The Contractor shall review and update this initial design as part of its LLD for Purchaser approval. If approved, the Purchaser will provide or update the hardware installation (rack & stack) based on the LLD provided by the Contractor.

SOW-0056 For any changes required on the infrastructure equipment, layout or installation, the Contractor shall provide an Engineering Change Proposal (ECP) request with details including the justification for Purchaser approval, at no additional cost impact in Contractor's scope of work. The Contractor shall proceed with the design, implementation and testing activities while the Purchaser implements the changes, if approved.

SOW-0057 The Contractor shall define and implement, in coordination with the Purchaser, a process to modify and/or update the hardware baseline configuration to be compliant with the design and the current industry standards. The Purchaser will decide on the necessity of these changes to the HW and SW baseline, and if agreed will initiate the procurement process.

SOW-0058 The Contractor shall define and implement, in coordination with the Purchaser, a process to add capacity and/or components to be procured by the Purchaser. The Purchaser will decide on the necessity of these changes to the HW and SW baseline, and if agreed will initiate the procurement process.

[0071] Further information for PFE is provided in Annex B.

4.4.4. Automation and Orchestration

[0072] A key element of the WP07 solution is the automation and orchestration effort that will be used to systematically test and deploy the deliverables. The automation and Orchestration tools, environment, processes and procedures will be jointly used by the Contractor and Purchaser to implement, operate and maintain the systems.

SOW-0059 The Contractor shall design and implement, in cooperation with the Purchaser who will approve the solutions, DevOps CI/CD pipelines (including tooling and processes) to deploy, implement, operate and maintain the services delivered within the scope of this contract.

SOW-0060 The Contractor shall document the solution and design aspects within the LLD and other relevant documentation.

SOW-0061 The Contractor shall provide the required licenses to establish and operate the CD/CI pipelines as further described in 4.4.4.

SOW-0062 The Contractor shall ensure that the CD/CI pipelines tools implemented are made available to the Purchaser for joint use as soon as the tools are implemented. The Purchaser may use these tools for the entirety of the ITM Recovery Project and relevant activities.

SOW-0063 The Contractor shall include all the procedures and processes for operation and maintenance within the Operating Model document.

SOW-0064 The Contractor shall implement and use the CI/CD pipelines for the development and implementation of the IaaS, ECS, CPS, SMC and Cyber Security systems.

SOW-0065 When developing and implementing automation for solutions based on containers, the Contractor shall align the solution with the Purchaser's Trusted container lifecycle management PFE/I-26.

SOW-0066 The Contractor shall include automated testing and Quality Assurance gates within CI/CD pipelines in line with the implementation principles defined in 4.2.

SOW-0067 The Contractor shall provide the required licenses for tools and system to establish the CD/CI DevOps pipelines and including at the minimum:

- SOW-0067.A Continuous Integration/Continuous Deployment (CI/CD) Tool: Ansible, Jenkins and an Artefact repository solution.
- SOW-0067.B Source Control Management (SCM) Tool: GitLab.
- SOW-0067.C Containerization Tool: Leverage VMware Tanzu provided as PFE and/or another solution validated with the Purchaser during development/validation phases.
- SOW-0067.D Infrastructure-as-Code (IaC) Tool: Terraform
- SOW-0067.E Monitoring and Logging Tool: Zabbix and integration with NATO Enterprise logging (Splunk).
- SOW-0067.F Security compliance tool: Runecast and/or other required security compliance tools.
- SOW-0067.G Credential Vaults: Hashicorp Vault.

SOW-0068 The Contractor shall ensure the tools listed above in SOW-0067 are the preferred tools used to implement automation and orchestration.

SOW-0069 The Contractor shall design and implement a security compliance system, in order to develop automated compliance dashboard, preferably based on commercial off the shelf solutions.

SOW-0070 The Contractor shall configure the security compliance system against industry best practices such as GDPR, NIST frameworks and ISO 27001 [Ref: ISO/IEC 27001].

SOW-0071 The security compliance system coverage shall be expanded to include security requirements of this project and the AC/322-D/0048-REV3 directive [Ref: AC/322-D/0048-REV3 (INV)].

SOW-0072 The Contractor shall provide the licenses for the automation and orchestration tools with the following requirement for the NATO ON (NS):

- SOW-0072.A Included for a minimum of 100 concurrent users.
- SOW-0072.B Including for a minimum of 10 000 target systems (physical and virtual).
- SOW-0072.C Enterprise versions when available.
- SOW-0072.D Supported on NS (disconnected from internet) networks.
- SOW-0072.E Valid for the duration of four (4) years from the effective date of the Task Order

SOW-0073 The Contractor shall provide the licenses for the automation and orchestration tools with the following requirement for the IREEN ON@NU:

- SOW-0073.A Included for a minimum of 100 concurrent users.
- SOW-0073.B Including for a minimum of 10 000 target systems (physical and virtual).
- SOW-0073.C Enterprise versions when available.
- SOW-0073.D Aligned with the NATO ON versions.

SOW-0073.E Valid for the duration of four (4) years from the effective date of the Task Order

SOW-0074 In addition to the licenses listed above, the Contractor shall provide any other licenses and tools (i.e. HW and SW) that may be required for the development, implementation and operation of the automation and orchestration solution.

SOW-0075 The Contractor may propose different licenses than above in line with the design and solution that is proposed for Purchaser's approval. The Contractor shall not implement these licenses without Purchaser's approval.

[0073] In case of the usage of NATO public cloud services, the Purchaser will provide some of the licenses as PFE.

SOW-0076 The Contractor shall provide all the licenses allowing the Purchaser to increase the number of concurrent users and target systems at any time during the execution of the contract.

SOW-0077 The Contractor provided licenses shall be out of the box solution and not be customized. In cases that this is not possible, the Contractor shall inform the Purchaser and request approval.

SOW-0078 The Contractor shall leverage the NATO Software Factory to the maximum extent, in order to establish the DevOps CD/CI pipelines aspects part of the reference environment IREEN ON@NU.

SOW-0079 The Contractor shall include a part of the DevOps CD/CI pipelines, the automated replication of code and products from low to high, from IREEN ON@NU to the NATO ON using Data Diode services (one way transfer).

SOW-0080 The Contractor shall automate (technical) test cases, including the Security Test and Verification Plan (STVP) tests. The automated test cases shall be executed on a DC, EN or SN infrastructure from a central location and shall be repeatable and log the test result.

SOW-0081 The Contractor shall ensure that the deployment of all ITM WP07 software products (VMware, Microsoft, Linux, VEEAM, Trellix, Oracle, Postgress, Splunk software, etc.) can be executed through a single integrated automation and orchestration capability. This capability shall be described in detail in LLD and Operating Model. The Contractor shall ensure that the automation software delivered uses open standards and is not limited for one or a sub-set of the software brands.

SOW-0082 The Contractor shall provide the Purchaser with access, tooling, source code, documentation and licenses necessary to enable the Purchaser to jointly develop on the automation and orchestration environment and make use of the CI/CD pipeline during the implementation and operation.

SOW-0083 The Contractor shall validate automated test cases on IREEN ON@ NU before being executed on a DC, EN or SN infrastructure from a central location and shall be repeatable and log the test result.

SOW-0084 The Contractor shall ensure that the automation and orchestration capability in IREEN ON@NU is ready for collaborative usage by both the Contractor and the Purchaser upon completion of IOA IREEN @NU as described in Section 0.

SOW-0085 The Contractor shall use declarative scripting in order to be able to rerun failed scripts.

SOW-0086 The Contractor shall adhere to the NATO security policies when developing, operating or deploying scripts.

SOW-0087 The Contractor shall design, document and implement a version control system for the automation scripts, templates, blueprints and other configuration artefacts.

SOW-0088 The automation and orchestration solution shall be interfaced with the Enterprise Request Portal where customers can request deployments of a registered application on the NATO ON private cloud.

SOW-0089 The Contractor shall utilise a DevOps/iterative approach to planning, development and release.

[0074] This iterative approach allows rapid development, deployment and testing. The change, configuration and release management processes reflect the flexibility and discipline required using this 'Agile' methodology.

SOW-0090 The Automation and Orchestration capability provided by the Contractor shall ensure that the release of a baseline can be done rapidly, efficiently and consistently onto each environment in the release process. An overview of the release environments can be found in the figure below.

4.4.5. Software Development Requirements

[0075] This section outlines the generic non-functional requirements for software development.

SOW-0091 The Contractor shall be compliant with the generic requirements described in this section during the implementation of all the SRS requirements.

SOW-0092 Source code artefacts delivered for the capability shall be written using US Standard English (e.g. for Classes, Methods, Variables etc.). Industry coding best practices shall be used.

SOW-0093 Software source code shall be documented as in-line comments providing sufficient readability and understandability. Comments can be extracted and formatted to augment technical documentation.

SOW-0094 Source code artefacts delivered for the capability shall be documented with in-line comments using United Kingdom Standard English. Industry best practices shall be used in the level of commenting.

[0076] Improper protection of account credential or session may compromise passwords, keys, session cookies or other tokens, allowing an attacker to bypass authentication restrictions or assume other Users' identities.

SOW-0095 In situations where a plain-text password is required, the capability shall use encryption to store the password.

SOW-0096 Authentication details shall not be hard-coded in any part of the source code.

SOW-0097 Decryption keys shall be strongly protected to prevent unauthorised access.

SOW-0098 In order to reduce the code size and improve the transfer time, the source code comments of the client applications must be removed by an automated process before entering into production.

SOW-0099 Source code shall clarify the intent of the code by considering the Basic Usage of Comments given in the Description in accordance with the following:

- SOW-0099.A Each class definition explaining the purpose of the class
- SOW-0099.B Each member function explaining what the function does, including descriptions of input parameters and return values
- SOW-0099.C Each member variable explaining what the variable means (including unit of measure where appropriate)
- SOW-0099.D Each type definition (enums) explaining what the type represents
- SOW-0099.E Explanation of a specific computation algorithm
- SOW-0099.F Algorithm references to external sources.

SOW-0100 Using Free and Open Source Software (FOSS) components shall comply with the NATO strategy on the use of Open Source Software in NATO systems [Ref: AC/322-D(2009)0015].

SOW-0101 Any component based on FOSS shall be provided with the source code of the FOSS.

SOW-0102 The source code shall correspond to the delivered component (i.e. same version), and that component shall be capable of being built from the delivered source code with the provided documentation.

SOW-0103 Source code of scripts and program shall be easily maintainable and updated.

SOW-0104 The Contractor shall use SonarQube, available as part of NSF, to calculate the Technical Debt Ratio (TDR) of all developed source codes, and it shall achieve a ratio lower than 5% using the default setting for TDR calculations.

4.5. Critical Design Reviews

SOW-0105 The principal purpose of the Critical Design Reviews (CDR) is to arrive at Purchaser acceptance of the detailed design documentation prior to the start of relevant activity group implementation. Such acceptance is based upon Contractor-supplied information and in no way relieves the Contractor's obligation to deliver a system conforming to the requirements in this Contract. Sufficient detailed information and test data shall be provided to assure the Purchaser that all functional and performance requirements have been fully complied with.

SOW-0106 The Contractor shall plan, organize[7] and execute two critical design review events as following:

SOW-0106.A Critical Design Review - Activity Group 1 and 2

SOW-0106.B Critical Design Review - Activity Group 3,4 and 5

SOW-0107 During the period leading up to the CDR event, the Contractor shall adopt an ‘agile’ design methodology, and perform agile design sprints, consisting of 4 weeks, in close cooperation with the Purchaser team.

SOW-0108 In preparation and conduct of CDRs, the Contractor shall:

SOW-0108.A Develop the agenda for the review meeting and provide it for Purchaser concurrence at least 4 weeks prior to the event(s).

SOW-0108.B Provide the technical documentation and data in ‘agile form’, by releasing an updated version at the end of each Design Sprint (within 3 business days following the final day of each Design Sprint), starting from the first Design Sprint. (If necessary, another update shall be submitted within 2 business days following the final day of the Sprint cycle.)

SOW-0108.C Update the technical documentation and data released at the end of each design sprint, in accordance with the Purchaser comments.

SOW-0108.D Provide the Purchaser with the technical documentation and data as described in Section 13.

SOW-0108.E Provide the IVV documentation and data as described in Section 11.

SOW-0108.F Provide the security accreditation inputs as described in Section 12.

SOW-0108.G Provide reports from and ensure participation by Sub-contractors, vendors and suppliers as necessary.

SOW-0108.H Develop, organise and present briefings as necessary.

SOW-0108.I Provide schedule, test and design data and supporting analysis for the review.

SOW-0108.J Provide appropriate technical personnel at the review.

[7] Unless otherwise specified by the Purchaser, the location of the design reviews will be the Purchaser facilities in the Hague, the Netherlands.

SOW-0108.K Provide the Purchaser with a summary meeting report within 5 business days, documenting as a minimum principal actions and agreements, at the conclusion of the review.

SOW-0109 The Contractor shall provide all the documentation and data artefacts for Purchaser review and approval minimum 4 weeks prior to the CDR event.

SOW-0110 The Contractor shall incorporate all Purchaser comments concerning deviations from and omissions of contract requirements, errors, inconsistencies and omissions. Purchaser comments concerning interpretation, suggestions and guidance shall be incorporated by the Contractor.

SOW-0111 The Contractor shall release the technical documentation and data in its final form latest within 7 business days following the CDR event(s).

SOW-0112 It remains the sole responsibility of the Contractor to prove the design through the regime of testing and other assurance mechanisms set forth in the Contract and it shall be the sole responsibility of the Contractor in the event that the design proves deficient in terms of the contract functional and/or performance requirements.

SOW-0113 At CDR, the preliminary allocation of SRS and SoW requirements to system design specifications and to verification methodologies shall be assessed and shall be subject of approval by the Purchaser.

5. TRANSITION OF CAPABILITIES INTO OPERATIONS

[0077] 'Transition to Operations' is identified as 'the deployment of the features developed and tested in development and pre-production environments' to 'the live production environment (i.e. BiSC-AIS NS or NATO ON) which is operating services at NATO Secret level'. In context of WP07, 'Transition to Operations' is an activity led by the Contractor and is a prerequisite for achievement of PSA milestone(s) as described in Section 2.5.

SOW-0114 For all capabilities delivered per Activity group, the Contractor shall be responsible for the integration and activation of the system into operations. Prior to transition to operations and (site) PSA, following changes introduced during the agile implementation sprints shall be implemented in each applicable site free of charge:

SOW-0114.A Changes that were introduced due to software failures and bug fixing for a certain site shall be implemented for all previously implemented applicable sites.

SOW-0114.B Changes that were introduced as part of the continuous improvement and development in DevOps lifecycles for a certain site shall be implemented for all previously implemented applicable sites.

SOW-0115 Prior to the completion of each TO implementing Sprints, as an exit criteria, the Contractor shall successfully complete the Intermediate & Candidate Release testing events. The aim is to create candidate releases that are ready for deployment to operations.

[0078] The Purchaser will be the decision authority on the timelines and frequency for release to operations, respecting the NATO processes such as security accreditation.

SOW-0116 The Contractor shall follow the guidance and timelines provided by the Purchaser and complete the transition of the capabilities into operations accordingly.

SOW-0117 The Contractor shall ensure that any activities on operational environments are coordinated and approved in advance with the Purchaser to minimize service interruption.

SOW-0118 The Contractor shall develop and execute Transition and Activation Plans in accordance with the requirements in Section 13.

SOW-0119 For all products delivered per Activity Group, the Contractor shall ensure that the Purchaser’s workforce can operate the provided capabilities for its customer, accomplished through a variety of documentation, training, collaboration within integrated teams and by providing Early Life Support.

5.1. Application Migration

[0079] In Activity Group 1 and 4, upon completion of WP07 Contractor led implementation activities and transition to operations, the Purchaser will migrate FASs onto the new IaaS through WP09 (Application Migration).

SOW-0120 As part of the implementation scope, the Contractor shall support FAS migration activities by ensuring configuration control, validating Purchaser provided APMP documentation for deployment and integration with the NATO ON, and preparing the IaaS, ECS, CPS systems to receive applications and user access to the migrated services. This shall include:

SOW-0120.A Analysis of the migration targets of application:

SOW-0120.B Migration of IaC deployment-enabled application (Ansible and Terraform scripts)

SOW-0120.C Validation of the high level schedule for migrating groups of applications

SOW-0121 The Contractor shall provide its feedback to the Purchaser provided APMP within two weeks of receipt of the document.

SOW-0121.A To support legacy non automated application migration for infrastructure modifications

SOW-0121.B For Creation/Configuration of VMs, SAN/VLAN integration, Platform/Core services adjustment, on request by WP09

SOW-0121.C To support workload migration of VMs on request by WP09.

SOW-0121.D To operate CPS services during migration, specifically:

SOW-0121.E The maintenance of MECM and VDI services during the AG2, AG4 user migration.

6. SUPPORT TO PURCHASER ACTIVITIES

SOW-0122 The Contractor shall provide support to various Purchaser activities on LoE basis as outlined in SSS rates and locations. This support shall be provided for the following activities throughout the execution of the Contract 'as needed basis':

SOW-0122.A Supporting Mons AG1&AG2 Implementation

SOW-0122.B Supporting the Application Migration

SOW-0122.C Supporting the Enterprise SMC and Enterprise Cyber Security Integration

SOW-0122.D Supporting Purchaser Governance Meetings (e.g. NSAB Meetings)

SOW-0122.E Supporting the Integration with NATO Services

SOW-0122.F Supporting Purchaser Test and Acceptance Events

SOW-0122.G Providing Early Life and O&M Support

SOW-0122.H Supporting Other Purchaser Activities

SOW-0123 The Contractor shall provide the type of resources as outlined in SSS and as per the skills, qualifications and experience described in Section 7.3.

[0080] The Purchaser reserves the right to use the same resources for a combination of the listed activities in line with the subject matter area of the SME and Contractor expertise for the services provided within the scope of this Contract.

SOW-0124 The Contractor shall make the resources available in Purchaser facilities, as outlined in SSS) within one week of the release of the associated Task Order.

SOW-0125 The Contractor personnel shall provide services during Purchaser business hours between 08.00-17.30, in the time zone of the specific sites the Contractor services are requested.

SOW-0126 The Contractor shall provide services outside of the business hours in circumstances requiring urgent intervention, in accordance with the SSS.

SOW-0127 The Contractor shall provide all the necessary resources, information, guidance, mentoring, data and subject matter knowledge available for the Contractor personnel to provide the sufficient support to the Purchaser throughout the duration of the Task Order.

SOW-0128 The Contractor personnel shall provide the support under the guidance of the Purchaser personnel and embedded within the Purchaser team.

[0081] Depending on the number of support resources, length and complexity of the contracted support scope, the Purchaser may also request the management support to provide more structured project management as outlined in SSS.

6.1. Supporting Mons AG1&AG2 Implementation

SOW-0129 The Contractor shall provide support for Purchaser implementation activities in Mons:

SOW-0129.A Assessing and verifying the site specific design elements

SOW-0129.B Verifying the site specific configurations, scripts and relevant data

SOW-0129.C Verifying the implementation work performed in Mons for Activity Group 1 and Activity Group 2 scope

SOW-0129.D Providing an assessment on the work needs to be completed for alignment with the other EN sites

SOW-0129.E Providing an assessment on the work needs to be completed for alignment for Activity Group 4 implementation

SOW-0129.F Performing the work required for alignment with other EN sites and in preparation for Activity Group 4 activities

[0082] The Purchaser may choose to contract the AG1&AG2 implementation for Mons in its entirety to the Contractor, as part of the Task Orders. In that case, the Purchaser will not use the support services.

6.2. Supporting the Application Migration

SOW-0130 For Purchaser led Application Migration, the Contractor shall provide support to the Purchaser teams in following areas in LoE basis as outlined in SSS:

SOW-0130.A To create deployment-side configuration management (GitOps)

SOW-0130.B To assist WP09 with the cross-domain design and implementation (Data Diode as a Service) of the application packaging repository

SOW-0130.C To operate the services during the application migration performed by WP09, including:

SOW-0130.D To support the correct operation of IaC capability (as designed and implemented) while WP09 performs and verifies the application migration via automation

6.3. Supporting the Enterprise SMC and Enterprise Cyber Security Integration

SOW-0131 If requested, the Contractor shall provide dedicated LoE based support for the integration activities performed by other WPs for the following services:

SOW-0131.A Enterprise SMC

SOW-0131.B Enterprise Cyber Security

6.4. Supporting Purchaser Governance Meetings

SOW-0132 If requested, the Contractor shall provide LoE based support for the preparation, attendance and follow-up actions for the Purchaser meetings held with the governance, such as NSAB Plenary Session, Stakeholder meetings for the systems and services provided within the scope of this Contract.

6.5. Supporting the Integration with NATO Services

SOW-0133 The Contract shall provide LoE based support to the following Purchaser's activities, for the systems and services provided within the scope of this Contract:

SOW-0133.A Capturing and maintenance the Service Roadmap and provide inputs to populate A&T Data in the A&T portfolio

SOW-0133.B Provision of up to date Software Media to be loaded and controlled via DML by the Purchaser

SOW-0133.C Provision the documentation listed in the System Submission Requirement Matrix (SSRM) below for new services

SOW-0133.D Provision of missing documentation and updates to existing documentation listed in the SSRM and in the Service Activation and Sign-off Deliverables list for modified services

SOW-0133.E Support the activation and sign off of the below documents:

SOW-0133.E.1 Service Design

SOW-0133.F Specific Support Plan included as part of the support information in SSRM

SOW-0133.G Deployment Plan (i.e. Service Deployment Plan (SDP) included as part of the Applications release information in SSRM

SOW-0133.G.1 Interface Design Definition

SOW-0133.G.2 CONOPS

6.6. Supporting Purchaser Test and Acceptance Events

SOW-0134 The Contractor shall provide support for following Purchaser test and acceptance activities for the systems and services provided within the scope of this Contract:

SOW-0134.A Support/Conduct ITM-RC1 Site Acceptance Event Tests

SOW-0134.B Support ITM-RC1 Migration Acceptance Event Tests

SOW-0134.C Support ITM-RC1 Operational Acceptance Event Test

SOW-0134.D Support Other ITM-RC1 Project Test and Acceptance Activities

SOW-0135 This support shall be provided in LoE basis as outlined in SSS.

SOW-0136 This support shall include all the documentation, preparation, conducting and implementing the follow-on corrective actions as a result of the test events.

SOW-0137 During the test events, the duration spent on the failed tests and corrective actions, will not be taken into account in the LoE based support, if these are due to the systems and services delivered within the scope of this Contract. The Contractor shall be fully responsible from providing the corrective actions and repeating the tests without any additional LoE based support contracted.

6.7. Early Life and O&M Support

SOW-0138 The Contractor shall provide system operational and maintenance support after the transition to production of provided services in LoE basis as outlined in SSS.

SOW-0139 The early life support shall consist at minimum:

SOW-0139.A Support the Purchaser staff in adapting to the new capabilities.

SOW-0139.B Support the Purchaser staff in the resolution of 3rd level support requests on the ON.

SOW-0139.C Support the Purchaser staff in adapting to the changes in the environment as part of standard O&M activities.

SOW-0139.D Support the Purchaser staff in adapting, maintaining and improving the DevOps capabilities.

SOW-0140 If the failure is caused by the scope implemented by the Contractor, the Contractor shall provide the activities required to recover the services as part of the Warranty requirements, see Section 12, free of charge. These activities shall not be covered by the LoE basis additional support.

SOW-0141 This early support shall be provided at the main ESOC in BEL-CAS-01 with occasional travel to the Purchaser facilities in Braine L'Alleud, Belgium; The Hague/ Netherlands and Brunssum/Netherlands.

SOW-0142 The Purchaser may also request support in Lago di Patria, Italy in LoE basis as outlined in SSS.

[0083] The Contractor should note that the deliverables for BEL-CAS-01 from Activity Group 1 and 2 will have been delivered by the Purchaser before Effective Date of Contract (EDC).

SOW-0143 The Contractor shall verify the configuration delivered at BEL-CAS-01 by the Purchaser. As a result of this verification, the Contractor shall plan, schedule and implement any required configuration changes needed to align the installations at BEL-CAS-01 with the Contractor developed, Purchaser approved, LLD for Activity Group 1 and 2. The Contractor shall support this activity in LoE basis as outlined in SSS.

6.8. Supporting Other Purchaser Activities

SOW-0144 The Contractor shall provide LoE based support for other Purchaser activities, such as User Transition, for the systems and services provided within the scope of this Contract.

SOW-0145 The Contractor shall also provide LoE based support via contracting the vendors for engineering support:

SOW-0145.A Microsoft

SOW-0145.B VMWare

SOW-0145.C Cisco

7. WORK PACKAGE MANAGEMENT

[0084] This section outlines the Work Package project management requirements for this Contract.

7.1. General Requirements

SOW-0146 WP07 shall be executed with a tailored Agile approach as guided by the ITM-RC1 implementation approach and the Purchaser constraints.

SOW-0147 The Contractor shall perform the following activities as part of the Work Package Management:

- SOW-0147.A Project Management
- SOW-0147.B Implementation Management
- SOW-0147.C Risk and Issue Management
- SOW-0147.D Configuration Management
- SOW-0147.E Quality Assurance and Control
- SOW-0147.F Integrated Product Support

[0085] To facilitate the efficient way of communication email is considered as an official communication channel, unless stated otherwise.

SOW-0148 For contractual communication, the Contractor shall acknowledge email receipt within 1 business day and answer email received from the designated Purchaser PoC within 3 business days.

SOW-0149 The Contractor shall be responsible for the project management of the deliverables in this Contract. The Contractor shall provide the following Project Management artefacts that shall be maintained through the lifetime of the project:

- SOW-0149.A Work Package Management Plan (WMP);
- SOW-0149.B Work Package Implementation Plan (WIP);
- SOW-0149.C Risk and Issue Management Plan (RIMP);
- SOW-0149.D Configuration Management Plan (CMP);
- SOW-0149.E Quality Assurance Plan (QAP);
- SOW-0149.F Integrated Support Plan (ISP)
- SOW-0149.G Product Backlog (PB);
- SOW-0149.H High Level Release Plan (e.g. per activity group, site etc.);

SOW-0150 The Contractor shall provide the development and delivery of the solutions of this project using an Agile methodology with its associated Integrated Project Teams.

7.2. Implementation Methodology

7.2.1. Agile Implementation

7.2.1.1. The Agile Process

SOW-0151 For Work Package execution the Contractor shall follow an Agile approach [Ref: AGILE MAN] in alignment with the below stated Project Management sections.

SOW-0152 The Contractor shall use time boxes to create or refine a set of features associated with defined scope and objectives, ensuring gradual build-up, allow for timely changes and focus on the results.

SOW-0153 The Contractor shall use the time-box for each sprint, with each time box duration as four (4) weeks.

SOW-0154 The Incremental development process is illustrated in Figure 3, below. Every incremental release shall be associated with a detailed LLD (and updated if required), and shall be documented in as-built documentation as described in Section 13.3.4.

SOW-0155 'Universally applicable requirements' shall be applicable by default for the implementation of each Activity Group requirement in a given Sprint.

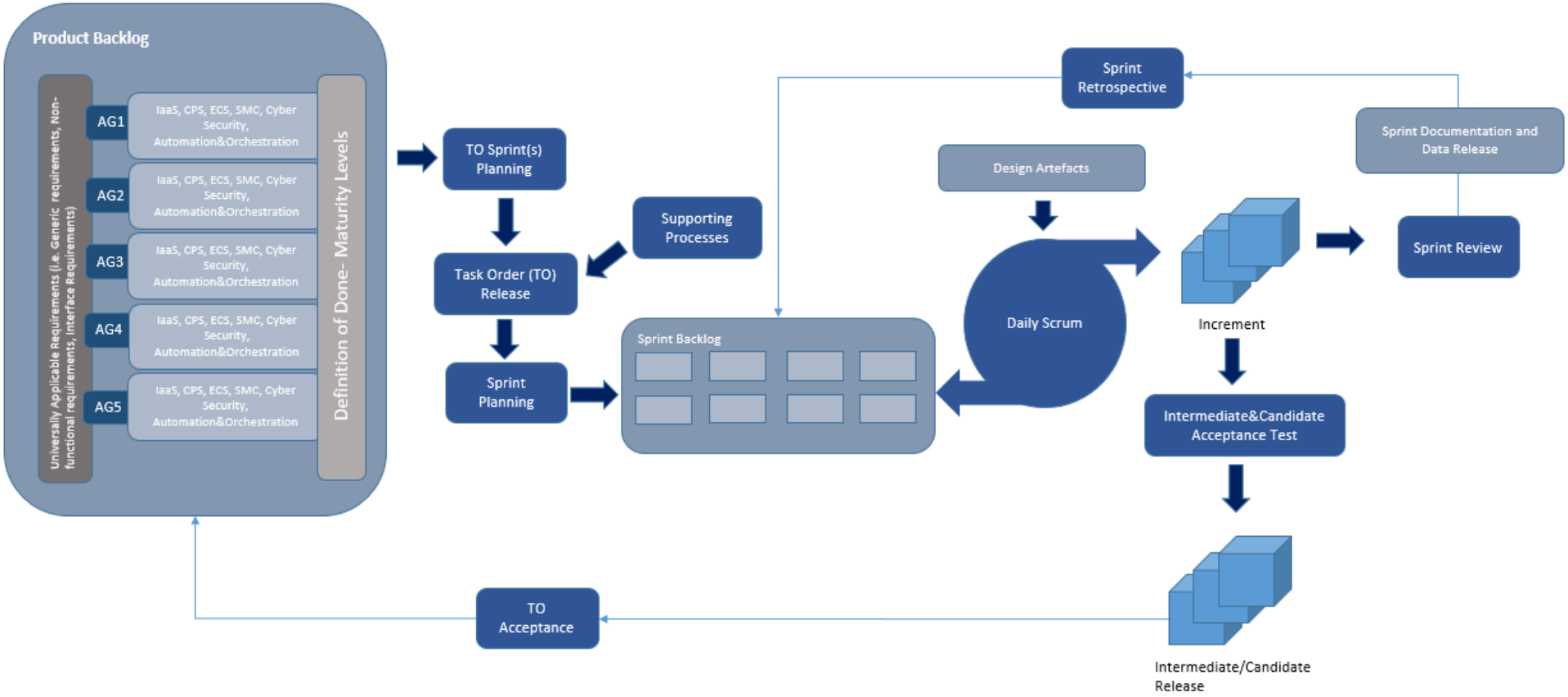

Figure 3 - Incremental Development Process

7.2.1.2. Execution of the Agile Process

[0086] Incremental development process during the execution of the agile approach is described in Figure 3 - Incremental Development Process.

SOW-0156 In the beginning of each cycle, and prior to the release of a TO, the Contractor shall organize the Task Order planning meeting in participation of the Purchaser.

SOW-0157 During the TO Planning Meeting, the Contractor shall propose the set of requirements and the MoSCoW prioritization [Ref: MOSCOW], with a provisional assignment to each Sprint that will be implemented as part of the TO. Final prioritization and allocation of the requirements to each TO will be subject to the Purchaser approval.

SOW-0158 If there are requirements that will require to be implemented in more than one Sprint as per the complexity rating (i.e. implementation duration between 1 month and 3 months), the Contractor shall ensure that the requirements is fully implemented within one Task Order.

SOW-0159 The Contractor shall complete the implementation of all requirements in a given Activity Group (ref. Appendix 1 SRS) within the maximum number of Sprints listed below, via assigning adequate number of requirements in each Sprint:

- SOW-0159.A AG1 and AG2 requirements within maximum of six (6) Sprints, ensuring the completion of IREEN ON@NU requirements within the first three (3) Sprints
- SOW-0159.B AG3 and AG4 requirements within maximum of fifteen (15) Sprints

SOW-0160 The planning shall be based on the High Level Release Plan, assigning the entirety of the Appendix 1 SRS requirements to the maximum number of Sprints identified above. High Level Release Plan shall be updated at the end of each sprint, and shall represent a forecast of releases and execution of the solution requirements.

SOW-0161 ‘Definition of Done’ shall be defined accordingly with the maturity levels described in Annex A. ‘Definition of Done’ may be fine-tuned when and if needed with Purchaser’s agreement. Purchaser will remain as the deciding authority on the final form and content of the ‘Definition of Done’.

SOW-0162 In the beginning of each Sprint, the Contractor shall:

- SOW-0162.A Maintain the set of “system and solution requirements” (See Appendix 1 SRS), as required, each of which is a high-level definition of a requirement.
- SOW-0162.B Create/update the “backlog” of the set of this ‘system and solution requirements’, which together represent the products (or “features”) necessary to implement the system and the solution
- SOW-0162.C Prioritise the requirements in the backlog as part of the Task Order and sprint planning, in full coordination and agreement with the Purchaser Point of Contacts (PoCs).
- SOW-0162.D Define and document the ‘Definition of Done’ based on the Maturity Levels defined in Annex A CIS Principles and Maturity Levels, and in full agreement with the Purchaser
- SOW-0162.E Estimate the duration required in implementing each requirement for planning,
- SOW-0162.F During the course of the sprint, develop and test the products identified for that sprint
- SOW-0162.G During the course of the sprint, meet frequently (i.e. daily “stand up”) within the IPT

SOW-0163 During each Sprint, the Contractor shall perform all required design, implementation and integration efforts including planning, preparation, development, requirements management, installation, configuration, testing (e.g. Engineering Tests, Qualification

Phase, Witness tests), configuration management and audits, integrated product support and security accreditation elements.

SOW-0164 During each Sprint, the Contractor shall at all times ensure the compliance with the high level and low level design. In case there is a need for a change in the design specifications, the Contractor shall raise it to the Purchaser in a form of ECP and implement the changes in the design documentation at the end of each sprint.

SOW-0165 At the end of each sprint, the Contractor shall:

SOW-0165.A demonstrate the completed product(s) for Purchaser approval, including the proof for successfully executed test cases.

SOW-0165.B update and release the 'Sprint Documentation and Data'.

SOW-0165.C Update the broader project plan as necessary, including timelines, risk logs and issue logs.

SOW-0165.D Repeat these steps until the project activities are complete.

SOW-0166 The Contractor shall include the following artefacts within the updated and released 'Sprint Documentation and Data' at the end of each sprint:

SOW-0166.A Product Backlog reflecting the latest status of the requirements for implementation

SOW-0166.B High Level Release Plan reflecting the latest Burndown and Burnup Charts, actual execution of the previous sprints (with mapping to implemented requirements) and more accurate planning for the upcoming Sprints

SOW-0166.C Technical Documentation and Data as described in Section 13

SOW-0166.D IVV Documentation as described in Section 11

SOW-0166.E Security Accreditation inputs as described in Section 8

SOW-0167 At the end of each Sprint:

SOW-0167.A All requirements in 'must have' category shall be implemented and accepted by the Purchaser in line with the 'Definition of Done'.

SOW-0167.B Minimum 80% of the requirements in each of the 'should have' and 'could have' categories shall be implemented and accepted by the Purchaser in line with the 'Definition of Done'.

SOW-0167.C Remaining requirements and no more than 20% of the 'should have' and 'could have' categories may be transferred to the following Sprint within the same Task Order.

SOW-0168 At the end of each Task Order, following the completion of the final Sprint:

SOW-0168.A All requirements in 'must have' category shall be implemented and accepted by the Purchaser in line with the 'Definition of Done'.

SOW-0168.B Minimum 80% of the requirements in 'should have' and 'could have' categories shall be implemented and accepted by the Purchaser in line with the 'Definition of Done'.

SOW-0168.C Remaining requirements and no more than 20% of each of the 'should have' and 'could have' categories may be transferred back to the Product Backlog.

[0087] Purchaser will release an amendment to the Task Order in line with the 'implemented' number of requirements and cost adjustment. The requirements that were not implemented will be deducted from the TO amount and transferred back to Product Backlog to be implemented in future Sprints.

SOW-0169 When requested by the Purchaser, the Contractor shall perform the activities required for transition of capabilities into operations (Section 5) and transition into services for all the requirements implemented as part of the previous related Task Orders. This may

occur following the completion of all requirements for the relevant Activity Group (following a series of Task Orders) or it may occur at the completion of each Task Order, depending on the security accreditation approach required by security accreditation authorities.

SOW-0170 The Contractor shall at all times provide access to the Purchaser for all files, scripts, software code, documentation, configuration files, passwords and any other type of data/information created within the scope of this Contract. This access shall not depend on the achievement of milestones or official acceptance, and shall be granted throughout the execution of the Contract starting from EDC.

SOW-0171 Deployment to the production (e.g. operational environment) shall be done with the full visibility and oversight of the Purchaser. The Purchaser will maintain rights for access and modifications as required for the delivery of the Customer services for all the Purchaser sites.

[0088] The Contractor may choose to create User Stories based on the requirements set without altering the scope, terms and conditions of this Contract. Purchaser will remain as the decisive authority on the usage of the User Stories.

7.2.2. Implementation – Cyber Security Monitoring

[0089] The Contractor shall design, implement and integrate the Cyber Security Monitoring services as described in Annex C including all relevant testing, security accreditation and integrated product support services. This implementation will follow the traditional waterfall approach.

7.3. Organisation

[0090] This section outlines the minimum requirements on team structures for both the Purchaser and Contractor and their responsibilities.

SOW-0172 To support the integration activities of new services with PFE deliverables or operational services, an Integrated Project Team (IPT) shall be established that consists of:

SOW-0172.A Contractor team;

SOW-0172.B Purchaser's team.

7.3.1. Purchaser Project Organisation

[0091] The Purchaser's Contracting Officer serves as the Purchaser's representative and will be the primary interface between the Contractor and Purchaser after the Effective Date of Contract (EDC) for day-to-day WP management and execution activities within the boundaries of the contractual requirements.

[0092] The Purchaser Work Package Lead is supported by a team consisting of specialists in areas who may be delegated to act on the Project Work Package lead's behalf in their respective area of expertise.

[0093] Neither the Purchaser's Work Package Lead nor any other NATO personnel may make changes to the Terms and Conditions of the Contract; they will only provide the Purchaser's interpretation of technical matters. All obligations and changes to the Contract will only be made through the Purchaser's contracting office. The Purchaser's Contracting Officer will be the primary interface between the Contractor and Purchaser for commercial topics, including any potential changes impacting the boundaries of the existing contractual requirements.

SOW-0173 The Contractor shall involve the designated Purchaser PoC in any communication with the other Purchaser team members. Information received from other Work Package

teams that affect the delivery/designs of WP07 shall be officially validated by the designated Purchaser PoC (e.g. WP07 lead).

7.3.2. Contractors' Project Management Organisation:

7.3.2.1. General

SOW-0174 Once the implementation starts, the Contractor shall establish and maintain a Project Management Office (PMO) in Purchaser facilities in The Hague, Netherlands to perform and manage all efforts necessary to discharge the responsibilities under this Contract.

SOW-0175 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-0176 From EDC onwards, all changes in Key Personnel or substitution of Key Personnel during contract execution shall be subject to Purchaser approval.

[0094] The following sections (7.3.3 and 7.3.4) outline minimum educational and experience qualifications for Contractor's key personnel assigned to this Contract.

SOW-0177 All Contractor's WP07 personnel shall have a valid NATO Security Clearance, NS or above, and maintain it throughout the lifecycle of the Contract.

SOW-0178 Contractor personnel who need System Administrator or Operator privileges when working on NATO S*CR*T systems shall hold NATO CTS (Cosmic Top S*CR*T) clearances.

SOW-0179 All Contractor's WP07 project key personnel shall have an English level of SLP 3333, as defined in STANAG 6001 [Ref: STANAG 6001]. The Purchaser may consider the other candidates, if the technical competency excels in certain areas.

[0095] Substitution of experience or education is allowed as outlined in Table 3 below:

Education	Equivalent Education + Experience	Equivalent Experience
Associate's degree		2 years of relevant experience
Bachelor's degree	Associates + 2 years of relevant experience	6 years of relevant experience
Master's degree	Bachelor + 4 years of experience	8 years of relevant experience

Table 3 - Experience / Education substitution

SOW-0180 The Contractor shall submit the Curriculum Vitae for all the Contractor key personnel for approval to demonstrate the compliance with the required education, skills and experience before their official assignment to the project.

SOW-0181 All Contractor's WP07 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.

[0096] The Purchaser will reserve the right to interview any of the proposed candidates before their assignment. The Purchaser will also reserve the right to decline any of the proposed candidates and request replacement, before their assignment or anytime during their allocation to the project.

7.3.2.2. Contractor Team – Design

SOW-0182 The Contractor shall provide the following key personnel at the time of the EDC to support the Task Order 1 design related activities:

SOW-0182.A Project Manager

SOW-0182.B Technical Lead

SOW-0182.C Work Package Architect

SOW-0182.D Engineers

SOW-0182.D.1 Chief engineers for IaaS, CPS, SMC, Cyber Security, ECS

SOW-0182.D.2 Engineers - Security

SOW-0182.D.3 Engineers- Identity and Access Management

SOW-0182.D.4 DevOps Engineers - Automation Architect

SOW-0182.D.5 DevOps Engineers - IaaS

SOW-0182.D.6 DevOps Engineers - Networking

SOW-0182.D.7 Test Engineers

SOW-0182.E Quality Manager

SOW-0182.F Risk Manager

SOW-0182.G Test Director

SOW-0183 The Contractor shall provide the Project Manager, Technical Lead and Work Package Architect on-site. The Contractor may choose to provide the remaining personnel on-site or off-site.

SOW-0184 For specified roles to be deployed on-site, the Contractor's team shall be available (i.e. working from the Purchaser premises in the Hague, unless otherwise specified by the Purchaser) during Central European Time (CET) time zone working hours (8:30 - 17:30 Monday-Thursday, and 8:30 - 16:30 on Fridays).

SOW-0185 The Contractor may propose one sufficiently qualified individual to undertake a combination of roles depending on the content of a Task Order. Such proposal shall clearly demonstrate the qualifications and experience of the proposed ‘key personnel’ and shall be presented for Purchaser approval.

7.3.2.3. Contractor Team – Implementation (Agile Sprints)

SOW-0186 In order to facilitate communication and effectiveness, the Contractor shall locate the Key Personnel at the Purchaser premises in the Hague, Netherlands, throughout the implementation of the Agile Sprints, unless otherwise informed by the Purchaser.

SOW-0187 The Contractor's team shall be available (i.e. working from the Purchaser premises in the Hague, unless otherwise specified by the Purchaser) during Central European Time (CET) time zone working hours (8:30 - 17:30 Monday-Thursday, and 8:30 - 16:30 on Fridays).

SOW-0188 The Contractor personnel shall travel to the other Purchaser facilities, if required for the implementation and integration activities including the testing events during the agile implementation. The cost of such travel will be based on the rates provided in the SSS.

SOW-0189 The Contractor shall provide the following key personnel on-site to perform the following roles and satisfy the requirements of each Task Order:

SOW-0189.A Project Manager

SOW-0189.B Technical Lead

SOW-0189.C Work Package Architect

SOW-0189.D Engineers

SOW-0189.D.1 Chief engineers for IaaS, CPS, SMC, Cyber Security, ECS

SOW-0189.D.2 Engineers - Security

SOW-0189.D.3 Engineers- Identity and Access Management

SOW-0189.D.4 DevOps Engineers - Automation Architect

SOW-0189.D.5 DevOps Engineers - IaaS

SOW-0189.D.6 DevOps Engineers - Networking

SOW-0189.D.7 Test Engineers

SOW-0189.E Quality Manager

SOW-0189.F Risk Manager

SOW-0189.G Scrum Master

SOW-0189.H Release and Integration Lead

SOW-0189.I Test Director

SOW-0190 The Contractor may propose one sufficiently qualified individual to undertake a combination of roles depending on the content of a Task Order. Such proposal shall clearly demonstrate the qualifications and experience of the proposed 'key personnel' and shall be presented for Purchaser approval.

