IFB-CO-14314-IEG-C

INFORMATION EXCHANGE GATEWAY (IEG) SOLUTIONS BETWEEN NATO SECRET AND NATO-LED MISSION SECRET DOMAINS

CP 9C0150 – SERIAL 2014/0IS03102

BOOK II - PART IV

STATEMENT OF WORK (SOW)

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

SECTION 1: INTRODUCTION

1.1. Purpose

1.1.1. NATO requires a data loss prevention capability, to prevent the unauthorised release of data from the NATO SECRET to a NATO/xFOR SECRET domain. The aim of this procurement project is to industrialize the existing prototype capabilities, thereby reducing risks to security, providing resilience, improving control, management and maintenance aspects, while adhering to newly approved NATO Standards.

1.1.2. The Information Exchange Gateway Scenario C (hereafter called IEG-C) project will provide:

1.1.2.1. Support for Information Exchange Services of information and real time data between the NATO Secret core network (which comprise NATO Commands, Agencies, and connected NATO Nations) and NATO/xFOR Secret networks (for NATO Responses Forces, NATO-led Coalition Exercises and Operations).

1.1.2.2. These services will be provided by a gateway system, which should be able to scale based on the needs of the supported mission, available bandwidth and required response times.

1.1.2.3. These gateways may be in deployed locations but will be centrally managed, monitored and controlled, while physical maintenance will be undertaken by local staff.

1.1.2.4. The main objective of the gateway is to protect NATO Secret (NS) information and CIS while supporting the required interactions between the NS and mission secret CIS. The gateway will mediate exchange of data for both ‘core’ and ‘functional’ services and will, whenever possible, conform to NATO Standardization Agreements (STANAGs) 4774 and 4778[1].

[SOW-1] *The Contractor SHALL take due account of all the elements of purpose described in this SOW and ensure during the execution of the contract that the purpose described in this SOW is completely addressed in the products and services provided.*

1.2. System Description

[1] References provided in Section 2

1.2.1. The IEG-C is a Data Loss Prevention bi-directional guard at the interface between the (or “a”) NATO SECRET (NS) domain and a NATO-led ‘mission’ domain, such as ‘Resolute Support’ or ‘KFOR’. The guard approves or rejects the transmission of data between the two security domains based on either a STANAG-compliant trusted classification label, such as ‘NATO <classification> Releasable to <mission>’ or trusted source to trusted destination mediated by firewall rule sets. The reason for the trusted source/destination path is that not all current NATO services and apps are ‘label aware’.

1.2.2. The overall requirement for the IEG-C is to allow a mission command structure to operate the full range of military command and control IT functions where the staff and users include NATO and non-NATO mission partners. All non-NATO mission partners will have security agreements with NATO such that they are authorised to access information classified up to NATO SECRET Releasable to <Mission>. In such a situation, two IT systems are provided; one classified ‘NATO SECRET’ to process information that is required for the mission but not releasable to non-NATO partners (typically J2 data) and one classified <Mission> SECRET that is accessible to all authorised mission partners, both NATO and non-NATO. For practical purposes, the majority of users are typically provided with access to the mission IT system. Users in the NS domain (both local and in the static NS domain) can be granted access to services and data in the <Mission> SECRET domain, but users in the <Mission> SECRET domain are prevented from any access to the NS domain.

1.2.3. The NATO requirement for users with elevated privileges (e.g. system administrators) to have a security clearance higher than the level of the system they operate means that only NATO cleared users can be granted such permissions. Where both NS and <Mission> SECRET IT systems are provided, data transfer requirements typically require the IEG-C to be deployed to the mission HQ so that LAN-level transfer speeds can be provided between the two IT systems. Where a mission has no NS component, the IEG-C can be located at the supporting HQ at the reach-back or mission anchor location. Possible configurations are shown below in Figure 1: IEG-C Modes of Operation:

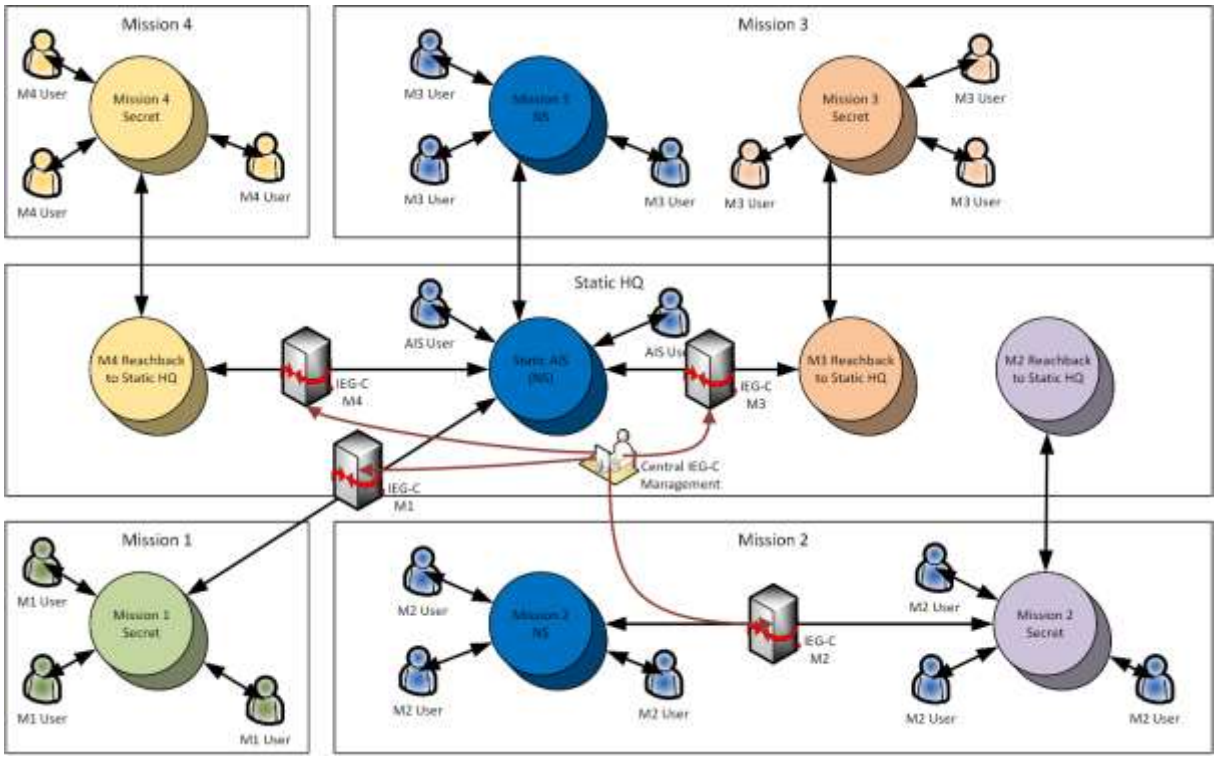


Figure 1: IEG-C Modes of Operation

1.2.4. The IEG-C requirement and operational prototype solutions have evolved over many years to a situation where there are two main variants in operation today; those with a 'DMZ' and those without. In the 'without' case, a firewall and a mail guard are connected in parallel between the two security domains. The 'DMZ' configuration adds a third domain mediated by the firewall that contains the mail guard and other guards and proxies, such as an XML web-guard and web reverse proxy.

1.2.5. The objective of the IEG-C project is to modernise and standardise the configurations to a single layout with a consolidated management suite like below in Figure 2: IEG-C Components and to add additional features required by, for instance, evolving security protection measures. It should be noted that configurations will never be fully identical as different missions will always operate different C2 tools and information exchange requirements due to the nature of the operation (Maritime-based, Land-based etc.). So there will be differences in the firewall rule sets and, of course, all missions have specific releasability labels.

Figure 2: IEG-C Components

1.2.6. As the IEG-C is a data release guard, it does not support any on-line users and, other than log files, only supports transient data. All of the IEG-C components will be centrally managed by a Border Protection Services management team from a central location.

1.2.7. The logical layout and data flows of the IEG-C is shown below in Figure 3: IEG-C Data Flows. Features to note are that physically separate firewalls are required for the interface to the NS domain and the interface to the <Mission> SECRET domain and that separate IEG-Cs are required for each mission. The diagram is illustrative of the data flows between the NS and <Mission> SECRET domain and shows both operational and management streams.

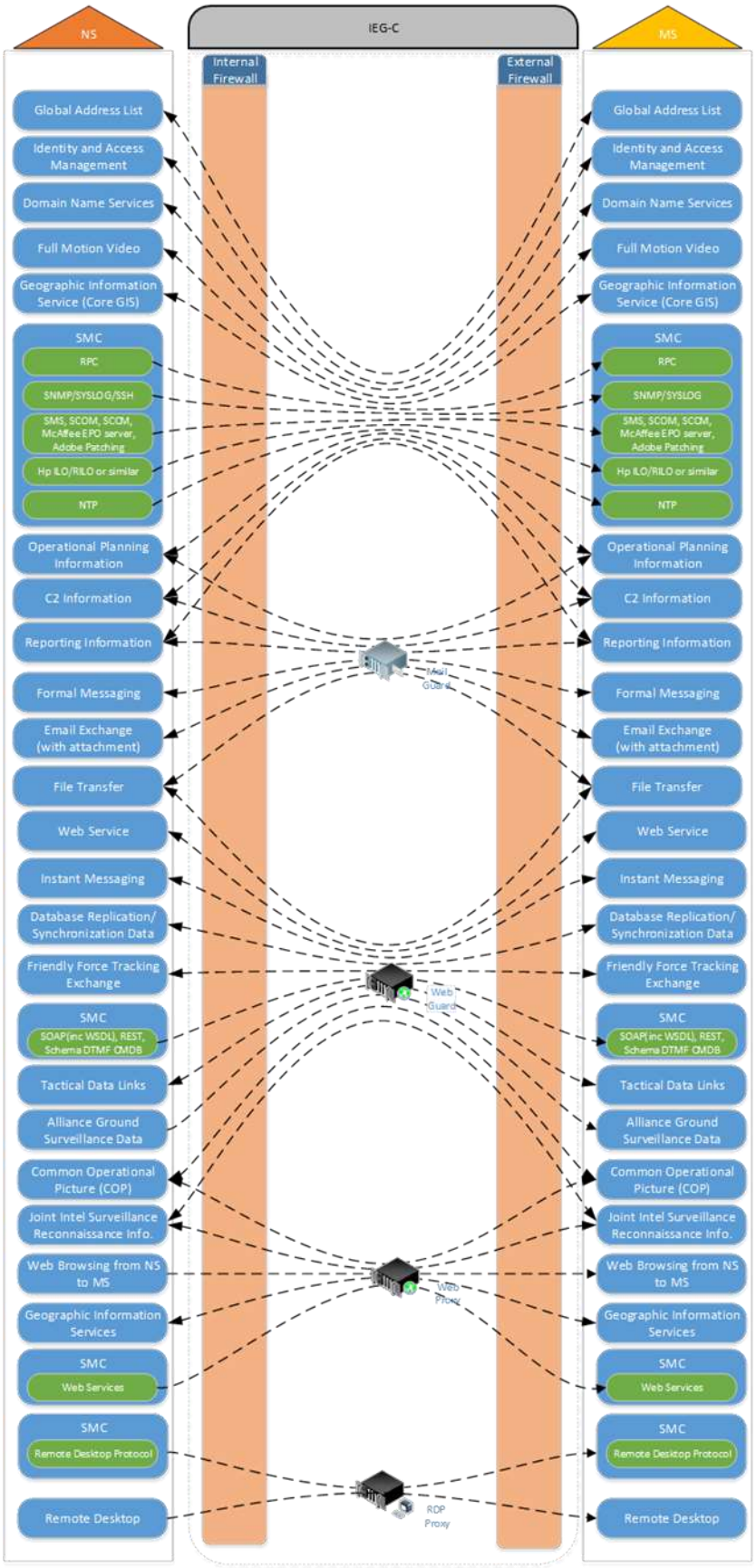


Figure 3: IEG-C Data Flows

1.3. Scope

1.3.1. The project will implement eleven (11) IEG-C systems in six (6) locations (listed in Annex B.1), where prototype gateways have been already installed to meet NATO requirements for boundary protection, including one (1) reference system and a management facility to be installed in the first location in the NCI Agency at SHAPE.

1.3.2. The project may also implement optional installations (7 IEG-C systems in 7 locations). Six (6) of these options will be exercised depending on NATO future operational requirements and the 7th one, a virtualized instance, will be exercised when funding and specifications finalize to support NCIA IV&V activities. Options are described in SECTION 16.

1.3.3. Finally the project will remove the legacy prototypes it intends to replace, including those in 3 locations that will not receive new gateways.

1.3.4. This Statement of Work (SOW) describes requirements, as well as development, delivery and implementation processes for the IEG-C through a series of work packages as shown below in Table 1: Work Packages:

Number[2]	Name
2	Phase 1 Initial Design and Build
2.1	Design and Build to Factory Acceptance
2.2	Installation of the Reference System
2.3	Integration into NATO Enterprise and Management Capability
3	Installation of Operational Gateways
4	Decommissioning legacy gateways (3 sites)
6	Hardware
7	Cyber Security Monitoring (former NCIRC)

Table 1: Work Packages

[SOW-2] *The Contractor SHALL deliver the **IEG-C** as detailed in the System Requirement Specifications (SRS).*

[2] WP1 was for the IEG-C Target architecture and is already executed

1.3.5. This Statement of Work (SOW) describes the responsibilities of and activities to be conducted by the Contractor to meet the requirements of the IEG-C project.

[SOW-3] *The Contractor SHALL provide all necessary resources to include services, personnel, materials, components, equipment[3], data[4] and documentation needed to accomplish all the tasks described in the SOW, to meet all the requirements of the SOW (including annexes) and to fulfil all other Contract provisions.*

[SOW-4] *The documents listed in SECTION 2: Applicable Documents will be revised over time. The Contractor SHALL always use the current version of each document.*

[SOW-5] *The Contractor SHALL be aware and comply with above mentioned documents throughout the Contract.*

1.3.6. Except otherwise stated, the delivery dates of the associated deliverables are provided in the Schedule of Supplies and Services (SSS) document.

[SOW-6] *The Contractor SHALL provide project management services.*

[SOW-7] *The Contractor SHALL provide systems engineering services to cover:*

- *Requirements review;*
- *System design and*
- *System Integration.*

[SOW-8] *The Contractor SHALL provide test, verification and validation services to prove the system Product Baseline is meeting its requirements.*

[SOW-9] *The Contractor SHALL fully document the design, operation, and maintenance of IEG-C by providing the required manuals, operational procedures, supporting technical data, computer software and drawings required by the Contract.*

[SOW-10] *The Contractor SHALL conduct all necessary activities to obtain Security Accreditation at the NATO SECRET (NS) and applicable Mission SECRET (MS) levels for all installed sites/instances.*

[SOW-11] *The Contractor SHALL provide System Services as described in SECTION 7*

[SOW-12] *The Contractor SHALL co-ordinate with the Purchaser to ensure that the site preparation activities are completed in accordance with the installation requirements of the delivered system.*

[SOW-13] *The Contractor SHALL procure and prepare the system components, as agreed in this contract, for delivery to the sites specified in this Contract.*

1.1.1. [3] Lists will be finalized in PDR milestone (PRM 2, EDC+3). Detailed instructions are provided at 16.1.3~~16.2~~ WP 6 and WP 7 (paragraphs 16.2 and 16.3 respectively) are not optional and are included in the main scope of the project.

WP 6 Hardware~~WP 6 Hardware~~.

[4] NATO specific data required for System or Component Configuration will be provided by the NCI Agency

[SOW-14] *The Contractor SHALL deliver the required software to the prepared sites, together with those that may be provided by the customer as PFE, and execute installation/deployment, on-site testing, training, and activation.*

[SOW-15] *The Contractor SHALL provide support to application and service management integration*

[SOW-16] *The Contractor SHALL provide Integrated Logistics Support (ILS), including training services, as described in SECTION 6 Integrated Logistics Support (ILS).*

[SOW-17] *The Contractor SHALL provide operation and maintenance support with appropriate service management interfaces both at information (monitoring / reporting) and process (request / incident) level (see Annex F Maintenance and Support Concept (After FSA)).*

[SOW-18] *The Contractor SHALL comply with all overarching requirements as described in the SOW (Testing process, Site survey process, Quality Assurance, Configuration Management).*

[SOW-19] *The Contractor SHALL meet or "exceed" the Notional schedule (see 3.2: Notional schedule).*

1.4. IEG-C Solution Constraints

1.4.1. The project will include a number of optional sites, to be confirmed at a later stage, depending on future operational requirements.