SOW-0191 The Contractor shall create two dedicated scrum teams at minimum to enable the simultaneous design and implementation of:

SOW-0191.A Activity Group 1 and 2

SOW-0191.B Activity Group 3, 4 and 5

SOW-0192 In each Scrum team, the Contractor shall assign the key personnel from different subject matter areas, as listed in SOW-0189, ensuring the sufficient representation and technical competency for the requirements delivered.

SOW-0193 The Contractor shall maintain the Scrum team member(s) after the completion of the implementation in support of the Purchaser activities, if requested by the Purchaser.

7.3.2.4. Contractor Team – Implementation (Cyber Security Monitoring)

SOW-0194 The Contractor shall provide a standalone team for the implementation of the Cyber Security Monitoring as outlined in Annex C.

SOW-0195 The Contractor team may provide the management and development activities from Contractor's facilities. The Contractor team shall provide the implementation, specifically the installation and testing activities in Purchaser facilities as listed in SSS.

7.3.2.5. Contractor Team – Support to Purchaser Activities

SOW-0196 The Contractor shall provide the contracted resources for support to Purchaser activities from designated Purchaser facilities as listed in SSS.

7.3.3. Contractors' Project Management Team

7.3.3.1. Project Manager

SOW-0197 The Contractor shall designate a Project Manager (PM), who will direct and co-ordinate the activities of the Contractor's project team.

SOW-0198 The Contractor's PM shall be responsible for project management, performance and completion of tasks and deliveries.

SOW-0199 The Contractor's PM shall be the Contractor's primary interface to the Purchaser's Work Package Lead.

SOW-0200 The Contractor's PM shall hold a University Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/ diplomas.

SOW-0201 The Contractor's PM shall hold valid Project Management certifications (e.g. PRINCE2 Agile Practitioner, Project Management Institute (PMI) Project Management Professional (PMP) or equivalent) and valid Information Technology Infrastructure Library (ITIL) Foundation Certificate at minimum.

SOW-0202 The Contractor's PM shall have a minimum of ten (10) years' experience as an Information and Computer Technologies (ICT) Project Manager as supported by project references, points of contact, and descriptions/scope of the projects managed in projects similar, in scale, scope and complexity, to the ITM Project. The experience shall include, as the project manager, the successful delivery of at least one similar project involving delivery of high resilience datacentres, migration of applications, integration of the capabilities and testing under one centralised service management and control system in an environment where security was a significant concern.

7.3.3.2. Senior Scrum Master

SOW-0203 The Contractor's Senior Scrum Master shall perform the following activities:

SOW-0203.A Leading the Scrum teams and facilitate the Scrum events (Sprint Planning, Daily Scrum, Sprint Review, and Sprint Retrospective).

SOW-0203.B Guide the development team on how to use Agile/Scrum practices and values.

SOW-0203.C Ensure that the development team is working effectively and efficiently towards the sprint goal and 'Definition of Done' is understood and followed.

SOW-0203.D Support the Project Manager for schedule management activities.

SOW-0203.E Support the technical scrum teams in planning the implementation of complex private cloud infrastructures sprints

SOW-0203.F Coaching the Scrum Teams on Agile, Scrum, Kanban as required

SOW-0204 The Contractor's Scrum Master shall be responsible from the Requirements Management functions as outlined below:

SOW-0204.A documenting and managing formal requirements documentation,

SOW-0204.B establishing, managing and analysing traceability between requirements and other architecture, design and verification artefacts, such as test cases and test results and,

SOW-0204.C producing reports on requirements and requirements traceability matrices, via a professional requirements management tool, such as IBM DOORS.

SOW-0205 The Contractor's Senior Scrum Master shall have:

SOW-0205.A relevant and recent experience in using the Scrum methodology and tools such as JIRA.

SOW-0205.B experience with implementing complex private cloud infrastructures and experience in managing teams in Private cloud projects

SOW-0205.C experience of leading Agile Scrum teams

7.3.3.3. Quality Manager

SOW-0206 The Contractor's Quality Manager shall be responsible for developing and implementing the project Quality Assurance Plan to align with section 8.2.

SOW-0207 The Contractor's Quality Manager shall be responsible for ensuring quality management policy and principles adhered to throughout the execution of the WP and shall ensure the deliverable quality before the release to the Purchaser.

SOW-0208 The Contractor's Quality Manager shall have minimum five (5) years of experience in the planning and execution of quality assurance activities.

SOW-0209 The Contractor's Quality Manager shall have minimum of three (3) years of experience in software/system/service life cycle quality management in ICT projects.

7.3.3.4. Risk and Issue Manager

SOW-0210 The Contractor's Risk and Issue Manager shall:

SOW-0210.A Develop and maintain the risk and issue management plans and logs (consistent with Purchaser risk management strategy and processes);

SOW-0210.B Identify risks, support the assessment of impacts, and the implementation of responses to decrease the probability of negative events and increase probability of positive outcomes;

SOW-0210.C Assess, establish and maintain the mitigation/response actions log and regularly review;

SOW-0210.D Monitor and report status of response actions regularly;

SOW-0211 The Contractor's Risk Manager shall have at least 3 years of practical experience in managing risks and issues of ICT projects and/or programmes.

7.3.4. Contractors' Engineering and Technical Team

7.3.4.1. Release and Integration Lead

SOW-0212 The Contractor's Release and Integration Lead shall coordinate the implementation and deployment of all services, design updates and/or changes to the Service design package.

SOW-0213 The Contractor's Release and Integration Lead shall be responsible for coordination with the Purchaser for defining and managing the release strategy for the WP products to be transitioned into operations.

SOW-0214 The Contractor's Release and Integration lead shall be responsible for the coordination with the designated Purchaser PoC's to ensure the organizational processes are followed. To ensure timely coordination, the Contractor's Release and Integration Lead shall inform the Purchaser PoC's 4 weeks prior to go live event (i.e. transition into operations).

SOW-0215 The Contractor's Implementation and Integration Lead shall have minimum of three (3) years experience with implementing complex private cloud infrastructures and managing teams.

SOW-0216 The Contractor's Implementation and Integration Lead shall have minimum of two (2) years of experience as Principal or Senior solution/segment architect.

7.3.4.2. Work Package Architect

SOW-0217 The Work Package (WP) Architect shall operate under the direction from the designated Purchaser PoC's (e.g. Purchaser Technical Lead, Purchaser Architect and Purchaser Technical Design Authority).

SOW-0218 The Contractor's Architect shall:

SOW-0218.A Refine, further develop and maintain the technical architecture of services within the scope of this SOW, including the refinement and further development of interface definitions to purchaser provided services;

SOW-0218.B Ensure alignment and coherence of the architecture with existing Purchaser provided architecture;

SOW-0218.C Ensure full architectural conformance of the Contractor's deliverables; and

SOW-0218.D Develop, refine and maintain architectural artefacts in ArchiMate.

SOW-0219 The Contractor's WP Architect shall have:

SOW-0219.A A minimum requirement of a University degree at a nationally recognized/certified University in a related discipline;

SOW-0219.B Certification for The Open Group Architecture Framework (TOGAF) or The Open Group Certified Architect certification or equivalent;

SOW-0219.C Certification for ArchiMate;

SOW-0219.D Proven familiarity with ITIL and COBIT

[0097] The lack of formal university degree or certifications may be compensated by the demonstration of equivalent expertise and experience in the domain with Purchaser's approval.

SOW-0220 The Contractor's WP Architect shall have:

SOW-0220.A A minimum of three (3) years of experience in cloud architecture definition for large ICT environments;'

SOW-0220.B Extensive experience in providing support and guidance to technical teams during implementation of large ICT and/or Software projects

SOW-0220.C Extensive experience managing relationships with senior stakeholders (internal and external)

SOW-0220.D Proven ability to apply analytical and systems thinking to complex problems.

SOW-0220.E Proven ability to moderate technical design related discussions with multi-disciplinary teams.

SOW-0220.F Proven ability to effectively communicate orally and in writing, with good briefing skills.

7.3.4.3. Technical Lead

SOW-0221 The Technical Lead shall be responsible from ensuring the technical coordination and orchestration of the project's high level and detailed designs across ITM Recovery Increment 1.

SOW-0222 The Contractor's Technical Lead shall support design activities, provide implementation guidance and proactively address technical integration issues.

SOW-0223 The Contractor's Technical Lead shall plan and co-ordinate engineering activities to meet the SRS requirements.

SOW-0224 The Contractor's Technical Lead shall provide comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance.

SOW-0225 The Contractor's Technical Lead shall supervise the work of a design, integration, test, and implementation team.

SOW-0226 The Contractor's Technical Lead shall have a recognised formal IT infrastructure (ITIL) and virtualization technologies (i.e. VMWare) certification.

SOW-0227 The Contractor's Technical Lead shall have minimum 10 years experience in leading engineering/integration teams delivering new capability in IT environments under demanding time critical situations.

7.3.4.4. Test Director (TD)

SOW-0228 The TD shall also be responsible for all testing and reporting for all related test activities conducted

SOW-0229 The TD shall coordinate the overall test, verification and validation plan with the Purchaser's IV&V Coordinator.

SOW-0230 The TD shall apply the V&V processes to the test events under the WP area of responsibility during the Engineering Test Phase, Qualification Test Phase, WP System Acceptance Test and WP Transition into Service Verification Phase.

SOW-0231 The TD shall create and develops the WP Master Test Plan, Test Event Plans, test Suites, test procedures, test cases and the Test Reports (including Fault Report and Off-Specification Report), and maintains all WP test artefacts.

SOW-0232 The TD shall support the independent test events under the TVV Assessment and SiAT phases by proposed test design, test procedures and test cases to validate and accept the solution under the Contractual area of responsibility.

SOW-0233 The TD shall ensure that the issues under the Contractual area of responsibility are verified and validated before proposing their closure during a formal acceptance test event.

SOW-0234 The TD shall ensure that all failure, deficiencies and errors are recorded and tracked until resolution.

SOW-0235 The TD shall prepare and conduct the Test Readiness Reviews (TRRs)

SOW-0236 The TD shall oversee the test events within the scope.

SOW-0237 The TD shall request test environment requirements implementation

SOW-0238 The TD shall analyse data and findings

SOW-0239 The TD shall report findings

SOW-0240 The TD shall maintain test data archives

SOW-0241 The TD shall request audits to verify compliance with requirements, test plans and procedures, and overall test configuration management.

SOW-0242 The TD shall generate and manage test result issues, finding, observations, and recommendations within the integrated repository

SOW-0243 The TD shall have a University Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master and supplemented by relevant postgraduate qualifications, supported by relevant certificates/ diplomas. Exceptionally extensive relevant experience may be considered if the above qualifications are not met.

SOW-0244 The TD shall have integration and testing engineering skills with minimum ten (10) years' leadership experience of large ICT projects, similar in scale, scope and complexity to ITM, supported by project references, PoC, and description of role/responsibilities/activities.

SOW-0245 The TD shall have demonstrated leadership and practical experience in planning, conducting and assessing Integration and Testing activities in support of large ICT projects for at least five (5) years, supported by project references, PoC, and description of role/responsibilities/activities.

SOW-0246 The TD shall have demonstrated practical and leadership experience in testing of IT infrastructure and ECS where the role of test engineer or integration engineer was exercised, supported by project references, PoC, and description of role / responsibilities / activities.

SOW-0247 The TD shall have demonstrated practical and leadership experience in ICT migrations where the role of test engineer or integration engineer was exercised for migration of ICT services (Active Directory, business applications and associated data), supported by project references, PoC, and description of role/responsibilities/activities.

SOW-0248 The TD shall have demonstrated practical knowledge and experience with QA standards (either AQAP or ISO), processes for integration and (pre) migration testing.

SOW-0249 The TD shall have a spoken and written fluency in English, at a minimum level of SLP 4343. as defined in STANAG 6001 [Ref: STANAG 6001].

7.3.4.5. Engineer(s) - Security

SOW-0250 The Contractor shall designate Engineers – Security, having as role:

SOW-0250.A To ensure Security baseline and security mechanism measures are appropriately designed and implemented.

SOW-0250.B To ensure to ensure that an adequate level of protection is achieved and maintained throughout the all project stages. This includes ensuring that the ON conforms to NATO security policy and supporting directives, and the CIS-specific security-related documentation.

SOW-0250.C To ensure the architecture and design is compliant with NATO Policy in order to achieve security accreditation. Security compliance is automated.

SOW-0250.D To act as the accountable Contractor PoC for the Security Accreditation matters and to provide technical input to the Security Accreditation documentation under guidance from the designated Purchaser PoC's.

SOW-0250.E To develop test cases to the Security Test and Verification Plan

SOW-0250.F To execute Security Test and Verification Plan.

SOW-0250.G To develop Security Test and Verification Report (STVR) in collaboration with the designated Purchaser PoC's.

SOW-0251 The Engineer-Security shall have minimum 5 years:

SOW-0251.A Experience as Security Engineer in IT environments or projects, specifically:

SOW-0251.A.1 with the application and maintaining of security controls;

SOW-0251.A.2 the identification and escalation of security risks and issues;

SOW-0251.A.3 basic risk assessment; and

SOW-0251.A.4 the definition of secure systems configurations in compliance with architectures

SOW-0251.B Experience in automating security baseline deployments and reports.

7.3.4.6. Engineer(s)- Identity and Access Management

SOW-0252 The Contractor shall designate Engineers – Identity and Access Management(IAM), having as role:

SOW-0252.A To implement IAM services according to the design.

SOW-0252.B To ensure deployment is automated/perform via Infrastructure as a code.

SOW-0253 The Contractor shall designate the Engineer-Identity and Access Management, with minimum 3 years' experience:

SOW-0253.A IDAM with Microsoft environment.

SOW-0253.B in automating security baseline deployments and reports.

7.3.4.7. DevOps Engineer(s) - Automation Architect

SOW-0254 The Contractor shall designate Automation Architects part of the cross-functional role which

SOW-0254.A Will support the other scrums within the project in all aspects related to automation

SOW-0254.B Update and/or Design solutions and automation strategies.

SOW-0254.C Lead the implementation of automation across all areas.

SOW-0254.D Write test automation code for all the components

SOW-0255 The Automation Architect shall have minimum 5 years of relevant experience in designing the automation for large multi-disciplinary projects, including the application of

tools, techniques and process to track, log and correct information related to configuration items.

SOW-0256 The Automation Architect shall have proficiency in major automation tools (Terraform, Ansible, Git and/or others) including the design and implementation thereof.

SOW-0257 The Automation Architect shall include management of the lifecycle of change requests impacting services and systems; change risk assessment; development of processes for changes and development change control process architecture.

7.3.4.8. DevOps Engineer(s) - IaaS

SOW-0258 The Contractor shall designate DevOps Engineers – IaaS, which would have the following responsibilities:

SOW-0258.A Implement Infrastructure services and automation services according to the design.

SOW-0258.B Update and/or design Infrastructure solutions.

SOW-0258.C Ensure the implementation is automated to the maximum extent

SOW-0258.D Lead the IaaS scrum team

SOW-0259 The DevOps Engineer – IaaS shall have minimum 5 years of:

SOW-0259.A Experience with Infrastructure automation deployment including network, processing, and storage.

SOW-0259.B Experience with major automation tools (Terraform, Ansible, git and/or others).

SOW-0260 The DevOps Engineer(s)-IaaS shall have minimum 5 years of relevant experience in implementing IaaS and automation services for large multi-disciplinary projects and proficiency in major automation tools (Terraform, Ansible, Git and/or others) including the design and implementation thereof.

SOW-0261 The DevOps Engineer(s) shall have experience VMware and Microsoft OS centralized and automated deployment and control familiarity.

7.3.4.9. DevOps Engineer(s) - Networking

SOW-0262 The Contractor shall designate a Senior DevOps Engineer – Networking, having as role:

SOW-0262.A Implement networking services and automation services according to the design.

SOW-0262.B Implement all the underlying networking elements

SOW-0262.C Update and/or design Infrastructure solutions.

SOW-0262.D Ensure the implementation is automated to the maximum extent.

SOW-0263 The DevOps Engineer – Networking shall have minimum 5 years:

SOW-0263.A Experience with Infrastructure automation deployment including network and firewalls.

SOW-0263.B Experience with major automation tools (Terraform, Ansible, git and/or others).

7.3.4.10. Test Engineers (TE)

SOW-0264 The TE shall have the experience as tester or independent verification and validation engineer, during all phases of the project lifecycle.

SOW-0265 The TE shall have the Higher Secondary education and completed advanced higher level vocational training in Electronics Engineering or Information Systems related discipline

leading to a professional qualification or professional accreditation with 4 years post experience.

SOW-0266 The TE shall perform testing in support of projects, exercises and interoperability events by providing assistance in assessment of requirements testability.

SOW-0267 The TE shall support test management activities, as needed mainly:

SOW-0267.A Testbed preparation for test events and reviewing test plans and test cases.

SOW-0267.B Supporting project and event stakeholders in the preparation leading up to a test event.

SOW-0267.C Participating in unit, system and integration testing with design and provide support to Projects for test automation.

SOW-0267.D Provide insight for structured performance testing based on non-functional requirements.

SOW-0267.E Producing test reports and updating data contained within test management tools.

SOW-0267.F The TE shall have Experience using test and test management tools such as JIRA and JIRA automation add-ons;

SOW-0267.G The TE shall have Experience in test automation and performance testing

7.3.4.11. Field Service Engineer(s)

SOW-0268 The Field Service Engineer(s) shall execute the following main activities, as part of Early Life and O&M Support:

SOW-0268.A Assisting the Purchaser's in-service personnel on site (ESOC, CSUs, Engineers) with isolating and eliminating faults and failures involving the hardware and software, and integration and configuration work furnished by the Contractor as part of this Contract;

SOW-0268.B Assisting the Purchaser's in-service personnel on site with operating the hardware and software, and integration and configuration work furnished by the Contractor as part of this Contract.

SOW-0268.C Assisting the Purchaser's in-service personnel on site with performing preventive, corrective, perfective, and adaptive maintenance of the hardware and software, and integration and configuration work furnished by the Contractor as part of this Contract.

SOW-0268.D Delivery of comprehensive On-The-Job (OTJ) Training to the Purchaser's in-service personnel on site. The OTJ Training shall be an extension of the Contractor's training received by the site personnel and entails the practical application of all that was taught at the training courses and all that was submitted as part of the training material package. Any OTJ Training shall be organised and executed by the Field Service Engineer, ad-hoc, informally, and as-required. The OTJ Training shall make use of the Contractor's technical documentation and training materials produced as part of this Contract.

SOW-0268.E Actively monitoring the Purchaser's in-service personnel on site of their daily conduct of operation and maintenance actives involving the hardware and software, and integration and configuration work furnished by the Contractor as part of this Contract, and to provide advice on potential problems and shortfalls thereof.

SOW-0268.F Assisting the Purchaser's in-service personnel on site with the invocation, monitoring, and closure of warranty cases, and the maintenance support services in scope of this Contract.

SOW-0269 The Field Service Engineer shall provide support, as specified in this Contract, and as tasked by the Purchaser's in-service personnel on site.

SOW-0270 The Field Service Engineer shall be a fully knowledgeable, experienced, trained, and skilled expert in the design, implementation, integration and configuration of any supplies, services and work delivered by the Contractor under this Contract.

7.4. Work Package Management Processes

[0098] The project measurements are a hybrid of predictive and empirical, value-based Agile ones.

SOW-0271 Work in progress and its status shall be reported by the Contractor by using Agile flow diagrams or alike, measuring the feature status in time.

SOW-0272 A comprehensive set of milestones as described in Section 0 of this SoW. The Contractor shall achieve all milestones defined in the contract within the time limits specified for achievement relative to the effective date of contract.

SOW-0273 Work Package 'Project Management Documentation' is described in Section 13.2.

7.4.1. Risk Management

SOW-0274 The Contractor shall establish and maintain a Risk Management process for the project, described in the RMP, and compliant with ITM-RC1 Risk Management Plan [Ref: ITM-RC1 RMP].

SOW-0275 The Contractor's Risk Management process shall at minimum enable and define identification of all types of risks, evaluation and prioritization of each risk, definition of proposed response strategy, owner and actions and suggested monitor and control mechanisms.

SOW-0276 The Contractor shall document and maintain status of all risks in the Risk Log (see 13.2.1.8) where he shall record and track all project risks regardless of their status.

SOW-0277 The Contractor shall update the project Risk Log at minimum on a monthly basis as an input for the Project Status Report (PSR).

SOW-0278 The Contractor shall add to the Risk Log additional risks identified by the Purchaser.

SOW-0279 Upon Purchaser request, the Contractor shall deliver the Risk Log to the Purchaser, throughout the duration of the Contract.

7.4.2. Issue management

[0099] A Project Issue is anything that could have an effect on the Project, either detrimental or beneficial (e.g., problem, error, anomaly, risk occurring, query, change in the project environment, change request, off-specification).

SOW-0280 The Contractor shall establish and maintain a process for identifying, tracking, reviewing, reporting, and resolving all project issues.

SOW-0281 The Contractor shall describe the Issue Management Process in the Risk and Issue Management Plan (RIMP) see section 13.2.1.7.

SOW-0282 The Contractor shall develop and maintain an Issue Log (see Section 13.2.1.9) where he shall record and track all project issues regardless of their status.

SOW-0283 The Contractor shall update Issue Log at minimum on a monthly basis as an input for the PSR.

SOW-0284 The Contractor shall add to the Issue Log additional issues identified by the Purchaser.

SOW-0285 Upon Purchaser request, the Contractor shall deliver the Issue Log to the Purchaser, throughout the duration of the Contract.

7.4.3. Configuration management

SOW-0286 The Contractor shall implement a Configuration Management plan to perform the Configuration Management functions as described in Section 10 of this SoW.

7.4.4. Quality Assurance (QA) and Quality Control (QC)

SOW-0287 The Contractor shall establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the period of performance of this Contract as described in section 8.2.

7.5. Project Management Communications

7.5.1. Formal Meetings

SOW-0288 The Contractor's PM or his designated representative shall participate in all formal project meetings (e.g. Kick-off Meeting, Sprint Planning Meetings, Sprint Review Meetings, Project Progress Review Meetings).

SOW-0289 The Contractor shall participate in a project kick-off meeting plan for each application major lifecycle phase or Spiral, which shall be held at the Purchaser's facility.

SOW-0290 The Contractor shall plan, organize and execute quarterly Work Package Progress Review Meetings, where the design, integration and implementation progress as well as the overall execution progress is presented for the management.

SOW-0291 The following provisions shall apply to all formal meetings to be held under the contract:

SOW-0291.A The Contractor shall take meeting minutes (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;

SOW-0291.B The final version of the meeting notes shall be posted by the Contractor on the Collaboration portal (see 7.5.11) within three (3) working days of receipt of Purchaser approval;

SOW-0291.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 an amendment to the Contract by the Purchaser's Contracting Officer; and

SOW-0291.D Any documentation, even in draft format, that may be useful to the Purchaser in preparing for Design or Project Progress Review Meetings and ensuring efficient discussions during the meetings shall be provided to the Purchaser no later than ten (10) working days before the meeting.

7.5.2. Scrums

SOW-0292 **Scrums Daily Call**: Per identified scrum teams (AG1&AG2 Scrum team, AG3&AG4 Scrum team, AG5 Scrum team), the Contractor shall organize the daily Scrum(s) organized by Contractor's team leads and in participation of the relevant Purchaser team members.

SOW-0293 **Scrum of Scrums**: The Contractor shall organize weekly Scrum of Scrums, and shall ensure participation of the other scrum team representatives.

SOW-0294 **Sprint Review and Retrospective Meeting**: The Contractor shall organize the Sprint Review and Retrospective Meeting(s) at the end of each Sprint. Current plan is to have monthly sprints.

SOW-0295 **Sprint Planning Meeting**: The Contractor shall organize a sprint planning meeting at the beginning of each Sprint. Current plan is to have monthly sprints.

7.5.3. Task Order Planning Meeting

SOW-0296 Task Order planning meetings shall be organized prior to the release of the Task Order, to identify and document the agreed scope of work.

SOW-0297 Task Order Planning Meeting shall be led by the Contractor Project Manager, in support of the Scrum Master and Technical Lead, with participation of the other key personnel that require to provide subject matter support.

7.5.4. Task Order Acceptance Meeting

SOW-0298 Task Order planning meetings shall be organized prior to the release of the Task Order, to identify and document the agreed scope of work.

SOW-0299 Task Order Planning Meeting shall be led by the Contractor Project Manager, in support of the Scrum Master and Technical Lead, with participation of the other key personnel that require to provide subject matter support.

7.5.5. Project Progress Review Meetings (PPRMs):

SOW-0300 PPRMs shall be held monthly at the Purchaser's facility.

SOW-0301 The PPRMs shall follow a standard agenda as indicated by the minutes requirements specified in Sections 7.5.5 and 7.5.13.1.

SOW-0302 The Contractor shall provide a Progress Status Report (PSR) two weeks in advance of the PPRM. The PSR shall summarize the activities and progress, including (but not limited to):

SOW-0302.A Changes in key Contractor personnel;

SOW-0302.B Summary of Contract activities during the preceding month, including the status of current and pending activities;

SOW-0302.C Progress of work and schedule status, highlighting any changes since the preceding report;

SOW-0302.D EVM KPIs, including Planned Value, Earned Value, Actual Cost, Schedule Variance, Schedule Performance Index, Budget at Completion and Estimate at Completion.

SOW-0302.E CSA report addressing all products in the Project Breakdown Structure;

SOW-0302.F Issue Log;

SOW-0302.G Change Requests status;

SOW-0302.H Off-Specifications status;

SOW-0302.I Risk Log;

SOW-0302.J Test(s) conducted and results;

SOW-0302.K Summary of any site surveys conducted;

SOW-0302.L Plans for activities during the following reporting period;

SOW-0302.M Provisional financial status and predicted expenditures.

7.5.6. Documentation Delivery and Review

[0100] Documentation delivery and review process is described in Section 13.

7.5.7. WP07 All Hands

SOW-0303 The Contractor shall attend WP07 All-hands organized by the Purchaser as required.

7.5.8. Security Accreditation Meetings

SOW-0304 The Contractor security SME's shall attend to the Purchaser led Security Accreditation meetings, where the inputs from design and implementation activities are collected monthly for the SADS document set created by the Purchaser.

7.5.9. Ad-Hoc Meetings

SOW-0305 The Contractor shall carry out ad-hoc project-level communication activities as needed to clarify project issues.

SOW-0306 The Purchaser and Contractor PM shall hold fortnightly contact from the Kick off meeting through the remaining contractual period.

SOW-0307 The Purchaser and Contractor shall exchange contact telephone numbers and agree on conference call requirements (day and time) during the project kick-off meeting.

SOW-0308 Action Items from the conference calls shall be drafted by the Contractor and added to the ITM-RC1 Action Item List by the Contractor within 2 days of the conference call.

7.5.10. Project Reporting

SOW-0309 The Contractor shall provide to WP07 Lead, no later than the third working day of each month, a Project Status Report (PSR). The Contractor's PSR shall be a monthly document to cover the previous month and include cumulative aspects of execution.

SOW-0310 The Contractor shall ensure that the PSR summarises activities and progress, including (but not limited to):

SOW-0310.A Changes in key Contractor personnel;

SOW-0310.B Summary of Contract activities during the preceding month, including the status of current and pending activities;

SOW-0310.C Progress of work and schedule status, highlighting any changes since the preceding report;

SOW-0310.D EVM KPIs, including Planned Value, Earned Value, Actual Cost, Schedule Variance, Schedule Performance Index, Budget at Completion and Estimate at Completion.

SOW-0310.E CSA report addressing all products in the Project Breakdown Structure;

SOW-0310.F Issue Log;

SOW-0310.G Change Requests status;

SOW-0310.H Off-Specifications status;

SOW-0310.I Risk Log;

SOW-0310.J Test(s) conducted and results;

SOW-0310.K Summary of any site surveys conducted;

SOW-0310.L Plans for activities during the following reporting period;

SOW-0310.M Provisional financial status and predicted expenditures.

SOW-0311 The Contractor's PSR shall at minimum summarise completed, ongoing, and upcoming activities, as well as attached updated WMS as needed, Risk and Issue Log.

[0101] The Purchaser will issue comments no later than one week after receipt of the document.

SOW-0312 The Contractor shall issue answers to Purchaser provided comments within one week after their receipt. No comment received within that timeframe means that the Contractor agrees to the comments issued by the Purchaser and will update the document accordingly.

SOW-0313 The Contractor shall provide an updated PSR, not older than 5 working days, as a base document for the PRM as sent to all PRM participants at least 2 business days in advance.

SOW-0314 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 WMP, WIP, Integrated Support Plan (ISP), QAP, Issue Log, Change Requests document etc.

SOW-0315 The Contractor shall address and discuss key project issues, risks and events with the Purchaser Project Manager promptly, and shall not postpone it until the next PRM.

7.5.11. Collaboration Portal

SOW-0316 The Contractor shall use the ITM-RC1 project portal provided by the Purchaser to create and maintain all up-to 'NATO Restricted' documents using a Purchaser provided REACH laptop (See Annex B of the Contract Special Provisions). This shall include all project deliverables, and all the files, documentation and data created within the scope and for this project, with the exception of NS data and NU data which will be maintained in the Purchaser provided NS and NU devices.

[0102] The Purchaser will provide the appropriate access rights to the Contractor for a working space which will be used by the Contractor team throughout the execution of the project.

SOW-0317 The Contractor shall maintain on this portal all unclassified and restricted documents, as soon as they are submitted in draft version to the Purchaser. For any official submission, the Contractor shall inform the Purchaser PoC via a dedicated e-mail, to initiate the review and approval process.

SOW-0318 In case there is downtime experienced in the Purchaser provided collaboration tools, the Contractor may create and maintain the artefacts in local copies. In this case, the Contractor shall upload the data to the portals as soon as services are available.

SOW-0319 The Contractor shall identify all relevant classified documents on the Project portal, by title, unless a title itself is classified higher than NR and shall state from where the classified document can be obtained.

SOW-0320 The Contractor shall be compliant with the Purchaser "Documentation Management SoP' [Ref: ITM-RC1 SOP DM] in creation and maintenance of all the documentation and data.

7.5.12. Meeting Locations

[0103] The Contractor shall organize the meetings to be held with physical participation in Purchaser facilities, where the IPT is located. However, if and when agreed by the Purchaser, the meetings can be organized with remote participation instead.

7.5.13. Summary of the Project Management formal meetings

[0104] The Purchaser or his designated representative will chair all meetings.

SOW-0321 The Contractor shall schedule project meetings (other than Daily Calls) in the WIP.

SOW-0322 The Contractor shall produce a draft agenda for the Purchaser's approval at least one week before the meeting.

Formal Meeting	Anticipated Frequency and Duration	Objective	Typical participants
Kick-Off	Once per major phase Maximum 2.5 days	Start a new stage, a new phase in the project as defined in the Project Lifecycle	All hands
Task Order Planning	Prior to each Task Order Maximum 1 day	Plan the detailed set of requirements to be covered in the upcoming Task Order	Management team and relevant scrum team(s)

Formal Meeting	Anticipated Frequency and Duration	Objective	Typical participants
Task Order Acceptance	For the acceptance of each Task Order Maximum 4 hrs	Status update and assessment on the services delivered as part of the task Order and acceptance status.	Management team and relevant scrum team(s)
Sprint Planning	Monthly Maximum 4 hrs.	Identify the value to be achieved per sprint, refine the backlog, estimate the 'requirements' to be implemented as part of the Sprint(s)	All scrum teams
Sprint Review and Retrospective	Monthly Maximum 4 hrs.	Per product review what was achieved Take decisions on what is not achieved Review the processes – continuous improvement	All scrum teams
Project Progress Review	Monthly Maximum 2 hrs.	Review the project from contractual point of view (identify concerns, discuss risks, situation of TOs, Change Requests)	All scrum teams
WP07 All Hands	Quarterly Maximum 3 hrs.	Present project status, receive feedback from larger team	All hands + external to WP07 stakeholders
Scrum Daily Calls	Daily Maximum 30mins	Identify blockers, ensure prioritization of tasks per scrum team	Per scrum team
Scrum of Scrums	Weekly Maximum 1 hr 30 mins	Identify blocker, ensure prioritization across scrum teams	Scrum leads
Change Control Board	Monthly or Ad-hoc Maximum 2 hrs.	Review Change Requests coming from the teams	Nominated CCB members
ITM Engineering Board (IEB)	Monthly or Ad-hoc Maximum 2 hrs.	Review Technical Change Requests coming from the entire ITM Recovery Inc1	Nominated WP07 leads Technical Leads from other WPs

Table 4 - Project Management Formal meetings

7.5.13.1. Meeting Documents

SOW-0323 The Contractor shall create and share the agenda for each meeting and share it minimum 5 business days in advance for Purchaser's planning.

SOW-0324 The Contractor shall summarise discussions, action items and decisions within 5 working days after the meeting within the Minutes of the Meeting (MoM) as listed below:

SOW-0324.A Subject heading. The subject heading shows the general purpose of the meeting, its location and date

SOW-0324.B Present. After the subject heading, list of participants at the meeting by name and job title, prefaced by the word 'Present'. List the Chairman first and the Secretary last.

SOW-0324.C Representatives. Some people come to meetings as a representative of someone who was due to attend, but could not. List a representative's details in the list of those Present, and also show the job title of the person they represented.

SOW-0324.D Attendance for part of a meeting. If people do not attend the whole meeting, record the items for which they were present, in one of the following ways:

SOW-0324.D.1 By exclusion. ‘(not for Item 1)’.

SOW-0324.D.2 By inclusion. ‘(Items 2 and 3 only)’.

SOW-0324.E Approval of previous meeting’s minutes and all resolutions;

SOW-0324.F Record of principle points discussed, action taken, and decisions made

SOW-0325 The Contractor shall have as a minimum the below standing agenda Items for any formal meeting:

SOW-0325.A Minutes of last (relevant) meeting;

SOW-0325.B Matters arising from last (relevant) meeting;

SOW-0325.C Any other business;

SOW-0325.D Arrangements for next meeting.

7.6. NATO Information Protection

SOW-0326 The Contractor shall implement the requirements for NATO Information Protection as outlined in Appendix 3, as applicable for the scope of the Contract.

7.7. Cyber Incident Reporting

SOW-0327 The Contractor shall implement the requirements for Cyber Incident Reporting as outlined in Appendix 3, as applicable for the scope of the Contract.

8. CIS SECURITY ACCREDITATION

8.1. CIS Security Accreditation Requirements (NATO ON)

[0105] The primary objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the NATO ON Communication and Information System (CIS). This includes ensuring that the NATO ON CIS conforms to NATO Security Policies and Directives and the NATO ON specific Security Accreditation Documentation Set (SADS) (see D.5).

[0106] The security accreditation statement is to be issued to the Purchaser by the NATO Security Accreditation Authority, hereinafter referred to as the Security Accreditation Authority (SAA), for the ON CIS to store, process and transmit NATO classified information in its operational environment.

[0107] The overall security accreditation of the ON is coordinated by the NATO CIS Security Accreditation Board (NSAB) representing three NATO primary SAAs (Allied Command Operations (ACO) SAA, Allied Command Transformations (ACT) Office of Security SAA and NATO Office of Security (NOS) SAA).

[0108] The Lead SAA for the security accreditation of the NATO ON is the ACO SAA.

[0109] For each NATO ON site, the Local SAA function is performed by one of the NATO primary SAAs mentioned above.

SOW-0328 The security accreditation of the ON shall follow a structured process based on the high level security requirements established in the AC/35-D/2005-REV3 Management Directive on CIS Security [Ref: AC/35-D/2005-REV3] as detailed in this section and in the ON Security Accreditation Plan (SAP). Deviations from this structured process shall always be documented and can only be authorised by the SAA, through the Purchaser.

SOW-0329 The security accreditation process for the ON shall be strictly followed by the Contractor under the guidance of the Purchaser, and shall encompass the overall development, and implementation of the ON.

[0110] Security accreditation for ON will need to be achieved before the system is transitioned to the operational live-environment, unless the SAA requires that some security related activities be conducted in the operational live-environment.

[0111] Roles and Responsibilities in the security accreditation process pertaining ITM Recovery are depicted in Figure 4 and described in this section.

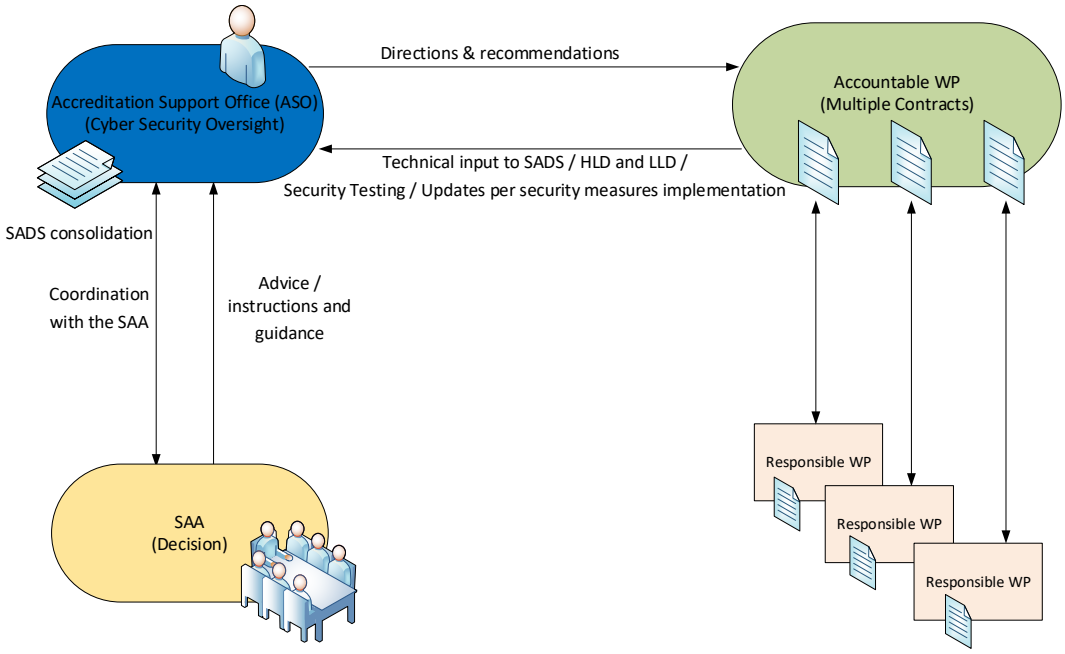

Figure 4 - Roles and Responsibilities in the security accreditation process

[0112] The Purchaser's Accreditation Support Office (ASO) will oversee the cyber security policy compliance aspects for the ON and be a focal NATO cyber security policy knowledge hub for the ITM Recovery project.

[0113] Specifically for this WP SoW, ASO will provide directions and guidance to the Contractor, including details related to NATO Security Policies and Directives, available and catalogued security configuration(s), security settings, installation guides and configuration guidelines.

[0114] ASO will facilitate and lead the coordination of the security accreditation process with the SAA. For some activities, the ASO may delegate the authority to other members of the Purchaser.

[0115] ASO will improve, consolidate and review the SADS and provide it to the SAA for their review and approval.

SOW-0330 The Contractor shall comply with the NATO Security Policies and supporting Directives identified in D.4.2 and any other guidance provided by the Purchaser, in the resulting ON system design and installation thereof.

SOW-0331 The Contractor shall ensure the ON architecture and design follow the "Security by Design principle", and shall take into account the initial CIS Description provided by the Purchaser in their design efforts.

SOW-0332 The Contractor shall ensure the ON is configured, deployed and tested accordingly to the developed architecture and design, complying with the security requirements (relevant and under the responsibility of the Contractor) as specified in the SADS (e.g. SRA, SSRS, STVP and SecOPs etc.).

SOW-0333 The Contractor shall provide and ensure implementation of all the security measures, for all relevant services and interfaces within the scope of their contract, as detailed by the Purchaser in the Security Risk Assessment (SRA), System-specific Security Requirement Statement (SSRS), System Interconnection Security Requirement Statement (SISRS), Security Operating Procedures (SecOPs), and other relevant accreditation documents, for all provisioned ON Nodes.

SOW-0334 The Contractor in collaboration with and following the guidance of the Purchaser, shall ensure through security testing that all the security measures within the scope of their (Contractor's) implementation responsibility, as per contract, and identified in the SRA, SSRS, SISRS and SecOPs, have been properly implemented in accordance with the requirements of the SAA.

SOW-0335 The Contractor shall achieve SOW-0534 via security testing conducted based upon the SAA approved STVP, which shall cover the security requirements identified and approved in form of the respective SSRS, and SISRS. The Contractor shall support all relevant security testing efforts that concern the security requirements under their contracted responsibility as System Integrator.

[0116] The ON security requirements implementation and effectiveness will be further verified by the independent security audit unless decided otherwise by the SAA.

SOW-0336 Within the SADS, the Contractor shall ensure that it presents to the Purchaser all required documents listed in the section 8.1.3.

SOW-0337 Contractor shall recognize that the SAA might require additional documents for the successful accreditation of ON especially after the interconnections of ON (i.e. a document capturing a specific set of security measures relevant to the self-protection of an interconnected component in the ON).

SOW-0338 The Contractor shall provide the technical input to the required SADS to the Purchaser, who in turn shall provide the Contractor with the guidance and templates for this task, as well as any additional information as relevant and necessary.

SOW-0339 The Contractor shall in no event deliver any documents directly to the SAA unless directed by the Purchaser. The Purchaser will conduct coordination and review criteria with the SAA.

SOW-0340 The Contractor shall provide timely updates related to the security measures implementation to the Purchaser as the ON development and implementation unfolds.

[0117] The SAA will provide advice and instructions to the Purchaser, which will be relayed to the Contractor, on any security implication emerging from findings and results of the risk assessments and/or security test results.

SOW-0341 The Contractor shall consider the advice, instructions and guidance from the SAA, taking action(s) to follow said input, carry out the necessary work and to implement additional measures, as necessary.

SOW-0342 The Contractor shall ensure adherence to the timelines and sequence of the required deliverables as specified by the Purchaser in the ON SAP.

SOW-0343 The Contractor shall ensure that in supporting the production of the SADS deliverables, the Contractor will closely engage directly with representatives of the Purchaser ASO and/or the SAA (strictly through the Purchaser) in order to discuss security-related requirements and enhance said deliverables.

SOW-0344 The Contractor shall ensure that they participate in any security meetings and workshops whereupon their technical input is necessary with the appropriate expertise representatives, along with representatives of the Purchaser. There shall be timely communication from the Purchaser pertaining dates and location/format of such meetings to the Contractor.

SOW-0345 Respective Contractor's Subject Matter Experts (SMEs) shall support these meetings.

[0118] It has been anticipated that at least two five days technical security accreditation related workshops yearly will be required. Location of the meetings and workshops will be defined by the Purchaser and will typically take place at the Purchaser's facility. Additionally, the Contractor may be invited to provide the briefings and/or technical expertise for meeting(s) with the SAA.

8.1.1. Security Accreditation Process

[0119] The achievement of security accreditation for ON depends on development and SAA approval of necessary Security Accreditation Documentation Set identified in Figure 5.