1.4.2. The aforementioned IEG-C Services shall include in particular, but will not be limited to:

- Text Chat
- Electronic mail
- Directory Services
- Web Services
- Common Operational Picture Data
- Tactical Data Links data
- Remote desktop services
- Video streams

1.4.3. IEG-C will utilise certificates provided by the NATO Public Key Infrastructure (NPKI) service.

1.4.4. The IEG-C as a system integrated in the NATO Enterprise infrastructure shall allow for automatic and seamless failover between multiple IEG-C gateways properly setup.

1.4.5. Reserved

1.4.6. Security enforcing products shall be evaluated in accordance with NATO Security Policy and supporting directives.

1.5. Statement of Work (SOW) organisation

1.5.1. This SOW describes the responsibilities of and activities to be conducted by the Contractor to meet the requirements of the IEG-C contract.

1.5.2. Section Relevance

1.5.2.1. SECTION 2 defines the applicable documents.

1.5.2.2. SECTION 3 to SECTION 15, as well as the Annexes, define requirements of this Contract.

1.5.3. SECTION 16 describes the Options of this Contract.

1.5.4. Standards for Interpretation of the SOW:

1.5.4.1. The use of shall, should and will is defined as follows:

1.5.4.1.1. SHALL: This requirement is mandatory and must be implemented by the contractor.

1.5.4.1.2. SHALL NOT: means that the definition is an absolute prohibition of the specification.

1.5.4.1.3. WILL: This term is not implemented within the System Requirements Specification (SRS) requirements.

1.5.4.1.4. SHOULD: This term is implemented within the SRS requirements.

1.5.4.2. The words “preliminary” or “initial” or “first draft” for documents referenced in this SOW that need to be produced by the Contractor mean a document at 60% or more maturity.

1.5.4.3. This SOW invokes a variety of Standard NATO 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.

1.5.4.4. Where a national or international standard exists that is not specifically referenced in the STANAGs (and underpinning documents) or MIL-STDs as being equivalent, the Contractor may propose to utilise such a standard if he can demonstrate to the satisfaction of the Purchaser that such a standard is equivalent to the STANAGs or MIL-STD in question.

1.5.4.5. The Purchaser, however, reserves the right to deny such a request and demand performance in accordance with the standard cited in the SOW.

1.5.5. An Overall Project Schedule is provided in Section 3.2.

SECTION 2: APPLICABLE DOCUMENTS

[SOW-20] *The Contractor SHALL be aware and comply with the documents listed in SECTION 2 throughout the Contract.*

2.1. NATO Documents

2.1.1. Security Documents

Abbreviation	Full document Name and Reference
AC/322-D/0030-REV5	INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS)
AC/322-D/0047-REV2 (INV)	"INFOSEC Technical & Implementation Directive On Cryptographic Security And Cryptographic Mechanisms"
AC/322-D(2017)0016 (INV)	Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products
AC/322-N(2014)0158-ADD3	Selection and Installation of Equipment for the Processing of Classified Information
AD 070-005	ACO Communication and Information Systems (CIS) Security
AC/35-D/1017-REV3	Guidelines for Security Risk Management of CIS
AC/35-D/1021-REV3	Guidelines for the security accreditation of communication and information systems (CIS), 31 January 2012
AC/35-D/2004-REV3	Primary Directive on CIS Security, 15 November 2013
AC/35-D/2005-REV3	Management Directive on CIS Security
AC/322-D(2004)0030	INFOSEC Technical And Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools (ST)
NS Reference Baseline	NATO SECRET CIS Security Reference Baseline – Security Mechanisms (SMs) Requirements for Core and Site Services
AC/322-D/0048-REV3	Technical and Implementation Directive on CIS Security
C-M(2002)49-COR12	Security Within The North Atlantic Treaty Organisation
AC/35-D/1030, 2005	Guidelines on Physical Security
AC/35-D/1014-REV3	Guidelines for the Structure and Content of Security Operating Procedures
AC/35-D/2001-REV3	Directive on Physical Security
AC/35-D/2002-REV5	Directive on the Security of NATO Classified Information
SDIP-27/2	NATO TEMPEST Requirements and Evaluation Procedures
SDIP-28/1	NATO Zoning Procedures

SDIP-29/2	Selection and Installation of Equipment for the Processing of Classified Information
PKE PP 2.8	U.S. Government Basic Robustness Public Key- Enabled Applications Protection Profiles

2.1.2. Quality Assurance Documents

Abbreviation	Full document Name and Reference
STANAG 4107 – Edition 11	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications (AQAP) Edition 11, dated 16 Jan 19, and underpinning AQAPs

2.1.3. Configuration Management Documents

Abbreviation	Full document Name and Reference
STANAG 4427 – Edition 3	Configuration Management In System Lifecycle Management – ACMP-2000 edition A & ACMP-2009 Edition A & ACMP-2100 Edition A, dated 18 Dec 14, and underpinning Allied Configuration Management Publications (ACMPs)
NCI Agency AI 06.03.01, 2015	NATO Communications and Information Agency - Agency Instruction 06.03.01, "Identification of Software Assets", 2015
NCI Agency SOP 23.01	Enterprise IT Change Management
NSO AAITP-09	NATO STANDARD BARCODE HANDBOOK

2.1.4. Technical Guidance

Abbreviation	Full document Name and Reference
FMN SI Informal Messaging	FMN Spiral 1 Service Instructions for Informal Messaging, 18th February 2016
INSTR TECH 06.02.01	Service Interface Profile for Security Services, 4th February 2015
INSTR TECH 06.02.02	Service Interface Profile for REST Security Services, 4th February 2015
INSTR TECH 06.02.06	Service Interface Profile for Messaging (SOAP), 4th February 2015
INSTR TECH 06.02.07	Service Interface Profile for REST Messaging, 4th February 2015