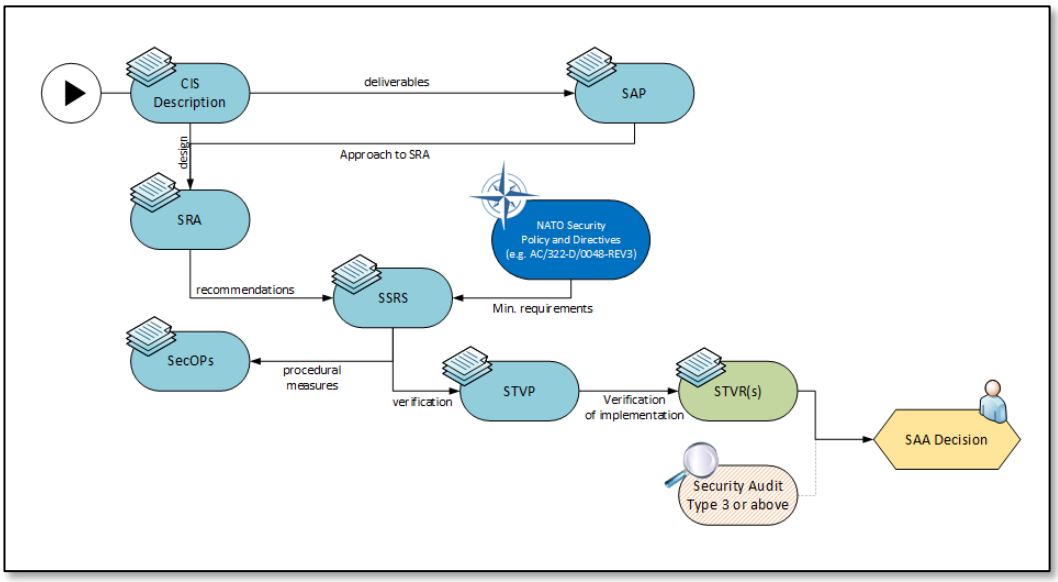

Figure 5 - SAA approval of Security Accreditation Documentation

[0120] The ASO reviews, consolidates and manages the SADS.

SOW-0346 The Contractor shall produce, collect and provide technical input to the SADS, as well as complement existing SADS documentation as directed by the Purchaser's ASO, in order to support the ON security accreditation process.

SOW-0347 The Contractor shall take into account that technical input provided to the SADS shall be approved by the Purchaser prior to delivery to the SAA.

SOW-0348 The Contractor shall take into account that only reviewed and SAA approved technical input can be accepted by the Purchaser as part of the Contractor's contribution to the security accreditation deliverables.

SOW-0349 If a document's acceptance requires multiple rounds of comments and amendments, the Contractor is obliged to comply with the requests of the Purchaser and/or the SAA pertaining the Contractor's technical input until the approval process is completed.

SOW-0350 The Contractor shall immediately inform the Purchaser in case of any potential (and realised) issues related to the implementation of any security requirement, or obtaining information of said implementation, which affects their technical input to the SADS.

[0121] In case of any potential timeline issues resulting in the unforeseen extension of the approval process of the SADS, and/or if the SAA formally communicates a delay in review to the Purchaser, then the latter shall inform the Contractor immediately.

SOW-0351 The SADS shall be developed in parallel to appropriate project deliverables related with the ON architecture and design as depicted in the points below.

SOW-0352 The Contractor shall produce the solution's designs accurately in relation to intended end-state of the ON, and provide frequent updates to the Purchaser on how the security measures are implemented in order to allow the ASO to develop and consolidate the SADS in a timely manner. .

SOW-0353 Final versions of the technical input to the CIS Description, SRA and SSRS shall be completed and released by the Contractor to the Purchaser's ASO by the same time as the LLD is released.

SOW-0354 CIS Description, SRA and SSRS shall be approved by the SAA before commencing formal security testing.

SOW-0355 Once approved by the SAA, the CIS Description becomes an authoritative design source for security and services implementation, and therefore the Contractor shall maintain the CIS Description under change control.

SOW-0356 The Contractor shall be aware of this throughout any ad-hoc mitigation/security improvement path for the CIS if such becomes relevant, and shall immediately report to the Purchaser should a risk of modification or substantial change to the CIS Description's (and to the LLD if applicable) information be identified in this improvement process.

SOW-0357 Final versions of the technical input to the SecOPs, STVP and SISRS shall be developed and released by the Contractor by the same time as the first draft of the LLD not later than 3 months prior to the start of the security testing.

SOW-0358 SecOPs and STVP shall be approved by the SAA before commencing security testing.

SOW-0359 SISRS shall be approved by the SAA before interconnection to another CIS is to take place as depicted in the CIS Description and required by SAP.

SOW-0360 Some SADS documents (especially SecOPs) might require further updates as recommended by the Contractor and/or Purchaser, based on the observations and lessons learned gathered during security tests and/or Functional Testing. New versions of every single security-related documentation shall have to be approved by the SAA to be considered final and authoritative.

SOW-0361 The Contractor shall conduct security testing in accordance with SAA approved STVPs for all ON Nodes (DC (including IREEN @NS), SN, EN, RN).

SOW-0362 The Contractor shall develop an STVR, under the guidance of the Purchaser's ASO, after each instance of security testing identified in the ON SAP where responsibility of testing is identified as the Contractor's.

SOW-0363 The Contractor shall develop a separate STVR for each ON Node (e.g. DC (including IREEN @NS), SN, EN, RN).

SOW-0364 The STVR shall be ready within 1 week after completion of the relevant security test event.

SOW-0365 The STVR shall be further amended upon any supplementary and additional security testing as required (i.e. regression testing of previously failed test cases).

SOW-0366 All identified CIS security related deficiencies documented in the STVR under Contractor responsibility, shall be either fixed by the Contractor or waived by the Purchaser before the specific ON Node shall be handed over to the Purchaser.

SOW-0367 In order to enable some specific activities (e.g. Independent Verification and Validation, Security Testing in accordance with STVP, SIT, etc.) the Contractor shall provide an Approval for Testing (AfT) Request, developed under guidance from the Purchaser.

SOW-0368 The AfT Request shall be released by the Contractor not later than 20 working days prior to each test activity requiring an AfT, unless a more comprehensive AfT is developed (i.e. multi-site/multi-node), in which case the 20 working days timeframe applies to that single AfT.

[0122] AfT request(s) are subject to SAA review (through the Purchaser). If approved, the SAA will issue the official AfT Statement.

SOW-0369 The AfT shall also be required if there will be a need to connect to some existing NATO CIS in order to finalize configuration (e.g. deployment of NPKI certificates, patch management, etc.) of specific components of the ON.

[0123] STVR approval by the SAA will be one of the conditions for the SAA to grant an (Interim) Security Accreditation statement to the ON node. .

SOW-0370 A Type 3 or higher Security Audit (Vulnerability Assessment) will be performed by the Purchaser, as required by the SAA, with support from the Contractor if relevant. All identified CIS security related deficiencies documented in the Type 3 or higher Security Audit Report, which fall under Contractor responsibility, shall either be fixed by the Contractor or waived by the Purchaser.

SOW-0371 If the achievement of the "full" Security Accreditation is not possible and the SAA will issue only the Interim Security Accreditation statement (ISA), the Contractor is to coordinate with the Purchaser whether the ISA can be considered as the acceptable process outcome, and shall further coordinate any pre-handover conditions that need to be met/fulfilled by the Contractor to ensure that conditions for full SA are met.

SOW-0372 By exception and for pressing operational deployment, an Interim Authorization to Operate (IATO) may be issued by the ON CIS Operational Authority (CISOA). The IATO has no impact on the ongoing accreditation process and shall not be considered a part of the accreditation process, but rather a temporary mitigation.

SOW-0373 It is the Purchaser's decision if an IATO shall be requested for ON.

[0124] The Purchaser reserves the right to decide whether the conditions justify accepting this as the outcome of the accreditation process, or requiring further support from the Contractor in achieving intended SA status.

SOW-0374 Considering the fact the ON will be delivered across all Nodes (e.g. DCs, SN, EN, RN) the first security accreditation shall be achieved before PSA. It shall be amended once additional Nodes will be implemented in dedicated location, and security tested based on STVP. The security accreditation statement might be amended few times to reflect addition of each ON Node separately (e.g. implementation of a specific ON Node).

SOW-0375 Purchaser and Contractor shall endeavour in best effort to achieve final security accreditation for the entire ON CIS before FOA.

[0125] All above activities and associated expected timelines are depicted in the Purchaser developed SAP.

8.1.2. Security Risk Assessment (SRA)

[0126] The SRA is a crucial and core component of the accreditation process.

[0127] The SRA is the process of identifying security risks, i.e. the threats and vulnerabilities to the CIS, determining their magnitude and identifying areas requiring countermeasures. The SRA identifies the risks that exist, the current security posture of the CIS in respect to handling information under said risks, and then assembles the information necessary for the selection of effective additional security countermeasures, based upon NATO Security Policy and supporting Directives and Guidance.

[0128] The main objective of the SRA is to define the security objectives of confidentiality, availability and integrity/authenticity of the designed ON CIS according/in tandem to the particular services to be provided by the resulting ON system, the values of the information stored and transported over the system, and the nature and levels of the particular threats being identified.

[0129] The SRA contributes to the decision on which security measures are required, and how the apportionment between technical and alternative security measures can be achieved. It shall produce an unbiased assessment of the evaluated residual risk.

[0130] The ASO will conduct and coordinate the ON SRA in accordance with AC/35-D/1017 [Ref: AC/35-D/1017-REV3].

SOW-0376 The Contractor shall contribute to the ON SRA based on the technical input and information provided by the Contractor in the CIS Description document, as well as any other expert technical input they can provide, along with the Purchaser's guidance.

SOW-0377 SRA is to be approved by the SAA in the form of an SRA Report in order to be considered formal and valid.

[0131] The Purchaser will use the SRA application PILAR 2022.1 with the NATO profile.

[0132] The SRA application will be available on the NATO NR AIS (via REACH laptop).

SOW-0378 The Contractor shall contribute to the SRA workshop(s) organized by the Purchaser at the Purchaser's facility. Respective Contractor's SMEs shall support an adequate assessment of the maturity of key security controls.

[0133] It has been anticipated that at least 2 (two) up to 5 (five) days SRA workshops will be required. This is separate from the days mentioned in statement [0118].

SOW-0379 The Contractor's technical input and support to the ON SRA process shall include but not be limited to the following:

SOW-0379.A Use of the AC/322-D/0048-REV3 Technical and Implementation Directive on CIS Security [Ref: AC/322-D/0048-REV3] as the source of security controls' maturity for the SRA, and taking the ON design into account for these perceived maturity levels;

SOW-0379.B Completing "Project Data" part in the PILAR specifically with proper identification of the security domains for ON, which falls under the Contractor's knowledge as System Integrator;

SOW-0379.C Determination of the essential information assets, with input from the Purchaser, which contribute to the fulfilment of the mission of the ON;

SOW-0379.D Determination of the value of the identified assets, with Purchaser's input, against the following impacts: disclosure, modification, unavailability and destruction;

SOW-0379.E Establishment of the Logical and Physical Zones for the ON SRA;

SOW-0379.F Identification of the threats and vulnerabilities to the ON, comprising the risk environment, and their level, with Purchaser's guidance pertaining relevance to NATO classified information;

SOW-0379.G Identification and valuation of the existing countermeasures for the treatment of risk, with guidance and input from the Purchaser;

SOW-0379.H Determination of the necessary additional countermeasures, with guidance and input from the Purchaser, and a comparison with existing measures; identifying and valuating those countermeasures, which are already installed, and identifying those countermeasures, which are recommended.

SOW-0379.I SRA valuations shall be substantiated with comments related to the particular valuation of security controls, under guidance and with input from the Purchaser.

[0134] Based on the results of the SRA, and following the evidence from the SRA Report, the Purchaser will identify areas of the ON Service that require additional/enhanced safeguards and the specific countermeasures to fully comply with NATO Security Policy and supporting Directives.

SOW-0380 Where the implementation of the security measures results in the modification of the design (without introducing additional components), other/different documentation requirements, and changes to the configuration of components, the Contractor shall evaluate/process and embody the change within the technical and financial scope of this Contract. In this instance, no ECP shall be generated. The relevant security accreditation documentation shall be amended to reflect any modification of the design.

SOW-0381 Where the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, the Contractor shall raise an ECP.

8.1.3. Security Accreditation Documentation Set

SOW-0382 The complete SADS, encompassing the entire ON CIS shall consist of the following documents:

SOW-0382.A Initial CIS Description (iCISD);

SOW-0382.B CIS Description (CISD);

SOW-0382.C SAP;

SOW-0382.D SRA Report;

SOW-0382.E SSRS;

SOW-0382.F SISRS;

SOW-0382.G SecOPs;

SOW-0382.H STVP;

SOW-0382.I STVR,

[0135] The Purchaser will provide to the Contractor after EDC the following initial part of the SADS.

A. iCISD;

B. SAP.

SOW-0383 The Contractor shall complement the information in the iCISD and SAP as per guidance from the Purchaser.

SOW-0384 The Contractor shall provide technical input to the SADS in support of the accreditation process, as managed by the Purchaser's ASO, into the following templates:

SOW-0384.A SAP – with respect to required timelines and other necessary updates;

SOW-0384.B CISD;

SOW-0384.C SRA Report;

SOW-0384.D SSRS;

SOW-0384.E SISRS;

SOW-0384.F SecOPs;

SOW-0385 The Contractor shall develop and complement the STVP and STVR in support of the accreditation process according to the following templates.

SOW-0385.A STVP;

SOW-0385.B STVR

SOW-0386 Only SAA is authorized to formally approve the security accreditation documents. The Contractor shall expect a number of review rounds per document before it will be approved.

[0136] The SAA has one (1) month reduced review cycle and a standard (3) month review cycle.

SOW-0387 Once approved, all changes to the document shall follow the standard approval and change management process.

[0137] The templates will be provided to the Contractor after EDC.

SOW-0388 The Contractor shall ensure that all input into the documents part of the SADS is developed adequately for the format of standalone documents (i.e. there shall be no single document containing both SRA and SSRS templates and input).

8.1.3.1. Security Accreditation Plan (SAP)

[0138] The SAP describes the steps to be taken to achieve security accreditation for ON.

[0139] The Purchaser will develop the ON SAP and seek approval of the SAP from the SAA. This SAP will be made available to the Contractor after EDC.

SOW-0389 The Contractor shall strictly adhere to the security accreditation activities described in the SAP as approved by the SAA. All activities related with the security accreditation process identified in SAP shall be included in the respective WIP, WMS and in the WMP.

[0140] The Purchaser will maintain the SAP during the project.

SOW-0390 The Contractor shall provide updates to the SAP in a timely manner regarding schedule of security accreditation based on relevant information available in the WMS and WIP, as well as emerging throughout the ON implementation.

SOW-0391 Any changes required by the Contractor to be incorporated into the SAP shall be provided to the Purchaser who will (if the proposed change is accepted) coordinate this with the SAA.

SOW-0392 The SAP is not the Project Schedule nor does it direct the latter. The Contractor shall not confound the two, as the SAP proposes the timelines and activities required for Security Accreditation as approved by the SAA.

8.1.3.2. Initial CIS Description (iCISD)

[0141] The iCISD will provide a framework for the development of the CIS Description and will be created by the Purchaser.

[0142] iCISD will provide for the commencing of the accreditation process and will be delivered to the SAA at the earlier stage of the accreditation process.

SOW-0393 The Contractor shall, in collaboration with the Purchaser, identify the areas within the Initial CIS Description requiring their technical input as per the scope of this contract, and shall continuously provide said technical input as updates of the CIS Description until this document materializes as completed.

8.1.3.3. CIS Description (CISD)

[0143] Together with the input for the SAP, the CISD for ON is the first document in support to security accreditation process to be developed after EDC.

SOW-0394 The Contractor shall provide technical input, under guidance of the Purchaser, to the CISD as per SOW-0617 , ensuring that it can be further enhanced as the project develops; however, any changes to the CISD that may affect the security posture of the system shall be finalized prior to the SRA)compilation and completion.

SOW-0395 The Contractor shall, at a minimum, provide the following information and technical input to the CISD document, in the services established in the scope of the contract and pertaining all system integration aspects:

- SOW-0395.A Detailed technical descriptions showing the main components at a high level, as well as detailed information flows, and how these are protected, inclusive of any data flow from leveraged networks/infrastructure (if any), as per LLD;
- SOW-0395.B Descriptions of all internal and external connections of the system including interconnections to other CIS, as per LLD;
- SOW-0395.C List of hardware and software components used, as per BOM;
- SOW-0395.D Overview of the security mechanisms which are going to be implemented in the ON and all its components.

SOW-0396 The input developed by the Contractor for the CISD shall be submitted to the Purchaser's ASO for review before it will be consolidated into the final CIS Description and provided to the SAA for approval.

SOW-0397 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall update their technical input to the CISD document as many times as necessary in order to obtain SAA approval.

[0144] The ASO shall maintain and keep the CISD document up to date throughout the project.

[0145] The ASO may provide the Contractor with any additional input relevant to the CISD sections identified as a responsibility of the Contractor, but which the respective full scope may not be strictly under the Contractor's responsibility, such as security mechanism information provided by the deliverables of other Work Packages.

8.1.3.4. Security Risk Assessment Report (SRA Report)

[0146] The Purchaser will use the NATO template "SRA Report (PILAR) Template", as listed in Annex D.5, to document the results of the SRA.

SOW-0398 The Contractor shall develop annexes to the SRA, under the guidance and additional input from the Purchaser, to address risks not covered in the NATO PILAR tool (due to its limitations), including risks related to modern CIS technologies and ON specific risks.

SOW-0399 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall update these SRA Report Annexes as many times as necessary in order to obtain SAA approval.

[0147] The ASO will maintain and keep the SRA Report document up to date throughout the project.

SOW-0400 The Contractor shall maintain and keep the SRA Report Annexes and all risk-relevant information up to date, under guidance from the Purchaser, throughout the project, as the ON development and implementation progresses.

8.1.3.5. System-specific Security Requirement Statement (SSRS)

[0148] The SSRS is a complete and explicit statement of the detailed security requirements to be met for the ON to be compliant to NATO Security Policy and Directives.

[0149] The SSRS specifies how security is to be achieved and maintained (in the form of implementation details).

- The Contractor shall provide technical input per AC/322-D/0048-REV3 Technical and Implementation Directive on CIS Security to the SSRS for the ON, based on Purchaser's provided template, as listed in [Ref: AC/322-D/0048-REV3], and guidance.

[0150] The SSRS shall be approved by the SAA (through the Purchaser).

SOW-0401 The Contractor shall implement the AC/322-D/0048-REV3 security measures under their (Contractor's) contractual obligations as system integrator and provide full traceability of these high-level security measures requirements down to the implementation level.

SOW-0402 The Contractor shall ensure their input to the SSRS is provided at the earliest stage of the project, and shall be enhanced and completed as the project develops.

SOW-0403 The Contractor's technical input to the SSRS shall at a minimum:

SOW-0403.A Be aligned to the SRA content;

SOW-0403.B Describe the minimum levels of security deemed necessary to countermeasure the risk(s) identified in the SRA

SOW-0403.C Specify the details on how the applicable AC/322-D/0048-REV3 security measures have been implemented.

SOW-0403.D Have an unique identifier for each security measure / requirement;

SOW-0403.E Indicate mandatory and recommended security measures, as per SRA Report's findings, Purchaser and SAA input and guidance.

[0151] The ASO shall cover the SSRS's parameters pertaining the operational environment, such as the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation and other Purchaser's and SAA's specific requirements.

SOW-0404 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall provide updated input to the SSRS document as many times as necessary in order to obtain SAA approval.

[0152] The ASO will maintain, consolidate and keep the SSRS up to date throughout the project.

8.1.3.6. System Interconnection Security Requirements Statement (SISRS)

SOW-0405 The Contractor shall provide technical input to the SISRS under the guidance of the Purchaser in order to cover the security requirements for the interoperability of ON with other CIS, as per INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS) [Ref: AC/322-D/0030-REV5], and INFOSEC Technical & Implementation Guidance for the Interconnection of Communication and Information Systems (CIS) Ref: AC/322-D (2005)0040].

SOW-0406 These security requirements shall be based further on scenario types provided by the Purchaser and documented in the CISD.

SOW-0407 The SISRS shall cover all identified external connections to ON.

[0153] The SISRS for ON will be developed by the Purchaser based on the input provided by the Contractor, and within the NSAB approved template, as listed in Annex D.5, and shall be approved by the SAA.

[0154] The Purchaser will provide the information required to formulate the SISRS that are not directly related with ON design (e.g., information about the CIS ON is to connect to).

SOW-0408 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall provide updated input to the SISRS document as many times as necessary in order to obtain SAA approval.

[0155] The ASO will maintain and keep the SISRS up to date throughout the project.

8.1.3.7. Generic Security Operating Procedures (SecOPs)

[0156] SecOPs are a description of the implementation of the security measures to be adopted when utilizing the CIS, the specific operating procedures to be followed and the responsibilities of the personnel.

[0157] ON SecOPs will be developed by the Purchaser with input from the Contractor, when relevant, and based on the NSAB approved template, as listed in Annex D.5, and shall be approved by the SAA.

SOW-0409 ON SecOPs shall contain separate sections for personnel performing security management as well as administrative functions (e.g. Core Administrators, Local Administrators, CIS Security Officer, Local CIS Security Officers) and ON users.

SOW-0410 The Contractor's input to the ON SecOPs, as a minimum, shall include the following:

SOW-0410.A Administration and organisation of security;

SOW-0410.B Relevant CIS Security information;

SOW-0410.C Incident and emergency procedures specific to the ON functionality;

SOW-0410.D Configuration management;

SOW-0410.E Acceptable use policy.

SOW-0411 As System Integrator, the Contractor shall also provide input to the ON SecOPs pertaining the security requirements identified in the SRA and SSRS, which are not fully fulfilled by technical countermeasures. I.e. the following security procedures should be addressed (not exhaustive list):

SOW-0411.A System configuration and maintenance;

SOW-0411.B System backup;

SOW-0411.C System recovery, et al.

SOW-0412 The Contractor shall take into account any comments from the Purchaser and SAA (provided to the Contractor through the Purchaser) and shall conduct updates to their input to the ON SecOPs document as many times as necessary in order to obtain SAA approval.

[0158] The ASO will maintain and keep ON SecOPs up to date throughout the project.

8.1.3.8. Security Test and Verification Plan (STVP)

[0159] The STVP is a description of the security testing and verification procedures of the security measures to be implemented for the ON, as documented and described in the SSRS, SISRS and SecOPs.

SOW-0413 The Contractor shall provide all necessary input to develop detailed test procedures into the STVP as per the Purchaser's provided template, listed in Annex D.5

SOW-0414 The STVP shall be approved by the SAA through the Purchaser.

SOW-0415 The STVP's detailed test procedures shall describe:

SOW-0416 A complete and detailed sequence of steps that shall be followed to prove that the security measures (controls) designed into ON enforce the security requirements identified in the SSRS, SISRS and SecOPs.

SOW-0417 The Contractor shall ensure that for each security test in the STVP template, the following details are identified in their technical input, in agreement and coordination with the Purchaser:

SOW-0417.A Test ID;

SOW-0417.B Test subject and an objective of the security test;

SOW-0417.C The SSRS security measure and its expected implementation details as per the approved SSRS;

SOW-0417.D An outline description of the security test procedure;

SOW-0417.E System element under test (e.g. DC, SN, EN, RN);

SOW-0417.F Planned location of the test. STVP shall also distinguish between tests to de conducted locally (on-site) or centrally (from DC);

SOW-0417.G Required verification method (i.e. Inspection, Analysis, Demonstration, Test);

SOW-0417.H The pass criteria for the security test.

SOW-0418 The Contractor shall ensure with guidance and support from the Purchaser that every security test is cross-referenced to the corresponding security requirements from the ON SSRS (identified by the unique identifier) and depicted in the Security Test Requirements Traceability Matrix (STRTM)

[0160] The Purchaser shall ensure all security requirements from the ON SSRS are planned for testing.

SOW-0419 The specific test procedures shall consist of the inspection procedures and a set of software scripts that shall allow a CIS Security Officer to verify that all components of the ON have been installed and configured property and comply with the SSRS and SecOPs.

SOW-0420 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct an update of the STVP document as many times as necessary in order to obtain SAA approval.

[0161] The Purchaser shall maintain and keep the STVP up to date throughout the project.

8.1.3.9. Security Test and Verification Report (STVR)

[0162] The STVR is a description of the results for every instance of security testing conducted based on the approved STVP.

SOW-0421 The Contractor shall conduct the security testing, producing the necessary STVR(s) with input and guidance from the Purchaser, based on the approved STVP.

[0163] The SME designated by the Purchaser will witness the execution of the STVP. The SME will countersign the respective STVR(s).

SOW-0422 The Contractor shall develop an STVR for every instance of security testing executed according to the STVP.

SOW-0423 The STVRs for the ON shall be developed by the Contractor based on the Purchaser's provided guidance and template, as listed in the Annex D.5, and shall be approved by the SAA.

SOW-0424 The Contractor shall, for each security test, identify the following within the STVR:

- SOW-0424.A Test ID;
- SOW-0424.B An outline description of the security test;
- SOW-0424.C A summary recount of the specific test procedures to support the test objective;
- SOW-0424.D The location of the conducted test;
- SOW-0424.E The pass criteria for the security test;
- SOW-0424.F The results of the security tests;
- SOW-0424.G Test status (e.g. in progress, passed, failed);
- SOW-0424.H Test completion (in percent);
- SOW-0424.I Failure severity (e.g. critical, high, medium, low, none);
- SOW-0424.J Test date;
- SOW-0424.K Any info about who conducted the test;
- SOW-0424.L An information about who witness the test.

SOW-0425 STVR shall contain overall test summary details:

- SOW-0425.A Identification of the element under tests (e.g. DC, SN, EN, RN);
- SOW-0425.B Tests starting date;
- SOW-0425.C Tests finishing date;
- SOW-0425.D Amount of all tests to be conducted;
- SOW-0425.E Amount of tests executed;
- SOW-0425.F Tests passed;
- SOW-0425.G Tests failed;
- SOW-0425.H Tests still in progress;
- SOW-0425.I Amount of findings with clear distinguish of their severity as agreed with the Purchaser (e.g. critical, high, medium, low, none).

SOW-0426 The Contractor shall take into account any comments from the Purchaser and/or the SAA (provided to the Contractor through the Purchaser) and shall conduct updates to

the STVR(s) (which might require some security tests to be re-conducted) as many times as necessary in order to obtain SAA approval.

8.1.4. Approval for Testing (AfT)

SOW-0427 The AfT request(s) for the ON will be developed by the Purchaser. The Contractor shall provide the technical input and relevant information for the AfT, using the template listed in Annex D.5.

[0164] Approval for Testing request(s) will be provided to the SAA.

SOW-0428 The Contractor shall provide at least the following information as an input for the AfT:

SOW-0428.A References to the existing Security Related Documentation for ON;

SOW-0428.B Objective of the tests;

SOW-0428.C Outline description of the ON components under tests (to include high level diagram);

SOW-0428.D Sites involved in testing;

SOW-0428.E Timeframe for testing;

SOW-0428.F Brief description of test activities planned to be conducted during test period.

[0165] The Purchaser will provide together with the AfT request(s) accreditation related documentation which is part of the SADS, even in the incomplete state if that would be required by the SAA to grant an AfT.

[0166] The Purchaser will coordinate all AfT request(s) with the SAA.

SOW-0429 Provided that required prerequisite deliverables are available, AfT technical input and information shall be provided by the Contractor to the Purchaser minimum 20 working days prior to the testing itself to allow the Purchaser for the sufficient coordination with the SAA.

SOW-0430 Planning for the AfT shall consider all the required prerequisites' delivery and approvals, e.g. STVP.

8.1.5. Security Defects Log

SOW-0431 The Contractor shall present a plan to the Purchaser for the Contractor's resolution of defect log entries associated with risks that are preventing ON accreditation.

SOW-0432 The Contractor shall correct the defects before PSA. The Purchaser may approve the Contractor to proceed to PSA, but only once a credible plan is presented to the Purchaser for rectifying the security defects identified in the STVR before FOA.

SOW-0433 The Contractor shall resolve all defects identified by the Purchaser within this plan, prior to the FOA.

8.1.6. Security Audits

[0167] Security audits will be performed to verify that NATO CIS and other CIS handling NATO classified information comply with NATO policies, directives and supporting documents on CIS Security, and operate in accordance to the security baselines defined by the CISP, in conjunction with the SAA

[0168] Security audits will be conducted in accordance with the requirements set in the appropriate directives on the management aspects of CIS Security and under the authority of the responsible SAA

SOW-0434 For NATO CIS, the Contractor shall support the security audits to:

SOW-0434.A verify that the security measures, resultant from the security risk management process, are correctly implemented and maintained;

SOW-0434.B validate the appropriateness of the security risk management process and results;

SOW-0434.C verify that security standards (e.g. security baselines, security architectures) are consistently adopted throughout NATO;

SOW-0434.D assess the maturity of CIS Security capabilities and the status of implementation of related programmes/projects;

SOW-0434.E assess the effectiveness of CIS Security processes and capabilities by means of measures and measurement.

[0169] Type 3 or higher on-site Security Audits are to be conducted by the NATO Cyber Security Centre (NCSC) and/or the Military Committee Communications and Information Systems Security and Evaluation Agency (SECAN) and/or authorized SA team.

[0170] Typically, “Program of Work for Type 3 or higher Security Audits” for NATO ON sites is decided by the SAA (during NSAB plenary meetings or on a case by case basis).

[0171] The following points shall supplement the accreditation process described for each NATO ON site:

A. Audit Report is to be provided to the SAA, CISOA, CISP/CISPIA, CIS Security Officer and Local Security Management Staff.

B. The applicable Local SAA as specified in the SAP (ACO SAA, ACT Office of Security or NOS) is to determine which audit findings shall be remediated by the CISP before (Interim) Security Accreditation (ISA) for the site in question could be issued.

[0172] Follow-up report(s) on remediation actions shall be delivered to the Local SAA on a periodical basic. Typically, the first follow-up report is to be provided within one month after issuance of the Audit Report. Frequency for additional follow-up-reports should be determined by the Local SAA based on the reported status of remediation.

SOW-0435 The Contractor shall support the Security Audit process, providing necessary information about the CIS or CIS elements within Security Audit scope.

SOW-0436 The Contractor shall provide technical input to the Security Audit by answering the Security Audit Questionnaire that shall be provided to the Contractor by the Purchaser in preparation for the audit activities.

SOW-0437 The Purchaser shall provide guidance to the Contractor in responding to the Scoping Questionnaire, as well as any additional information outside of the Contractor’s AOR.

SOW-0438 The Contractor shall rectify and/or implement mitigation of the findings identified during the security audit which pertain the security measures under the Contractor’s responsibility as per contractual obligation as System Integrator.

SOW-0439 The Contractor shall note that the duration of the Security Audit process may range between 3 months - 6 months, including the long idle (waiting) times due to the processing by governance or the feedback.

8.1.7. Approved Software

[0173] Software used on the NATO ON shall undergo the official Request for Change (RFC) process, unless already listed in the appropriate Agency Authorized Software List (A2SL) maintained by the CISP, and specifically authorised for use within the system by the appropriate SAA.

[0174] Any deviation from the A2SL and/or from the RFC process for a specific ON site are to be formally requested, evaluated/approved by the Local SAA and explicitly endorsed by the CISOA for the ON.

[0175] The RFC process requires several steps, including but not limited to:

A. The roadmap for the software is to be captured in the A&T Portfolio,
B. the media is uploaded to the electronic Definitive Media Library (eDML),
C. The software and associated documents is submitted for verification and penetration testing for it to be added to the A2SL.

SOW-0440 The Contractor shall follow the official RFC process, in coordination with the Purchaser, for any new software, software updates and new/modified services that the Contractor includes in the WP07 solution.

8.1.8. Security Related Responsibilities

[0176] Table 5 below summarises responsibilities related to each security document given at section 8.1.3 above, required for security accreditation process.

[0177] The column "Baseline/Guidance" lists available templates, relevant NATO Security Directives and Guidance, and similar documentation.

[0178] The table below does not exclude all responsibilities and processes as detailed in Section 7.3. and 7.4, nor does it exclude the principles laid out in Section 7.1 and 7.2.

SOW-0441 The Contractor shall undertake the work identified in the column 'Contractor Responsibility' in Table 5 below:

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall)	Purchaser Responsibility (The Purchaser will)
SAP	SAP Template	• Provide updated input to the SAP as per section 7.3.1. • Ensure that the SAP is considered in the development of the WIP and in the WMP • Deliver updates of the timelines per relevant developments	• Develop the SAP • Provide applicable documents, templates and guidance to the Contractor • Review all changes • Coordination with the SAA
iCISD	CIS Description Template	• Update the document in the necessary sections identified as per contract scope. • Progress the iCISD with their technical input updates into the CIS Description, as per 7.3.2.	• Develop iCISD • Provide iCISD to the Contractor • Provide input and guidance to the Contractor for their updates of the iCISD • Approve input and updates from Contractor and manage and maintain iCISD until its uplift into CIS Description (as per 7.3.2.)
CISD	CIS Description Template	• Provide technical input to the CISD under Purchaser guidance	• Maintain and consolidate updates to

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall)	Purchaser Responsibility (The Purchaser will)
		• Based on the intended design adjust the relevant CISD sections focusing on CIS security aspects • Provide updates to the CISD as the Project develops	the CISD during project duration • Provide applicable documents, templates and guidance to the Contractor • Review and approve Contractor's updates and technical input, as per 7.3.3. • Coordination with the SAA
SRA	[AC/35-D/1015] [AC/35-D/1017] Tool for formal SRA: NATO PILAR SRA Report Template	• Support Purchaser in conducting SRA via provision of the required security technical inputs, as per system design • Provide input for assets identification • Provide input for safeguards (technical and organizational measures – information security) identification (implementation details) and valuation(implementation maturity) • Provide technical input into the specific risk annexes as detailed in SOW-0628 in section 7.3.4	• Conduct and coordinate the SRA • Maintain and consolidate the SRA during project duration • Develop SRA Report • Coordination with the SAA • Review Contractor's input to the SRA Report and their specific risk annexes as per 7.3.4 SOW-0628.
SSRS	[AC/35-D/1015] SSRS Template	• Provide technical input to the SSRS (how the security measures shall be implemented)	• Develop the SSRS • Maintain and consolidate the SSRS during project duration • Provide the SSRS to the Contractor for their input • Indicate SSRS sections that require technical input by the Contractor • Provide guidance to the Contractor

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall)	Purchaser Responsibility (The Purchaser will)
			• Review • Coordination with the SAA
SISRS	SISRS Template	• Provide technical input to SISRS	• Develop SISRS • Provide SISRS to the Contractor • Indicate SISRS sections that require technical input by the Contractor • Provide guidance to the Contractor • Review • Coordination with the SAA
SecOPs	[AC/35-D/1014] SecOPs Template	• Provide input to SecOPs for users and system administrators	• Develop the SecOPs • Maintain and consolidate SecOPs during project duration • Provide the SecOPs to the Contractor • Indicate SecOPs Sections that require input by the Contractor • Provide guidance to the Contractor • Review • Coordination with the SAA
STVP	[AC/35-D/2005] STVP template	• Develop detailed STVP test cases / test procedures per relevant security measure/requirement, as per 7.3.8 • Develop STRTM under the guidance of the Purchaser	• Develop and provide the STVP and all necessary guidance to the Contractor • Review • Coordination with the SAA

Document	Baseline/ Guidance	Contractor Responsibility (The Contractor shall)	Purchaser Responsibility (The Purchaser will)
STVR	[AC/35-D/2005] STVP template	• Execute the STVP for each ON Node • Record the results of each ON Node testing in the form of a STVR, to be developed under guidance of the Purchaser	• Provide STVR template and guidance to the Contractor • Review results for each ON Node security testing Coordination with the SAA • Witness the testing conducted by the Contractor • Review the STVRs and ensure appropriateness and accuracy and that all test cases have been covered.

Table 5 - Security Accreditation Related Responsibilities

8.2. CIS Security Accreditation Requirements (Activity Group 1 and 2)

[0179] The security accreditation process is described in detail in Section 8.

SOW-0442 For AG1 and AG2 the security accreditation process shall differ slightly.

[0180] The main difference between security accreditation process for NS Bi-SC AIS and NATO ON is that NS Bi-SC AIS is an in-service CIS, with its own security accreditation documentation.

[0181] The objective of the accreditation activities for the AG1 and AG2 shall be providing an up to date Security Accreditation Documentation Set (SADS) and Security Risk Assessment that accurately reflect the state of security of NS Bi-SC AIS post AG 1 and 2 activities.

SOW-0443 Section 7.1 shall define Purchaser's expectations in terms of the contribution of the Contractor for the update activities.

8.2.1. Security Accreditation Documentation Set (NS Bi-SC AIS)

[0182] The complete SADS, encompassing the entire NS Bi-SC AIS consist of the following documents:

A. CIS Description;
B. Security Accreditation Plan (SAP);
C. Security Risk Assessment (SRA) Report;
D. System-specific Security Requirement Statement (SSRS);
E. Security Operating Procedures (SecOPs);
F. Security Test and Verification Plan (STVP);
G. Security Test and Verification Report (STVR),

SOW-0444 The Contractor shall provide technical input to the SADS in support of the security accreditation process in the form of accurate information pertaining the enhancements, implementations etc. brought into NS Bi-SC AIS AG1 & 2 activities.

8.2.1.1. Security Accreditation Plan (SAP)

[0183] The Purchaser will develop the NS Bi-SC AIS SAP update.

[0184] The Purchaser will maintain the SAP during the project.

SOW-0445 The Contractor shall provide updates to the SAP according to the implementation schedule of AG1 & 2 via and under guidance of the Purchaser.

SOW-0446 Any changes required by the Contractor to be incorporated into the SAP shall be provided to the Purchaser who will (if the proposed change is accepted) coordinate said change.

SOW-0447 The SAP is not the Project Schedule nor does it direct the latter. The Contractor shall not confound the two, as the SAP proposes the timelines and activities required for Security Accreditation as approved by the SAA.

8.2.1.2. CIS Description

[0185] The Purchaser will develop the NS Bi-SC AIS CIS Description update.

SOW-0448 The Contractor shall provide technical input, under guidance of the Purchaser, to the CIS Description, ensuring that it reflects all of the component, software and hardware and other technical changes delivered by AG 1 & 2 to the NS Bi-SC AIS.

SOW-0449 The Contractor shall, at a minimum, provide the following information and technical input to the CIS Description document, in the services established in the scope of the contract and pertaining all system integration aspects pertaining AG 1 & 2:

SOW-0449.A Detailed technical descriptions showing the main components at a high level, as well as detailed information flows, and how these are protected, inclusive of any data flow from leveraged networks/infrastructure (if any);

SOW-0449.B Descriptions of all internal and external connections being changed of added to the system including interconnections to other CIS, as per LLD;

SOW-0449.C List of hardware and software components used, as per BOM;

SOW-0449.D Overview of the security mechanisms, which are going to be implemented in the NS Bi-SC AIS via AG 1 & 2 enhancement and all its components.

SOW-0450 The input developed by the Contractor for the CIS Description shall be submitted to the Purchaser's ASO for review before it will be consolidated into the final NS Bi-SC AIS CIS Description and provided to the SAA for approval.

[0186] The ASO will maintain and keep the CIS Description document up to date throughout the project.

8.2.1.3. Security Risk Assessment Report (SRA Report)

[0187] The Purchaser will develop the NS Bi-SC AIS SRA update.

SOW-0451 The Contractor shall develop annexes to the SRA to address risks related to modern CIS technologies introduced with NS Bi-SC AIS enhancements by AG 1 & 2.

SOW-0452 The Contractor shall provide the maturity assessment for all security mechanisms being improved and / or introduced by the AG 1 & 2 enhancements, under a guidance of the Purchaser.

SOW-0453 The Contractor shall engage with the Purchaser to discuss and agree on the perceived maturity levels reported by the Contractor.

[0188] The Purchaser will collate and coordinate the information resulting from these activities and update the SRA accordingly.

8.2.1.4. System-specific Security Requirement Statement (SSRS)

[0189] The Purchaser will develop the NS Bi-SC AIS SSRS update.

SOW-0454 The Contractor's technical input to the SSRS shall describe at a minimum:

SOW-0454.A The technical implementation details of any security measures being introduced by AG 1 & 2 enhancements to the NS Bi-SC AIS, as per AC/322-D/0048-REV3.

SOW-0454.B The technical implementation details of changed / uplifted / enhanced security measures affected in such ways by AG 1 & 2 NS Bi-SC AIS, as per AC/322-D/0048-REV3.

SOW-0454.C Be aligned to the SRA updated content;

[0190] The Purchaser will provide in depth guidance to the Contractor throughout this update process.

[0191] The ASO will maintain, consolidate and keep the SSRS up to date throughout the project.

8.2.1.5. Generic Security Operating Procedures (SecOPs)

[0192] The Purchaser will develop the NS Bi-SC AIS SecOPs update.

SOW-0455 The Contractor's input to the NS Bi-SC AIS SecOPs, as a minimum, shall include the specific operating procedures for the node resulting from the AG 1 & 2 enhancements.

[0193] The Purchaser will provide in depth guidance to the Contractor throughout their input process.

[0194] The ASO will maintain and keep NS Bi-SC AIS SecOPs up to date throughout the project.

8.2.1.6. Security Test and Verification Plan (STVP)

SOW-0456 The Contractor shall provide all necessary input to develop detailed test procedures into the STVP resulting from the AG 1 & 2 enhancements, meaning that all security measures introduced to NS Bi-SC AIS and improved by AG 1 & 2, as per AC/322-D/0048-REV3, shall have a corresponding security test case to prove appropriate implementation.

[0195] The updated STVP will be approved by the SAA through the Purchaser.

SOW-0457 The STVP's detailed test procedures shall describe:

SOW-0457.A A complete and detailed sequence of steps that shall be followed to prove that the security measures (controls) designed into NS Bi-SC AIS N enforce the security requirements identified in the updated SSRS and SecOPs.

SOW-0458 The Contractor shall ensure that for each security test in the STVP template, the following details are identified in their technical input, in agreement and coordination with the Purchaser:

SOW-0458.A Test ID;

SOW-0458.B Test subject and an objective of the security test;

SOW-0458.C The updated SSRS security measure and its expected implementation details as per the approved updated SSRS;

SOW-0458.D An outline description of the security test procedure;

SOW-0458.E System element under test (e.g. DC, SN, EN, RN);

SOW-0458.F Planned location of the test. Updated STVP shall also distinguish between tests to de conducted locally (on-site) or centrally (from DC);

SOW-0458.G Required verification method (i.e. Inspection, Analysis, Demonstration, Test);

SOW-0458.H The pass criteria for the security test.

SOW-0459 The Contractor shall ensure with guidance and support from the Purchaser that every security test within a scope of AG 1 & 2 enhancements is cross-referenced to the corresponding security requirements from the updated NS Bi-SC AIS SSRS (identified by the unique identifier) and depicted in the Security Test Requirements Traceability Matrix (STRTM)

SOW-0460 The specific test procedures shall consist of the inspection procedures and a set of software scripts that shall allow the NS Bi-SC AIS CIS Security Officer to verify appropriate configuration and installation of all components.

SOW-0461 The Contractor shall take into account any comments from the Purchaser and/or SAA (provided to the Contractor through the Purchaser) and shall conduct changes of the updated STVP document as many times as necessary in order to obtain SAA approval.

[0196] The Purchaser will provide in depth guidance to the Contractor throughout their input process.

[0197] The Purchaser will maintain and keep the updated NS Bi-SC AIS STVP throughout the project.

8.2.1.7. Security Test and Verification Report

[0198] The Purchaser will develop the NS Bi-SC AIS STV Report, post execution of the updated NS Bi-SC AIS STVP.

SOW-0462 The Contractor shall conduct the security testing relevant to the security measures introduced / enhanced by AG 1 & 2 activities in the NS Bi-SC AIS, producing detailed descriptions / comments of the obtained results and document it for the Purchaser.

[0199] The Subject Matter Expert (SME) designated by the Purchaser will witness the execution of the updated STVP. The SME will countersign the respective STVR(s).

SOW-0463 The Contractor shall support development of the STVR with all relevant technical information pertaining security testing within the scope of all changes introduced by AG 1 & 2.

8.2.1.8. Security Audits

SOW-0464 The Contractor shall support the Security Audit process, providing necessary information about the enhancements introduced to the NS Bi-SC AIS under the scope of AG 1 & 2.

SOW-0465 The Contractor shall provide technical input relevant to the AG 1 & 2 to the Security Audit by answering the Security Audit Questionnaire that shall be provided to the Contractor by the Purchaser in preparation for the audit activities.

[0200] The Purchaser will provide guidance to the Contractor in responding to the Scoping Questionnaire, as well as any additional information outside of the Contractor's AOR.

SOW-0466 The Contractor shall rectify and/or implement mitigation of the findings identified during the security audit which pertain the security measures under the Contractor's responsibility as per contractual obligation as System Integrator, within the scope of AG 1 & 2 enhancements.

SOW-0467 The Contractor shall note that the duration of the Security Audit process may range between 3 months - 6 months, including the long idle (waiting) times due to the processing by governance or the feedback.

9. QUALITY ASSURANCE AND CONTROL

9.1. Definitions

SOW-0468 Unless otherwise specified in the SoW, STANAG 4107 and underpinning AQAPs [Ref: STANAG 4107], PRINCE2 and ITIL definitions shall apply.

[0201] Quality Assurance (QA) is a process and set of procedures intended to ensure that a product or service, during its definition, design, development, test and deployment phases will meet specified requirements.

[0202] Quality Control (QC) is a process and set of procedures intended to ensure that a manufactured product or performed service adheres to a defined set of quality criteria and meets the requirements of the customer.

[0203] Under the Contract, the terms “QA process” will shall also include Quality Control process.

[0204] A “Project document” is a document developed and maintained to help in the management of the project. Typically the plans (amongst which, the Quality Assurance Plan (QAP)) are project documents.

SOW-0469 The term "NATO Quality Assurance Representative" (NQAR) shall apply to any of the Purchaser appointed Quality Assurance Representative.

SOW-0470 The term "Contractor Quality Assurance Representative" (CQAR) shall apply to any of the Contractor appointed Quality Assurance Representative.

9.2. Introduction

SOW-0471 The Contractor shall establish, execute, document and maintain an effective QA programme throughout the period of performance of this Contract.

SOW-0472 The QA programme shall apply both the contractual requirements and the NATO requirements for quality identified by AQAP 2110, AQAP 2210 and AQAP 2310 and AQAP 2105 [all underpinning AQAPs of Ref: STANAG 4107], to provide confidence in the Contractor’s ability to deliver products that conform to the Contractual requirements.

SOW-0473 If any inconsistency exist between the SoW requirements and the references, the SoW requirements shall prevail.

SOW-0474 The Contractor‘s QA effort shall apply to all services and products to be provided under the Contract. This includes all hardware, software, firmware and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract (including deliverable and non-deliverable items like test and support hardware and software), without limitation.

SOW-0475 The Contractor‘s QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.

9.3. Roles and Responsibilities

[0205] During the entire Contract implementation, the NQAR(s) assures the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirements. The Purchaser, through its NQAR(s), is the authority concerning all Quality related matters.

SOW-0476 The Contractor shall be responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the life-cycle of the Contract.

SOW-0477 The CQAR shall be accountable for the provision of the QA Plan and the compliance to the defined QA process.

SOW-0478 The CQAR shall define the major quality checkpoints that will be implemented while executing the project and the quality process to be used at each checkpoint.

SOW-0479 The CQAR shall establish and maintain the project quality register on a dedicated Project Portal that lists all planned and performed quality checks on Contractor deliverables. The quality register(s) shall be exported and provided as an Annex to the QAP at each release.

SOW-0480 The CQAR shall be responsible for assessing that the Contractual requirements have been complied with, prior proposing the Contractual services and products.

SOW-0481 The CQAR shall report to a distinct manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.

SOW-0482 The CQAR shall be the PoC for interface with and resolution of quality matters raised by the NCI Agency or its delegated NQARs.

SOW-0483 The Contractor shall support any NCI Agency or its delegated NQARs activity focused on monitoring Contractor activities at Contractor’s facilities or other sites related to the development, testing and implementation.

SOW-0484 In particular, the Contractor shall:

SOW-0484.A Make himself/herself available to answer questions and provide information related to the project,

SOW-0484.B Allow the Purchaser representatives to inspect and monitor testing activities, and management, technical and quality processes applicable to the project.

SOW-0484.C Transfer to the Purchaser representatives all information deemed necessary to perform the QA activities, on his/her own initiative or on request by the Purchaser representative.

SOW-0485 The Contractor shall ensure that CQAR(s) have the required qualifications, knowledge, skills, ability, practical experience and training for performing their tasks.

SOW-0486 The CQAR(s) shall have sufficient responsibility, resources, authority and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective actions.

SOW-0487 The CQAR(s) shall participate in the early planning and development stages to ensure that all quality related requirements are specified in plans, standards, specifications and documentation.

SOW-0488 After establishment of attributes, controls and procedures, the CQAR(s) shall ensure that all elements of the QA Process are properly executed, including inspections, tests, analysis, reviews and audits.

SOW-0489 The Contractor, through its CQAR(s), shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services which conform to contractual requirements only.

SOW-0490 The Contractor shall maintain and, when required, deliver objective evidence of this conformance.

SOW-0491 The Contractor shall give written notice to the NQAR(s) at least four weeks in advance that the services and/or products are being presented for review, testing, verification, validation and acceptance.

SOW-0492 Testing shall only be permitted by using test procedures and plans approved by the Purchaser.

9.4. Quality Management System (QMS)

SOW-0493 The Contractor shall establish, document and maintain a Quality Management System (QMS) in accordance with the requirements of ISO 9001:2015 (**Error! Reference source not found.**).

SOW-0494 The Contractor's and Sub-Contractor's QMS relevant to performance under the Contract shall be subject to continuous review and surveillance by the cognizant NQAR(s).

SOW-0495 The Contractor shall include in orders placed with its Sub-Contractor(s) and Supplier(s), the QMS requirements necessary to ensure the supplies and services covered by the Sub-Contract(s) and/or Purchase Orders conform to the requirements of the prime Contract.

SOW-0496 The Contractor shall specify in each order placed with its Sub-Contractor(s) and Supplier(s), the Purchaser's and its NQAR(s) rights of access to all premises where contractual work is performed, in order to carry out audits, inspections, tests and other functions as may be required by the NQAR(s).

SOW-0497 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.

9.5. Quality Assurance process

SOW-0498 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-0499 The requirements for these processes shall be derived from the Contract, the QMS, the applicable AQAPs and referenced best practices, in that sequence of priority.

SOW-0500 The Contractor shall prepare, perform and document System Requirements Review (SRR) according to the contractual requirements and IEEE 15288.2:2014 [Ref: IEEE 15288.2].

SOW-0501 The Contractor shall prepare the testing process, and the associated documentation, according to the contractual requirements and ISO/IEC/IEEE 29119 [Ref: ISO/IEC/IEEE 29119].

SOW-0502 The Contractor shall perform verification and validation of the Contractual deliverables before proposing them for the Purchaser review and approval.

SOW-0503 The Contractor's QA process shall be described in the QA Plan as outlined below. The process is subject to approval by the Purchaser.

SOW-0504 The Contractor shall demonstrate, with the Quality Assurance process, that the processes set up to design, develop, test, produce and maintain the product will assure the product will meet all the requirements.

SOW-0505 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-0506 On request, the Contractor shall provide the Purchaser with a copy of any Sub-Contracts or orders for products related to the Contract.

SOW-0507 The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser NQAR(s).

SOW-0508 The Contractor shall ensure that all contractual requirements are included in internal audits.

9.6. The Quality Assurance Plan (QAP)

SOW-0509 The Contractor shall provide a QAP for review to the Purchaser in accordance with the requirements identified in the AQAP-2105 [As part of Ref: STANAG 4107] and the SoW requirements.

SOW-0510 The Contractor's QAP shall be compatible and consistent with all other plans, specifications, documents and schedules, which are utilised under the Contract.

SOW-0511 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-0512 The QA Plan and all related QA procedures, and all their versions/revisions, shall be subject to NQAR(s) approval based on an agreed checklist.

SOW-0513 The acceptance of the QAP by the Purchaser only means 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-0514 The Contractor shall review its QA programme periodically and audit it for adequacy, compliance and effectiveness.

SOW-0515 The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

SOW-0516 The Contractor shall inform the NQAR(s) of deficiencies identified during internal audit unless otherwise agreed between the NQAR and/or the Purchaser and the Contractor.

SOW-0517 The Contractor shall include a risk management section within the QAP including the risks connected to the sub-Contractors of the Contractor.

SOW-0518 The Contractor shall make its quality records, and those of its Sub-Contractors, available for evaluation by the NQAR(s) throughout the duration of the Contract.

SOW-0519 The Contractor shall update the document, as required, from the delivery date of the initial QAP through FOA under Configuration control.

SOW-0520 The Contractor shall provide a copy of each new version of the QAP to the Purchaser for review and approval.

9.7. Risks

SOW-0521 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-0522 The Contractor shall start planning with risk identification during Contract review and updated thereafter in a timely manner. The Purchaser reserves the right to reject QAPs, Risk Plans and their revisions.

9.8. Deficiencies

SOW-0523 The Contractor shall implement a quality/product Issue Tracking Capability (ITC) to ensure prompt tracking, documentation and correction of problems and deficiencies, during the lifecycle of the Contract.

SOW-0524 For that purpose, by default, the Contractor shall use the Purchaser toolset, as defined in section 11.4. As an alternative, the Contractor may propose another tool, which will then be approved by the Purchaser.

SOW-0525 The ITC shall implement a life-cycle (status, as well as responsibilities, relationship to affected Contract requirements, if applicable, and due dates) for each recorded deficiency.

SOW-0526 If the Contractor becomes aware at any time before acceptance by the Purchaser that a deficiency exists in any supplies, the Contractor shall log it in the ITC, coordinate with the Purchaser and promptly correct it.

SOW-0527 The Contractor shall demonstrate that all deficiencies are solved / closed before product acceptance.

SOW-0528 When the Contractor establishes that a Sub-Contractor or a PFE product is unsuitable for its intended use, it shall immediately report to and coordinate with the Purchaser the remedial actions to be taken.

SOW-0529 The Contractor shall ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.

SOW-0530 The NQAR should be able to access the ITS when performing 2nd party QA audits or inspections.

9.9. Support Tools

SOW-0531 The Contractor shall make all support tools available for demonstration to the NQAR, upon request.

SOW-0532 The Contractor shall also make available to the Purchaser for review upon request, associated records and documentation, including but not limited to, control, authorization for use, calibration, validation, qualification, as applicable, per respective Contract requirement.

9.10. Certificates of Conformity

SOW-0533 A Certificate of Conformity (CoC) is a document, signed by the Supplier / Vendor of a product, stating that the product conforms to contractual requirements and regulations. A Certificate of Conformity template is available in AQAP-2070[{As part of Ref: STANAG 4107]

SOW-0534 The CoC, provides an evidence that the items produced or shipped comply with test procedures and quality specifications prescribed by the customer.

SOW-0535 The Contractor should be accountable for the conformance to requirements, of products provided to the Purchaser.

SOW-0536 The Contractor shall deliver all the CoCs for Commercial-off-the-Shelf (COTS) products (software, including firmware, and hardware) released by the COTS Vendors.

SOW-0537 The CoCs delivered by the Contractor shall be part of the acceptance data package of the product.

SOW-0538 The Contractor shall provide a CoC at release of product to the Purchaser unless otherwise instructed.

10. CONFIGURATION MANAGEMENT

10.1. General Requirements

[0206] This section addresses the Configuration Management (CM) requirements of the ITM-RC1 Work package 07. These requirements aim to ensure that the Contractor establishes and executes an effective, efficient and NATO-compliant Configuration Management process and associated procedures during the execution of the project.

SOW-0539 The Contractor shall establish and maintain CM policies, processes and procedures in conformance with the STANAG 4427 [Ref: STANAG 4427] and underpinning Allied Configuration Management Publications (ACMP) [Ref: ACMP-2000, ACMP-2009, ACMP-2009-SRD-41, ACMP-2100], to implement and manage the CM functions:

- SOW-0539.A Configuration Management Planning
- SOW-0539.B Configuration Identification;
- SOW-0539.C Configuration Control[8];
- SOW-0539.D Configuration Status Accounting;
- SOW-0539.E Configuration Verification and Audit.

SOW-0540 The Contractor shall implement the CM activities for any Configuration Item (CI) type, like hardware, software and firmware delivered, integrated, tested and/or customized and document provided, used or defined in the frame of this project.

SOW-0541 During the whole lifecycle of the project, the Contractor shall feed CM information and baselines into the Purchaser's Configuration Management Database (CMDB) as part of its CM program.

SOW-0542 The Contractor shall fully integrate the COTS elements-data in order to implement a unique CM framework.

SOW-0543 The Contractor shall have/obtain a NATO Commercial and Government Entity (NCAGE) Code. If sub-Contractors are involved in the execution of the Contract, the Contractor shall ensure that each of them obtains an NCAGE number.

SOW-0544 The Contractor shall ensure that there is full traceability through all baselines back to the functional baseline.

[0207] Release and Transition Management support the planning and implementation of baselined sites, and/or changes to baselined sites into operational use.

10.2. Configuration Management Responsibility

10.2.1. Responsibilities and Authorities

[0208] The Purchaser will retain all authorities on configuration decisions that impact the capability requirements, the functional requirements and any change to these.

[0209] The Purchaser will reserve the right to audit the Contractor's CM process.

SOW-0545 All proposed changes (e.g. ECP, Request for Deviation/Waiver (RFD/W)) shall be submitted and authorised by the Contractor's Configuration Control Authority (CCA) prior to submission to the Purchaser.

SOW-0546 The Contractor's CCA shall be defined in the Contractor's Configuration Management Plan (CMP).

[8] Configuration Control is also sometimes called Change Management. Unless otherwise specified, both terminology cover the same concept.

[0210] The Purchaser will be the disposition authority for the

A. The Contractor's CMP.
B. The selection of configuration items (CI).

[0211] The Purchaser will be the final dispositioning authority on

A. configuration/engineering changes;
B. contractually required baselines.
C. contractually required audits.
D. parts substitution and variances.

10.3. Configuration Management Planning

SOW-0547 The Contractor shall identify the means by which continuity of effort and understanding is achieved between their Sub-Contractors and them, and between the Purchaser and them and internally within their organization, for the allocated CI, integrating, interfacing or otherwise related CI, Contractor organizations, test and evaluation activities, and managers.

SOW-0548 The ITM-RC1 Configuration Management Plan (CMP) [Ref: ITM-RC1 CMP] shall be used by the Contractor as reference to develop their Configuration Management Plan (CMP) for ITM-RC1 WP07 deliverables.

[0212] The Contractor's CMP shall follow the ITM-RC1 CMP guidance and it shall be submitted to the Purchaser for approval. In case of contradictions, the ITM-RC1 CMP shall take precedence.

SOW-0549 The CMP, when approved, shall serve as a baseline document to plan, guide, and measure the CM process.

10.4. Configuration Identification

10.4.1. Baselines

10.4.1.1. Functional Baseline (FBL)

[0213] The functional baseline is the approved configuration documentation that describes a system's or top-level CI's performance requirements (functional, interoperability, and interface characteristics).

SOW-0550 The Purchaser provides the initial FBL in form of SoW requirements, and SRS requirements. Any changes to the FBL shall be agreed by the Purchaser, and baselined FBL shall be maintained by the Contractor.

SOW-0551 During the Sprints, any changes to the FBL shall be agreed by the Purchaser and shall be reflected and (re)released in the requirements artefacts by the Contractor.

SOW-0552 The Contractor shall maintain the FBL under Configuration Control, and provide the Configuration Status Accounting (CSA) information as and when requested by the Purchaser.

SOW-0553 FBL shall include the following requirement artefacts at minimum:

SOW-0553.A Requirements Traceability Matrix (RTM)

SOW-0553.B Requirements database (DOORS or equivalent)

SOW-0553.C Product Backlog

SOW-0553.D Sprint Backlog

10.4.1.2. Allocated Baseline (ABL)

[0214] The Allocated Baseline constitutes the design of a Product or Service and its conformity to the related Functional Baseline. It typically contains the Design Specifications for the Product(s), System(s) and/or Service(s) to be considered as the outcome of the project.

[0215] In the ITM-RC1 context, there is a distinction between an ABL with high-level design specifications and ABL with low-level design specifications. The approved baseline is a combination of all FBL artefacts and those identified specifically within the ABL.

SOW-0554 The High-Level design specifications ABL shall be called the “Initial ABL”. The Low-Level design specifications ABL shall be called the “Final ABL”.

[0216] The Purchaser will provide to the Contractor the initial ABL with High-Level Design.

SOW-0555 The Contractor shall deliver the Final ABL with Low-Level Design specifications to the Purchaser for approval.

SOW-0556 Final ABL(s) shall be established in the completion of the CDR, accordingly and applicable for each Activity Group.

SOW-0557 During the Sprints, any changes to the Final ABL shall be agreed by the Purchaser and shall be reflected and (re)released in the ABL artefacts (see Section 13.3 Technical Documentation and Data) by the Contractor.

SOW-0558 The Contractor shall maintain the ABL under Configuration Control, and provide the Configuration Status Accounting (CSA) information as and when requested by the Purchaser.

SOW-0559 ABL development configuration documentation shall include but are not limited to:

- SOW-0559.A The functional characteristics that are allocated based on the functional baseline;
- SOW-0559.B The tests required to demonstrate achievement of those functional characteristics;
- SOW-0559.C The necessary interface characteristics with associated CI; and Design constraints.

SOW-0560 ABL shall include the following artefacts at minimum, provided and updated by the Contractor after each Sprint:

- SOW-0560.A FBL (latest version(s))
- SOW-0560.B Design Specifications (i.e. HLD and LLD per Activity Group and applicable per site)
- SOW-0560.C System Implementation Plan
- SOW-0560.D Transition and Activation Plan
- SOW-0560.E Operating Model
- SOW-0560.F Test Specifications

SOW-0561 The Contractor shall establish the ABL for each CI.

SOW-0562 The Final ABL shall meet the functional requirements allocated in the FBL.

SOW-0563 The Final ABL development configuration documentation shall be in the form of development specification(s), referenced interface control documents, and other applicable documentation.

10.4.1.3. Product Baseline (PBL)

[0217] Initial PBL starts from the release of the Final ABL when physical products and documentation are created.

[0218] Upon completion of each Sprint, the PBL shall be validated against the hierarchal structure associations to the allocated baseline items. Upon the completion of successful validation and correction(s), the PBL shall be established by the Contractor.

SOW-0564 PBL shall include the following artefacts at minimum, provided and updated by the Contractor after each Sprint:

SOW-0564.A ABL (latest version(s))

SOW-0564.B As-built Documentation (ABD)

SOW-0564.C Technical Manuals

SOW-0564.D Test Reports

SOW-0565 The Contractor shall establish the Product Baseline (PBL) for each CI.

SOW-0566 The Contractor shall create and maintain the PBL per site, including a clear traceability between the scripts and configurations deployed per site.

SOW-0567 The PBL product configuration documentation shall be in the form of product, material, and process specifications, engineering drawings and other technical documentation and data for the CI that satisfactorily reflects the requirements of Purchaser's and Contractor's ABLs and the FBL.

SOW-0568 PBL product configuration documentation shall include but not be limited to:

SOW-0568.A All necessary physical and functional characteristics of CI;

SOW-0568.B Selected functional characteristics designated for production acceptance testing;

SOW-0568.C Production acceptance test; and

SOW-0568.D PCA and FCA documentation.

10.4.1.4. Operational Baseline (OBL)

[0219] The Operational Baseline is the instantiation of the PBL for a specific target environment (e.g. site) at the time of the Operational Acceptance (i.e. IOA and FOA). It shall contain all up-to-date configuration information (i.e. HW, SW, documentation) for the baseline handed-over to operations, per Activity Group and per site.

SOW-0569 The Contractor shall provide the OBL artefacts, as outlined in PBL section, for Purchaser approval as part of the approval of Site PSA, and as part of Operational Acceptance (i.e. IOA and FOA).

10.5. Configuration Identification

SOW-0570 The Contractor shall recommend a structured list of potential CIs to the Purchaser, using the selection criteria specified below.

[0220] The final selection of CI will be made by the Purchaser.

SOW-0571 The Contractor shall adopt on the project Purchaser's final selection of CI.

SOW-0572 Criteria for selection of CIs shall include, but not be limited to:

SOW-0572.A Safety of personnel and/or equipment;

SOW-0572.B Criticality, complexity, and state-of-the-art, high cost items;

SOW-0572.C Critical performance or operational effectiveness;

SOW-0572.D Functionality and performance;

SOW-0572.E Interface with other systems, government or sub-contractor furnished items, NATO standard items and support equipment;

SOW-0572.F Integrated product support;

SOW-0572.G Applications that effect a delivered product;

SOW-0572.H Reliability and maintainability.

SOW-0573 Supporting data to be submitted with each CI proposal shall include but not be limited to the following:

SOW-0573.A Project name;

SOW-0573.B CI/Joint CI affected;

SOW-0573.C Documentation;

SOW-0573.D Identification number and title;

SOW-0573.E Reasons for proposal;

SOW-0573.F Consequences of approval or disapproval;

SOW-0573.G Interface with other systems;

SOW-0573.H Alternatives;

SOW-0573.I Originator's data (name, address, NCAGE…)

SOW-0573.J Change authority; and

SOW-0573.K Date of submittal.

SOW-0574 The Contractor's identification numbering system shall be used to assign a unique identifier to each CI and its associated documentation. That unique identifier shall include the Contractor's (or sub-Contractor's) NCAGE number.

SOW-0575 Configuration Identification shall identify the documents that establish each baseline.

SOW-0576 The identification process shall continue as long as the capability is undergoing change.

SOW-0577 The Contractor shall assign nomenclature in accordance with the approved CMP.

SOW-0578 Non-Developmental Items identified as CI, when modified to satisfy project requirements, shall be re-identified as a project modified CI, and documented and controlled in accordance with the approved Contractor's CMP.

SOW-0579 For each CI, the Contractor shall develop and maintain configuration identification documentation.

SOW-0580 The Contractor shall document the functional and physical characteristics of all selected CI.

SOW-0581 The Contractor shall recommend to the Purchaser, the types of Configuration Documentation that shall be used to establish each CI.

SOW-0582 The Contractor shall identify each baseline by:

SOW-0582.A The baseline item CI number;

SOW-0582.B Baseline type; and

SOW-0582.C System designation.

SOW-0583 The Contractor shall provide, for each baseline, a list of documents, identified by title, and including the following:

SOW-0583.A Identification and NCAGE number;

SOW-0583.B Revision status;

SOW-0583.C Type;

SOW-0583.D Use in other related systems; and

SOW-0583.E Approval date.

SOW-0584 The Contractor shall ensure that the configuration documentation defining the configuration baselines required in this contract, are mutually consistent and mutually compatible.

SOW-0585 The Contractor shall ensure that the relationships between baselines, from FBL to OBL is documented.

SOW-0586 The Contractor shall control and maintain the approved configuration documentation for each baseline.

SOW-0587 The Contractor shall submit the complete configuration documentation for each baseline.

SOW-0588 The Contractor shall propose for Purchaser approval, as a part of the configuration identification process, the Product Structure, the CI's, the required baselines, the interfaces, and the associated identification/numbering schemes.

SOW-0589 The Product Structure shall be in the form of a top-down hierarchical breakdown – i.e. the Product Breakdown – on which each node/leaf is clearly defined and identified, as:

SOW-0589.A Configuration Item (CI);

SOW-0589.B Computer Software Configuration item (CSCI);

SOW-0589.C Computer Software Component (CSC).

SOW-0590 The Contractor shall incorporate under a unique Product Breakdown, all the information relevant to the OEMs/COTS hardware, software and firmware used and integrated in the capability.

10.6. Configuration Control

10.6.1. Engineering Change Proposals (ECP)

[0221] An ECP is the formal documentation that is prepared for an engineering change. It provides a means to introduce changes, corrections, additions or deletions to equipment, firmware, software, interfaces, and documentation for all supported systems/products/services.

SOW-0591 Changes shall be introduced and managed using ECPs.

SOW-0592 For following engineering changes as part of the agile implementation, the Contractor shall propose an agile way of introducing and maintaining the ECPs:

SOW-0592.A Adjustments to the Product Backlog items as part of the Sprint Planning

SOW-0592.B Change in categorization of the requirements from one activity group to another

SOW-0592.C Changes in approved design ABL (at CDR) during the sprint activities

SOW-0593 The type of changes as part of the agile implementation shall be at no additional cost to the Purchaser.

SOW-0594 All ECPs, their promotion along their lifecycle and all their attributes shall consistently be recorded in the CMDB.

[0222] A Change Advisory Board (CAB) is a forum that is responsible for screening, evaluating and implementing decisions regarding ECPs. The primary mission is to ensure that all change requests are handled efficiently and that a proper decision is made for each of them.

SOW-0595 The Contractor shall implement a Change Advisory Board for screening, evaluation and decision about ECPs. Its process shall be described in the CMP.

SOW-0596 An ECP shall be Class I (Product Enhancement) or Class II (Product Correction).

SOW-0597 Product Enhancement ECPs shall be submitted to the Purchaser for approval.

SOW-0598 Product Correction ECPs shall be submitted to the Purchaser for concurrence on the classification and for Information.

SOW-0599 The Contractor shall prepare and process ECP in accordance with Agency Instructions 16.32.02 [Ref: AI 16.32.02].

SOW-0600 The Contractor shall review and disposition the approved engineering changes in the CI and in its configuration documentation, update status accounting records, distribute change documentation, and verify change implementation.

SOW-0601 The Contractor shall use the templates described in [Ref AI 16.32.02] for ECP.

SOW-0602 Classified data, essential to the evaluation and disposition of an ECP, shall be submitted separately in accordance with the approved NATO security procedures referred to in Annex D.4.

10.6.2. Request for Deviation/Waiver (RFD/W)

SOW-0603 The Contractor shall prepare and process RFD/W for permission to use or release a product that has nonconforming characteristics within specified limits for an agreed time or quantity of that product.

SOW-0604 If the Contractor determines, prior to deployment of an item, that it is impossible to satisfy the mandatory requirements of the specification, the Contractor shall prepare and submit an RFD/W to the Purchaser.

SOW-0605 If the Contractor determines, either during or after development of an item, that the item does not meet specified requirements, but nevertheless believes that the item is suitable for use "as is", the Contractor shall have a procedure for preparing and submitting an RFD/W to the Purchaser.

SOW-0606 The Contractor shall prepare and process RFD/W in accordance with Agency Instructions 16.32.03 [Ref: AI 16.32.03].

SOW-0607 The Contractor shall submit data that is required to justify and describe the change/deviation/waiver and to determine its total impact.

SOW-0608 Concurrent with the preparation of an ECP, the Contractor shall prepare a Notice Of Revision (NOR) for each specifications and other non-specification type documents (comprising the configuration identification for an item) which would require revision if the ECP were approved.

SOW-0609 NOR shall be attached to their related ECP.

SOW-0610 The Contractor approved configuration documentation shall be used for all Contractor and Purchaser activities.

SOW-0611 The Contractor shall also ensure that information about the newly released and approved configuration documentation is incorporated into the Contractor’s Configuration Management Database (CMDB).

10.7. Configuration Status Accounting (CSA)

SOW-0612 The Contractor shall be responsible to acquire, deliver and provide access to the configuration information necessary to operate, maintain and support the system.

SOW-0613 The Contractor, as part of the CMP, shall describe how the Contractor created and maintained configuration data will be integrated with the Purchaser’s CMDB. For software development this may be comprised of automated processes, while for documentation data it may follow manual releases for incorporation.

SOW-0614 CMDB information and reporting systems shall be suitable to address the needs of all stages of this project appropriate to the contract and as such be tailored if necessary.

SOW-0615 At the commencement of each project stage, CMDB information shall be reviewed against the needs of that stage.

SOW-0616 CMDB shall be ready to accept data and provide the required information not later than the milestones specified in the contract.

SOW-0617 The Contractor shall utilize data elements to be able to:

SOW-0617.A Identify the current, approved configuration documentation, and identifier associated with changes;

SOW-0617.B Record and report the status of proposed engineering changes from initiation to release;

SOW-0617.C Record and report the results of configuration audits, including the status of identified discrepancies and action items;

SOW-0617.D Record and report the status of deviations/waivers;

SOW-0617.E Provide traceability of design and reconciliation of physical and logical configurations;

SOW-0617.F Track configuration identifiers for HW/SW and configuration files/scripts;

SOW-0617.G Record and report test data, test results and test procedures; and

SOW-0617.H Prepare CMDB records and reports.

SOW-0618 If a need arises for data elements not included in SOW-0617, the Contractor shall identify the data element to the Purchaser along with a proposed definition.

SOW-0619 The Contractor shall identify a focal point for the CMDB to interface with the Purchaser concerning potential or actual problems or deficiencies detected as a result of reviewing the output.

SOW-0620 The Contractor shall allow the Purchaser or its designates to access the Contractor’s configuration data at all times.

SOW-0621 The CMDB shall also include the identification of all proprietary or restricted data and the CI to which each agreement applies.

SOW-0622 The Contractor shall retain a complete configuration data historical record.

SOW-0623 In order to continue Configuration Status Accounting during the in-service phase, the Contractor shall transfer CMDB project-specific information to the Purchaser.

SOW-0624 The means and format of transfer of this data shall be as described in the CMP.

SOW-0625 The Contractor shall provide, to the satisfaction of the Purchaser, explanations and training on the interpretation of each CMDB data output.

SOW-0626 The Contractor's CSA shall provide the following reports:

SOW-0626.A An historical list of (sub-) contracts which will include information on the contact number, contractor's name and NCAGE and contract purpose;

SOW-0626.B A list of configuration documents for a CI;

SOW-0626.C A list of serial numbers for a CI (if applicable);

SOW-0626.D A list of all parts including the OEM's part number and the NATO Stock Number (if applicable) that comprise a CI;

SOW-0626.E A list of all ECP, RFD/W against a CI;

SOW-0626.F An historical list of all changes including information on the change status and implementation status (e.g. progress);

SOW-0626.G A list of all outstanding, programmed or planned audits;

SOW-0626.H A list of all outstanding actions, corrective and otherwise, as a result of an audit against a CI;

SOW-0626.I A list of CI which have been subject to an audit with the date of the audit, the result of the audit and the status of the audit; and

SOW-0626.J A breakdown list of the top level CI and all lower level CI.

SOW-0627 Each report shall be marked such that it will identify the nature of the report and the time and date of the report.

SOW-0628 In general, the reports shall be sufficient for the Purchaser to establish, but not be limited to, the following:

SOW-0628.A To control the status of the project in regard to the status of CI;

SOW-0628.B To control the status of a CI and all the changes involved; and

SOW-0628.C Reports shall be made available as specified in ABL and PBL Templates [Ref: AI 16.32.04 and AI 16.32.05, respectively).

10.8. Configuration Verification and Audit

10.8.1. Functional Configuration Audit

SOW-0629 The Contractor shall be responsible for conducting the Functional Configuration Audits (FCA).

SOW-0630 FCA shall take place on the CI, which is representative of the configuration to be released for production.

[0223] FCA may be conducted incrementally.

SOW-0631 FCA shall not be considered complete until integration testing is complete.

SOW-0632 The Contractor shall conduct the FCA for the CI in accordance with the FCA checklist provided, or approved, by the Purchaser.

SOW-0633 The Contractor shall review all updates to previously delivered documents to ensure accuracy and consistency throughout the documentation set.

SOW-0634 The Contractor shall document the physical configuration of the CI for which the test data are verified.

SOW-0635 The Contractor shall ensure that all test reports, procedures and data used for the FCA shall be made a matter of record of the FCA minutes.

SOW-0636 The Contractor shall ensure that test data essential to development are included on, or furnished with, the CI documentation.

10.8.2. Physical Configuration Audit

SOW-0637 The Contractor shall be responsible for conducting the Physical Configuration Audits (PCA).

SOW-0638 The Contractor's conduct of the PCA shall include a detailed audit of design documentation, technical data, and manuals for CSCI.

SOW-0639 The PCA shall also include an audit of the released engineering documentation and quality control records to make sure the as-built configuration is reflected by this documentation.

SOW-0640 The Contractor shall perform the PCA only when all data pertinent to the CI audit is available for the audit.

SOW-0641 The Contractor shall compile and make data pertinent to the CI audit available to all PCA participants two weeks in advance of the scheduled audit date.

SOW-0642 Required data pertinent to the CI audit shall include:

SOW-0642.A CI product specification; the current Purchaser approved issue of the development specification, software requirements specification and the interface requirements specification(s) to include Purchaser approved specification change notices, deviations/waivers;

SOW-0642.B A list delineating both approved and outstanding changes against the CI; Identification of all changes actually made during test; Identification of all required changes not yet completed;

SOW-0642.C Complete Shortage list;

SOW-0642.D Acceptance Test Procedures and associated Test Data.

SOW-0643 The Contractor shall review all records of baseline configuration for the CI by direct comparison with the appropriate engineering release system and change control procedures to establish that the configuration being produced does accurately reflect released engineering data.

SOW-0644 The Contractor shall perform the following actions for each CSCI being audited:

SOW-0644.A Review the design documentation which will comprise the SAD, DDD and UIS for accuracy and completeness;

SOW-0644.B Compare top-level software design descriptions with lower-level software design descriptions for consistency;

SOW-0644.C Compare all lower-level software design descriptions with all software listings for accuracy and completeness; and

SOW-0644.D Review the annotated listings for compliance with approved coding standards.

SOW-0645 The Contractor shall recommend acceptance of CI, which have demonstrated compliance with the product specification and shall certify by signature that the configuration item has been built in accordance with the drawings and specifications

10.8.3. General Audit Requirements

SOW-0646 The Contractor shall perform the audit(s) as scheduled in the CMP.

SOW-0647 A CI shall not be audited without prior Purchaser approval of the Functional and Allocated (development) baselines.

SOW-0648 A current set of listings shall be provided for each CSCI being audited.

SOW-0649 The Contractor shall be responsible for ensuring that subcontractors, vendors, and suppliers participate in audits, as appropriate.

SOW-0650 The Contractor shall be responsible for providing facilities for conducting audits.

SOW-0651 Accordingly, the Contractor shall be required to provide the necessary resources and material to perform the audits

SOW-0652 The Contractor shall prepare for each audit consistent with the scope and magnitude of the audit.

SOW-0653 The Contractor shall be responsible for establishing the time, place and agenda for each audit in accordance with the master milestone schedule, subject to coordination with the Purchaser.

SOW-0654 This shall be accomplished sufficiently in advance of each audit to allow adequate preparation for the meeting by the Contractor, any Sub-Contractors, and the Purchaser or designated representative.

SOW-0655 The Contractor shall provide the following information on CI(s) to the Purchaser prior to audit(s):

SOW-0655.A Contractor Team Composition;

SOW-0655.B Identification of CI to be audited;

SOW-0655.C Nomenclature;

SOW-0655.D Specification Identification Number;

SOW-0655.E Configuration Item Numbers;

SOW-0655.F Serial/License Numbers;

SOW-0655.G Part Numbers;

SOW-0655.H NCAGE;

SOW-0655.I Software inventory numbering system;

SOW-0655.J Current listing of all ECP, RFD/W against the CI, either requested of, or approved by the PM; and

SOW-0655.K Status of test programs to test CI with automatic test equipment (when applicable).

SOW-0656 The Contractor shall review the test procedures and results for compliance with specification requirements.

SOW-0657 Discrepancies shall be recorded in the audit minutes.

10.8.4. Post Audit Requirements

SOW-0658 After completion of the audit(s), the Contractor shall publish and distribute copies of audit minutes.

[0224] The Purchaser will officially acknowledge completion of the audit.

SOW-0659 The Contractor shall prepare and submit to the Purchaser for approval, audit report(s) complete with evidence of the closure of outstanding action items, in a format agreed to by the Purchaser.

[0225] The Purchaser will:

A. Provide the name, organization and security clearance of each participating individual to the Contractor prior to each audit;

B. Review the minutes and ensure that the minutes reflect all significant Purchaser inputs; and

C. Provide formal acknowledgement to the Contractor of the accomplishment of each audit after receipt of the audit minutes. The Purchaser establish the adequacy of the Contractor's audit performance by notification of:

D. Approval – to indicate that the audit was satisfactorily completed;

E. Contingent Approval – to indicate that the audit is not considered accomplished because some action items still remain outstanding (costs incurred for the resolution of all outstanding action items are the Contractor's responsibility), or

F. Disapproval – to indicate that the audit was seriously inadequate.

[0226] The Purchaser will acknowledge partial completion of audits(s) for those configuration items whose final approval is contingent upon completion of integrated systems testing.

SOW-0660 The Contractor shall record the accomplishment of the audit(s) in the Contractor's CMDB.

10.8.5. Internal CM Process Verification

SOW-0661 The Contractor shall plan Configuration process audits to assure an efficiently tailored CM system is implemented and that the configuration baselines have been set at the appropriate time in the contract.

SOW-0662 The Contractor shall perform the configuration management process audits, in accordance with approved CMP.

SOW-0663 The Contractor shall capture configuration process audit planning, results, and action closures as part of the CM activities and information and make this available to the Purchaser.

[0227] The Purchaser will reserve the right to conduct its own process audits of the Contractor, if the approved CMP is not matched by process execution results and presents risk(s) to the Contract.

11. TEST AND ACCEPTANCE

11.1. Introduction

[0228] This section details the Test, Verification and Validation TV&V processes and requirements to be applied and performed under the Contract, which are required for the verification and validation of the requirements set forth under the Contract by the Purchaser.

[0229] All Contract-related deliverables supplied by the Contractor will be verified and validated to ensure they meet the requirements of this Contract. Both fitness-for-use and fitness-for-purpose will be assessed using a quality-based approach.

[0230] The verification and validation approach will not only involve delivered equipment, but also interfaces and interoperability among ITM-RC1 defined capabilities as well as with existing NATO and/or national equipment, here considered as PFE.

[0231] The main objectives of the Testing on ITM-RC1 are:

A. to provide verifiable objective evidence that the system is fit for purpose and that the system satisfies all requirements in the requirements specification;

B. to detect and eliminate all defects;

C. to maximize test automation to increase the maintainability and repeatability of the tests and support regression testing.

[0232] Test at unit, component and system and service level are applicable within the scope of this Contract that is part of a global ITM-RC1 test strategy that includes:

A. Unit test, component test and system test of the other ITM-RC1 solution building blocks.

B. Additional integration tests, fit for purpose and fit for use of the complete solution. Those additional tests may identify defects on the products of this Contract, and those defects will be communicated to the Contractor for their timely resolution.

C. Requirements based testing, quality based testing, service based testing, and risk based testing and integration test activities during the development phase.

D. A consistent approach applicable to the different ITM-RC1 Work Packages and Contractors involved in testing.

[0233] Rigorous configuration management and version control will be a critical test readiness review criteria.

[0234] Acceptance Test-driven approach with be applied to analyse and design tests and to develop test cases.

[0235] The verification and validation of PFE is out of the scope of the Contract.

[0236] In this document, the term “deficiency” is considered to be an inadequacy or incompleteness process definition or execution, while the term “defect” is an error, a fault or a malfunction inside a Configuration Item.

[0237] Requirements verification methods, as defined in ISO/IEC/IEEE 29148 [Ref: ISO/IEC/IEEE 29148], will be used in order to obtain evidence(s) that requirements have been fulfilled.

SOW-0664 For each requirement, the Contractor shall select a verification method, which shall be approved by the Purchaser.

11.2. TV&V activities

SOW-0665 The Contractor shall perform and evidence the execution of the testing and acceptance lifecycle in accordance with the ITM-RC1 Test and Acceptance Plan (TAP) [Ref: ITM-RC1 TAP].

SOW-0666 All information items used during the verification and validation activities shall be handled according to their security classification, in accordance with ACO Security Directive [Ref: AD 070-001]

SOW-0667 The Contractor shall have the overall responsibility for meeting the Test and Acceptance requirements. This includes the development of all TV&V documentation required under the Contract, the conduct of all independent verification and validation as well as the evaluation and documentation of the results.

SOW-0668 The Contractor shall verify and validate all Contract-related deliverables before a formal release in order to assess the level of compliance with the requirements of this Contract.

SOW-0669 All document-based deliverables shall be produced in a manner compliant with the templates provided by the Purchaser.

SOW-0670 The Contractor shall perform verification to confirm that each element properly reflects the specified requirements, design, integration and documentation.

SOW-0671 The Contractor shall conduct SoW, SRS and SSRS requirement verification assessment to confirm that the Contractor's solution has met associated requirements, as these requirements are the objective basis for acceptance of the Contractor's solution.

SOW-0672 The Contractor shall support Purchaser led Validation activities to confirm that the solution is fit for purpose.

SOW-0673 The Contractor shall be responsible for the planning, execution and follow-up of all TV&V events related to the Contractor assigned scope.

[0238] The Purchaser will assist in preparations by reviewing and providing feedback on all Contractor produced Configuration Items. The Purchaser will also provide testing and engineering SME during all TV&V events to witness and assist with these events.

SOW-0674 The Contractor shall coordinate and allow NCI Agency witnessing of all the formal test events and their previous dry-runs.

SOW-0675 The Contractor shall demonstrate to the Purchaser that there is a Test Process in place for the project, supported by Contractor Quality Assurance (QA).

SOW-0676 The Contractor shall provide test data to support all TV&V activities.

SOW-0677 The Contractor shall follow the Purchaser defined TV&V processes [Ref: ITM-RC1 TAP].

SOW-0678 The Contractor shall adhere to the ITM-RC1 Testing and Acceptance Plan (TAP) [Ref: ITM-RC1 TAP].

SOW-0679 If the Contractor wishes to propose a modification to the process, the proposal shall be approved by the Purchaser and documented accordingly.

SOW-0680 The Contractor shall ensure that rigorous testing, including regression testing when required, 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-0681 All test, verification and validation material developed and used under the Contract shall be delivered to the Purchaser.

SOW-0682 The Contractor shall analyse and verify the requirements before the sprint planning meetings.

SOW-0683 The Contractor shall analyse and verify the design before starting the sprint tests.

SOW-0684 The Contractor shall present during the sprint retrospective the proposed improvements to the development and construction processes applied during the sprints.

SOW-0685 The Contractor shall generate test material (test cases, test scripts, test data, RTM, test results, test logs, defects and test reports) during each sprint.

SOW-0686 The Contractor shall perform sprint test events.

SOW-0687 The Contractor shall apply requirements based testing, risk based testing, service based testing and quality based testing practices during the sprint and release testing.

SOW-0688 The Contractor shall perform test at unit, component and system level, and at service level when applicable.