NAC AC/322-D(2004)0019(INV), 2004	North Atlantic Council Document AC/322-D(2004)0019(INV), “INFOSEC Technical and Implementation Guidance for the Protection of CIS from Malicious Software”, March 2004
AC/322-D(2004)0024-REV3-COR1, 2018	North Atlantic Council Document AC/322-D(2004)0024-REV3-COR1 “CIS Security Technical And Implementation Directive On The NATO PKI Certificate Policy”, April 2018
AC/322-D(2007)0002-REV1, 2015	North Atlantic Council Document AC/322-D(2007)0002-REV1, “CIS Security Technical And Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects”, March 2015
AC/35-D/1032, 2005	North Atlantic Council Document AC/35-D/1032, 2005 “Guidelines on the Security of Information”, May 2005
NCIA RD-3381, 2012	NATO Communications and Information Agency, Reference Document 3381, “High Level Design for the NATO High Assurance Automated Guard”, April 2012
NCIA TN-1485 v1.1, 2012	NATO Communications and Information Agency, “Common Criteria (CC) Protection Profile (PP) for a Medium Assurance NATO XML-Labelling Guard, Version 1.1”, K. Wrona, S. Oudkerk, December 2012
NC3A TN-1486, 2012	NATO Consultation, Command and Control Agency Technical Note 1486, “NATO Content Inspection Policy Enforcement Framework Functional Specification”, A. Ross, S. Oudkerk, April 2012.
NC3B AC/322-D(2019)0034 (INV), 2019	NATO C3 Board AC/322-D(2019)0034 (INV), "C3 Taxonomy Perspective Baseline 23.1", 2019
NCIA SMC TA, 2018	NATO Communications and Information Agency, "Target Architecture - Enterprise Service Management and Control", 2018
NCIA TR-2012-SPW008418-29, 2014	NATO Communications and Information Agency , “Cryptographic Access Control In Support Of Object Level Protection”, S. Oudkerk, K Wrona, February 2014
NC3A TR/2012/SPW007959/03	NATO Consultation, Command and Control Agency , Technical Report, “Content Inspection Policy Enforcement Profile for a Medium Assurance NATO XML-Labelling Guard”, April 2012.
NCIA TR/2016/NSE010871/01, 2017	NATO Communications and Information Agency , , “Information Exchange Gateway Scenario C Phase 1: Target Architecture – Final”, IEG-C Team, January 2017
[NCI Agency TR/2017/NCB010400/12, 2017]	NATO Communications and Information (NCI) Agency Technical Report 2017/NCB010400/12, “NATO Enterprise Security Monitoring Guidance Version 1.0”, Sébastien Gay, Philippe Lagadec, Jean-Francois Agneessens, Nikolaos Virvilis-Kollitiris, NCI Agency, The Hague, The Netherlands, June 2017 (NATO RESTRICTED).
NAC AC/322-D(2012)0022, 2013	North Atlantic Council, Consultation Command and Control Board (C3B)“Technical Implementation Guidance on

	Cryptographic Mechanisms in Support of Cryptographic Services", January 2013 (NATO RESTRICTED)

2.1.5. Standard Guidance

Abbreviation	Full document Name and Reference
STANAG 1059	Letter Codes for Geographical Entities
STANAG 4774	Confidentiality Metadata Label Syntax
STANAG 4778	Metadata Binding Mechanism
STANAG 4778 SRD.2	Standard Related Document SRD.2 "Binding Profiles
NATO STANAG 6001, 2014	NATO Standardisation Agreement 6001, "Language Proficiency Levels", Ed. 5, 2014
MILSTD810, 2000	Environmental Engineering Considerations and Laboratory Tests
AECTP300, 1998	Climatic Environmental Tests
MILSTD461E, 1999	EMC Testing

2.1.6. NATO Templates

Abbreviation	Full document Name and Reference
[NTEMP-1]	Interface Control Document template
[SRA template]	Security Risk Assessment (SRA) Report template
[STVR template]	Security Test and Verification Report template
[SISRS template]	System Interconnection Security Requirements Statement (SISRS) template
[STVP template]	

2.1.7. Others

Abbreviation	Full document Name and Reference
IEG-C description	Information Exchange Gateway Scenario C (IEG-C) description
IEG-C SAP	NATO Security Accreditation Plan (SAP) for Information Exchange Gateway Scenario C (IEG-C)
NATO VIG v3	NATO Visual Identity Guidelines Version 3 (online: https://www.nato.int/vigs/pdf/NATO-VIGs-2016-en.pdf)

2.2. Non-NATO Documents

Abbreviation	Full document Name and Reference
AIA/ASD SX000i, 2016	Aerospace Industries Association/Aerospace and Defence Industries Association of Europe SX000i, "International guide for the use of the S-Series Integrated Logistic Support (ILS) specifications (issue 1.1)", 2016
AIA/ASD S3000L, 2014	Aerospace Industries Association/Aerospace and Defence Industries Association of Europe S3000L - International specification for Logistics Support Analysis – LSA (issue 1.1), 2014
EVM Practice Standard	Practice Standard for Earned Value Management (2011), Project Management Institute
IETF RFC 791, 1981	Internet Engineering Task Force (IETF) Request For Comments (RFC) 791, “Internet Protocol, DARPA Internet Program Protocol Specification”, September 1981.
IETF RFC 854, 1983	Internet Engineering Task Force (IETF) Request For Comments (RFC) 854, “Telnet Protocol Specification”, May, 1983
IETF RFC 959, 1985	Internet Engineering Task Force (IETF) Request For Comments (RFC) 959, “File Transfer Protocol (FTP)”, October 1985
IETF RFC 1983, 1996	Internet Engineering Task Force (IETF) Request For Comments (RFC) 1983, “Internet Users' Glossary”, August 1996
IETF RFC 2119, 1997	Internet Engineering Task Force Request for Comments 2119, "Key Words for Use in RFCs to Indicate Requirement Levels", 1997
IETF RFC 2312, 1998	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2312, “S/MIME Version 2 Certificate Handling”, March 1998.
IETF RFC 2789, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2789, “Mail Monitoring MIB”, March 2000.
IETF RFC 2818, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2818, “HTTP Over TLS”, May 2000.
IETF RFC 2865, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2865, “Remote Authentication Dial In User Service (RADIUS)”, June 2000.
IETF RFC 3339, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3339, “Date and Time on the Internet: Timestamps”, July 2002.
IETF RFC 3410 – 3418, 2002	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3410 through 3418, “S/MIME Version 2 Certificate Handling Introduction and Applicability Statements for Internet Standard Management Framework”, December 2002.
IETF RFC 3461, 2003	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3461, “Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)”, January 2003.

IETF RFC 3464, 2003	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3461, “An Extensible Message Format for Delivery Status Notifications”, January 2003”, January 2003.
IETF RFC 4251, 2006	Internet Engineering Task Force (IETF) Request For Comments (RFC) 4251, “The Secure Shell (SSH) Protocol Architecture”, January 2006.
IETF RFC 4253, 2006	Internet Engineering Task Force (IETF) Request For Comments (RFC) 4253, “The Secure Shell (SSH) Transport Layer Protocol”, January 2006.
IETF RFC 4510-4519, 2006	Internet Engineering Task Force (IETF) Request For Comments (RFC) 4510 through 4519, “Lightweight Directory Access Protocol (LDAP)”, June 2006.
IETF RFC 5280, 2008	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008.
IETF RFC 5321, 2008	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5321, “Simple Mail Transfer Protocol”, October 2008.
IETF RFC 5322, 2008	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5322, “Internet Message Format”, October 2008.
IETF RFC 5424, 2009	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5424, “The Syslog Protocol”, March 2009.
IETF RFC 5652, 2009	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5652, “Cryptographic Message Syntax (CMS)”, September 2009.
IETF RFC 6125, 2011	Internet Engineering Task Force (IETF) Request For Comments (RFC) 6125, “Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)”, March 2011.
IETF RFC 6353, 2011	Internet Engineering Task Force (IETF) Request For Comments (RFC) 6353, “”,
IETF RFC 6960, 2013	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2818, “HTTP Over TLS”, May 2000.
IETF RFC 7030, 2013	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7030, “Enrolment over Security Transport” (EST).
IETF RFC 7230, 2014	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7230, “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing”, June 2014.
IETF RFC 7231, 2014	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7231, “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”, June 2014.
IETF RFC 7414, 2015	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7414, “A Roadmap for Transmission Control Protocol (TCP) Specification Documents”, February 2015.

IETF RFC 7525, 2015	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7525, “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”, May 2015
IETF RFC 7540, 2015	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7540, “Hypertext Transfer Protocol Version 2 (HHTP/2)”, May 2015.
IETF RFC 7817, 2016	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7817, “Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols”, March 2016
IETF RFC 8200, 2017	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2460, “Internet Protocol, Version 6 (IPv6) Specification”, July 2017.
IETF RFC 8446, 2018	Internet Engineering Task Force (IETF) Request For Comments (RFC) 8446, “The Transport Layer Security (TLS) Protocol Version 1.3”, August 2018.
IETF RFC 8550, 2019	Internet Engineering Task Force (IETF) Request For Comments (RFC) 8550, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling”, April 2019.
IETF RFC 8551, 2019	Internet Engineering Task Force (IETF) Request For Comments (RFC) 8551, “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification”, April 2019.
IPMI V2.0, 2013	Intel, Hewlett-Packard, NEC, Dell “IPMI – Intelligent Platform Management Interface Specification Second Generation, v2.0” Document Revision 1.1, October 2013
ISO 9000, 2015	International Organization for Standardization 9000 Series, "Quality Management Principles (Version 2015)", 2015
ISO 10012, 2003	International Organization for Standardization 10012 (Version 2003), "Measurement Management Systems – Requirements for measurement processes and measuring equipment", 2003
ISO/IEC 12207, 2017	International Organization for Standardization/International Electrotechnical Commission 12207, "Information Technology – Software Lifecycle Processes", 2008
ISO/IEC 25010, 2011	International Organization for Standardization/International Electrotechnical Commission 25010, "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models", 2011
ISO/IEC/IEEE 29119, 2013	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers 29119-Part 1, "Concepts and definitions. Part 2 Test processes. Part 3 Test documentation", 2013
ISO/IEC 15408, v.3.1	Common Criteria for Information Technology Security Evaluation

ITIL v3, 2007	Office of Government Commerce, "Information Technology Infrastructure Library (ITIL) V.3", 2007
MIL-STD 882E, 2011	US Department of Defense Military Standard 882E, "System Safety", 2011
NIAP PP_APP_V.1.2, 2016	Protection Profile for Application Software Version 1.2
NIAP PP_OS_V.4.1, 2016	Protection Profile for General Purpose Operating Systems
NIAP CPP_FW_V.1.0, 2015	Collaborative Protection Profile for Stateful Traffic Filter Firewalls
NIAP CPP_ND_V.1.0,2015	Collaborative Protection Profile for Network Devices
NIAP PP_NDCP_IPP_EP_V .2.1, 2016	Collaborative Protection Profile for Network Devices/Collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS)
NIAP PP_ESM_V.2.1, 2013	Standard Protection Profile for Enterprise Security Management Policy Management
NIAP PP_ESM_AC_V.2.1, 2013	Standard Protection Profile for Enterprise Security Management Access Control
RDP Overview, 2019	“Remote Desktop Services Protocols Overview”, May 2019, available at: https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-RDSOD/%5bMS-RDSOD%5d.pdf
W3C SOAP 1.1, 2000	World Wide Web Consortium, Note, “Simple Object Access Protocol (SOAP) 1.1”, May 2000
W3C SOAP 1.2, 2007	World Wide Web Consortium, Recommendation, “SOAP Version 1.2 Part 1: Messaging Framework”, April 2007
W3C Canonical XML Version 1,1, 2008	World Wide Web Consortium, Recommendation, “Canonical XML Version 1,1”, May 2008
W3C XML Schema 1.0, 2004	XML Schema Definition Language (XSD) 1.0, 2004
W3C XML Path Language 1.0, 1999	World Wide Web Consortium, Recommendation, “XML Path Language (XPath) Version 1.0”, 25 March 2003
W3C XPointer, 2003	World Wide Web Consortium, Recommendation, “XPointer Framework”, 25 March 2003