SOW-0689 The Contractor shall define automated test scripts and run fully automated tests for both unit testing and end to end testing applied during acceptance test events. Deviations to this automation approach shall be communicated formally following the Configuration Management process and approved.

SOW-0690 The Contractor shall provide a solution for automation testing that is integrated into the continuous deployment Pipeline.

SOW-0691 If during the project execution phase (including warranty period) defects are identified by other ITM-RC1 Work Packages, the Contractor shall resolve it and demonstrate the resolution on a specific test event within the next ITM-RC1 Sprint/timebox.

[0239] The Defects Triage Board [Ref: ITM-RC1 TAP] will decide on whether defects are to be resolved within one or the other WP.

[0240] Table 6 below lists and describes the different TV&V phases and associated activities during the ITM-RC1 Project execution. Each phase is addressed in one to many test events. The phases could be repeated during the sprints/timeboxes or distributed among the sprints/timeboxes.

[0241] The WMS will trace the ITM-RC1 actual sprints/timeboxes and checkpoints where TV&V Phases will be performed and the actual participation of the Contractor, user community and SMEs on each of these TV&V phases.

SOW-0692 The Contractor shall appoint a Test Director (TD) for the phases defined in Table 6 who will work closely with the Purchaser's assigned TVV Manager and NATO Quality Assurance Representative (NQAR)

SOW-0693 The Contractor shall lead the intermediate Acceptance Test of the release(s) and delivery package(s) provided within the scope of the Contract.

SOW-0694 The Contractor shall propose the number of Intermediate & Candidate Releases Acceptance Tests in accordance with the release roadmap proposed by the Contractor aligned with the ITM-RC1 release strategy. Purchaser will be the ultimate authority deciding on the release frequency, adhering to the existing NATO policies (e.g. Security Accreditation).

SOW-0695 The Contractor shall address within the scope of each Intermediate & Candidate Releases Acceptance Test(s): Integration tests, fit for purpose (including Quality Based Testing (QBT)) and fit for use (including Service Based Testing (SBT)) of the release(s) and delivery package(s) provided within the scope of the Contract.

SOW-0696 The Contractor shall consider the Intermediate & Candidate Releases Acceptance Tests the main formal acceptance test events and shall conduct them to demonstrate to the Purchaser that a system meets the requirements of a specification or contract as agreed by the Purchaser and the Contractor. The formal tests events scope will be focused, but not limited to component tests, system integration test, coexistence test, fault tolerance test, interface test, load and performance test, security test, user interface test, reliability tests, maintainability tests, functional test, operational acceptance tests.

SOW-0697 The Contractor shall propose all the test material required for the TRR.

SOW-0698 The Contractor shall provide the relevant test information to allow inviting the operational community to the test event at least three months in advance to the scheduled acceptance test event.

SOW-0699 The Contractor shall perform as many dry-runs as considered required in order to assure the success of the Candidate Release Acceptance Test(s).

SOW-0700 The Contractor shall deliver the Dry-run Report for review during the Test Readiness Review (TRR).

SOW-0701 Once the Request for Change (RFC) authorizes the deployment of the Work Package release and delivery package and the Security Accreditation (SA) is granted, the Contractor shall led the Transition into service test phase.

SOW-0702 The Contractor shall perform the Site Acceptance Test (SiAT) of the integrated solution on the different locations and deployment sites.

SOW-0703 The Contractor shall provide an assessment on the Operational Acceptance Criteria (OAC) status covered by the Work Package Contract based on evidenced during the acceptance test event(s).

[0242] The Purchaser will appoint TV&V Test Engineers and SMEs for each test event.

SOW-0704 The Contractor shall identify and use previously agreed Key Performance Indicators (KPIs) to measure process execution and identify opportunities for quality improvement, provide solutions and update the plans, the achievement of defined objectives like coverage of risks, requirements, supported configurations, supported operational scenarios, etc.

SOW-0705 The Contractor shall propose for each Activity Group in the scope of the implementation approach; which TV&V phases will be applied in the Master Test Plan. Any deviation from the TV&V phases given in the Table below; shall be approved by the Purchaser.

SOW-0706 The Contractor shall have the overall responsibility for conducting all related activities defined in Table 6 below, which describes TV&V phases.

TV&V Phases	Scope	Purchaser Involvement
Engineering Test Phase	*Internal Contractor activities executed during development phase (as part of each sprint/timebox) of the system to ensure the system conforms to its design specifications and to the requirements, that both the product quality characteristics and the contribution to the ITM-RC1 services are built in, and that the contribution to the Operational Acceptance (OA) is on track.* *During this phase the main objective is to detect issues and problems as soon as possible and assure the readiness for formal acceptance testing and confirm the qualifications based on certifications* SOW-0707 The Contractor shall organize witness tests (end to end & high risks) with a periodicity agreed with the Purchaser and not later than every four (4) sprints. SOW-0708 Test activities shall be reported and presented on dashboards and boards by the Contractor.	Review: Test Reports for Unit, Integration and System tests

TV&V Phases	Scope	Purchaser Involvement
Qualification Phase	Activities executed to verify the design and manufacturing process, ensure the system meets necessary design requirements, and provide a product baseline for subsequent acceptance tests. Possible activities: • TEMPEST Testing ** • Fault Tolerance Testing ** • Physical Functional System Testing ** • User Interface Testing (Eligible and non-eligible users) ** • Component Testing * • Interface Testing * • Security Testing * • Integration Testing (internal to the project deliverables) * *Intermediate and Candidate Release ** Candidate Release	Review: Event Test Plan, Test Cases/Scripts, Test Reports, Test Data, Test Environment Baseline, Existing defects. Participate: Test Readiness Review (TRR), Test Execution, Event Review Meeting (ERM) Provide: Test Event Assurance Reports
Intermediate & Candidate Releases Acceptance Test (I&C RAT) Phase[9]	To verify that Work Package candidate products and delivery comply with the requirement/design specifications and assess whether it can be released to other WP. To verify that production units to be delivered by the Work Package comply with the requirement/design specifications and assess whether production can start. Confirm that all required engineering-level testing activities have been completed in accordance with the requirements. Determine if the Work Package deliverables in the form of Work Package candidate releases are ready (from the Functional and non-functional perspective, from the service perspective and from the Operational Acceptance (OA) perspective) contributing as such to the subsequent TV&V activities. This acceptance test covers integration tests, fit for purpose and fit for use of the release(s) and delivery package(s) provided within the scope of the Contract. SOW-0709 At the end of each Task Order, the Contractor shall lead and execute Intermediate Candidate Release (Witness) Events (for internal releases that are not yet to be deployed	Review: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects. Dry Run results. **Participate:** Dry Run (Optional Purchaser participation), TRR, Test Execution, Event Review Meeting (ERM)

[9] "Intermediate & Candidate Releases Acceptance Test Phase" equals the "WP Candidate Acceptance Test Phase" in the Test and Acceptance Plan (TAP).

TV&V Phases	Scope	Purchaser Involvement
	to operations), Candidate Release (Witness) Event (for deliverables considered ready for the operational environment) and the preceded Dry-run events (to assure the readiness before involving NATO witnesses). SOW-0710 The Contractor shall report and present test events and cumulative results dashboards and boards. SOW-0711 A subset of tests conducted during this phase shall also support the TV&V Assessment Phase. The witness tests will be time boxed within each WP. Functional Configuration Audit (FCA) and Physical Configuration Audit (PCA) activities, regression testing or simplified entry control check are to be performed again by the Work Package receiving a release. As part of this verification process a different WP can identify defects on the release that will trigger an updated release request that will go through the previous phases.	
TV&V Assessment Phase	Independent assessment to determine whether or not a system satisfies user needs, functionality, requirements, and user workflow processes etc. before it gets into operation. Ensures Product Quality Criteria, for the following tests: ● Security Tests – Tests focused on ensuring the security criteria are met. ● System Acceptance Test (SAT) Tests focused on ensuring compliance with the requirements and the product quality characteristics. ● RFC Evaluation – Review by Agency Change Managers and execution of any additional evaluation as requested by Change Managers. ● User Acceptance Test (UAT) – Scenario based testing, focused on validating the system as per user needs, including both service needs and operational acceptance criteria. Service operations (ESOC), CIS Support Units (CSUs) and related business areas (NATO Infrastructure Services Centre (NISC)) are operating for both eligible and non-eligible users.	**Review:** Event Test Plan, STVP, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **Participate:** TRR, Test Execution, Event Review Meeting (ERM). User Reviews (including internal users)

TV&V Phases	Scope	Purchaser Involvement
	SOW-0712 The Contractor shall lead SAT and UAT assessment and execute the associated test events within the Contract scope. SOW-0713 The Contractor shall run Security Testing in order to de-risk the security test results that will be obtained by NCI Agency during the RFC testing and any necessary Security Accreditation processes as identified in the relevant section of this SOW. SOW-0714 The Contractor shall report and present test events and cumulative results dashboards and boards. SOW-0715 The Contractor shall support this activity when lead by IVVQ for the complete solution final acceptance.	
Transition into service[10] phase	To ensure migration related tests and integration with PFE. Based on the migration strategies confirms the post migration benchmark and functionality for all migrated systems and applications. SOW-0716 The Contractor shall lead and execute the migration and transition into service test events within their Contractual scope. SOW-0717 The Contractor shall report and present test events and cumulative results dashboards and boards.	**Review:** Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **Participate:** TRR, Test Execution, Event Review Meeting (ERM)
Site Acceptance Phase (SiAT)	To ensure that the specific site/node is installed properly per site/node installation plan and the service meets the requirements stated in the SRS. Site Acceptance Testing is also to ensure compatibility and integration of the product with the site environment.	Review: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects

[10] 'Transition to Services' is identified as 'the integration of the features deployed to the live environment with the existing NATO Services', 'completion of the application and user migration and transition activities' and 'the transition of the capabilities to the Business Areas for service delivery'. In context of WP07 and ITM RC1, 'Transition to Services' is an activity led by the Purchaser, with support from the Contractor for the WP07 scope of work, and is a prerequisite for achievement of IOA and FOA milestone(s) as described in Section 2.5.

TV&V Phases	Scope	Purchaser Involvement
	Migration related tests are also covered under this tests. This includes integration with PFE. SOW-0718 The Contractor shall support as level of effort (inc. planning, execution ad reporting) the SiAT and Regression Test within the Contractual scope.	Participate: TRR, Test Execution, Event Review Meeting (ERM)
Operational Test and Evaluation	To ensure that all the Operational Acceptance Criteria (OAC) such as performance and availability have been successfully implemented. Sites are successfully integrated and tested on the network level. Demonstrate that all components of the System/Application have been integrated (including other systems) to meet all OACs as well as all security requirements defined in the relevant Security Accreditation Documentation Package. Ensure end to end delivered system works as expected and can interoperate with other Purchaser equipment. SOW-0719 The Contractor shall support as level of effort (inc. planning, execution and reporting) additional performance Reliability, Availability and Maintainability (RAM) tests and verifications within the scope of the Contract. SOW-0720 The Contractor shall support as level of effort (inc. planning, execution and reporting) Operational Live Test within the Contractual scope.	**Review:** Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **Participate:** TRR, Test Execution, Event Review Meeting (ERM)

Table 6 - TV&V Phases

SOW-0721 The Contractor shall be accountable and responsible for the following Engineering, Qualification Intermediate & Candidate Releases Acceptance Test, Transition into service phases and associated events direction, specification, planning, execution, reporting and completion within the scope of the Contract.

SOW-0722 The Contractor shall be responsible for the TV&V Assessment, SiAT and OT&E Phases dry-runs and formal events specification, planning, execution, reporting and completion within the scope of the Contract.

11.2.1. Agile Testing

SOW-0723 The Contractor test team shall perform in keeping with the agile method of work followed within the work package.

SOW-0724 The Contractor test team work shall be integrated in the agile backlog that will plan and control the agile items status until completion.

SOW-0725 The Contractor shall manage the Test Cases and defects resolution within the Product Backlog.

SOW-0726 The Contractor shall define test related backlog items, including the story points and discuss them with the Purchaser.

SOW-0727 The Contractor shall identify, analyse, implement and review agile test work items within the context of the Work Package and the integration of its results within the complete solution.

SOW-0728 The Contractor shall verify, also within a sprint/timebox approach, the transition to the in service state confirming the solution readiness together with the supporting capabilities.

SOW-0729 The Contractor shall use the instances of the NCI Agency agile test management tools. These tools will be provided by the NCI Agency as PFE/Is.

SOW-0730 The Contractor test personnel shall participate in the agile meetings identified by the Purchaser.

SOW-0731 The Contractor shall ensure the generation of Verifiable Objective Evidence (VOE)[11] as a consequence of the Contractor's TV&V and technical review activities.

[0243] Agile activities and performed work are handled on the NCI Agency Environment (Section 11.5.5).

SOW-0732 The Contractor shall apply Test Driven Development (TDD), when applicable, in order to ensure automated unit tests to test function's specific behaviours are built during the development within each sprint. The Contractor shall timely run continuous unit testing and supports timely refactoring before moving to the next unit tests defined during the next sprint.

SOW-0733 The Contractor shall develop and apply automated end to end testing that will be also used for regression test and acceptance test events.

SOW-0734 The Contractor shall include regression test suites as part of the acceptance test events.

SOW-0735 The Contractor shall, when applicable based on a cost benefit analysis, perform and evidence pairing/peer reviews during sprint, where one person review while the other perform the task, during the development activity.

SOW-0736 The Contractor shall include quality assurance and automated verification checks within the pipeline during the Continuous Development and Continuous Integration (CD/CI).

SOW-0737 The Contractor shall maintain the solution and the configuration tree until its lower level configuration items under a rigorous configuration management.

SOW-0738 The Contractor manage the changes to the release proposed for acceptance testing using technical change request.

[0244] The Purchaser reserves the right to monitor and inspect the Contractor's TV&V activities to verify their compliance with the requirements set forth in this Contract.

SOW-0739 The Contractor shall only proceed to the next formal TV&V activity, after the successful completion of the previous TV&V activity and after the agreement/approval by the Purchaser.

11.3. Deliverables

SOW-0740 The Contractor shall provide a System Test Documentation Package, following documentation templates referenced by the TAP, that is comprised of documents in the Figure 6 – IVV Documentation (Test Deliverables and products.

[0245] The following figure presents the list of test documents provided as PFE / Purchaser Furnished Documentation (PFD) and required as Contractual Deliverables. The connectors identify the sub-products within a deliverable.

[11] Objective Evidence. Data supporting the existence or verity of something (ISO 9000:2015).

[0246] The Contractor shall submit the documentation and data deliverables in accordance with the requirements of Section 13.

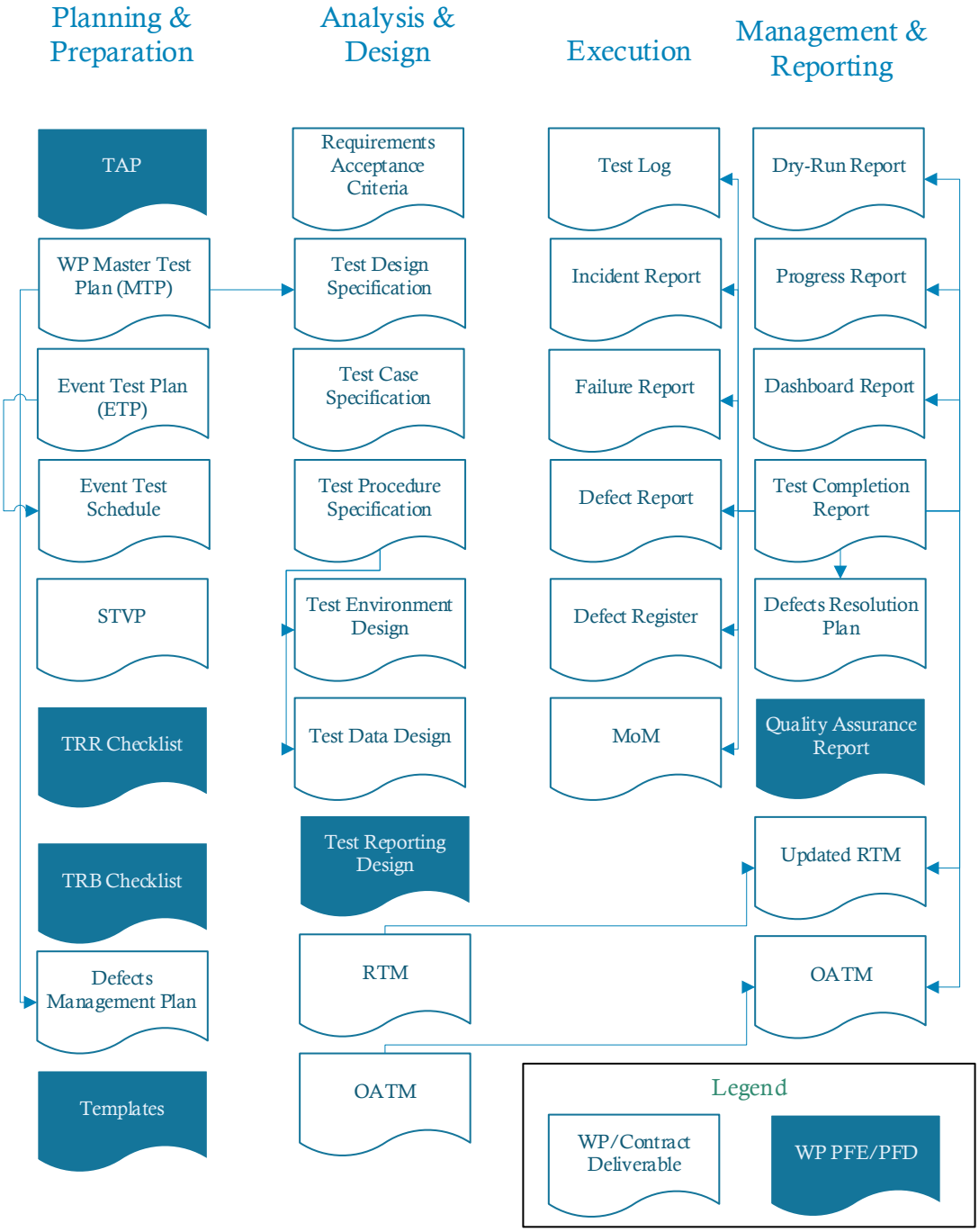

Figure 6 – IVV Documentation (Test Deliverables and products)

SOW-0741 If applicable, the Contractor shall develop and validate any Test Harnesses, simulators and stubs, including all script/code/data/tools required to execute the planned functional and non-functional tests in the Test Environment. The Test Harnesses for PFE will be provided by the Purchaser.

[0247] The following timeline indicates by when the deliverables need to be provided to the Purchaser (and approved by the Purchaser) for each Test Event:

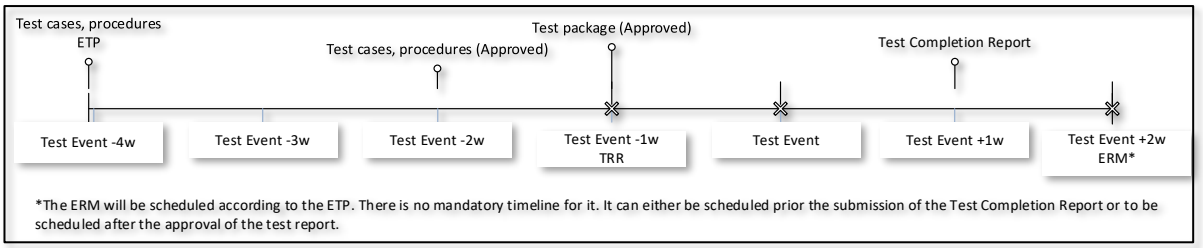

Figure 7 - Test Event timeline

SOW-0742 Modification of inaccurate or inadequate TV&V deliverables and any subsequent work arising as a result shall be carried out at the Contractor's expense.

SOW-0743 All TV&V materials developed and used under the Contract shall be baselined for each Activity Group particularly and delivered to the Purchaser.

SOW-0744 The Contractor shall comply with and use the Purchaser-provided IVV templates during contract execution for the following deliverables:

- SOW-0744.A Assurance Report Template
- SOW-0744.B TRR Checklist
- SOW-0744.C Minutes of Test Readiness Review Meeting
- SOW-0744.D Project software Checklist
- SOW-0744.E Test Plan Template
- SOW-0744.F Test Report Template
- SOW-0744.G Summary Test Review Minutes
- SOW-0744.H Master Test Plan Template
- SOW-0744.I Project Requirements Traceability Matrix Template
- SOW-0744.J Requirement or Test Case Waiver Template
- SOW-0744.K Security Test and Verification Plan Template
- SOW-0744.L Test Case Specification Template
- SOW-0744.M Test Completion Report Template
- SOW-0744.N Test Design Specification Template
- SOW-0744.O TRM-Checklist

[0248] Latest versions of these templates will be communicated and incorporated at EDC. These templates will also be provided electronically.

SOW-0745 In case the Contractor would like to deviate from the Purchaser-provided templates, the Contractor shall request a change with the appropriate change process.

SOW-0746 All deliverables shall undergo as many review cycles are required, and shall be approved once all deficiencies have been corrected.

11.3.1. Master Test Plan (MTP)

SOW-0747 The Contractor shall identify and describe in the Master Test Plan (MTP) which best practices and international standards will be applied and how.

SOW-0748 The Contractor shall produce a Master Test Plan (MTP) to address the plans for each TV&V activities listed in this document. The Purchaser will monitor and inspect the Contractor’s MTP activities to ensure compliance.

SOW-0749 The Contractor shall keep the MTP always up to date.

SOW-0750 The Contractor shall describe how the Quality Based Testing is addressed and implemented in the MTP. Figure 8 - Product Quality Criteria is based on ISO 25010 [Ref: ISO] and should be used as product quality criteria model.

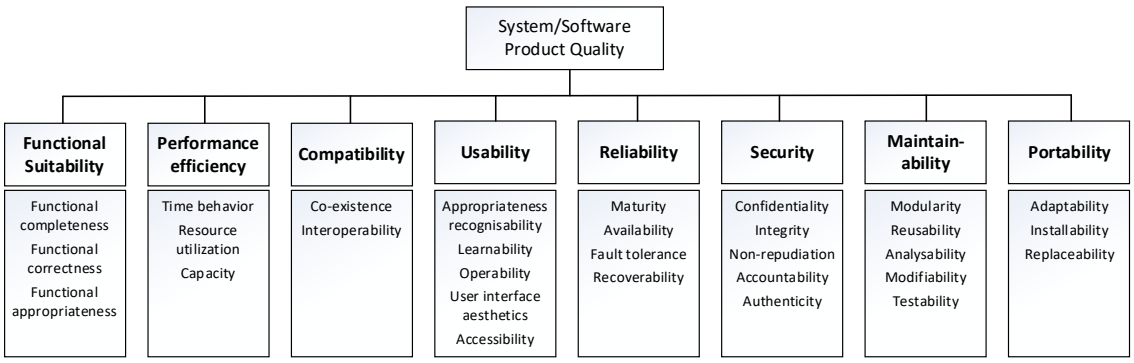

Figure 8 - Product Quality Criteria

SOW-0751 The Contractor shall describe all formal TV&V activities in the MTP with a testing methodology and strategy that fit the development methodology chosen by the project.

SOW-0752 The Contractor proposed testing methodology shall describe the method of achieving all the test phases, defined in Table 6 successfully.

SOW-0753 The Contractor shall describe in the MTP how the following objectives will be met:

SOW-0753.A Compliance with the requirements of the Contract;

SOW-0753.B Verification that the design produces the capability required;

SOW-0753.C Compatibility among internal system components;

SOW-0753.D Compliance with the SRS requirements;

SOW-0753.E Compliance with external system interfaces and/or systems;

SOW-0753.F Confidence that system defects are detected early and tracked through to correction, including re-test and regression approach;

SOW-0753.G Compliance with Purchaser policy and guidance (i.e. security regulations, etc.);

SOW-0753.H Operational readiness and suitability;

SOW-0753.I Product Quality Criteria;

SOW-0754 The Contractor shall describe the Contractor's test organization and its relationship with the Contractor's Project Management Office and Quality Assurance (QA) functions in the MTP.

SOW-0755 The Contractor shall describe in the MTP "Entry and "Exit" criteria for each of the formal TV&V events. The Contractor shall seek and obtain approval of all criteria related to an event not later than the TRR of the event

SOW-0756 The Contractor shall provide in the MTP the schedule, location and scope for all the events to be run, specifying to which phase they belong. When the Contractor identifies that multiple events are required for a phase, this shall also be specified in the MTP.

SOW-0757 Together with the MTP, the Contractor shall provide a defect reporting and management process to be applied during the TV&V activities.

SOW-0758 The Contractor shall describe how defects/non-conformances encountered during TV&V events will be reported, managed and remedied

SOW-0759 The MTP shall include the Contractor's approach to Test Reviews including Test Readiness Reviews and Event Review Meetings for each TV&V event.

SOW-0760 The Contractor shall provide Contractor's provisions and strategy for building/maintaining of the Reference Environment in the MTP.

SOW-0761 The MTP shall identify any specialised or long-lead items required for testing.

11.3.2. Test Cases and Test Procedures

SOW-0762 The Contractor shall develop test and use cases to verify and validate all requirements in the SoW, requirements specifications and final design. The test cases shall follow the template provided by the Purchaser

SOW-0763 The Contractor shall submit the draft test cases for the TV&V event to the Purchaser for approval no later than four (4) weeks prior to the execution of the tests, unless differently stated in a work package. The Purchaser shall provide comments or approval within four (4) weeks of receipt. The Purchaser must have the final version of the test cases and Event Test Plan available one (1) week prior to the TRR for a specific TV&V event

SOW-0764 Any updates required from the execution of test cases during each phase shall be incorporated into the relevant test cases by the Contractor for use during independent verification, validation and acceptance. If only certain sections are affected, then it shall be sufficient to up-date and re-issue those sections plus cover sheet with amendment instructions. Should major changes in contents or page re-numbering be needed, then the complete section shall be re-issued by the Contractor. All changes shall be made with the agreement and approval of the Purchaser.

11.3.3. Event Test Plan (ETP)

SOW-0765 The Contractor shall create an Event Test Plan (ETP) per each event detailing all the information required for that event, which shall follow the template provided by the Purchaser.

SOW-0766 The Contractor shall describe in the event test plan what training (if any) will be provided prior to formal TV&V events.

SOW-0767 The Contractor shall identify, in the ETP, which environment(s) to be used at each TV&V event and the responsibilities for configuration control, operation and maintenance of the environment.

SOW-0768 The ETP shall describe when an agreement shall be reached between the Contractor and the Purchaser on the defect categorization and defect priority of failures encountered, as well as a way forward (if either at the end of each day of a TV&V event or at the Event Review Meeting). If agreement is not reached, the disputed items shall be escalated to the Purchaser’s and Contractors’ Project Managers

11.3.4. Requirements Acceptance Criteria

[0249] Requirement Acceptance criteria represent a condition that states whether the specified SRS requirements are fulfilled or not. Written in simple language, the Acceptance Criteria is complementary to each contractual requirement in the SRS and provides the basis of a shared understanding for what is to be delivered and what is required as objective evidence to assess that a requirement has been met. Acceptance Criteria for requirements with V&V Method of Test and Demonstration for instance can be written in “Given/When/Then” format. It is meant to provide a logical description which actions would lead to meeting the requirements. It is not meant to provide detailed input or physical description (as this is the actual Test Case/Script).

SOW-0769 The Contractor shall translate each requirement in the SoW/SRS, in an acceptance criteria that will clearly detail how the requirement will be fully met (clear pass/fail or yes/no outcome)

SOW-0770 The Contractor shall address the Purchaser's comments and update the Acceptance Criteria accordingly.

SOW-0771 The Acceptance Criteria shall be agreed by both Contractor and Purchaser prior to the creation of the Test Cases/ Scripts.

SOW-0772 The agreed Acceptance Criteria shall be translated into Test Cases to provide details of full requirements coverage

11.3.5. Requirements Traceability Matrix (RTM)

SOW-0773 The Contractor shall produce and maintain the Requirement Traceability Matrix (RTM), which includes all functional and non-functional requirements, to track the TV&V status of all requirements throughout the Contract execution (especially during the TV&V activities).

SOW-0774 The RTM shall comply with the requirements depicted in Section 3 Requirements Management and Traceability.

SOW-0775 The RTM shall also trace the requirements to the design. It shall also define how the requirements will be validated or verified at each of the TV&V activities:

- SOW-0775.A The verification method: Inspection, Analysis, Test or Demonstration
- SOW-0775.B Correspondent TV&V phase(s) for each requirement
- SOW-0775.C Coverage Status
- SOW-0775.D Corresponding Sprint

[0250] The Purchaser will review and approve the proposed RTM. In addition, another document, called Operational Acceptance Traceability Matrix (OATM), will be maintained by the Purchaser to trace the Operational Acceptance Criteria along the TVV activities execution.

SOW-0776 The Contractor shall maintain the RTM updated during the project lifecycle.

SOW-0777 The RTM shall be provided and maintain as a standalone annex to the design specifications, extend this matrix to the Development Baseline, Product Baseline / As-Built configuration and the Master Test Plan (MTP) to ensure verification throughout the project.

SOW-0778 The RTM shall guarantee the two-way link between requirements (SRS) and technical specifications.

SOW-0779 The Contractor shall provide the Purchaser with updates (via the tools identified by Section 11.4) to the RTM daily during the execution of an event, and following the conclusion of each event defined in the MTP. A workflow for updating the RTM shall be proposed by the Contractor and approved by the Purchaser.

SOW-0780 The Contractor shall verify each requirement using a verification methods as defined in the TAP [Ref: ITM-RC1 TAP]. Selected verification method for each requirement shall be subject to Purchaser approval.

SOW-0781 If the verification method per requirement is not provided beforehand, the verification method shall be either test or demonstration. Any deviation to this requirement is subject to Purchaser approval.

11.3.6. Operational Acceptance Traceability Matrix (OATM).

[0251] Operational Acceptance is the formal process, and decision, with respect to confirming whether or not a system/project satisfies the operational requirements, user needs and is sustainable over the course of its expected life.

[0252] An Operational Acceptance Criteria (OAC) is a requirement that a system, project, service, or capability must satisfy in order to be accepted by a user, customer or other authorized entity.

[0253] The Purchaser will provide a collection of Operational Acceptance Criteria in the SRS and in an Operational Acceptance Traceability Matrix (OATM).

SOW-0782 The process for updating the OATM shall be provided by the Purchaser and coordinated with the Contractor.

SOW-0783 For each OAC in OATM, the Contractor shall provide a proposal of evidence for achievement of the OAC. The proposal shall be approved by the Purchaser.

SOW-0784 The Contractor shall provide the Purchaser with updates (via the tools) to the OATM during the execution of an event, and following the conclusion of each event defined in the MTP.

11.3.7. Test Completion Report

[0254] The Test Completion Report provides a summary and the evidences of the testing performed during the Test Event, including the Dry-Run Test events.

SOW-0785 The Contractor shall provide, in the Test Completion Report, a log/record of the event, including but not limited to individual test results, defects found (with a way forward for the ones remaining open), requirement coverage (planned and executed), test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

11.4. Tools

SOW-0786 The Contractor shall generate and deliver automated test procedures/cases and scripts compatible with Purchaser test management and automation tools (i.e. JIRA).

SOW-0787 The Contractor shall make use of automated testing and supporting testing tools (test management, requirement coverage, defect management, etc.) to the maximum applicable extent, for all system development, implementation, internal and formal tests. The process and proposed supportive tools shall be described in the Master Test Plan (MTP). In areas where the Purchaser already uses specific tools, the Contractor shall make use of the tools in use by the Purchaser

SOW-0788 Tools supporting requirements coverage, defect management and test management shall be selected and hosted by the Purchaser NR environment and used by the Contractor. For any internal work, the Contractor may use their own internal tools, but the tools used for the Contractor's internal work shall be able to natively interface with the tools selected and hosted by the Purchaser in order to keep all TV&V related data for the complete ITM-RC1 project in the Purchaser tools.

SOW-0789 The Contractor shall prepare the test management tools and manage the interface with the requirements management tool (See Section 3) to support the ITM RC1 Requirements Landscape depicted in Figure 2 and the generation of automated test and verification reports.

11.5. TV&V Events and results

SOW-0790 The Contractor shall conduct testing during the Project lifecycle compliant with the following requirements:

SOW-0791 The Contractor is responsible for conducting all testing during the Project lifecycle. The Contractor shall provide evidence to the Purchaser of the results of these testing activities. The Contractor shall respond to any Purchaser clarification requests regarding test results or performance within two working days

SOW-0792 The Contractor shall conduct all testing activities for any architectural changes.

SOW-0793 The Contractor shall support post go-live activities during the Operational Acceptance phase, to evaluate the project capability performance and establish benchmarks for future enhancements, including any changes made to fulfil the requirements.

SOW-0794 The Contractor shall provide status reports to the Purchaser regarding verification and validation activities during the planning/design and development phases, via the use of a dashboard report within the test management tool set and through meetings. The Contractor shall provide report(s) to the Purchaser following the completion of any TV&V event.

[0255] The Purchaser will approve the report and its findings within two business days.

SOW-0795 Progress and results measurement shall be approved by the Purchaser and focused on KPIs.

SOW-0796 Test results shall be recorded in the test management tool set. All results of all formal acceptance testing performed during a given day must be recorded in the test management tool. The Contractor shall provide these test results for any given day by the starting of the next business day (0800 AM), but as a minimum not later than 24 hours following the execution of any test.

11.5.1. Test Readiness Review (TRR)

SOW-0797 The Contractor shall conduct a Test Readiness Review (TRR) meeting at least one week prior to the events defined in the MTP. The TRR shall ensure that all entry criteria for the events have been met. Documentation that requires review by the Purchaser prior to a TRR, as defined in the Event Test Plan (ETP), shall be provided no less than 2 weeks prior to TRR.

SOW-0798 The Purchaser has the right to cancel the TRR and/or any formal test event if the evidence demonstrates that execution of the test event will not be effective.

SOW-0799 The Contractor shall demonstrate that all the internal tests and dry runs are successful with test reports and results delivered to the Purchaser at least 2 weeks prior to start of any Contractual test activities.

SOW-0800 Formal acceptance testing, including installation testing, shall be performed always on an environment with the up to date security settings, latest approved patches and antivirus applied and on a solution that has followed the security guidelines and policies.

11.5.2. Event Review Meeting

SOW-0801 The start and/or ending of any test session shall be subject to the Purchaser approval. In the event that critical issues are encountered which impact the process of the testing or if the other functions depends on the failed test cases, the Purchaser has the right to stop the testing for Contractor's investigation. The tests can only re-start if Purchaser agrees to continue testing from the point of failure or re-start testing from the beginning.

SOW-0802 The Contractor shall convene an Event Review Meeting (ERM) as defined in the ETP. The ERM shall ensure that the event results, defect categorization and a way forward to fixing the defects (if required) is agreed between the Contractor and the Purchaser. If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Managers.

11.5.3. TV&V Event

[0256] An event starts with the Test Readiness Review (TRR) and finishes off with the Event Review Meeting (ERM).

SOW-0803 During formal TV&V phases, a daily progress debrief shall be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.

SOW-0804 For each TV&V event, the Contractor shall provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution

durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

SOW-0805 Contractor shall facilitate and support up to five days of ad hoc testing by Purchaser personnel during each test phase. The Contractor shall record and assess for Contract relevance any discrepancies identified during ad hoc testing. The Contractor shall include the ad hoc testing results on the Test Completion Report.

SOW-0806 At the end of the project, the Contractor shall provide the final version of all artefacts (regardless of format) created during the execution of all TV&V activities.

11.5.4. Deliverable Release Acceptance Review

[0257] The Deliverable Release Acceptance Review serves as a Close-out Meeting for the last candidate release that must have gone through test, verification and validation.

[0258] The Deliverable Release Acceptance Review can take place when all Must Have requirements defined for the deliverables have been delivered, and there are no recorded defects with a severity above “Minor”.

SOW-0807 At the end of each Candidate Release, the Contractor shall by default meet, in person, with the Purchaser’s Project Manager and Purchaser’s SMEs at the Purchaser’s facility (either The Hague-Netherlands, Brussels-Belgium or Mons-Belgium, at the discretion of the Purchaser) for a Deliverables Acceptance Review. If agreed between Purchaser and Contractor, the meeting could be done as a video-conference meeting.

SOW-0808 The Contractor shall one week prior to the Deliverables Release Acceptance Review provide a deliverables acceptance request.

SOW-0809 The Contractor shall at the Deliverables Release Acceptance Review Meeting present the VOEs and that reflect the deliverables and tests produced/ reported in this release.

11.5.5. Test/reference environments

[0259] The environments where the test events will take place, is depending on the implementation phases of ITM-RC1 with Site DC Acceptance as the relevant major milestone.

[0260] Implementation and testing of ITM-RC1 will start with a so-called green field approach. Until the Site DC Acceptance milestone there will be a staging area including a pre-staging tenant that includes the sites DC Mons and DC Lago Patria. During this phase IREEN ON@NU and IREEN ON@NS have to be considered as two implementation sites that follow the green field approach as well.

[0261] The Purchaser and the Contractor shall have both access to the test & reference environments throughout the lifetime of this project.

[0262] After the Site DC Acceptance milestone the staging area will be declared the production environment and consequently the pre-staging tenant will become the pre-production tenant. The production environment will be ready for operational use. At the same time IREEN ON@NU and IREEN ON@NS will become ready for use as the ITM reference environment.

SOW-0810 The Contractor shall obtain the approval of the Purchaser regarding the environments the formal events will take place on and in requesting the approval, indicate what support is required from the Purchaser to configure and prepare the environment. This includes any data from the Purchaser required for the test event. The test environments configuration shall be formally controlled using configuration management tools, and each baseline that will enter into a contractual event shall be delivered to the Purchaser for approval prior to TRR.

SOW-0811 The Contractor shall ensure that all test/reference environments are under proper configuration management, especially configuration control. The Configuration Management toolset and process shall be approved by the Purchaser.

SOW-0812 The Contractor shall make sure that the test environments used to conduct WP Release Acceptance Tests and TV&V Assessment is representative of the actual operational environment, including (but not limited to): Design and configuration; Performance; Security settings; Software versions.

SOW-0813 For non-classified new software, the NATO Software Factory shall be used by the Contractor to enable the use of standardised software engineering processes and common tooling shared by NCI Agency, Industry and potentially by Nations.

SOW-0814 The Contractor shall perform initial Integration and testing activities on IREEN ON@NU.

SOW-0815 Sprint testing shall be performed on the IREEN ON@NU.

SOW-0816 Formal verification and validation activities during the TV&V Phases (Table 6), including formal integration testing, shall be executed on the environments previously identified.

SOW-0817 The Contractor shall coordinate with the Purchaser the testing in multiple environments approach and readiness based on the AfT.

SOW-0818 The Contractor shall provide the necessary information for obtaining the AfT for test procedures requiring connection with operational network (i.e. NATO ON and NS) and NATO services. The Contractor shall follow the requirements depicted in Section 8.1.4 Approval for Testing (AfT).

11.5.6. Test Waivers

SOW-0819 The Contractor may request a Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. The Purchaser, after review of test waivers and analysis of their impact, reserves the right to require test and certification of the modified equipment at no cost to the Purchaser. The Purchaser has the right to reject any test Waiver.

SOW-0820 In respect to a requested Test waiver, the Contractor shall certify that the test environment to be implemented is identical to that which was originally used for testing, or inform the Purchaser of design/construction changes which affect form, fit or function.

SOW-0821 The Contractor shall record and log all waiver requests along with their resolution submitted for the Purchaser's approval.

11.5.7. Failed events

SOW-0822 In the event of failed TV&V event and the need to return to a site for re-testing; travel and per diem expenses of NATO personnel shall be borne by the Contractor.

11.6. Test Defect Categorization

SOW-0823 The Contractor shall use the Purchasers' categorization nomenclature for all defects and non-compliances

SOW-0824 Should a failure be identified during a TV&V event/activity, a defect shall be recorded in the Agency's' test management and defect management systems. Once the event has concluded, the defect shall be reviewed during the event review meeting to agree on the severity, priority and category. The event test report shall then report the disposition of all defects recorded during the event and the defect management system shall be updated accordingly. Classification shall follow the definitions in Table 7 - Definitions for Defect Categorization:

Attributes	Definition
Severity	The severity of a defect is the degree of impact that the failure has on the development or operation of a component, a system or a user function. The severity 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 Purchase's PM will set the priority.
Category	The type of observation identified during the execution of a test case.

Table 7 - Definitions for Defect Categorization

11.6.1. Severity

SOW-0825 According to their severity, defects shall be classified as one of the following in Table 8 - Classification of defects based on severity:

Severity	Definition
Critical	The failure of testing of a requirement. The failure results in the termination of the complete system or one or more component of the system. The failure causes extensive corruption of data. The failed function is unusable and there is no acceptable alternative method to achieve the required results
Major	A significant failure that causes severely impaired functions but does not prevent operational processing. Applies to conditions under which the complete system or one or more component of the system are partially inoperative, but are still usable by the users. A work around may be available, but it may require manual intervention. Examples: * Absence of expected modules/ object or Unit * failure of business operational process that affects a large group of users * complete failure of a module
Moderate	The failure does not result in the termination and all functions are available but causes the system to produce incorrect, incomplete or inconsistent results. When resources are available and budgeted, should be resolved.
Minor	The failure does not result in termination and does not damage the functioning of the system. The desired results can be easily obtained by working around the failure.
Cosmetic	The failure is related to the look and feel of the application, typos in a document or user interfaces (amongst others), and not part of the immediate usability or contractual requirements. The failure does not adversely affect the overall system operation.

Table 8 - Classification of defects based on severity

11.6.2. Priority

SOW-0826 According to their priority, defects shall be classified as one of the following in Table 9 - Priority Classes for Defect Classification:

Priority	Description
Urgent	The defect should be resolved as soon as possible. Required to complete independent verification and validation activities.
Medium	The defect should 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 9 - Priority Classes for Defect Classification

11.6.3. Category

SOW-0827 According to their category, defects shall be classified with one of the values defined in Table 10 - Defects Categories:

Category	Description
Defect	An imperfection or deficiency in a work product where it does not meet its requirements or specifications. This category of defect could drive to the creation a Class II (Product Correction) ECP.
Enhancement	This type of defect is used to record an Improvement to the product baseline. This category of defect would typically drive to the creation of a Class I (Product enhancement) ECP.
Document	This category is used to record defects encountered in the system documentation (test cases, test procedures, RTM, test plan, manuals, design, procedures…).
Clarification	This category is used to record deficiencies encountered during the test execution, which must be clarified.
Waiver	This category is used to record when a waiver is required to address a specific observation or defects.

Table 10 - Defects Categories

12. INTEGRATED PRODUCT SUPPORT (IPS)

12.1. Support Planning

SOW-0828 The Contractor shall submit an Integrated Support Plan (ISP). The ISP shall explain in detail how the Contractor shall fulfil all IPS requirements in this Contract. The ISP shall include:

SOW-0828.A A description of The Contractor's IPS organisation, roles, staffing, and responsibilities used to fulfil the requirements of this Contract;

SOW-0828.B Maintenance Support Plan section, detailing all hardware and software warranty and support procedures, including practical details on how to invoke, monitor, and close warranty cases and support service requests;

SOW-0828.C Supply Support Plan section, planning and describing all PHS&T (packaging, handling, storage and transportation) procedures, including supply chain security measures, notification of shipment, packing lists, customs clearance (when required), delivery reporting, reception and handover at final destination, and formal sign-off, and including a detailed schedule of all deliveries planned for this Contract;

SOW-0828.D Technical Documentation Plan section, planning and describing the development and provisioning of all documentation deliverables, such as: manuals, as-built drawings, and COTS-documentation;

SOW-0828.E Training Plan section, planning and describing the development and provisioning of all training material and training courses.

SOW-0828.F Operating Model section, planning and describing the development and delivery of the Operating Model as described in Section 13.3.5.

SOW-0829 All Contractor and Purchaser activities and milestones related to IPS shall be identified and included in the project master schedule.

SOW-0830 The ISP shall cover the period starting from Contract Award until FOA.

12.2. Maintenance Support

12.2.1. Specific software support

SOW-0831 The Contractor shall provide software maintenance support for each and every software instance delivered under this Contract.

SOW-0832 For Cyber Security Monitoring, software maintenance support shall run starting from date of the implementation till Site PSA+1 year of the site where the software was installed.

SOW-0833 For Automation and Orchestration licenses, the duration of support and license validity shall be provided as described in SSS.

SOW-0834 During the agile implementation sprints, if a software code is found to be faulty in a certain site, the Contractor shall fix the software and implement/deploy the corrected software baseline to all the sites implemented previously, with no additional cost to the Purchaser.

SOW-0835 Software maintenance support shall include the following services:

SOW-0835.A Update/upgrade – The Contractor shall provide any feature and maintenance updates and upgrades during the period of performance, together with release notes and installation/ configuration instructions. The availability of updates and upgrades shall be made known to the Purchaser uninvited and at its earliest possible point in time.

SOW-0835.B Bug fixing – The Contractor shall fix any and all bugs identified in the procured software as per his internal procedures, as quickly as possible, and with the highest priority allocated.

SOW-0835.C Licensing – The Contractor shall ensure that all software procured under this Contract have valid software licenses for the duration of the support period. The Contractor shall provide the Purchaser with license documentation and license keys before the start of the support period.

SOW-0835.D On-site interventions – The Purchaser intends to resolve software maintenance problems without Contractor intervention, but the Contractor shall provide on-site intervention in case the software problem is beyond the capability of the Purchaser. If so requested, the Contractor shall arrive on site within 24 hours of the Purchaser's request to intervene.

12.2.2. Warranty and warranty support

SOW-0836 The Contractor shall warrant that all equipment and software furnished under this Contract and all design, implementation and deployment work performed under this Contract conform to the requirements and is free of any defect in material, code or workmanship:

SOW-0836.A for the duration of the project until FOA and for a period of three (3) months for the scope covered under the implementation of Activity Group requirements.

SOW-0836.B for the duration of the project until Site PSA+ 1 year for the scope covered under the implementation of Cyber Security Monitoring.

SOW-0837 If the warranty request is pertaining to the hardware procured, the Contractor shall provide Next Business Day (NBD) support and shall provide the repaired/replacement item latest within 10 business days after the Purchaser has provided the failure notification in writing (e.g. via e-mail).

SOW-0838 If the warranty request is pertaining to the system implementation, integration and documentation, the Contractor shall fix the issue within 5 business days of receipt of the notification from the Purchaser including dispatching an engineer on-site for resolution if required.

SOW-0839 The Contractor shall provide a specific PoC for all warranty and support requests with the relevant procedures. The PoC shall respond to the warranty and support requests within one (1) business day. The Contractor PoC shall also respond to the Technical Assistance requests from the Purchaser during the warranty period, corresponding to information demands limited to the perimeter of delivered products which are not included in the supplied technical documentation.

SOW-0840 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 procurement and design under this Contract. However, in such cases the Contractor shall propose the original alternative item for the Purchaser approval. The alternative item shall conform to all the specified quality requirements within the scope of the contract and standards.

SOW-0841 Defect magnetic, solid state and electronic media storage devices (e.g., CD-ROM's, DVD's, Universal Serial Bus (USB) sticks, solid state storage drives, hard drives) shall remain NATO property, at no additional cost, and not be returned to the Contractor when being replaced. Nonetheless, the Contractor shall deliver replacement items with storage media included at no additional cost to the Purchaser.

SOW-0842 During the warranty period, the Contractor shall be responsible for supplying all COTS software upgrades and updates at no additional cost to the Purchaser.

12.3. Supply Support

SOW-0843 The Contractor shall submit a Supply Support Plan, as a part of the ISP (i.e. a separate section in the ISP). The supply support plan shall describe in detail how the Contractor shall fulfil all supply support requirements in the Contract, as specified in this section.

12.3.1. Inventory

SOW-0844 The Contractor shall provide the Purchaser with a system Inventory in electronic Microsoft Excel format at least ten (10) working days before the first delivery of equipment. The System Inventory is to be site-specific and shall include all items furnished under this Contract, as follows:

SOW-0844.A all installed hardware;

SOW-0844.B all ancillary items essential to the operation of the installed hardware, such as cables, adapters, storage drives, et cetera;

SOW-0844.C all spare parts (i.e. all spares, repair parts and technical consumables; if applicable);

SOW-0845 An inventory template together with a full content description for each data element will be provided to the Contractor after Contract Award at the request of the Contractor.

12.3.2. Codification

SOW-0846 On the basis that an adequate manufacturer's identification numbering system is in place, NATO codification (as described in the General Provisions) is not required. In all other cases, NATO codification is required and the Contractor shall support the NATO codification process in accordance with the Allied Codification Publication 1 (ACoDP-1) and the STANAGs included in ACoDP-1.

12.3.3. Software delivery

SOW-0847 The Contractor shall provide a detailed Software Bill of Material (SBOM) as part of the As-Built Documentation and/or procurement of software licenses, which shall detail comprehensively all Computer Software Configuration Items (CSCI) and associated software, firmware and feature/performance licenses provided under this Contract. The SBOM shall include the following data elements:

SOW-0847.A CSCI identification number;

SOW-0847.B nomenclature;

SOW-0847.C version number;

SOW-0847.D license key (if applicable);

SOW-0847.E type of license;

SOW-0847.F license renewal date (if applicable);

SOW-0847.G warranty/support expiration date;

SOW-0847.H date of distribution;

SOW-0847.I distribution target (server);

SOW-0847.J distribution location (geographically);

SOW-0847.K inventory of all open source components

SOW-0847.L component details version, release date, etc.

SOW-0847.M security vulnerabilities and criticality

SOW-0847.N licenses and risk levels

SOW-0847.O possible licensing conflicts

SOW-0847.P transitive dependencies

SOW-0847.Q software weaknesses

SOW-0847.R safer component version recommendations

SOW-0848 The Contractor shall ensure that all licenses are registered with the Purchaser as end-user.

12.3.4. Packaging

SOW-0849 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-0850 Packing lists shall accompany each shipment, which shall as a minimum include the following:

SOW-0850.A The Purchaser's contract number;

SOW-0850.B The NATO project number;

SOW-0850.C Name and address of the Contractor and the Purchaser;

SOW-0850.D Name and address of the Carrier, Consignor and Consignee (if different from Contractor or Purchaser name and address);

SOW-0850.E final destination address and PoC;

SOW-0850.F method of shipment;

SOW-0850.G For each item shipped: Contract Line Item Number (CLIN) as per the Schedule of Supplies and Services (SSS); nomenclature; part number and serial number; quantity; and

SOW-0850.H For each box, pallet and container: box/pallet/container ID number and number of boxes/pallets/containers; weight; dimensions.

12.3.5. Handling and storage

SOW-0851 The Contractor shall be responsible for all handling and storage of equipment, packages, boxes and containers during the project. The Contractor shall also be responsible for organising and operating any handling equipment and storage facilities required.

SOW-0852 In the case of hazardous/ dangerous goods and goods requiring export licenses, the Contractor shall ensure that all required forms and certificates are provided and that all applicable regulations for such goods are followed.

12.3.6. Transportation

SOW-0853 The Contractor shall be responsible for transportation of all equipment furnished under this Contract from its site in a NATO nation to final destination. The Contractor shall be responsible for any insurance covering these shipments.

SOW-0854 The Contractor shall also be responsible for transportation of repaired/ replacement items under warranty to the original location. Return of unserviceable equipment to Contractor facility for (warranty) repair/replacement is the responsibility of the Contractor.

SOW-0855 The Contractor shall provide the Purchaser's IPS PoC with a Notice of Shipment at least two (2) weeks in advance of each shipment. One additional copy of the packing list shall be attached to this notice.

12.3.7. Supply chain security

SOW-0856 The Contractor shall warrant that all supplies furnished under this Contract are genuine and free of malicious components, firmware and software.

SOW-0857 The Contractor shall confirm in each notification of shipment that all products to be delivered have been checked for technical integrity and protected from malicious tampering.

SOW-0858 The Contractor shall ship supplies furnished under this Contract directly to final destination as indicated by the Purchaser, without stopping at intermediate locations not approved by the Purchaser.

SOW-0859 Where possible and reasonably practical, shipments shall use transportation modes and vehicles dedicated to the shipment of goods to be supplied under this Contract.

SOW-0860 Transportation vehicles and supplies shall be protected against unauthorized access, and protected from malicious tampering during handling, storage, and transportation.

SOW-0861 All supplies under this Contract shall be stored and shipped in neutral packaging, not readily identifiable as NATO supplies.

SOW-0862 The Contractor shall ensure that all supplies furnished under this Contract are marked or labelled to identify the supplier.

SOW-0863 The Contractor shall allow and support ad-hoc spot checks and audits by the Purchaser of any part of their supply chain security measures at any of the Contractor's locations and facilities used in the Contractor's supply chain relevant to this Contract.

SOW-0864 The Purchaser reserves the right to reject any supplies delivered which do not conform to the supply chain security requirements in this Contract, or which show evidence of tampering. The Contractor shall immediately replace such rejected supplies at no cost to the Purchaser.

12.3.8. Customs

SOW-0865 The Contractor shall be responsible for customs clearance of all shipments into the destination countries. It is the Contractors responsibility to take into account delays at customs. The Contractor 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 Custom Forms 302.

SOW-0866 Prior to a shipment by the Contractor, the Purchaser will upon request issue a custom form 302, which facilitates the duty free import/export of goods. The Contractor shall be responsible for requesting the issue of a form 302 ten (10) working days prior to shipment. The request for a form 302 shall be accompanied by one (1) additional packing list. The request is normally processed by the Purchaser within three (3) working days. The requested 302 forms will be sent by courier. Original 302 forms shall accompany the shipment and therefore no fax or electronic copy shall be used, nor provided to the Contractor.

SOW-0867 If a country refuses to accept the Form 302 and requires the payment of customs duties, the Contractor shall pay these customs duties. Should such an event occur, the Contractor shall immediately inform the Purchaser by the fastest means available and before paying, obtain from the Customs Officer a written statement establishing that his Country refuses to accept the Form 302.

12.4. Technical Manuals

12.4.1. General requirements

SOW-0868 The Contractor shall submit a Technical Documentation Plan, as a part of the ISP (i.e. a separate section in the ISP). The documentation plan shall describe in detail how the Contractor shall fulfil all technical documentation requirements, as specified in this section of the Contract.

12.4.2. COTS technical manuals

SOW-0869 The Contractor shall provide printed versions of all COTS technical documentation, such as operation, maintenance, user, and administration manuals, for each hardware and software item furnished under this Contract. The Contractor shall also make available, in the same way, any documentation required to operate and maintain the furnished hardware and software, such as release notes and software configuration files.

12.4.3. Bespoke technical manuals

SOW-0870 The Contractor shall provide one Operation (i.e. User) Manual for each hardware and software item furnished under this contract.

SOW-0871 An Operation Manual shall:

SOW-0871.A describe the item by its main purpose, main components, and main operating functions;

SOW-0871.B describe, in detail, the step-by-step operating instructions and procedures required to execute all of the functions of the hardware or software item;

SOW-0872 The Operation Manual shall contain drawings and illustrations where appropriate to aid in the readability and understandability of the operating instruction.

SOW-0873 The Contractor shall provide one Maintenance Manual for each hardware and software item furnished under this contract.

SOW-0874 A Maintenance Manual shall:

SOW-0874.A include a full and detailed illustrated parts breakdown list with accompanying diagrams, clearly showing all parts of interest to the maintenance of the item (i.e. all maintenance significant items; not applicable to software);

SOW-0874.B describe, in detail, the step-by-step maintenance instructions and troubleshooting procedures required to resolve all and any faults and failures resulting from all and any known failure modes of the hardware or software item;

SOW-0875 The Maintenance Manual shall contain drawings and illustrations where appropriate to aid in the readability and understandability of the maintenance procedure.

SOW-0876 The Maintenance Manual shall cover all phases of a maintenance procedure, including (when applicable): fault identification, fault isolation, shut-down and start-up, connect and disconnect, assemble and disassemble, backup and restore, diagnostics and built-in testing, routine maintenance, and disaster recovery.

SOW-0877 The Contractor shall provide one Technical Integration Manual covering all integration and configuration work furnished under this Contract.

SOW-0878 The Technical Integration Manual shall:

SOW-0878.A Describe in detail all hardware and software configuration settings of all hardware and software in scope of this Contract, both Contractor furnished, and PFE.

SOW-0878.B Describe, in detail, all procedures required to rebuild and reconfigure all integration and configuration work furnished by the Contractor as part of this Contract. These procedures shall enable the Purchaser to completely rebuild from scratch any integration and configuration work performed under the Contract.

SOW-0878.C Describe, in detail, the step-by-step maintenance instructions and troubleshooting procedures required to resolve all and any faults and failures related to the integration and configuration work furnished under this Contract;

SOW-0878.D Describe, in detail, the installation instructions for all HW, SW and configurations delivered as part of this Contract;

12.5. Training

12.5.1. General training requirements

SOW-0879 The Contractor shall develop, organise and conduct a training programme covering the training of operation and maintenance procedures for all hardware and software furnished under this Contract, and for all integration and configuration work conducted under this Contract.

SOW-0880 The Contractor shall ensure that sufficient training is provided to enable the Purchaser's O&M personnel to operate and maintain all Contractor-procured hardware and software, and all integration and configuration work in scope of this Contract.

SOW-0881 The Contractor shall assume that the Purchaser's O&M personnel is qualified, trained and skilled to operate and maintain any Purchaser furnished hardware and software used in this Contract.

SOW-0882 The Contractor shall provide the following trainings:

SOW-0882.A Standard operation and maintenance training for the orchestration and automation software purchased under this Contract.

SOW-0882.B Standard operation and maintenance training for the cyber security monitoring hardware and software purchased under this Contract.

SOW-0882.C Bespoke training to ensure full knowledge transfer, from the Contractor to the Purchaser's O&M personnel, of all integration and configuration work performed under this Contract.

SOW-0883 Training shall be conducted in the form of instructor-led classroom training courses at Purchaser designated NATO facilities in NATO locations that are in scope of this Contract. The Purchaser intends to designate NATO HQ/NCI Agency, Brussels, Belgium; SHAPE/NCIA Agency, Mons/Braine L'Alleud, Belgium; JFC Naples, Lago di Patria, Italy; or NCI Agency, The Hague, The Netherlands.

[0263] Training rooms will be provided and organised by the Purchaser at the Purchaser selected training sites. The Purchaser may also provide accessories, such as a projector and white boards, and the Contractor may use these when provided.

SOW-0884 However, the Contractor shall provide, install, and organise any training hardware, software, and accessories needed to conduct the training courses. This shall include any hardware and software required to build training systems in support of training, such as laptops, switches, and software licenses. This shall also include any accessories needed, such as white boards, projectors, and writing materials.

SOW-0885 The Contractor shall be responsible for all preparations required to conduct the training courses and all dismantling required after the training courses.

SOW-0886 As an option to the Contract, the Contractor shall provide and organise its own training facilities and training rooms, in the vicinity of the Purchaser designated training locations, fully equipped, if so required, with training system and training accessories, as described in this section. The Purchaser intends to activate this Contract option if and when the Purchaser is not able to provide and organise Purchaser training rooms on location.

[0264] The Purchaser will select the students and assign them to each training course procured under this Contract. The Purchaser will also ensure and organise student attendance at their assigned training courses at the agreed time and place.

SOW-0887 The Contractor shall allow up to 30 students per training course.

SOW-0888 The Contractor shall design and determine the duration of each training course. Training course durations shall be sufficient to ensure that the overall training objective is fulfilled, namely to ensure that the Purchaser's O&M personnel is fully capable of operating and maintaining all Contractor-furnished hardware and software, and all integration and configuration work in scope of this Contract.

SOW-0889 The Contractor's training course instructors shall be fully qualified, skilled, trained, and experienced SMEs on every topic taught in the course for which they are instructor, as well as fully familiar with the design and implementation of the systems and work in scope of this Contract.

SOW-0890 The Contractor's training course instructors shall teach in the English language and meet a minimum English language proficiency equivalent to 4444, in accordance with NATO STANAG 6001 [Ref: STANAG 6001].

12.5.2. Training planning

SOW-0891 The Contractor shall submit a Training Plan [Ref: AI 16.31.04], as a part of the ISP (i.e. a separate section in the ISP). The training plan shall describe in detail how the Contractor shall fulfil all training requirements in the Contract. The training plan shall include:

SOW-0891.A Detailed description of the Contractor's training concept and strategy;

SOW-0891.B Detailed description of the Contractor's training organisation and stakeholders and their responsibilities;

SOW-0891.C Detailed description of all stages, activities, deliverables, and milestones required to execute the training programme, explaining how the Contractor shall develop all training course materials; plan, organise and execute training courses; and evaluate the training outcome;

SOW-0891.D List and describe in detail all training courses to be provided under this Contract, including a per-course description of the Learning Objectives;

SOW-0891.E Detailed training schedule, in sync with the project's master schedule, for all training related activities, for both Contractor and Purchaser activities.

SOW-0891.F All Contractor and Purchaser activities and milestones related to training shall be identified and included in the project's master schedule.

12.5.3. Training courses

SOW-0892 The Contractor shall supply the following training courses:

SOW-0892.A A standard O&M Training Course covering the automation & orchestration software furnished under this Contract;

SOW-0892.B A standard O&M Training Course covering the cyber hardware & software furnished under this Contract;

SOW-0892.C A bespoke Initial IaaS Integration Course;

SOW-0892.D A bespoke Initial ECS Integration Course;

SOW-0892.E A bespoke Initial CPS Integration Course;

SOW-0892.F A bespoke Initial Cyber Integration Course;

SOW-0892.G A bespoke Advanced IaaS Integration Course;

SOW-0892.H A bespoke Advanced ECS Integration Course;

SOW-0892.I A bespoke Advanced CPS Integration Course;

SOW-0892.J A bespoke Advanced Cyber Integration Course;

SOW-0893 The standard O&M training courses shall ensure that the Purchaser's personnel is fully capable to operate and maintain the hardware and software furnished under this Contract. Such training courses shall train:

SOW-0893.A every operating function provided by the pertinent hardware and software, including the step-by-step operating instructions to execute and use such functions;

SOW-0893.B every maintenance significant function for the pertinent hardware and software, including the step-by-step maintenance instructions to execute such functions;

SOW-0893.B.1 For hardware: any procedure or instruction required to: shut down and start the item; connect and disconnect; remove and replace; assemble and disassemble; test and diagnose; identify and isolate faults and failures; trouble shoot known failure modes; et cetera.

SOW-0893.B.2 For software: any procedure or instruction required to: shut down, reset, start up the item; patch and install/ re-install; update and upgrade; automate; backup and restore; test and diagnose; identify and isolate faults and failures; trouble shoot known failure modes; et cetera.

SOW-0894 An Integration Course shall ensure that the Purchaser's personnel is fully capable of rebuilding from scratch, and re-configure, any integration and configuration work furnished by the Contractor as part of the Contract and covered under the Task Orders. Such a training course shall train:

SOW-0894.A The overall architecture and detailed design of the integration and configuration work.

SOW-0894.B The step-by-step procedures and instructions required to rebuild and reconfigure all integration and configuration work furnished by the Contractor as part of this Contract, including the specific information tailored for each site implemented within the scope of the Contract.

SOW-0894.C The step-by-step maintenance instructions and troubleshooting procedures required to resolve faults and failures related to the integration and configuration work furnished under this Contract, including the specific information tailored for each site implemented within the scope of the Contract.

SOW-0895 Initial Integration Courses shall focus on the implementations in scope of Activity Group 1 and Activity Group 2. Advanced Integration courses shall focus on the implementations in scope of Activity Group 3 and Activity Group 4. Advanced Integration courses shall build upon the Initial Integration Courses.

SOW-0896 Initial and Advanced training courses shall be furnished in four variations each, as listed above. The IaaS courses shall focus on training of all integration and configuration work related to IaaS. The ECS courses shall focus on training of all integration and configuration work related to ECS. The CPS courses shall focus on training of all integration and configuration work related to CPS. The Cyber courses shall focus on training of all integration and configuration work related to Cyber. All Initial and Advanced training courses shall also address the SM&C aspect.

SOW-0897 The Contractor shall execute the training courses before the start of the Purchaser's in-service, O&M phase, in time for the Purchaser to start the operation and maintenance of systems delivered under this Contract and as specified in the relevant Task Order. Additionally:

SOW-0897.A All Initial Integration courses shall be completed before the IOA ON IaaS Ready milestone and before the first Site-PSA.

SOW-0897.B All Advanced Integration courses shall be started after the Initial Integration Courses and shall be completed before the agency operation and maintenance phase of the DC E2E Services starts.

SOW-0897.C Standard O&M hardware and software courses shall be completed before the IOA ON IaaS Ready milestone.

12.5.4. Training material

SOW-0898 The Contractor shall provide all training materials required for all training courses. Training materials shall be developed to the extent and quality necessary to ensure that all Learning Objectives are achieved.

SOW-0899 The training material shall be in complete alignment with the solution (or system) requirements implemented and Technical Documentation and Data created in accordance with Section 13.

SOW-0900 All training material and training equipment shall be delivered to the various training sites and rooms by the Contractor.

SOW-0901 The Contractor shall make optimal (re-)use of supplies already provided under this Contract, such as manuals and as-built drawings, to support the training courses and to develop the training material.

SOW-0902 The training material shall be organised and structured into a training material package, specific to each type of training course.

SOW-0903 The Contractor shall provide each student, at each training course attended, with a hard copy and a soft copy of the training material package. This package will be used and retained by the student.

SOW-0904 Each training material package shall include:

SOW-0904.A a learning guide, listing the course content, section-by-section, as well as listing the Learning Objectives relevant to the course;

SOW-0904.B a student handbook, containing the course learning material;

SOW-0904.C a quick reference card (if applicable);

SOW-0904.D upon completion, a course certificate with a course evaluation feedback form.

SOW-0905 All training material is subject to approval by the Purchaser before the start of a training course.

12.5.5. Training evaluation

SOW-0906 The Contractor shall instruct each student at the end of each course to complete and return the course evaluation feedback form provided as part of the training material package.

SOW-0907 The Contractor shall consolidate and forward student feedback to the Purchaser following each session in the form of a training course evaluation report. The report shall also recommend changes and improvements to the training material and training courses based on the consolidated student feedback. The report shall also address student attendance, problems encountered and actions taken to resolve the problems.

SOW-0908 The Contractor shall revise/ refine all training materials and training courses to reflect the consolidated student feedback and proposed improvements in the course evaluation report.

13. DOCUMENTATION MANAGEMENT

13.1. General Requirements

SOW-0909 The Contractor shall use the ITM-RC1 project portal provided by the Purchaser to create and maintain all up-to 'NATO Restricted' documentation and data using a Purchaser provided REACH laptop (See Annex B of the Contract Special Provisions). This shall include all project deliverables, and all the files, documentation and data created within the scope and for this project, with the exception of NS data and NU data which shall be maintained in the Purchaser provided NS and NU devices.

SOW-0910 The Contractor shall maintain on this portal all unclassified and restricted documents, as soon as they are submitted in draft version to the Purchaser. For any official submission, the Contractor shall inform the Purchaser PoCs via a dedicated e-mail, to initiate the review and approval process.

SOW-0911 The Contractor shall identify all relevant classified documents on the Project portal, by title, unless a title itself is classified higher than NR and shall state from where the classified document can be obtained. The security classification of the documentation shall follow NATO security directives, guidelines and instructions, as defined in the AD 0070-001

SOW-0912 The Contractor shall use Project Document Security guideline [Ref: PDOC-SEC-CLAS-GDL] for security labelling on Work Packages artefacts.

SOW-0913 The Contractor shall be compliant with the Purchaser "Documentation Management SoP' [Ref: ITM-RC1 SOP DM] in creation and maintenance of all the documentation and data.

SOW-0914 The Contractor shall submit all documentation deliverables with all the appropriate signatures assuring the quality criteria are met.

SOW-0915 The Contractor shall provide all the documentation in British English language.

SOW-0916 Documentation shall not contain warnings or copyrights statements limiting the rights to use or reproduce.

SOW-0917 Documents shall be complete, concise and sufficiently detailed for its purpose.

SOW-0918 All the documentation shall be kept updated by the Contractor and under configuration control for the entire life cycle of the Contract. Each document shall have a dedicated section listing the changes in each release, with sufficient details to ease the review of the Purchaser and future referencing.

SOW-0919 Each document shall contain a maintained version number. The version number format shall be "X.Y", where "X" is the version number and "Y" is the revision number

SOW-0920 The document file name shall not contain any variable parts like version numbers, maturity indicators, etc.

SOW-0921 The convention to be used for numbers appearing in textual documents is for a comma to be the thousands separator and a period to be the decimal separator (e.g. 1,365,276.24).

SOW-0922 The convention to be used for dates appearing in free text (e.g. quoting dates of meetings) is "day-month-year" exclusively (e.g. 06-04-2022 or 6 April 2022).

SOW-0923 All the activities, milestones and actors associated with the development of documentation shall be described in the Documentation Plan (DP).

SOW-0924 The Contractor shall submit all documentation in editable electronic format to the Purchaser for review and comments as applicable.

SOW-0925 The following guidelines shall be used:

SOW-0925.A MS Word for generating text documents;

SOW-0925.B MS Excel for tabular or matrix data;

SOW-0925.C MS Visio or MS PowerPoint for drawings;

SOW-0925.D MS Project for schedule; and

SOW-0925.E MS PowerPoint for briefings

SOW-0925.F Both original files and exports from software and other tools for design artefacts.

SOW-0926 The Contractor shall submit the final and accepted versions of documentation deliverables in Portable Document Format (PDF), with an Object Character Recognition (OCR) capability format.

SOW-0927 For all design documents provided by the Contractor, the following criteria shall apply:

SOW-0927.A All information that is essential for the document is contained into the document itself. References to external documents, are only for potential additional information, or NATO policy documents. The intention of this criteria is that the document can be read as a 'stand-alone' document.

SOW-0927.B It aligns with the PPDD / [Ref: ITM-RC1 ADP]

SOW-0927.C It meets the requirements, set forward by the contract documents, like the SoW and the SRS.

SOW-0927.D It aligns with NATO policies in Annex D

13.1.1. Documentation Reviews

SOW-0928 The Purchaser shall require a draft copy of documents minimum 4 weeks prior to the final approval, unless otherwise specified in the SoW or the Task Order.

SOW-0929 For sprint documentation during the agile implementation, the documentation shall be submitted within 3 business days following the final day in the sprint cycle. If necessary, another update shall be submitted within 2 business days following the final day of the Sprint cycle.

SOW-0930 The Contractor shall update the documents in accordance with the Purchaser comments and resubmit for Purchaser approval. The acceptance of the documentation shall be a prerequisite for the Task Order acceptance.

SOW-0931 The Contractor shall not provide any Contractual documentation in a partial or gradual manner.

SOW-0932 The Contractor shall ensure that any documentation delivered to the Purchaser has been properly reviewed according to Contractor quality management process, utilizing the Project Portal and other shared resources, and minimizing use of personal storage and email, to the extent possible.

[0265] Except otherwise stated for specific documents, the following provisions will apply for any documentation to be provided by the Contractor under this Contract.

SOW-0933 The Contractor shall provide a first version of each deliverable for Purchaser review. The first version shall be substantially complete and correct.

[0266] The Purchaser will provide questions, comments, corrections, and suggested changes to the Contractor within 4 (four) weeks of receipt, excluding security accreditation documentation for which 3 months will be required. 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-0934 The Contractor shall not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.

SOW-0935 The Contractor shall resubmit the document as a revised version addressing the Purchaser's comments within two (2) weeks after receipt.

[0267] The Purchaser will then provide further comments, corrections, and suggested changes to the Contractor within three (3) weeks of receipt, excluding security accreditation documentation for which 3 months will be required.

SOW-0936 The Contractor shall provide an updated version of the document within two weeks of receipt of the Purchaser's comments on the revised version.

[0268] The above cycle will continue until the document reach a quality level acceptable by the Purchaser, excluding security accreditation documentation for which NSAB approval will be required.

SOW-0937 If the document is included as part of the 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-0938 The terms “Accepted (A)”, “Accepted with Comments (AwC)” and “Rejected (Rej)” shall be considered, following Agency Instructions on use of the Comments Collector [Ref: AI 06.04.08] for tracking document review and open comments:

SOW-0938.A **A**: Either there are no comments by the Purchaser or all Purchaser comments have been addressed/incorporated;

SOW-0938.B **AwC**: All severity ‘1’: Critical, ‘2’: High, or ‘3’: Medium Purchaser comments have been addressed/incorporated and remaining comments have to be addressed by an agreed future date and an updated document released, if comments are not resolved in accordance with the terms of the SoW then approval will be revoked;

SOW-0938.C **Rej**: Severity ‘1’: Critical, ‘2’: High, or ‘3’: Medium Purchaser comments have not been addressed/incorporated. Outstanding comments have to be addressed by an agreed future date and an updated document released for a repeat review.

SOW-0939 The terms "Initial", “Preliminary”, "Updated" and "Final" are recurrently used in the SoW, and shall be interpreted as follows:

SOW-0939.A The terms “Initial” and “Preliminary” are understood as a document version that is structurally complete (meeting all requirements/guidance as provided), populated with information at hand. The table of contents is complete and the main sections are developed to a 60% completion state. Some subsections containing non-essential information may be partially or not developed. The document contains placeholders for missing information which will be further filled in following the existing structure at a later time, when more information is available. The document has however to be at a level such that a first review by the Purchaser can be conducted. As a result of that review, the structure and the content of the document may have to undergo substantial changes, resulting in a new Initial version, in the interim (i.e. before the next deadline calling for a Final Draft is reached) or leading to the first Final Draft.

SOW-0939.B The term “Updated” is understood as a document version that is complete, concise and structurally correct (meeting all requirements/guidance as provided), without any placeholders, self-contained and ready for use by the Purchaser. A document will be considered an “updated” version of the document if, after Purchaser review, the Purchaser assigns the document with “Accepted with Comments (AwC)” status.

SOW-0939.C The term “Final” is understood as a document version that has been extensively reviewed by the Purchaser through one or more intermediate releases by the Contractor (Initial version and Updated version), it is complete and formally Accepted (A). Further changes to the document have only to take

place by agreement and in exceptional circumstances, upon request by the Purchaser.

SOW-0940 The review process of MS Word documents shall be guided by use of the Purchaser's Comments Collector tool as per [Ref. AI 06.04.08].

SOW-0941 The Contractor shall submit all documentation for Purchaser review as described below. At each review cycle, the Purchaser will state if the document is likely to be accepted in its Final version.

SOW-0942 The Purchaser reserves the right to approve, approve with comments, decline with comments or reject documentation submittals.

SOW-0943 During the development, the Contractor shall provide subsequent draft versions of the documents, if applicable, for the Purchaser comments, until final document version is approved by the Purchaser.

SOW-0944 Subsequent draft versions of documents required to address Purchaser comments shall be provided by the Contractor at no additional cost for the Purchaser.

SOW-0945 The Contractor shall provide the last draft version of each deliverable for Purchaser review.

SOW-0946 The Purchaser reserves the right to return without review a document that has significant deficiencies.

SOW-0947 The Contractor shall submit documentation, intended for review by the Purchaser, with each modification identified through the change tracking feature or otherwise marked.

SOW-0948 The last version of each deliverable for Purchaser review shall be substantially complete and correct, and the delivery dates specified.

SOW-0949 The Contractor shall not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.

SOW-0950 Until end of Warranty the Contractor shall remain responsible for updating all the deliverable documents to reflect necessary changes.

13.2. Project Management Documentation

13.2.1.1. Work Package Management Plan (WMP)

SOW-0951 The WMP shall describe how the Contractor will implement the totality of the project, including details of the project control that will be applied.

SOW-0952 The WMP shall describe how the Contractor shall implement project/contract administration, including details of the controls that shall be applied to supervise Sub-Contractor performance.

SOW-0953 The Contractor's WMP shall be provided to the Purchaser for acceptance.

SOW-0954 After approval by the Purchaser, the final version of the WMP shall be the official document against which the Contractor is expected to conduct the performance of the Contract. The approved WMP shall however not supersede the Contract, and the Schedule of Supplies and Services (SSS) in particular.

SOW-0955 The Contractor shall ensure that the WMP remains current throughout the duration of the Project to reflect the actual state of the Contractor's organization and efforts, and maintain a current copy on the Project Portal.

SOW-0956 The Contractor shall present any changes to the WMP during the Project Review Meetings for Purchaser approval. Any change with an impact on the contractual requirements shall be made via an amendment to the Contract in accordance with the CSP and General Provisions (GP).

SOW-0957 The WMP shall provide sufficient detail to allow the Purchaser to assess the Contractor's plans and capabilities in implementing the entire project in conformance with the requirements specified.

SOW-0958 The WMP shall describe the Contractor's organization, assignment of functions, duties, and responsibilities, management procedures and policies, and reporting requirements for the conduct of contractually-imposed tasks, projects, or programmes.

SOW-0959 The WMP shall identify all major Contractor operating units and any Subcontractors involved in the development of System and a description of the portion of the overall effort or deliverable item for which they are responsible.

SOW-0960 The WMP shall cover all aspects of the project implementation, including the Contractor's project management structure and project control processes, personnel assignments, and external relationships necessary to provide the System as required by this Contract.

SOW-0961 The WMP shall cover at least the following areas and details:

SOW-0961.A Project organization:

SOW-0961.A.1 Internal structure, including a project organizational diagram;

SOW-0961.A.2 Roles and responsibilities of each organizational unit;

SOW-0961.A.3 Key personnel, their qualifications, and their responsibilities;

SOW-0961.A.4 Organizational boundaries between the project organization and the parent and subcontracted organizations.

SOW-0961.A.5 Team composition and assignment of roles and responsibilities for design, implementation of agile Sprints and implementation of Cyber Security Monitoring (in accordance with the roles identified in the Contract)

SOW-0961.B Project management processes:

SOW-0961.B.1 A description of the Contractor's project management methodology and approach to be used for this project;

SOW-0961.B.2 A description of the Contractor's implementation of agile delivery approach, indicating for which product and how this shall be introduced to achieve synergies between the Purchaser and Contractor;

SOW-0961.B.3 Project start-up, including staffing, basis of cost and schedule estimates, and project infrastructure;

SOW-0961.B.4 Work Package control measures, including monitoring, reporting of work packages;

SOW-0961.B.5 Communications management, including the Collaborative Environment and its establishment, maintenance and use; Project Progress Reports; Project Checkpoint Reviews; and all other communications with the Purchaser and Sub-Contractors;

SOW-0961.B.6 Sub-Contractor Management including the details of the scope of work that will be outscored with the rationale and the process to manage the performance of the Sub-Contractors;

SOW-0961.B.7 Lessons Learned management, including the identification, reporting, and logging of lessons learned in a Lessons Learned Log;

SOW-0961.B.8 Implementation of Agile methodology;

SOW-0961.B.9 Risk and Issue Management;

SOW-0961.B.10 Quality Management;

SOW-0961.B.11 Staffing Plan;

SOW-0961.B.12 Agile Implementation Plan including Testing and Acceptance.

SOW-0962 The WMP shall describe the Contractor's methodology and planning that will be put in place for satisfying the Purchaser requirements for 'Support to Purchaser Activities' throughout the execution of the Contract. This shall include the considerations for staff planning, readiness to deploy the staff on-site, source data, documentation and mentoring that will be required throughout the duration of the support.

SOW-0963 The WMP shall include the following annexes as standalone deliverables in accordance with the requirements of the following sections:

SOW-0963.A Product Breakdown Structure (PBS)

SOW-0963.B Work Package Master Schedule (WMS)

13.2.1.2. Work Package Implementation Plan (WIP)

[0269] This is the key document in the planning and execution of implementation activities is the Contractor's WIP.

SOW-0964 The Contractor shall provide a WIP, which will describe how the Contractor will implement the Project in accordance with the requirements of this section.

SOW-0965 The approval of the WIP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This approval does not relieve the Contractor from its responsibilities to meet the requirements stated in this SoW.

SOW-0966 The WIP shall be kept up to date throughout the project, and shall be subject of review at each Project Review Meeting (PRM), until and including FOA. The WIP shall also include the security accreditation process and relevant activities.

SOW-0967 The site survey(s) and installation sequence and dates reflected in the WIP shall be co-ordinated by the Contractor with the Purchaser and the Site PoC to accommodate site-specific requirements, exercises, holiday periods, and other considerations.

SOW-0968 The Contractor shall include in the WIP 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. The High Level Release Plan and WIP shall be maintained and coordinated with each other.

SOW-0969 The WIP shall contain the following information:

SOW-0969.A Executive Summary which describes managerial level description of how the plan the Work Package will be implemented;

SOW-0969.B The Contractor's approach to all system implementation tasks (including the sequence of activation of the sites to be implemented);

SOW-0969.C The Contractor organisation and key personnel involved in sites system integration;

SOW-0969.D The overall schedule for implementation activities including site survey, site preparation, site installation and activation. This schedule shall show all planned outages of any kind in the sites;

SOW-0969.E Assumptions and Constraints concerning the development and execution of the implementation plan addressing items like:

SOW-0969.E.1 Schedule;

SOW-0969.E.2 Hardware;

SOW-0969.E.3 Software and other technology to be reused or purchased;

SOW-0969.E.4 Interfaces constraints.

SOW-0969.F Implementation Plan which describes the framework for the approach taken to create the project schedule.to deliver WP07;

SOW-0969.G Automation and Orchestration. DevOps CI/CD Pipelines;

SOW-0969.H Security management:

SOW-0969.H.1 Security management, including personnel and facility security;

SOW-0969.H.2 System security accreditation process;

SOW-0969.I Purchaser involvement:

SOW-0969.I.1 Purchaser involvement via Joint Reviews, informal meetings, reporting, modification and change, implementation, verification, approval, acceptance and access to facilities;

SOW-0969.I.2 Expected PFE and associated timelines;

SOW-0969.I.3 Delivery procedures for the documentation and the products. This includes control of Purchaser Property, export control process.

SOW-0969.J Subcontracting plan demonstrating that the Contractor can effectively manage, monitor and control the sub-Contractors and that the sub-Contractors will agree to abide by the requirements of the prime Contract as pertains to flow-down provisions.

SOW-0969.K Risk and Contingency Planning which details 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;

SOW-0969.L A list of all hardware needed for installing and testing the WP07 services. Identify the hardware by make, model and configuration; and any information on warranty/maintenance contract(s);

SOW-0969.M A list of all software (software, operating systems, utilities, etc. and identify the software as COTS, custom developed or legacy) required for implementation, licensing, usage, and maintenance contract and associated costs;

SOW-0969.N 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;

SOW-0969.O any post-activation tasks and the "back-out" procedures;

SOW-0969.P Gant Chart of schedule of activities

SOW-0970 The Contractor shall submit the detailed implementation sequence of Technical Services and User services. The sequence shall carefully consider and adapt to the ITM implementation sequence in order to minimize the impacts on both projects.

SOW-0971 The Contractor shall structure the WIP so that general implementation information is maintained in the body of the plan and site-specific details are kept as annexes.

13.2.1.3. Work Package Master Schedule (WMS)

SOW-0972 The Contractor shall establish and maintain a WMS, as an annex to the WMP, which shall be based on realistic time estimates, subject to Purchaser acceptance:

SOW-0972.A Contain all Contract events and milestones

SOW-0972.B Correlate with the products defined in the PBS and sequentially ordered

SOW-0972.C Incorporate the WBS

SOW-0972.D Be provided in Microsoft Project format

SOW-0972.E Identify the critical path for the overall project

SOW-0972.F Identify the start and finish dates, duration, predecessors, constraints (as necessary) and the total slack of each task

SOW-0972.G Identify key resources needed for each task completion

SOW-0972.H Identify the main project milestones (see section 0) and intermediate milestones as required

SOW-0972.I Identify the "physical" progress for each task

SOW-0972.J Identify the applicable baseline, and shall show progress against the baseline

SOW-0972.K Minimise the use of constraints and absolute dates

SOW-0972.L Provide network, milestone, Gantt and Tracking Gantt views

SOW-0972.M Identify the main deliverables.

SOW-0973 The Contractor shall provide the WMS to the Purchaser for acceptance.

SOW-0974 The Contractor shall use the PBS, the WBS, the PFD and the WMS as the primary framework for Contract planning and reporting to the Purchaser.

13.2.1.4. Product Breakdown Structure

SOW-0975 The Contractor shall establish and maintain a Product Breakdown Structure (PBS), as an annex to the WMP, as the primary framework for Contract planning and reporting to the Purchaser.

SOW-0976 The Contractor shall establish and maintain a PBS, which shall:

SOW-0976.A Identify all products and shall distinguish between management products and specialist products.

SOW-0976.B 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 WP07 System.

SOW-0976.C 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-0977 The Contractor shall establish and maintain a Product Flow Diagram (PFD), which shall sequence all products in their logical order of creation.

SOW-0978 The Contractor shall use the latest commercial version of the MS Project to create the PBS and shall use that version of MS Project throughout the life of the ITM project.

SOW-0979 The PBS shall define the ITM tasks needed to guarantee the successful management, delivery and acceptance of the in scope services: design, testing, delivery, installation, service and site activation, system acceptance, and support as well as management products (e.g. project plans, Project Status Reports, Purchaser reviews, provision of specific Purchaser-furnished items), including at least the initial version and the final one.

SOW-0980 The PBS shall be traceable to performance and delivery requirements of the Schedule of Supplies and Services.

SOW-0981 The Contractor shall not change the PBS without the approval of the Purchaser.

SOW-0982 The PBS shall be provided to the Purchaser for acceptance and any changes to the PBS are required to be approved by the Purchaser's PM for acceptance.

SOW-0983 The acceptance of the PBS and 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.

13.2.1.5. Product Backlog

SOW-0984 The Product Backlog shall identify Essential, High Priority and Low Priority features as provided by the Purchaser.

SOW-0985 The Product Backlog shall represent the scope of work to a level that exposes all project risk factors and allows for estimation, resource requirements and prioritization.

SOW-0986 The Product Backlog shall be traceable to performance and delivery requirements of the Schedule of Supplies and Services.

SOW-0987 The Contractor shall not change the Product Backlog without the approval of the Purchaser.

SOW-0988 The Product Backlog shall be provided to the Purchaser for acceptance and any changes to the Product Backlog are required to be approved by the Purchaser's PM for acceptance.

13.2.1.6. High Level Release Plan

SOW-0989 The Contractor shall provide a High Level Release Plan describing the proposed allocation of the Activity Group requirements to the Sprints, based on the estimated number of sprints described in Section 0.

SOW-0990 The Contractor shall ensure that the proposed planning allocates the entirety of the Activity Group requirements to the maximum number of sprints described in Section 0.

SOW-0991 The Contractor shall distinguish the implementation of the requirements for the first site and the follow-on sites, with the assumption that more requirements can be implemented in one Sprint for follow-on sites.