SECTION 3: MILESTONES

3.1. Introduction

3.1.1. This section provides a notional view of the project logical schedule as well as the list of key project milestones and criteria to be met by the Contractor to achieve them.

3.1.2. Key project milestones are defined as follows:

- Effective Date of Contract (EDC)
- System Requirements Review (SRR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Factory Acceptance Test (FAT)
- Acceptance of IEG-C security accreditation package
- System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT)
- Deployment Authorization (DA)
- Preliminary System Acceptance (PSA)
- Site Accreditation
- Site Acceptance Phase (SA)
- Operational Test & Evaluation (OT&E)
- Final System Acceptance (FSA)
- Decommissioning

[SOW-21] *The Contractor SHALL note that the above milestones have been defined in a chronological order. The start of activities leading to a milestone requires the acceptance of the previous milestone (for example, the start of system implementation activities (SECTION 13) requires the prior acceptance of the DA milestone).*

3.2. Notional schedule

Figure 3 provides the Overall Project Schedule with expected timeline for each Work Package. Each Work Package scope is defined in Annex B.2

3.2.1. Work Package Scope

3.2.2. Project will start with Effective Date of Contract (EDC) milestone.

[SOW-22] *The Contractor SHALL adhere to the Overall Project Schedule. Contractor SHALL reflect this in all relevant Project Management Documentation (Section 4.4: Project Management Documentation).*

3.2.3. Effective Date of Contract (EDC)

[SOW-23] *The Effective Date of Contract (EDC) SHALL be established at the time of Contract Award (CAW).*

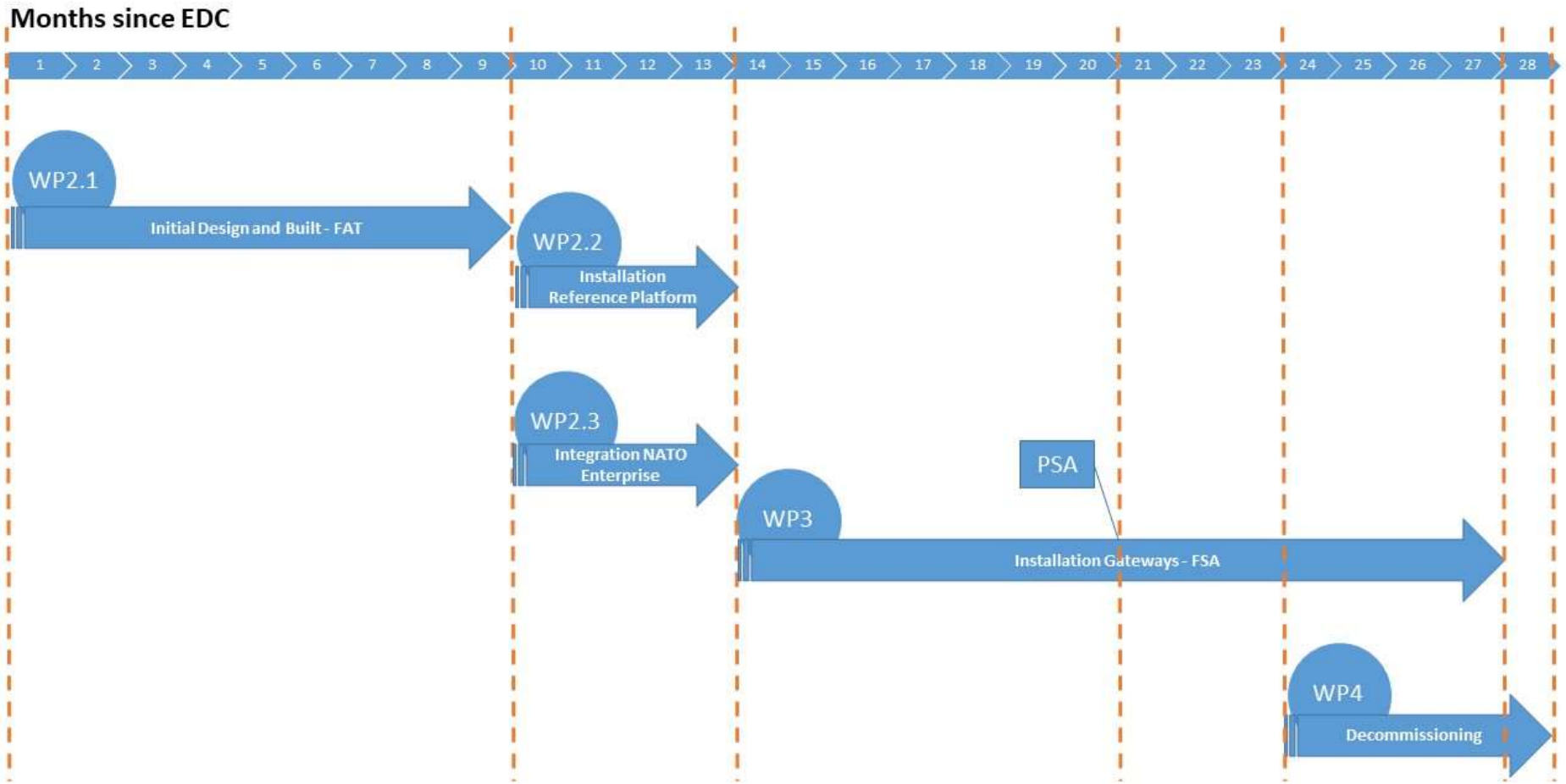


Figure 3: Overall Project Schedule

[SOW-24] *The Contractor SHALL integrate IEG-C in its Project Master Schedule at minimum by committing to deliver:*