SOW-0992 The High Level Release Plan shall include the 'Burndown Chart' showing the amount of requirements implemented in each Sprint completed. Burndown Chart shall be provided for the set of requirements allocated for each Activity Group.

SOW-0993 The High Level Release Plan shall include the 'Burnup Chart' showing the amount of requirements that will be implemented in the upcoming Sprints. Burndown Chart shall be provided for the set of requirements allocated for each Activity Group.

SOW-0994 The High Level Release Plan shall include the proposed logical grouping of the solution requirements (based on the dependencies with each other) for design, implementation, testing and deployment purposes. This shall also include requirements with dependencies and their allocation to each Sprint.

SOW-0995 The Contractor shall provide the assessment for ratings for level of complexity (i.e. in a scale of 1-4) for each requirement.

13.2.1.7. Risk and Issue Management Plan (RIMP)

SOW-0996 The Contractor shall establish and maintain a RIMP which shall describe how the Contractor will implement the Risk Management process, with at least the following details:

- SOW-0996.A Overall Risk Management approach
- SOW-0996.B Key Risk Management processes
- SOW-0996.C Key Risk Categories
- SOW-0996.D Risk Prioritization Matrix
- SOW-0996.E Risk Management roles and responsibilities
- SOW-0996.F Risk Log template which shall at minimum follow the outline recommended in this SoW (see Section 13.2.1.8).

SOW-0997 The Contractor's RMP shall establish and maintain a Risk Log for the project, which is available on the ITM project website.

SOW-0998 The Contractor shall ensure that risks are identified early, assessed accurately, and quickly mitigated with the Purchaser.

SOW-0999 The Contractor shall identify any management, technical, schedule, and cost risks, evaluate each risk, and select a proposed response for each risk mentioned in the Risk Log.

SOW-1000 Each risk shall be rated based on its probability of occurrence and impact.

SOW-1001 The Contractor shall propose an appropriate response for each risk.

SOW-1002 If the Contractor and the Purchaser agree that the response to a risk is other than accept it, the Contractor should plan risk response tasks (having: start, finish, work required, resources to be used, result expected).

SOW-1003 The Contractor shall include in the Project Status Report a chart that lists all active risks rated high on any factor and note any significant forecasted changes in these risks.

SOW-1004 The Contractor shall update and brief the Risk Log at every Project Progress Review Meeting and Design Review Meeting

SOW-1005 The Contractor shall describe how the Contractor will implement the Issue Management process within the RIMP, with at least the following details:

SOW-1005.A.1 Capturing Issues

SOW-1005.A.2 Assessing Issues: Management, response urgency, exposure, thresholds, roles and responsibilities

SOW-1005.A.3 Propose Corrective Actions

SOW-1005.A.4 Decide on Corrective Actions

SOW-1005.A.5 Implement Corrective Actions

SOW-1005.A.6 Supporting Tools

13.2.1.8. Risk Log

SOW-1006 The Contractor shall provide the Risk Log listing the risks, and indicating for each one the following information (but not limited to):

SOW-1007 Risk identifier: unique code to allow grouping of all information on this risk;

SOW-1007.A Description: brief description of the risk;

SOW-1007.B Risk category (e.g., management, technical, schedule, and cost risks);

SOW-1007.C Impact: effect on the project if this risk were to occur;

SOW-1007.D Probability: estimate of the likelihood of the risk occurring;

SOW-1007.E Risk rating (High, Medium, Low);

SOW-1007.F Proximity: how close in time is the risk likely to occur;

SOW-1007.G Response strategy: avoidance, mitigation, acceptance, transference

SOW-1007.H Response plan(s): what actions have been taken/will be taken to counter this risk;

SOW-1007.I Owner: who has been appointed to keep an eye on this risk;

SOW-1007.J Author: who submitted the risk;

SOW-1007.K Date identified: when was the risk first identified;

SOW-1007.L Date of last update: when was the status of this risk last checked;

SOW-1007.M Status: e.g., closed, reducing, increasing, no change.

13.2.1.9. Issue Log

SOW-1008 The Contractor shall ensure that the Issue Log comprises the following information (but not limited to):

SOW-1008.A Project Issue Number;

SOW-1008.B Project Issue Type (ECP, Off-specification, general issue such as a question or a statement of concern);

SOW-1008.C Author;

SOW-1008.D Date identified;

SOW-1008.E Date of last update;

SOW-1008.F Description;

SOW-1008.G Action item;

SOW-1008.H Responsible person. (Individual in charge of the action item);

SOW-1008.I Suspense date (Suspense date for the action item);

SOW-1008.J Priority;

SOW-1008.K Status.

13.3. Technical Documentation and Data

SOW-1009 The Contractor shall provide the Technical Documentation and Data, detailed in this section, in accordance with the generic requirements and technical requirements outlined in this Contract.

SOW-1010 The Contractor shall follow the approach and structure provided in Figure 9 - Technical Documentation and Data in creation and update of the technical information:

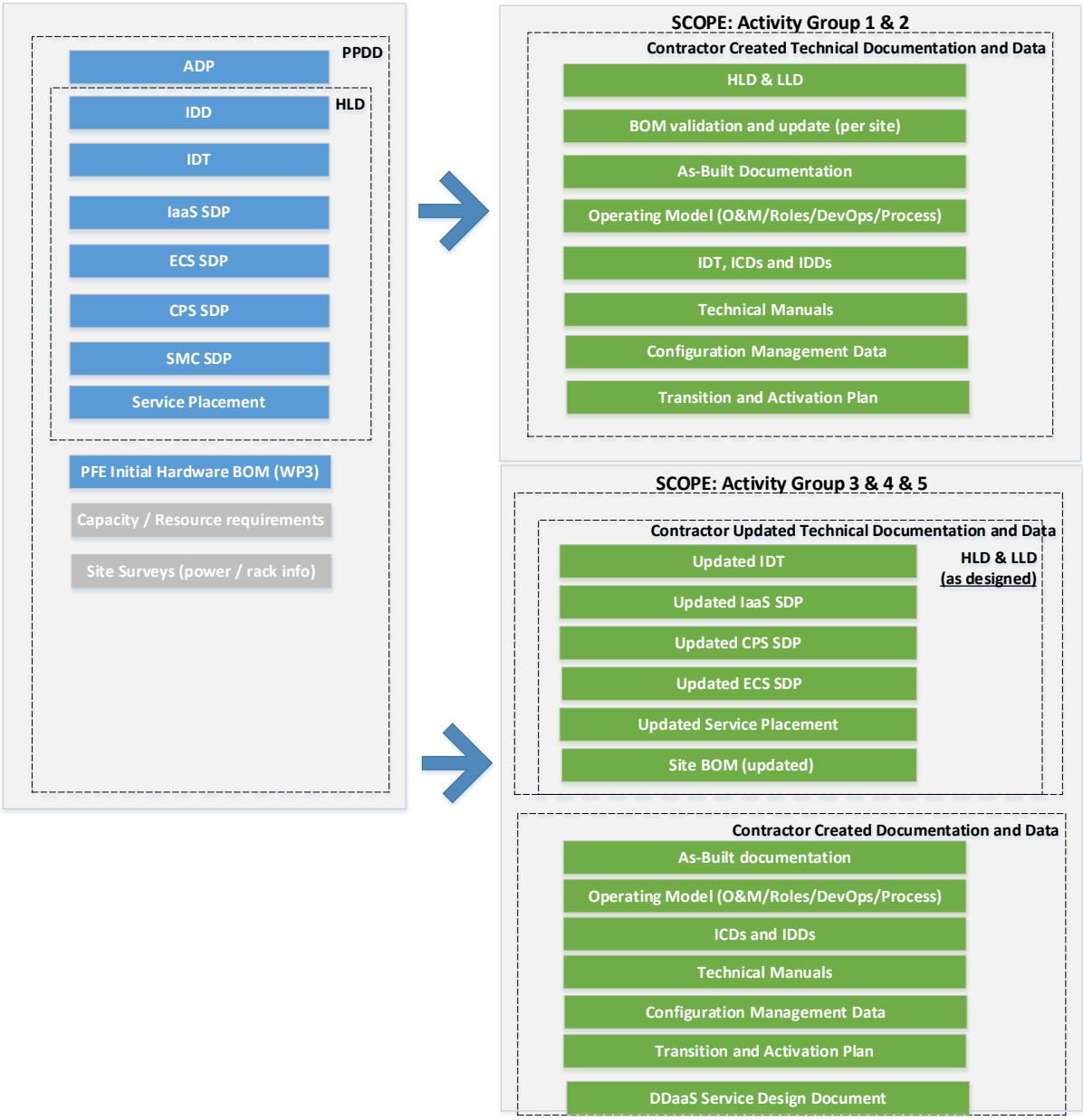

Figure 9 - Technical Documentation and Data

[0270] The Service Design Packages (SDPs) in combination with IDT and IDD are also referred to as HLD in this SoW.

SOW-1011 The Contractor shall ensure that delivered documentation (LLD, SDPs (updated), IDDs, as-build documentation, Operating Model) has the necessary roles and responsibility information so that the Purchaser can plan its support organization for the capabilities implemented within the scope of this contract.

SOW-1012 The Contractor shall provide the bespoke training for the operation, configuration and maintenance of all HW, SW and services provided within the scope of this Contract.

SOW-1013 The Contractor shall ensure that delivered documentation (LLD, SDPs (updated), IDDs, as-build documentation, Operating Model) has the necessary information so that the required prerequisite training to operate the provided WP07 services could be identified.

SOW-1014 The Contractor shall ensure that operating model information is included for each SDP, addressing the people (roles), processes and technology.

SOW-1015 The Contractor shall update and release (for approval) all the technical documentation described in this section for each Task Order activated by the Purchaser.

13.3.1. Design Specifications

SOW-1016 The Contractor shall use the design and integration requirements included in this SoW to develop the design documentation.

SOW-1017 The Contractor shall provide and maintain the design specifications for the following:

- SOW-1017.A AG1&2 Design Specification Set: Including the aspects of HLD and LLD
- SOW-1017.B AG3&4&5 Design Specification Set: Including the LLD updates to the PPDD

SOW-1018 The Contractor shall use the following PFI documentation, which constitutes PPDD as a whole, for the development of the ITM-RC1 LLD:

- SOW-1018.A Architecture Design Package [Ref: ITM-RC1 ADP]
- SOW-1018.B Service Design Package – IaaS [Ref: ITM-RC1 SDP IAAS]
- SOW-1018.C Service Design Package – ECS [Ref: ITM-RC1 SDP ECS]
- SOW-1018.D Service Design Package – CPS [Ref: ITM-RC1 SDP CPS]
- SOW-1018.E Service Design Package - Enterprise SMC [Ref: ITM-RC1 SDP SMC]
- SOW-1018.F Cyber Security Services – Information across provided SDP's
- SOW-1018.G Interface Definition Documents (IDDs)/ Interface Definition Table (IDT)[Ref: ITM-RC1 IDT]
- SOW-1018.H Service Placement [Ref: ITM-RC1 PLACEMENT] (which provides an overview and dependencies, of the services and components defined in the SDPs)
- SOW-1018.I High Level Architecture and Design Cover Document

SOW-1019 Additionally, the Purchaser will provide the reports for the Site Surveys performed in implementation sites after EDC.

SOW-1020 The Contractor shall note that PFI HLD aims at target SDDC solution, hence it focuses on the AG3 and AG4 deliverables. Therefore, the Contractor shall create the AG1&AG2 HLD as part of the LLD effort.

SOW-1021 The Contractor shall provide a LLD, including the HLD aspects, for the target solution for activity group 1 and 2, addressing the "SDDC ready" infrastructure stack and the end-user client and application provisioning services.

SOW-1022 CDR shall include Contractor's feedback and proposal for modifications of PPDD based on Contractor's technical assessment for concurrence, proposed improvements and required changes.

SOW-1023 If agreed by the Purchaser, the Contractor shall apply all the agreed modifications to the HLD and release it for baselining (see ABL). These modifications shall not constitute grounds for any additional cost.

SOW-1024 The Contractor's design documentation shall not have any contradiction with the PPDD, unless modifications specifically agreed by the Purchaser.

SOW-1025 The Contractor shall include updates to the LLD in each sprint and include a validation activity in the next sprint for the Purchaser. The Contractor shall baseline the accepted HLD/LLD upon the completion of the design reviews. The changes to the design resulting from the Sprints shall be documented in the updated versions of HLD/LLD.

SOW-1026 The Contractor shall create a LLD for each delivery within WP07 and not produce one LLD for the complete WP07 delivery.

SOW-1027 The Contractor's LLD shall include the following at minimum:

- SOW-1027.A Architecture block diagrams
- SOW-1027.B Automation and orchestration
- SOW-1027.C Interface diagrams
- SOW-1027.D Virtual Environment Overview
- SOW-1027.E Platform Sizing
- SOW-1027.F Hardware Definition and Configuration Requirements based on the latest available technology
- SOW-1027.G Rack layout design and cabling/wiring diagrams
- SOW-1027.H Network connectivity
- SOW-1027.I Authentication
- SOW-1027.J Monitoring
- SOW-1027.K Parameters
  - SOW-1027.K.1 Hostname and Firmware Versions
  - SOW-1027.K.2 IP parameters
  - SOW-1027.K.3 Licenses
  - SOW-1027.K.4 Cluster Configuration

SOW-1028 The Contractor's LLD shall include, as a standalone deliverable, the Bill of Material (BoM) including the following information:

- SOW-1028.A Part Number
- SOW-1028.B Manufacturer
- SOW-1028.C Vendor, if different than the manufacturer
- SOW-1028.D Quantity
- SOW-1028.E Site identifier
- SOW-1028.F Activity Group identifier, if applicable
- SOW-1028.G License number
- SOW-1028.H Configuration (i.e. modules, chassis, hard drives) breakdown with identifiers listed above

SOW-1029 The Contractor shall make use of the Purchaser provided hardware and software for which an initial list is provided in Annex B, and use it as baseline to provide an updated Bill of Material (BoM), as part of LLD.

SOW-1030 The Contractor shall also take into account the capacity and resource requirements provided by the Purchaser for creation of BoM, and LLD in general.

SOW-1031 BoM shall cover both the required HW/SW for the infrastructure (i.e. PFE) and HW/SW procured by the Contractor.

SOW-1032 As part of the development of the LLD, the contractor shall propose changes to the hardware, software and/or configuration requirements in case the change will provide significant benefits (e.g. newer generation hardware, compatibility with updated design).

SOW-1033 The Contractor shall ensure that the updated documentation contains sufficient information and details to finalize the implementation of all capabilities to be delivered per activity group as detailed in Appendix 1 SRS.

13.3.2. Transition and Activation Plan

SOW-1034 The Contractor shall develop and execute Transition and Activation Plan(s) for:

SOW-1034.A All activities and provisions to transition:

SOW-1034.A.1 from current state (i.e. AS-IS) to ON Ready IaaS and EUD at the completion of AG1&AG2

SOW-1034.A.2 from ON Ready IaaS node to the E2E DC Services (i.e. TO-BE) at the completion of AG4

SOW-1034.B The site activation activities;

SOW-1034.C Any post-activation tasks;

SOW-1034.D Deployment Plan for each deployment in each site;

SOW-1034.E The "back-out" procedures. The back-out section to the WIP shall enable deactivation and/or removal of all installed WP07 components and restoration of existing services without disruption of those services.

SOW-1034.F 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-1035 The Design Documentation shall be updated to include the Transitional architecture and design artefacts required to develop the Transition and Activation Plan(s).

13.3.3. DDaaS Service Design Documentation

SOW-1036 The Contractor shall provide service design documentation for DDaaS that specifies the purpose, scope and costing model of DDaaS. The Contractor shall use the document templates provided by the Purchaser.

SOW-1037 The Contractor shall provide service design documentation that specifies the Service Design and Topology for DDaaS, including the service topology, components, dependencies and interrelations. The Contractor shall use the document templates provided by the Purchaser.

SOW-1038 The Contractor shall provide service design documentation that specifies the Service Solution for DDaaS, including a description of each sub-service solution and component implementation design and rationale for service levels. The Contractor shall use the document templates provided by the Purchaser.

SOW-1039 The Contractor shall provide service design documentation that specifies the Service Management and Tools for DDaaS, including a description of the SMC processes and tools detailed implementation for specific component design. The Contractor shall use the document templates provided by the Purchaser.

SOW-1040 The Contractor shall provide service design documentation that specifies the Service Processes for DDaaS, including the Standard Operating Procedures (SOPs). The Contractor shall use the document templates provided by the Purchaser.

SOW-1041 The Contractor shall provide service design documentation that specifies the Service Organisation Skill Level Requirements for DDaaS, including the level of manpower to operate and maintain the service linked to job descriptions, skill levels and training. The Contractor shall use the document templates provided by the Purchaser.

SOW-1042 The Contractor shall provide service design documentation that specifies the Service Measurement for DDaaS, including definition of the metrics such as KPIs, SLA, OLA and the approach to collect, analyse and report against prescribed metrics. The Contractor shall use the document templates provided by the Purchaser.

SOW-1043 The Contractor shall provide service design documentation for DDaaS that specifies the purpose, scope and costing model of DDaaS. The Contractor shall use the document templates provided by the Purchaser.

13.3.4. As-Built Documentation (ABD)

SOW-1044 The Contractor shall provide as-built documentation and data which reflect the complete installation and configuration conducted by the Contractor, in accordance with the design specifications. The as-built documentation shall include at minimum:

SOW-1044.A A set of low-level, physical, Rack Layout diagrams for all racks in which the Contractor installs and/or configures hardware and software, in scope of this Contract, clearly and completely indicating any and all equipment in the racks, including any PFE with which the Contractor's equipment is directly connected.

SOW-1044.B A set of Cable Management diagrams, showing all cable connections and runs for all Contractor installed cabling, per security classification, clearly identifying the location and labelling of each cable, together with the termination at both ends and the use of the cable;

SOW-1044.C Network diagrams

SOW-1044.D Device build parameters

SOW-1044.E Provisioning guides with logical configuration data and as-built parameters

SOW-1044.F Automation and orchestration scripts, and software source codes

SOW-1044.G DevOps lifecycle tools, scripts, parameters

SOW-1044.H HW and SW details (e.g. part numbers, license details, quantities etc.)

SOW-1044.I Site specific configurations

SOW-1044.J Software BOM as described in Section 11.3.4

SOW-1044.K Other as-built parameters for design specs

SOW-1045 The Contractor shall produce and provide four separate sets of ABDs, one each after finalizing the implementation of Activity Group 1 and 2 combined, Activity Group 3, Activity Group 4, and Activity Group 5 respectively.

SOW-1046 Each set of ABDs shall describe the full as-built implementation of all sites and systems that are in scope for that Activity Group. Any differences between sites shall be clearly indicated.

SOW-1047 The Contractor shall update the ABD's for all the contractual options as they are activated by the Purchaser.

SOW-1048 The Contractor shall ensure that all as-built drawings are cross-referenced and consistent with each other and with any other documents provided under this Contract, such as manuals and training materials.

SOW-1049 The Contractor shall produce all as-built drawings using Microsoft Visio, in a version compatible with the Purchaser's version of Visio.

SOW-1050 The Contractor shall produce as-built drawings in such a way that the Purchaser can edit and augment the diagrams (e.g. to change the drawings to reflect future modifications).

SOW-1051 As-built drawings shall use layered views as appropriate, such as separate layers for physical and logical components, connections, and links, et cetera.

13.3.5. Operating Model

SOW-1052 The Contractor shall develop the Operating Model for the operation and maintenance of the systems and services in scope of this Contract, based on the industry best practices. Purchaser will use this information as an input to the organizational Operating Model created by the Purchaser.

SOW-1053 The Operating Model shall describe a proposed organisational structure for the operation and maintenance of systems and services implemented by the design, based on industry best practice, including roles, number of full-time equivalent posts, and skills required for each role.

SOW-1054 The Operating Model shall use standardized IT roles and skills as defined by an industry standard skills framework, such as SFIA (Skills Framework for the Information Age, or e-CF (European e-Competence Framework), or equivalent framework (-s).

SOW-1055 The Contractor shall include the following information within the Operating Model at minimum:

SOW-1055.A Detailed description of the processes delivered within the scope of this Contract (e.g. DevOps Lifecycle, Automation and Orchestration processes)

SOW-1055.B Standard Operating Procedures (e.g. operation, maintenance)

SOW-1055.C Organization (i.e. organizational structure, roles, responsibilities/RACI, skills and manpower required to operate and maintain the different systems and services delivered)

SOW-1055.D Technology (i.e. tools, scripts, source code, licenses and hardware infrastructure specifics)

SOW-1055.E Performance indicators (e.g. KPIs) and monitoring

SOW-1055.F Operating Model Maturity Levels

SOW-1056 The Contractor shall detail the integration of security policies and measures within the scope of the Operating Model, as an integral part of the DevOps lifecycle.

SOW-1057 In accordance with the industry best practices, the Contractor shall propose a schema for Operating Model Maturity Levels aligned with the established DevOps Lifecycle and including the following themes:

SOW-1057.A Organization

SOW-1057.B Delivery

SOW-1057.C Automation

SOW-1057.D Testing

SOW-1057.E Security

SOW-1057.F Monitoring

SOW-1057.G Operations

13.3.6. Technical Manuals

SOW-1058 The Contractor shall develop all Technical Manuals compliant with the requirements in SoW section 12.

13.3.7. Configuration Management Data

SOW-1059 As part of the Technical Documentation and Data, the Contractor shall provide and maintain the following configuration management artefacts in accordance with the Section 10:

SOW-1059.A Configuration Baselines (i.e. FBL, ABL, PBL, OBL)

SOW-1059.B ECPs, RfD, RfW (if applicable)

SOW-1059.C CMDB (including the Configuration Status Accounting data)

Annex A CIS PRINCIPLES AND MATURITY LEVELS

A.1. CIS Principles – Maturity Level per Activity Group

[0271] In order to guide the development of the detailed design and the execution of system integration activities over time, the Purchaser has developed Maturity levels describing the expected level of service maturity :

Maturity level		Description
0	Non-existing	Local Approach
1	Basic	
2	Progressing	Enterprise Approach (standardized and consistent delivery of services)
3	Established	
4	Proficient	Established Enterprise Service (enable fast pace changes with limited or no operational impact)
5	Exceling	
6	Perfect	Advanced Enterprise Service (providing advance capabilities, immediate response to NATO employees need)

Table 11 - Maturity level definitions

SOW-1060 The systems and components shall be integrated and configured to meet the following maturity for each CIS Principle:

CIS Principle ID	CIS Principle	CIS Driver	Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
P01	CIS Services Continuity and High Availability	Cloud	2	3	3	4	4
P02	Maximizing the Utility of Increasingly Scarce Resources	Cloud	2	2	3	3	3
P03	Secure Multi-Tenancy	Cloud	2	2	3	4	4
P04	Flexibility	Cloud	3	3	3	4	4
P05	Scalability	Cloud	2	2	3	3	3
P06	Virtualisation	Cloud	3	3	4	4	4
P07	Automation and Orchestration	Cloud	2	3	3	3	3
P08	Be future proof	Cloud	3	3	4	4	4
P09	Standardization and Interoperability	Cloud	3	3	4	5	5
P10	NATO Green IT Principles	Cloud	2	2	2	3	3
P11	Security by Design	Cyber Security	3	3	4	5	5
P12	Identity and Access Management	Cyber Security	1	1	3	4	4
P13	NATO Cyber monitoring / detection / response capability	Cyber Security	2	2	3	4	4
P14	Service Orientation	SMC	2	2	3	4	4
P15	Remote administration and Management	SMC	2	2	3	4	4
P16	Enterprise Configuration and Change Control	SMC	1	1	3	4	4
P17	Data integration	SMC	1	1	2	4	4
P18	User Experience	Digital Desktop	2	2	3	4	4
P19	Roaming	Digital Desktop	0	1	1	3	3
P20	Single Access Point for H-to-H communication	Digital Desktop	0	1	1	3	3

Table 12 – CIS Principles maturity level per Activity Group

SOW-1061 The system and components implemented and/or integrated in Activity Groups by the Contractor shall meet the following maturity levels through the services provided:

CIS Principles	Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
[Cloud] CIS Services Continuity and High Availability	[2][Progressing]No obsolete infrastructure and obsolescence management organized, services are designed to sustain infrastructure incidents however it may required manual interactions. There are no single point of failure systems.	[3][Established]Redundant and up to date infrastructure, services are designed and implemented to sustain infrastructure incidents in automated manner.There are no single point of failure systems.	[3][Established]Redundant and up to date infrastructure, services are designed and implemented to sustain infrastructure incidents in automated manner.There are no single point of failure systems.	[4][Proficient]Systems are configured to leverage other sites IaaS when needed (not automated, manual capacity management) to improve availability and service continuity. HA services may be deployed automatically if templates exist. Capacity is reviewed/extended on a regular basis. There are no single point of failure systems.	[4][Proficient]Systems are configured to leverage other sites IaaS when needed (not automated, manual capacity management) to improve availability and service continuity. HA services may be deployed automatically if templates exist. Capacity is reviewed/extended on a regular basis. There are no single point of failure systems.
[Cloud] Maximizing the Utility of Increasingly Scarce Resources	[2][Progressing]Virtual infrastructures are leveraged to share capacity however it is limited to single NATO "entity, there may still be many infrastructures in use.	N/A	[3][Established]Secure Mutli-tenancy is leveraged to share capacity for multiple NATO "entities". However there are still separate infrastructures used to segregate services and/or some entities.	[3][Established]Secure Mutli-tenancy is leveraged to share capacity for multiple NATO "entities". However there are still separate infrastructures used to segregate services and/or some entities.	[3][Established]Secure Mutli-tenancy is leveraged to share capacity for multiple NATO "entities". However there are still separate infrastructures used to segregate services and/or some entities.
[Cloud] Secure Multi-Tenancy	[2][Progressing]Logical segregation is provided (e.g. storage and VLANs) but there are no advance security functions in place and/or IaaS management is not segregated.	N/A	[3][Established]Provide local multi-tenancy. It is possible to logically segregate resources across local IaaS resources. IaaS Management is segregated	[4][Proficient]Provide multi-tenancy across the NATO ON. It is possible to logically segregate resources across all IaaS nodes. Integration with other enterprise security and management services is implemented.	[4][Proficient]Provide multi-tenancy across the NATO ON. It is possible to logically segregate resources across all IaaS nodes. Integration with other enterprise security and management services is implemented.
[Cloud] Flexibility	[3][Established]local resources are configured to be pooled. Resource reservation and prioritisation can be requested and assigned automatically via template	N/A	[3][Established]local resources are configured to be pooled. Resource reservation and prioritisation can be requested and assigned automatically via template	[4][Proficient]Local resources are configured to be pooled. Resource reservation and prioritisation are requested and assigned automatically via template. Some IaaS nodes are configured to be able to leverage resources from other IaaS nodes	[4][Proficient]Local resources are configured to be pooled. Resource reservation and prioritisation are requested and assigned automatically via template. Some IaaS nodes are configured to be able to leverage resources from other IaaS nodes
[Cloud] Scalability	[2][Progressing]scalability available up to 25% of resources at a node. Sites may not be able to support more.	N/A	[3][Established]Instant scalability available up to 25% of resources at a node . Site prep work possible to increase the capacity	[3][Established]Instant scalability available up to 25% of resources at a node . Site prep work possible to increase the capacity	[3][Established]Instant scalability available up to 25% of resources at a node . Site prep work possible to increase the capacity
[Cloud] Virtualisation	[3][Established]Processing, storage, network and security virtualisation functionality are leveraged. Basic templates available for single servers, partially automated.	N/A	[4][Proficient]Majority of all services (80%) are virtualised on Processing, Storage, Networking, Security functionalities. Application blueprints available for some applications/services. Non virtualized services are integrated and configuration changes partially automated.	[4][Proficient]Majority of all services (80%) are virtualised on Processing, Storage, Networking, Security functionalities. Application blueprints available for some applications/services. Non virtualized services are integrated and configuration changes partially automated.	[4][Proficient]Majority of all services (80%) are virtualised on Processing, Storage, Networking, Security functionalities. Application blueprints available for some applications/services. Non virtualized services are integrated and configuration changes partially automated.
[Cloud] Automation and Orchestration	[2][Progressing]Some templates are used to deploy resources.	[3][Established]Templates and resource management is performed in a coordinated way across sites. It is possible to automate and/or orchestrate the allocation of resource in a "centralized" manner even if not all nodes are covered. Some self service functions are implemented.	[3][Established]Templates and resource management is performed in a coordinated way across sites. It is possible to automate and/or orchestrate the allocation of resource in a "centralized" manner even if not all nodes are covered. Some self service functions are implemented.	[3][Established]Templates and resource management is performed in a coordinated way across sites. It is possible to automate and/or orchestrate the allocation of resource in a "centralized" manner even if not all nodes are covered. Some self service functions are implemented.	[3][Established]Templates and resource management is performed in a coordinated way across sites. It is possible to automate and/or orchestrate the allocation of resource in a "centralized" manner even if not all nodes are covered. Some self service functions are implemented.
[Cloud] Be future proof	[3][Established]Up to date capabilities at all sites, deficiencies are known but there are not always plans for future improvements.	N/A	[4][Proficient]Up to date capabilities at all sites, deficiencies are known and some improvement plans/roadmaps exist.	[4][Proficient]Up to date capabilities at all sites, deficiencies are known and some improvement plans/roadmaps exist.	[4][Proficient]Up to date capabilities at all sites, deficiencies are known and some improvement plans/roadmaps exist.
[Cloud] Standardization and Interoperability	[3][Established]Services are leveraging the same HW and SW baselines, but are also configured in a similar manner/according to similar topologies.	N/A	[4][Proficient]Services are leveraging the same HW and SW baselines, are configured in a similar manner/according to similar topologies and changes are implemented across all sites in a coordinated manner.	[5][Exceling]Services are leveraging the same HW and SW baselines, are configured in a similar manner/according to similar topologies and most changes are implemented across all sites in an automated manner.	[5][Exceling]Services are leveraging the same HW and SW baselines, are configured in a similar manner/according to similar topologies and most changes are implemented across all sites in an automated manner.

Figure 10 - CIS Principles Maturity Levels for Activity Groups (1/3)

CIS Principles	Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
[Cloud] NATO Green IT Principles	[2][Progressing]There is a clear effort to reduce environmental impact, by procuring energy efficient hardware, planning for the use of renewable energies, and/or limiting the use/procurement of unnecessary resources. Design and architecture development takes into account some green IT principles.	N/A	[2][Progressing]There is a clear effort to reduce environmental impact, by procuring energy efficient hardware, planning for the use of renewable energies, and/or limiting the use/procurement of unnecessary resources. Design and architecture development takes into account some green IT principles.	[3][Established]Design and architecture lead to the implementation of services according to energy efficient and sustainable principals. Design and architecture development integrate green IT principles.	[3][Established]Design and architecture lead to the implementation of services according to energy efficient and sustainable principals. Design and architecture development integrate green IT principles.
[Cyber Security] Security by Design	[3][Established]Security baseline are defined and implemented, new services are designed taking into account security from the start.	[3][Established]Security baseline are defined and implemented, new services are designed taking into account security from the start.	[4][Proficient]Security baseline are defined and implemented and sometimes in automated manner, new services are designed taking into account security from the start. Some dashboards are allowing to provide visibility on security compliance of some services.	[5][Exceling]Security baseline are defined and implemented in automated manner, new services are designed taking into account security from the start. Dashboards are allowing to provide visibility on security compliance of most of the services, and ensure changes to not introduce vulnerabilities.	[5][Exceling]Security baseline are defined and implemented in automated manner, new services are designed taking into account security from the start. Dashboards are allowing to provide visibility on security compliance of most of the services, and ensure changes to not introduce vulnerabilities.
[Cyber Security] Identity and Access Management	[1][Basic]There is a limited level of trust on the authorization and authentication mechanism implemented. Devices are given access to the network based on basic access controls. Identity information is not consistent across the various system.	N/A	[3][Established]Role base access is implemented for administrative access but not always enforce for end user access to application. Strong authentication is most of the time leveraged. Devices are mainly authenticating to the network based on strong authentication. Identity information is most of the time consistent across the system.	[4][Proficient]Strong authentication mechanism are implemented and used widely, access control is mostly done in an automated manner based on Role base access for both administrative and application. Devices are authenticating to the network based on strong authentication, and some level of logical separation is ensured. Identity information is consistent across the system , even if some information is not available in a single authoritative source.	[4][Proficient]Strong authentication mechanism are implemented and used widely, access control is mostly done in an automated manner based on Role base access for both administrative and application. Devices are authenticating to the network based on strong authentication, and some level of logical separation is ensured. Identity information is consistent across the system , even if some information is not available in a single authoritative source.
[Cyber Security] NATO Cyber monitoring / detection / response capability	[2][Progressing]The capability is integrated with some services providing improved visibility. Most deployment of new service is not automated. Monitoring, detection and response capabilities still require some consequent coordination effort..	[2][Progressing]The capability is integrated with some services providing improved visibility. Most deployment of new service is not automated. Monitoring, detection and response capabilities still require some consequent coordination effort..	[3][Established]The capability is well integrated with services providing a good visibility. There is some automation in place to integrate new services. Monitoring, detection and response capabilities still require some coordination effort..	[4][Proficient]The capability is most of the time integrated with all other services. Most deployment of new service is automatically triggering the configuration changes required. Monitoring, detection and response capabilities are enabled with some level of automation and with little coordination required.	[4][Proficient]The capability is most of the time integrated with all other services. Most deployment of new service is automatically triggering the configuration changes required. Monitoring, detection and response capabilities are enabled with some level of automation and with little coordination required.
[SMC] Service Orientation	[2][Progressing]There is some effort to centralize asset management and automate the discovery. The maturity of the information linked to asset varies. It is not possible report on capacity/performance/usage.	[2][Progressing]There is some effort to centralize asset management and automate the discovery. The maturity of the information linked to asset varies. It is not possible report on capacity/performance/usage.	[3][Established]Most of the hardware and software asset management is consolidated and discovered automatically. The maturity of the information is allowing to report on capacity but not always on performance and live usage. Assets are linked to global services allowing to improve service reporting/monitoring/charge back.	[4][Proficient]Most of the hardware and software asset management is consolidated. The maturity of the information is allowing to report on capacity, performance and live usage. Assets are linked to global services allowing to improve service reporting/monitoring/charge back.	[4][Proficient]Most of the hardware and software asset management is consolidated. The maturity of the information is allowing to report on capacity, performance and live usage. Assets are linked to global services allowing to improve service reporting/monitoring/charge back.
[SMC] Remote administration and Management	[2][Progressing]Multiple system have centralized administrative capabilities in place. Processes are not very mature but some Role Based Access is implemented. Some services are leveraging strong authentication to access services. Access is usually controlled from specific location (not granular per device). Out of band management is configured to provide access to the assets from centralized locations.	[2][Progressing]Multiple system have centralized administrative capabilities in place. Processes are not very mature but some Role Based Access is implemented. Some services are leveraging strong authentication to access services. Access is usually controlled from specific location (not granular per device). Out of band management is configured to provide access to the assets from centralized locations.	[3][Established]Most system have centralized administrative capabilities in place. Processes are in place to implement Role based access via PAM. Most services are leveraging strong authentication to allow access. Access is usually controlled from specific location (not granular per device). Out of band management is configured to provide access to the assets from centralized locations.	[4][Proficient]Only few systems have no centralized capabilities. Only authorized admin are accessing the services using strong authentication. Access is most of the time enforced from the right device and according to defined patterns (PAM). Some exceptions may still exist. Out of band management is configured to provide access to the assets from centralized locations.	[4][Proficient]Only few systems have no centralized capabilities. Only authorized admin are accessing the services using strong authentication. Access is most of the time enforced from the right device and according to defined patterns (PAM). Some exceptions may still exist. Out of band management is configured to provide access to the assets from centralized locations.

Figure 11 - CIS Principles Maturity Levels for Activity Groups (2/3)

CIS Principles	Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
[SMC] Enterprise Configuration and Change Control	[1][Basic]There are some local and centralized configuration and change management in place, but the information is not always accurate and or not standardized nor covering all system and assets.	N/A	[3][Established]There are system in place to record, report and archive/audit the majority of the required configuration changes. The data imported is not covering the whole scope of the enterprise. The data is sometimes not accurate but this has limited impact.	[4][Proficient]There are system in place to record, report and archive/audit the majority of the required configuration changes. The data imported is not covering the whole scope of the enterprise, but data is accurate and trusted.	[4][Proficient]There are system in place to record, report and archive/audit the majority of the required configuration changes. The data imported is not covering the whole scope of the enterprise, but data is accurate and trusted.
[SMC] Data integration	[1][Basic]Data is aligned and synchronized between some system across the NATO enterprise. Many exception exist and have a negative impact on some services or efficiency. Information is often not trusted and manual audits and verifications are required most of the time.	N/A	[2][Progressing]Data is aligned and synchronized across the most critical system across the NATO enterprise. Many exception exist and have a negative impact on services or efficiency. Information is sometimes trusted through the use of technical controls and limited automated reporting. Manual audits and verifications are still extensively required.	[4][Proficient]Data is aligned and synchronized across all the system across the NATO enterprise. Few exception may exist. Information is highly trusted through the use of technical controls but few manual audits are required.	[4][Proficient]Data is aligned and synchronized across all the system across the NATO enterprise. Few exception may exist. Information is highly trusted through the use of technical controls but few manual audits are required.
[Digital Desktop] User Experience	[2][Progressing]User access to application is similar from the various locations and/or when using another device and there are limited differences affecting user experience. Performance varies depending on device and location.	[2][Progressing]User access to application is similar from the various locations and/or when using another device and there are limited differences affecting user experience. Performance varies depending on device and location.	[3][Established]User experience across the enterprise is consistent, access to application is similar from the various locations and/or when using another device and there are limited differences allowing for an easy use of the environment. Performance is usually similar depending on device and location.All applications required are available to users, and can also be provisionned automaticaly based on the role and/or position of users	[4][Proficient]User experience is the same across the enterprise, with some performance and access differences depending on location and time.All applications required are available to users, and are also often provisionned automaticaly based on the role and/or position of users	[4][Proficient]User experience is the same across the enterprise, with some performance and access differences depending on location and time.All applications required are available to users, and are also often provisionned automaticaly based on the role and/or position of users
[Digital Desktop] Roaming	N/A	[1][Basic]Users are able to use devices from other offices and sites (when part of the same organization) however they do not have the same access to application and data.	N/A	[2][Progressing]Users are able to use devices from other offices and sites (when part of the same organization) and have the same access to application and data.	[2][Progressing]Users are able to use devices from other offices and sites (when part of the same organization) and have the same access to application and data.
[Digital Desktop] Single Access Point for H-to-H communication	N/A	[1][Basic]Users are able to leverage a single consolidated environment to ensure their usual daily H-to-H communication inside their organization and sometimes outside their organization. There are still many exception for specific purpose (e.g. external communication, sensitive communication, or specific party)	N/A	[3][Established]Users are able to leverage a single consolidated environment to ensure all their H-to-H communication inside their organization and most of the time outside their organization. Sensitive communication is still usually leveraging a separate environment.	[3][Established]Users are able to leverage a single consolidated environment to ensure all their H-to-H communication inside their organization and most of the time outside their organization. Sensitive communication is still usually leveraging a separate environment.

Figure 12 - CIS Principles Maturity Levels for Activity Groups (3/3)

Annex B PURCHASER FURNISHED EQUIPMENT (PFE) AND PURCHASER FURNISHED INFORMATION (PFI)

B.1. Hardware

[0272] The Purchaser has identified an initial list of equipment required to conform to SRS and in general to fulfil the goal of this project.

[0273] The Purchaser will provide all the hardware for implementation of Activity Groups, with the exception of Cyber Security Monitoring. In order to meet the project timelines, the Purchaser ordered part of the required equipment. Remaining equipment will be ordered and installed in accordance with the project timelines, and made available for Contractor activities.

SOW-1062 The contractor shall use the specified equipment in order to implement the systems. However the Contractor will have the opportunity to review and propose changes to the Hardware baseline for the following hardware orders.

[0274] The initial Hardware Baseline is summarized in the following table :

Sub-service/component	DC IaaS	EN IaaS	SN IaaS
Directory: Domain Controller (Physical)	DL360 Gen10 8SFF Plus	N/A	N/A
ESXi: Cloud Infrastructure Management cluster	DL365 8SFF 2x32c 512GB	DL365 8SFF 2x32c 512GB	TBD
ESXi: Workload Cluster 1 (General)	DL385 24SFF 2x32c 768GB	DL325 8SFF 1x32c 256GB	DL325 8SFF 1x32c 256GB
ESXi: Workload Cluster 4 (VDI)	DL385 16SFF 2x16c 512GB 1xA16	DL385 16SFF 2x16c 512GB 1xA16	N/A
Disaster Recovery Cluster 1	DL385 24SFF 2x32c 768GB	N/A	N/A
Workload Cluster 5 (DMZ)	DL325 8SFF 1x32c 256GB	N/A	N/A
Cisco APIC (Large)(DC)	APIC Cluster L3	APIC Cluster M3	TBD
Nexus Dashboard (Large)	Nexus Dashboard L3	N/A	N/A
Spine switches	N9K_C9364C_GX	N9K_C93600CD_GX	N9K_C93600CD_GX
Leaf switches	N9K_C93180YC_FX3	N9K_C93180YC_FX3	N9K_C93180YC_FX3
Site External switches	C9500_24Y4C_A_	C9500_24Y4C_A_	C9500_24Y4C_A_
Out of Band management switch	C9300_24T_A	C9300_24T_A	C9300_24T_A
BPS1 - Firewall (Palo Alto)	Palo Alto 5250	Palo Alto 3260	Palo Alto 3260
F5 Physical Loadbalancers/ADC and WAF	F5 BIG-IP i5800	N/A	N/A
Tier-1 Backup Storage	DL380 Gen10 12LFF - Backup	DL380 Gen10 12LFF - Backup	DL380 Gen10 12LFF - Backup
Tier-2/3 Backup Storage	StoreOnce 3640 48TB DD3300 16TB TBD	TBD	TBD
Tier-4 Archive storage (ECS)	Dell ECS	N/A	N/A

Table 13 – PFE Hardware Baseline summary

[0275] For Tier-2 Storage, the Purchaser may either use EXAGRID (also TIER-1), EMC Data domain or HP StoreOnce.

SOW-1063 The Contractor shall follow the official 'Handover Takeover Process' documenting the inventory details for the hardware that will be physically taken over by the Contractor team for the transfer of liability.

B.2. Virtualized Environment / NATO Public Cloud Services

[0276] Section 4.2.7 describes IREEN ON@NU.

[0277] If decided by the Purchaser, NATO Software Factory services will be provided to the Contractor as Purchaser Furnished Service (except automation and orchestration licences described in 4.4.4).

[0278] The NSF environment is currently composed of :

A. M365 including Teams and SharePoint
B. Azure DevOps
C. GitLab
D. Jenkins
E. SonarQube
F. Sonatype Nexus
G. JIRA
H. MediaWiki (internal knowledge sharing platform for NSF)
I. Kubernetes
J. Azure Container Registry
K. Ansible
L. Terraform

SOW-1064 If it is not possible to use the NSF, the Contractor shall notify the customer before EDC+3MO and an alternative solution will be commonly sought.

B.3. Software Licenses

[0279] Following SW licenses will be provided by the Purchaser as PFE:

M. All Microsoft products, including OS Server, Workstations, SCOM, RDP etc.
N. McAfee
O. VMWare
P. Adobe
Q. Palo Alto
R. Cisco

B.4. IT Equipment

[0280] The Purchaser will provide to the Contractor NR classified laptop(s), otherwise called REACH, in order to facilitate classified communication (up to the NATO RESTRICTED level), coordination between NCI Agency and Contractor teams, raising ITSM tickets and maintenance of the Purchaser's project portal as defined in 4.6.3.

[0281] Details for the delivery of these laptop(s) (including licenses and user credentials) will be agreed right after EDC so that they are activated before the first PRM.

[0282] The Purchaser will provide the Contractor with access to the NS workstations that will be required during implementation phase including the development and testing activities. NS workstations will be available on-site in Purchaser facilities.

[0283] The quantities of NR and NS equipment will be decided by the Purchaser based on the actual necessity and phase of the project.

SOW-1065 The Purchaser will provide the Contractor with the NU laptops for the implementation (e.g. automation and orchestration) during the different phases of the project. The Contractor shall at all times use these devices to create, implement and maintain the technical artefacts (e.g. software code, scripts, configuration files, technical data etc.) at NU level.

SOW-1066 The Contractor shall provide the Purchaser with the access to all IT devices used during the work package execution activities, including passwords, file locations, and physical access.

SOW-1067 The Contractor shall follow the official ‘Handover Takeover Process’ documenting the inventory details for the IT equipment that will be physically taken over by the Contractor team for the transfer of liability.

B.5. List of PFE/PFI

[0285] The Purchaser will make the applicable PFE and PFI available as per the applicable Task Order(s).

#	Name	By
PFE/I-01	High Level Architecture and Design Cover Document	NCIA
PFE/I-02	ICD Template	NCIA
PFE/I-03	ADP	NCIA
PFE/I-04	IaaS SDP	NCIA
PFE/I-05	ECS SDP	NCIA
PFE/I-06	CPS SDP	NCIA
PFE/I-07	SMC SDP	NCIA
PFE/I-08	IDT	NCIA
PFE/I-09	Subset of IDDs	NCIA
PFE/I-10	Service Placement Document	NCIA
PFE/I-11	REACH Laptops	NCIA
PFE/I-12	Hardware (including installation)	NCIA
PFE/I-13	Virtualized Environment/ NATO Public Cloud Services	NCIA
PFE/I-14	Software Licenses	NCIA
PFE/I-15	Client Devices(for testing and integration)	NCIA
PFE/I-16	Client LAN Environment	NCIA
PFE/I-17	Printing and Scanning Service (for testing and integration)	NCIA
PFE/I-18	Instances of NCI Agency agile test management tools	NCIA
PFE/I-19	Site Surveys	NCIA
PFE/I-20	Security Accreditation Document Set Templates	NCIA
PFE/I-21	IVV Templates	NCIA
PFE/I-22	Cyber Security Audit Process Template	NCIA
PFE/I-23	AFT Template	NCIA
PFE/I-24	Hardening guides	NCIA
PFE/I-25	Endpoint Security Baseline	NCIA
PFE/I-26	NATO Trusted container lifecycle management	NCIA
For NCSC Cyber Security monitoring enclaves:		
PFE/I-27	• Rack space, power and cooling for the Tier-3 enclaves	NCIA
PFE/I-28	• NetWitness Full Packet Capture hardware and software licences	NCIA
PFE/I-29	• Splunk Software and Licences	NCIA
PFE/I-30	• OCF AccessData software and licences	NCIA
PFE/I-31	• OVA Tenable Nessus software and licences	NCIA

Table 14 - PFE and PFI

Annex C CYBER SECURITY MONITORING IMPLEMENTATION

C.1. Introduction

[0286] The NCSC Security Operations Centre (SOC), referred to in this SoW as Tier 2, operates NCSC Cyber Security Services (CSS12) installed at each operational site, referred to in this SoW as Tier 3 sites.

[0287] The NCSC equipment hosting infrastructure at Tier 3 sites (DCs, ENs & SNs) is referred to as an NCSC Enclave and includes network switches, local administration workstations, Full Packet Capture (FPC) appliances, network packet brokers (NPB), a gateway firewall and physical servers with storage providing a virtual machine (VM) hosting environment.

[0288] The virtual hosting environment is known as the NCSC Cyber Defence Platform (NCDP) and hosts CSS such as Online Computer Forensics (OCF) and Online Vulnerability Assessment (OVA), in addition to supporting infrastructure servers. The architecture of the combined Tier-2 and Tier-3 environment is depicted in Figure 13.

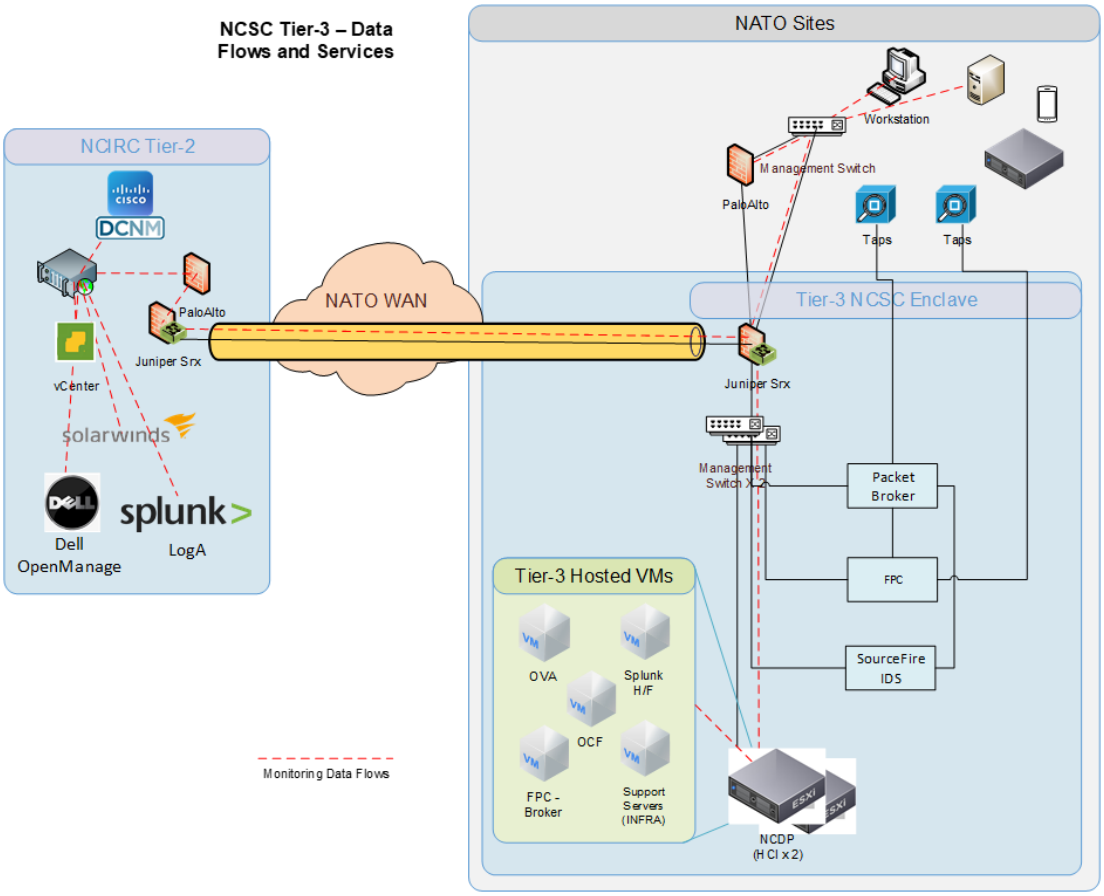

Figure 13 - NCSC Cyber Security Monitoring Architecture

[12] Previously known as NATO Cyber Incident Response Capability (NCIRC) Full Operational Capability (FOC))

C.2. NCSC Cyber Security Enclave Components Description

[0289] This section does not explicitly specify requirements, it is included to provide the bidder with some background of the functionality of the existing NCSC monitoring capability.

C.2.1. Enclave VPN and Firewall

[0290] A Juniper SRX firewall provides two services at the Tier-3 sites. Firstly it is used to provision a VPN tunnel across the NATO WAN to a larger Juniper Gateway firewall running at Tier-2. The VPN tunnel provides a secure connection between the NCSC Tier-2 central management servers and the Tier 3 hosted services. Note also that firewall rules are applied to the VPN entry points to ensure only approved connections can be initiated through the tunnel.

[0291] Secondly the Juniper Firewall 2 is used to provide a security gateway between the Enclave and the Tier-3 monitored site infrastructure. Firewall rules control connectivity and Network Address Translation (NAT) facilitates connectivity between the site and enclave IP addressing schemes.

[0292] The Tier-3 Juniper SRX devices are currently managed via a management server installed at Tier-2 running JunoSpace v 20.3R1

C.2.2. NATO Cyber Defence Platform

[0293] The NATO Cyber Defence Platform (NCDP) is the core enclave component providing virtualized hosting of the various NCSC Tier 3 services. It is composed of two Hyper Converged Infrastructure (HCI) servers. HCI is defined as an IT infrastructure that provides, at a minimum, virtualized computing (a hypervisor), a virtual SAN (VSAN or software defined storage) and virtualized networking (software-defined networking).

[0294] The HCI nodes are managed via the existing Tier-2 VMware vCenter servers.

C.2.3. Network Packet Broker

[0295] The Network Packet Broker (NPB) receives an exact copy of the network traffic traversing each of the monitoring points, in this case either network taps or ERSPAN.

[0296] The NPBs match each network packet to a defined policy to de-duplicate, truncate, modify, enrich, or leave intact for its onward journey to the Full Packet Capture (FPC) Decoders.

[0297] For this project packets will be copied and forwarded to the NPB via one of two mechanisms:

C.2.3.1. Network Taps

[0298] Network taps are physical devices that are installed directly into the network, effectively breaking the link that they are installed to monitor. They are designed to introduce minimal latency, to fail-safe (i.e. allow operational packets to flow on failure) while forwarding an exact copy of all packets to the monitoring device, usually via the NPB.

[0299] The taps are to be chosen to match the network to be monitored and come in a variety of media (fibre, copper) and also various speeds.

C.2.3.2. Encapsulated Remote SPAN Network Taps

[0300] Encapsulated Remote SPAN (ERSPAN) is a technology to forward network packets to a remote collection device, in this case a NBP. ERSPAN operates at layer 3, and is used

to forward traffic across an IP network facilitated by the addition of a Generic Routing Encapsulation (GRE) header. It is possible to configure an ERSPAN to forward to an external destination all packets traversing one or more virtual NIC or one or more specific VM hosted within the NSX-T layer.

C.2.4. Online Computer Forensics

[0301] The Online Computer Forensics (OCF) services is comprised of a suite of forensic tools provided by a company named Exterro (formerly AccessData) known as Forensic Toolkit (FTK) Enterprise. The specific products deployed are the Enterprise Examiner and Enterprise Central Manager (ECM). Both tools communicate either directly or indirectly with an OCF Agent installed on every monitored client and server throughout the Enterprise.

[0302] Enterprise Examiner facilities remote Random Access Memory (RAM) and Hard Disk Drive (HDD) acquisitions. ECM facilitates all other forensic analysis such as enterprise wide searches for unauthorised files, registry keys, malware and other known indicators of compromise.

[0303] Tier 2 consists of 5 virtual machines facilitating OCF Central Management including Evidence Processing and Storage.

[0304] Two OCF servers are installed at each Tier 3 Enclave, an Enterprise Examiner server plus a Child Site Server (CSS). NCSC Forensics Analysts at Tier 2 connect via web browser to the ESM at Tier 2 to communicate with the CSS in the Tier 3 Enclave and they connect directly over the WAN to the Tier 3 Examiner server via Remote Desktop protocol (RDP).

[0305] For smaller sites without a Tier 3 CSS, the CSS at SHAPE connects directly to the agents installed at the site.

C.2.5. Online Vulnerability Assessment

[0306] The Online Vulnerability Assessment (OVA) consists of two pre-packaged virtual appliances installed on the Tier 3 Enclave NCDP. One VM is the Tenable Scanner, based on Tenable.sc the second VM is the Agent Management server. The Tier-3 scanner connects to the central management OVA servers at NCSC Tier-2.

[0307] OVA service covers: endpoints (agent-based scanning), servers (agent-based scanning), network infrastructure (network-based scanning) and the VMWare virtualization platform (network based scanning).

C.2.6. Full Packet Capture

[0308] The Full Packet Capture (FPC) service is comprised of a suite of RSA NetWitness (NW) devices. Central Management at Tier 2 comprises a NW Event Stream Analysis (ESA) server, a NW Admin server and in some cases a NW Broker server.

[0309] Two or more NW Decoder appliances are deployed at each Tier 3 site and one or more Concentrators. The convention is to deploy Decoders to Concentrators at a ratio of 2:1.

[0310] The NW Decoders receive raw network packets from the Network Packet Brokers, they generate metadata of the collected packets forward this to the NW Concentrators where it is indexed in order to facilitate fast searches. Each appliance has dedicated attached storage; high density lower speed for the Decoders and lower density higher speed for the Concentrators.

[0311] When a Tier-3 site has more than one Concentrator a virtual NW Broker13 has to be deployed, hosted on the NCDP, to facilitate load balancing between concentrators.

[0312] The current version of the NetWitness software is 11.6.1.

C.2.7. Network Intrusion Detection and Prevention

[0313] Network Intrusion Detection and Prevention (NIDS/NIPS) is provided by the use of the Palo Alto Firewall Threat Prevention service. All Palo Alto firewalls are licensed to include the Threat Prevention service. Alerts are transferred to the Splunk based Enterprise Logging service via a log forwarding connection from the Palo Alto central manager, known as Panorama.

C.2.8. Enterprise Logging and Security Information and Event Monitoring

[0314] The current (CSSR delivered) Security Information and Event Monitoring (SIEM) based on Splunk is based on Splunk forwarding components installed on the NCDP in the NCSC Enclave. Logs from the site need to be forwarded through the NCSC Juniper Firewall to the Splunk forwarders deployed in the Enclave.

[0315] The ITM-R project will deliver an entirely new Enterprise Logging and SIEM service, also based on Splunk, installed on the new ITM IaaS infrastructure. .

[0316] The Splunk Indexers will be deployed in a high availability (HA) configuration on a dedicated cyber security zone (IaaS tenant) in the two ITM DCs. The Splunk infrastructure in each DC will be capable of providing a full logging service in the event of a failure of one DC.

[0317] A new NCSC Security Information and Event Monitoring (SIEM) will be provided based on the use of Splunk Enterprise Security running on top of the Splunk Enterprise service.

[0318] A Splunk log forwarding infrastructure will be deployed at Tier-3 in the same dedicated NCSC security zone (tenant) on the new ITM-R IaaS infrastructure. The Tier-3 Splunk Log Forwarding infrastructure will be a combination of Universal Forwarders (UF), Heavy Forwarders (HF) and an Agent Management (Deployment Server) service. This proposed architecture is depicted in Figure 14.

[0319] Logs are collected from the monitored systems via either the installation of a Splunk Universal Forwarder, the configuration of a Syslog server address of the configuration of the Heavy Forwarder to log into systems and pull the logs.

[13] The NetWitness Broker is a dedicated VM running RSA Netwitness software and should not be confused with the Network Packet Broker (NPB) appliance.

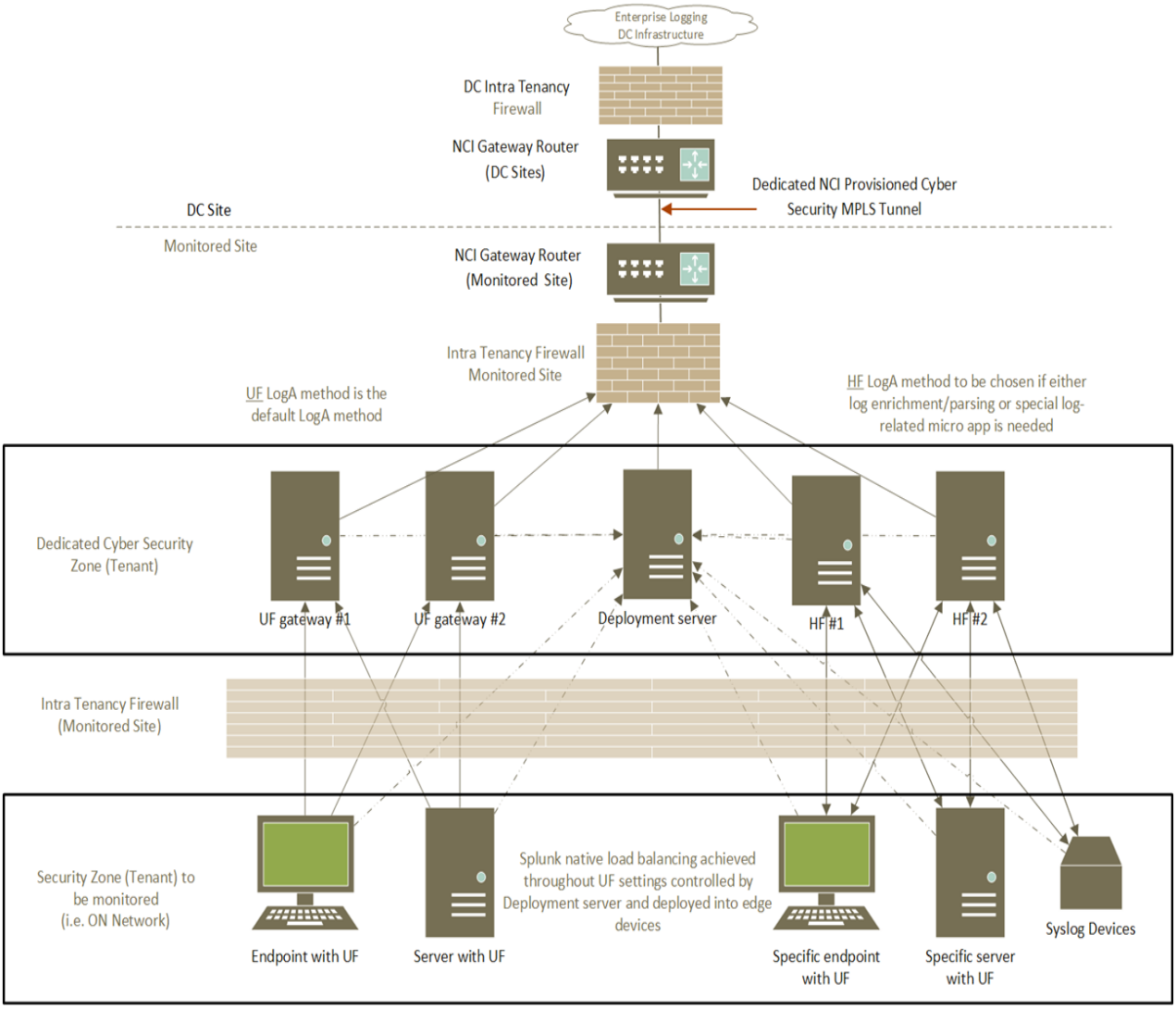

Figure 14 - Proposed ITM-R Enterprise Logging Architecture

C.3. Specific Work to be carried out by the Contractor

C.3.1. Introduction

[0320] The Cyber Security System Refresh (CSSR) project (not part of ITM) is replacing the current NCSC Cyber Security enclave with the new enclave equipment at all DC, EN and SN sites, with the exception of the sites listed in Table 15.

Command	Site Name	Place	Country	Spiral
NATO HQ	NATO HQ	Evere	BE	1
1st NATO Signal Battalion	Schill Barracks	Wesel	GE	3 (option)
3rd NATO Signal Battalion	Szubinska 105	Bydgoszcz	PL	3 (option)
2nd NATO Signal Battalion	Grazzanise Air Base	Grazzanise	IT	3 (option)

Table 15- List of sites without an NCSC Cyber Security Enclave

SOW-1068 The Contractor shall procure and deploy new NCSC Cyber Security Enclaves to the four sites listed in Table 15.

SOW-1069 The Contractor shall procure and upgrade the equipment as described in Table 20 for the SJLSG HQ site listed in Table 19.

SOW-1070 The Contractor shall integrate the NCSC monitoring enclaves with the new IaaS infrastructure at all DC, EN and SN sites, including the 4 new ones, listed in Table 1. Note that Integration means all monitoring services as described in sections C.3.7.2, C.3.9.2, C.3.10.2, C.3.11.2 C.3.12.2 and C.3.14.

[0321] The four new enclaves to be deployed shall be based on the design and configuration of the systems being delivered by the Cyber Security System Refresh (CSSR) project. All relevant documentation and configuration will be provided to the Contractor by the Purchaser. This includes, but is not restricted to, System Designs, Accreditation Paperwork, Test Documentation and Configuration guidance.

[0322] During the implementation of the activities detailed in this Annex, the Contractor shall follow the requirements as described in various sections of this SoW (e.g. Security Accreditation, Test and Acceptance, Configuration Management, Quality Assurance, Integrated Product Support, Documentation Management etc.) and referred in SSS.

[0323] The Contractor shall cooperate with the Purchaser team(s) and third parties as directed by the Purchaser as necessary for the implementation activities.

C.3.2. NCSC Monitoring Enclave Standard Equipment.

[0324] The specific make and model of the equipment to be deployed in the new enclaves is listed in Table 16. The table also indicates whether this is to be procured by the Contractor or by the Purchaser to be handed over to the Contractor.

[0325] The versions of the hardware in Table 16 are listed as an indication of type / model only from October 2021, and should not be seen as a requirement for a specific version if it has been superseded.

Description	Part Number
NetWitness FPC Concentrator	NW S6 SED CORE TP APPL- NO SW LIC (E39S)
NetWitness FPC Decoder	NW S6 SED CORE TP APPL- NO SW LIC (E39S)
FPC Concentrator Storage	NW PV HP 78TB SED (E03J)
FPC Decoder Storage	NW PV HD 96TB SED (E03J)
Management switch	Cisco N9K-C92160YC-X 48P Cisco 1G Copper SFPs x 24 Cisco 1G Fibre SFPs x 8 Cisco 10G Fibre SFPs x 8
HCI Hosting Platform (NCDP)	Dell HCI Node VSAN-RN R7515 AMD 7742 2.25GHz, 64C/128T,256M, 225W,3200 12 x 64GB RDIMM, 3200MT/s 12 x Dell 6.4TB 2.5 SFF Drive 2 x Dell 750GB NVMe Ultra Performance Flash VMware ESXi 7.0 U1 Embedded Image (634-BWZG) OpenManage Integration for VMware vCenter - 1 host increment, 3 year license (634-BJBD) Dual Power Supply
Juniper SRX380 Service Gateway	SRX380-P-SYSJB-AC Juniper SFPs 1G-SR MMF x 4 Juniper SFPs 10G-SR MMF x 4

	Dual Power Supply
Medium Site Packet Broker	Keysight Vision Edge 10S - SYS-E10S-16P-AC
DC Site Packet Broker	Keysight Vision 400 Network Packet Broker - SYS-V400-BASE-AC
Dell KVM	Dell Digital KVM switch 8 port (dMPU108e) 1 x DMPUIQ-VMCHS for Dell SIM for VGA interface 2 x Dell DMPUIQ-SRL for Dell SIM for serial interface 1 x DKMMLED185 – 001 Ingernational English KB
Network Taps	1x TPX-10-SR-50-50
Network Tap Rack Mount	1x RK-FLEX-24
SFP+	Compatible with the Keysight Packet Brokers

Table 16 - Standard NCSC Enclave Equipment

C.3.3. New NCSC Enclaves to be Deployed

SOW-1071 The Contractor shall install the equipment at NATO HQ, based on the specific brands and models described in Table 16 - Standard NCSC Enclave Equipment.

Quantity	Equipment	Procurement Method
2	FPC Concentrator	PFE
4	FPC Decoder	PFE
2	FPC Concentrator Storage	PFE
4	FPC Decoder Storage	PFE
2	Management switch	PFE
2	HCI Nodes (NCDP)	PFE
1	Juniper SRX 380 Service Gateway	PFE
1	Data Centre Packet Broker As per Table 16 - Standard NCSC Enclave Equipment	PFE
1	Dell KVM	PFE
1	RSA NetWitness Virtual Broker	PFE

Table 17 - Equipment to be installed at NATO HQ

SOW-1072 The Contractor shall procure and install the equipment detailed in Table 18 at the three NATO Signal Battalion (NSB) sites listed in Table 15, based on the brands and models as described in Table 16.

Quantity	Equipment	Procurement Method
1	FPC Concentrator	PFE
2	FPC Decoder	PFE
1	FPC Concentrator Storage	PFE
2	FPC Decoder Storage	PFE
2	Management switch As per Table 16 - Standard NCSC Enclave Equipment	Contractor Provided
2	NCDP (HCI virtual hosting) As per Table 16 - Standard NCSC Enclave Equipment	Contractor Provided
1	Juniper SRX 380 Service Gateway As per Table 16 - Standard NCSC Enclave Equipment	Contractor Provided
1	Medium Packet Broker As per Table 16 - Standard NCSC Enclave Equipment	Contractor Provided
1	Dell KVM As per Table 16 - Standard NCSC Enclave Equipment	Contractor Provided

Table 18 - Equipment to be delivered to the 3 signal battalion sites

C.3.4. Additional FPC Hardware at JLSG Ulm

SOW-1073 The Contractor shall upgrade the FPC hardware at the following site listed in Table 19 to bring the configuration in line with the standard NCSC Enclave configuration for an EN.

Command	Site Name	Place	Country	Spiral
HQ Standing Joint Logistics Support Group (SJLSG HQ)	Wilhelmsburg Barracks	Ulm	GE	2 (option)

Table 19 - Site to receive and FPC Upgrade

SOW-1074 The Contractor shall install and configure the equipment detailed in Table 20 at SJLSG HQ.

Quantity	Equipment	Procurement Method
1	FPC Concentrator	PFE
2	FPC Decoder	PFE
1	FPC Concentrator Storage	PFE
2	FPC Decoder Storage	PFE

Table 20 - FPC Equipment to be installed at SJLSG HQ.

C.3.5. Network Taps and Packet Broker SFPs

SOW-1075 The Contractor shall procure 10G network fibre taps and compatible SFPs as described in Table 16 to be installed at every DC, EN and SN sites listed in Table 1, on links as directed by the Purchaser.

Site Type	Equipment	Quantity	Procurement Method
DC	Network taps	10	Contractor Provided
EN	Network taps	6	Contractor Provided
SN	Network taps	6	Contractor Provided
DC	SFPs	20	Contractor Provided
EN	SFPs	12	Contractor Provided
SN	SFPs	12	Contractor Provided
DC	Network Tap Rack Mount	1	Contractor Provided
EN	Network Tap Rack Mount	1	Contractor Provided
SN	Network Tap Rack Mount	1	Contractor Provided

Table 21 – Network taps to be installed at DC, EN and SN sites.

C.3.6. NCSC Monitoring Equipment Specific Requirements

[0326] The following sections describe requirements related to the deployment and configuration of the NCSC Enclave equipment. The requirements for each equipment type is divided into two sections, one relating specifically to the work required to deploy the four new enclaves described in the previous sections and a second one related to the work to be carried out at all sites, including the 4 new enclaves.

C.3.7. Generic Enclave Requirements

C.3.7.1. Generic Enclave Requirements at the four new NCSC Enclave sites only

SOW-1076 The Contractor shall deploy and configure a single pair of redundant switches in each Tier-3 enclave. The Make and Model of switches is listed in Table 16.

SOW-1077 The Contractor shall configure the management port of each physical device installed in the enclave and physically connect it to the management switch.

SOW-1078 The Contractor shall integrate all Cisco Management switch with the Cisco DCNM management service hosted at Tier-2

SOW-1079 The Contractor shall integrate all compatible components of the enclave with the Purchaser's monitoring capability, based on the SolarWinds platform

SOW-1080 The Contractor shall integrate all compatible components of the solution with the Dell OpenManage, hosted at NCSC Tier-2

SOW-1081 The Contractor shall install the KVM in the rack and connect it to the keyboard, video and mouse ports of all devices (servers and appliances).

C.3.7.2. Generic Enclave Requirements all ITM DC, EN and SN sites

SOW-1082 The Contractor shall integrate the new ITM-RC1 infrastructure at the Tier-3 sites with NATO's existing cyber security monitoring capabilities.

C.3.8. NCSC Cyber Defence Platform Requirements

[0327] The NCSC Cyber Defence Platform (NCDP) sub-system is described in section C.2.2.

C.3.8.1. NCSC Cyber Defence Platform at the four new NCSC Enclave sites only

SOW-1083 The Contractor shall deploy the software listed in Table 22 on the HCI Cluster based on configuration guidance provided by the Purchaser.

Component Description	Manufacturer	Qty
VMware vSphere Enterprise Plus for 1 processor	VMware	1
VMware vSAN Advanced for 1 processor	VMware	1
VMware NSX Data Centre Advanced per Processor	VMWare	1

Table 22 - NCDP Hosting Software

SOW-1084 The Contractor shall configure each HCI node in such a manner that all servers have dual connectivity to both enclave switches and be configured to provide failover and high availability.

SOW-1085 The Contractor shall integrate the VMWare HCi-based virtualized environment, deployed on the new enclaves, with the existing NCSC vCenter management service hosted at Tier-2.

SOW-1086 The Contractor shall provision virtual machines on the NCDP HCI based on the resources listed in Table 23.

VM	Role	vCPU	RAM (GB)	NICs	HDD1 (GB)	HDD2 (GB)	Total (GB)
OVA	Nessus Scanner	8	8	2	4.5	100	104.5
OVA	Nessus Agent Manager	8	8 (16 NATO HQ)	2	4.5	100	104.5
OCF	Exterro Child Site Server (CSS)	32	64	2	512	40000	40512
OCF	Exterro Examiner Server	32	64	2	512	0	514
OCF	OCF - Misc. Tools	32	64	2	512	0	512
FPC	FPC Broker (NATO HQ only)	12	64	1	40	1536	1653

Table 23 - NCDP Virtual Machine Hosting Resources

C.3.9. Network Packet Broker and Tap Requirements

[0328] The Network Packet Broker (NPB) and Taps sub-system is described in section C.2.3 and C.2.3.1.

C.3.9.1. Network Packet Broker and Taps at the four new NCSC Enclave sites only

SOW-1087 The Contractor shall install and commission a new Network Packet Broker at each of the four new NCSC enclaves in accordance with a design and configuration to be provided by the Purchaser.

SOW-1088 The make and model for the new DC site is listed in Table 17. This includes a number of connectivity modules as described.

SOW-1089 The make and model for the 3 SN sites is listed in Table 18. This includes a number of connectivity modules as described.

C.3.9.2. Network Packet Broker and Taps at all ITM DC, EN and SN sites

SOW-1090 At every DC, EN and SN site, the Contractor shall provision a 10G fibre connection between a port on the Network Packet Broker (NPB) and a designated switch within the new IaaS infrastructure.

SOW-1091 At every DC, EN and SN site, the Contractor shall configure ERSPAN in the NSX-T layer of the IaaS infrastructure in order to forward packets from selected virtual machines to the NPB, as directed by the Purchaser.

SOW-1092 The Contractor shall procure and install 10G network fibre taps to be installed on links as directed by the Purchaser.

SOW-1093 The Contractor shall procure and install network taps at every DC, EN and SN site in accordance with the quantities listed in Table 21.

SOW-1094 The Contractor shall procure and install SFPs into the Network Packet Brokers and connect the Taps to the SFPs at every site, in accordance with the quantities listed in Table 21.

C.3.10. Enclave VPN/Firewall Requirements

[0329] The Enclave VPN/Firewall system is described in is section C.2.1.

C.3.10.1. Enclave VPN/Firewall activities at the four new NCSC Enclave sites only

SOW-1095 The Contractor shall provide a 10G fibre connection between the Enclave VPN/Firewall and the NATO WAN infrastructure, to provide physical connectivity for the VPN connection to Tier 2.

SOW-1096 With the support of the Purchaser the Contractor shall integrate enclave VPN/Firewall appliance at each site with the Juniper Central Management server installed at Tier-2.

SOW-1097 The Contractor shall coordinate with the NCIA operations staff to ensure that all routing, NAT configuration and Firewall rules are in place to facilitate the VPN connection between the Tier-3 site and Tier-2.

SOW-1098 The Contractor shall configure a VPN between the Juniper VPN/Firewall and the NCSC Tier 2 Juniper VPN Gateway in Mons, using NATO PKI certificates to facilitate authentication and encryption.

C.3.10.2. Enclave VPN/Firewall at all ITM DC, EN and SN sites

SOW-1099 The Contractor shall provision a physical 10G fibre connection between the NCSC Enclave VPN/Firewall and a designated (by the Purchaser) switch within the DC, EN or SN IaaS site infrastructure.

SOW-1100 The Contractor shall configure the NAT and routing at each DC, EN or SN site to ensure that IP network traffic can flow between the NCSC Enclave and the site.

C.3.11. Online Computer Forensics Requirements

[0330] The Online Computer Forensics (OCF) sub-system is described in section C.2.4.

C.3.11.1. Online Computer Forensics at the four new NCSC Enclave sites only

SOW-1101 With the support of the Purchaser, the Contractor shall determine IP/FQDN for the new Tier 3 OCF servers

SOW-1102 The Contractor shall install a new Exterro Child Site Server (CSS)

SOW-1103 The Contractor shall integrate the CSS with the existing Tier 2 central management infrastructure

SOW-1104 The Contractor shall deploy and configure the Known File Filter (KFF) service on the CSS

SOW-1105 The Contractor shall deploy and configure the Exterro Enterprise Examiner service

SOW-1106 The Contractor shall integrate the new OCF servers with NCSC Active Directory

SOW-1107 The Contractor shall integrate the new OCF servers with the Trellix Anti-Virus

SOW-1108 The Contractor shall request, Generate and Deploy NATO PKI certificate for all new Tier 3 OCF servers

C.3.11.2. Online Computer Forensics at all ITM DC, EN and SN sites

SOW-1109 The Contractor shall support firewall rules updates on sites to enable a required traffic between FTK agents on monitored endpoints and the FTK instance in the designated NCSC enclave

SOW-1110 The Contractor shall support GPO updates at the site if determined to be required

SOW-1111 The Contractor shall support changes to routing and NAT configuration

SOW-1112 The Contractor shall support endpoint host FW changes to allow agent communication

SOW-1113 The Contractor shall deploy agents on Windows Servers and Workstations using SCCM

SOW-1114 The Contractor shall deploy Linux agent packages on all Linux servers

SOW-1115 The Contractor shall apply exclusions for the FTK agent to the McAfee (Trellix) EPO server

SOW-1116 The Contractor shall test Agent functionality, based on a test plan to be provided as PFE.

C.3.12. Online Vulnerability Assessment Requirements

[0331] The Online Vulnerability Assessment (OVA) sub-system is described in section C.2.5.

C.3.12.1. Online Vulnerability Assessment at the four new NCSC Enclave sites only

SOW-1117 The Contractor shall install a VM on the NCDP with the Nessus Scanner running on Red Hat Enterprise Linux.

SOW-1118 The Contractor shall install a VM on the NCDP with the Nessus Agent Manger Child Node running on Red Hat Enterprise Linux.

SOW-1119 With the support of the Purchaser, the Contractor shall determine IP/FQDN for the local Nessus Scanner and Agent Manager servers.

SOW-1120 The Contractor shall Request/Generate/Deploy NPKI certificate for the local Nessus Scanner and Nessus Agent Manager servers.

SOW-1121 The Contractor shall configure the Nessus Scanner to be under control of the Tier 2 Central Manager (Tenable.sc).

SOW-1122 The Contractor shall configure the Juniper Enclave firewall rules to allow the required connections, through the VPN, between the Tier 3 hosted Nessus Scanner and Nessus Agent Manager and the Tier 2 Central Manager (Tenable.sc).

C.3.12.2. Online Vulnerability Assessment at all ITM DC, EN and SN sites

SOW-1123 The Contractor shall ensure that all local site routing, Network Address Translation (NAT) and Firewall (both site firewalls and the Juniper SRX enclave firewall) rules are in place to ensure that the OVA server running in the NCSC enclave has TCP/IP network connectivity to all devices to be scanned in the target network, including but not limited to servers, clients, virtualization hosting and networking equipment.

SOW-1124 The Contractor shall deploy Nessus Agents using SCCM on all systems with supported operating systems, as directed by the Purchaser.

SOW-1125 For systems that do not support Nessus Agents, the Contractor shall configure accounts to facilitate authenticated vulnerability scans. Configuration guidance for each individual type of system will be provided by the Purchaser. This includes but is not limited to servers, clients, virtualization hosting and networking equipment.

SOW-1126 The Contractor shall configure the Trellix (formerly McAfee) ENS, via ePO, to allow the OVA scan to bypass the Trellix Intrusion Prevention service on all supported (by Trellix) systems.

SOW-1127 The Contractor shall configure other Endpoint host FW changes to allow scanning

C.3.13. Full Packet Capture Requirements

[0332] The Full Packet Capture (FPC) sub-system is described in section C.2.6.

C.3.13.1. Full Packet Capture at the four new NCSC Enclave sites only

[0333] The FPC Decoders at the existing sites are already connected to the Network Packet Broker and as such there are no FPC requirements related to sites with a pre-existing NCSC enclave. The new Taps connecting the IaaS infrastructure to the Network Packet Broker will ensure traffic from the new infrastructure is collected via the FPC.

SOW-1128 The Contractor shall install and configure two RSA NetWitness Concentrators and four RSA Netwitness Decoders, along with the appropriate attached storage, to NATO HQ DC as listed in Table 17.

SOW-1129 The Contractor shall install an RSA NetWitness Broker as a virtual machine hosted on the NATO HQ NCDP HCI node. Note that the Netwitness Broker is only required at sites with two or more Concentrators and facilitates searches distributed searches across multiple Concentrators installed at the same site.

SOW-1130 The Contractor shall install and configure one RSA NetWitness Concentrator and two RSA Netwitness Decoders, along with the appropriate attached storage, at each SN site as listed in Table 18.

SOW-1131 The Contractor shall connect all of the RSA NetWitness appliance Integrated Dell Remote Access Controller (IDRAC) ports to the local enclave switch and configure the IDRAC service.

SOW-1132 The Contractor shall upgrade the software of the RSA Netwitness appliances to the same version as the FPC central management.

SOW-1133 The Contractor shall integrate the newly deployed Decoders, Concentrators and Netwitness Brokers with the RSA central management (Event Stream Analysis, Admin and Netwitness Broker) servers, installed at Tier 2.

SOW-1134 The Contractor shall connect the RSA NetWitness appliance Integrated Dell Remote Access Controller (IDRAC) ports of all Decoders and Concentrators to the local enclave management switch and configure the IDRAC service.

SOW-1135 For each FPC component (Decoder, Concentrator and NetWitness Broker) the Contractor shall replace the self-signed certificate (used for the https based management GUI) with a certificate from the NATO PKI.

SOW-1136 The Contractor shall connect the RSA Netwitness Decoder traffic monitoring ports to the local Network Packet Broker via 10Gbps cable.

SOW-1137 The Contractor shall replicate the existing configuration of the Decoders, Concentrators and NetWitness Brokers to forward system log messages to Splunk via syslog.

SOW-1138 The Contractor shall integrate the new FPC Concentrators, Decoders with the NCIRC Security Incident Information and Event Management (SIEM) based on Splunk Enterprise Security (ES).

SOW-1139 The Contractor shall replicate the existing mechanism to allow PCAPs to be downloaded directly from the Splunk PCAP Management Dashboard.

SOW-1140 The Contractor shall install the latest GeoIP database to all Decoders, The Database shall be provided as PFE in MMDB format.

C.3.14. Enterprise Logging Requirements at all ITM DC, EN and SN sites

SOW-1141 For Activity Groups 1 and 2 the contractor shall configure forward logs (as designated by the Purchaser) to the legacy CSSR log collection infrastructure.

[0334] The Enterprise Logging (EL) service will be a new service to be deployed by the Contractor at all ITM sites as described in section C.2.8. EL will be deployed on the new ITM-RC1 IaaS Infrastructure, so this section has no separate requirements for existing and new sites.

SOW-1142 For Activity Groups 3 and 4 the Contractor shall deploy a Splunk Log Forwarding service, as described in section C.2.8, on the dedicated NCSC security zone at each of the ITM sites, with the exception of the two DCs[14]. Configuration guidance shall be provided by the Purchaser.

SOW-1143 The resources to be allocated for the Splunk forwarding infrastructure is provided in Table 24.

Role	Number	vCPU	RAM (GB)	NICs	HDD1 (GB)	HDD2 (GB)	Total (GB)
Universal Forwarders	2	16	32	2	30	5120	5200
Heavy Forwarders	2	16	32	2	30	5120	5200
Deployment Server	1	8	32	2	30	256	328

Table 24 - Hosting Requirements for the Splunk virtual servers.

[14] The Splunk forwarding infrastructure at the DCs will be provisioned by a dedicated EL contractor.

SOW-1144 The Contractor shall configure log forwarding from all WP07 provisioned servers, networking equipment and security devices to the Splunk Log Forwarding Infrastructure at each site. This will be a combination of the installation of Universal Forwarders, Syslog and Configuration of the Heavy Forwarders to pull logs. Configuration details will be provided by the Purchaser and all configuration changes will be made via the Splunk Deployment server.

Annex D REFERENCES AND APPLICABLE DOCUMENTS[15]

D.1. References

SOW-1145 Appendix 6 lists the references mentioned in this SoW. The Contractor shall use the information from these references as input for their design and implementation activities. Unless otherwise specified, all references point to the latest published version of the documents.

SOW-1146 The Contractor shall be aware and comply below mentioned documents throughout the Contract. These are also listed in Appendix 6.

D.2. Other NATO Documents

- GEN IPv4
- GEN IPv6

D.3. Non-NATO Standards

- RIPE-772

D.4. Security Documentation

SOW-1147 The following NATO Security Policies and supporting documents shall apply throughout the project (all NR).

D.4.1. SECAN Doctrine and Information Publication

- SDIP-29/2
- SDIP-28/1
- SDIP 293/1

D.4.2. NATO Security Policy and Information Assurance Documents

- C-M(2015)0041 REV2
- AC/322-D(2019)0038 (INV)
- AC/322-D/0049-REV1
- AC/322-D(2019)0021
- AC/322-D(2004)0024-REV3-COR1
- AC/322-D(2015)0029
- AC/35-D/2003-REV5
- AC/35–D/2000–REV8
- AC/35–D/2001–REV3
- AC/35–D/2002–REV4
- AC/35–D/2002–REV5

[15] References without an explicit classification (e.g. NATO Restricted) can be assumed as 'NATO Unclassified'.

- AC/322-N(2011)0130
- AC/35-D/1021-REV3
- AC/322-D/0030-REV5
- AC/322-D/0047-REV2 (INV)
- AC/322-D(2004)0030
- AC/322-D(2004)0019(INV)
- AC/322-D(2012)0012
- AC/322-D(2005)0044
- AC/35-D/2005-REV3
- AC/322 D(2019)0032 REV2
- AC/322 D(2016)0001
- AC/35-D/2004-REV3
- AC/35-N(2015)0022 (CISS)
- NCSC SEC CONFIG CAT
- C-M(2002)49-REV1
- AC/35-D/1034
- AC/322-D/0048-REV3
- AC/322-D(2019)0041 (INV)
- AC/322-D(2017)0016 (INV)
- C-M(2002)60
- C-M(2007)0118

D.5. NATO Security Accreditation Templates[16]

- TPL SAP
- TPL CIS DESC
- TPL SRA REP
- TPL SSRS
- TPL SISRS
- GEN SecOPs
- GEN STVP
- TPL AFT

[16] NATO Security Accreditation Templates will be provided after EDC.