- *System Requirements Review (SRR)*
- *Preliminary Design Review (PDR)*
- *Critical Design Review (CDR)*
- *Factory Acceptance Test (FAT)*
- *Acceptance of IEG-C security accreditation package*
- *System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT)*
- *Deployment Authorization (DA)*
- *Preliminary System Acceptance (PSA)*
- *Site Accreditation (security accreditation of interconnection via particular instance of IEG-C)*
- *Site Acceptance Phase (SA)*
- *Operational Test & Evaluation (OT&E)*
- *Final System Acceptance FSA*

Project Milestones

Milestone	No later than
Effective Date of Contract (EDC)	EDC
System Requirements Review (SRR)	EDC+2mo
Preliminary Design Review (PDR)	EDC+3mo
Critical Design Review (CDR)	EDC+6mo
Factory Acceptance Test (FAT)	EDC+9mo
Acceptance of IEG-C security accreditation package	EDC+13mo
System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT)	EDC+17mo
Deployment Authorization (DA)	EDC+20mo
Preliminary System Acceptance (PSA)	EDC+20mo
Site Accreditations	EDC+25mo
Site Acceptance Phase (SA)	EDC+25mo
Operational Test & Evaluation (OT&E)	EDC+26mo
Final System Acceptance FSA	EDC+27mo
Decommissioning	Up to 4 months after FSA

Table 2: Project Milestones

[SOW-25] *The Contractor SHALL meet or "exceed" the milestones mentioned in the above schedule. "Exceed" SHALL be understood as a situation where the Contractor has delivered earlier than the dates (i.e. EDC + 'x' months) mentioned in the above schedule, and the Purchaser has accepted the milestone accordingly.*

[SOW-26] *The Contractor SHALL implement 11 IEG-C on the sites marked as "Mandatory Sites" in Table Annex B 15 – Site Type and Location of Annex B.1*

[SOW-27] *The Contractor SHALL propose the implementation sequence of the sites in Master Test Plan. The final sequence will be determined in coordination with the Agency.*

[SOW-28] *Upon the exercise of a contract option, the Contractor SHALL implement up to 7 additional **IEG-C** on the sites marked as "Optional Sites" in Table Annex B 15 – Site Type and Location of Annex B.1*

[SOW-29] *The Contractor SHALL execute all project management activities (see SECTION 4: Project Management) due for each milestone, and all associated deliverables will have been approved by the Purchaser to enable successful completion of each milestone.*

3.3. System Requirements Review (SRR)

3.3.1. The System Requirements Review (SRR) is a multi-disciplined review to ensure that the requirements under review can proceed into initial systems development, and that all system requirements and performance requirements derived from the approved SRS are defined and testable, and are consistent with cost, schedule, risk, technology readiness, and other system constraints.

[SOW-30] *The Contractor SHALL organize and conduct the SRR (EDC+2MO) at the Purchaser's facility to present the updated SRS with its proposed changes for the design and integration of the **IEG-C** which will then become the Functional Baseline (FBL).*

[SOW-31] *The Contractor SHALL use as a main source for SRR the ISO/IEC/IEEE29148 (Systems and software engineering — Life cycle processes — Requirements engineering), the IEEE12207 and the IEE15288 (Systems Engineering).*

[SOW-32] *The Contractor SHALL review the Contractual **IEG-C** System Requirements Specification (SRS) and all other applicable documents, including:*

- *liaise with NATO subject matter experts as necessary;*
- *prepare its recommendations in terms of proposed changes to the System Requirements Specification (SRS);*
- *propose changes to the SRS (if any), in order to resolve inconsistencies and/or make improvements; such proposals will be considered by the Purchaser through the CCB process after Systems Requirements Review Meetings.*

[SOW-33] *The Contractor SHALL identify any inconsistencies within the requirements or that are in conflict (e.g. with design constraints).*

[SOW-34] *The Contractor SHALL justify any proposed changes to the requirements with the expected system cost, schedule, performance, and supportability impacts.*

[SOW-35] *The Contractor SHALL use as its SRS the Purchaser provided SRS with approved changes and, as required, extended with additional details supporting the approved scope.*

[SOW-36] *The Contractor SHALL deliver proposed changes to the SRS prior to SRR (EDC+2MO).*

3.3.2. SRR Entry Criteria

[SOW-37] *In planning the SRR meeting, the Contractor SHALL include Entry Criteria given in Table 3: The SRR Entry Criteria and make them available to the Purchaser at least two (2) weeks prior to the SRR (EDC+2MO)*

Serial	Activities/Documents
1.	A preliminary SRR agenda
2.	Use Case documentation
3.	Success Criteria (enhanced or adapted)
4.	System Requirements Specification (SRS)
5.	Draft Security Risk Assessment Report (SRA-R)
6.	Draft System Interconnection Security Requirements Statements (SISRS)
7.	Preliminary system requirements allocation to the next lower levels.
8.	Updated schedule
9.	Preliminary software development plan
10.	Preliminary verification and validation approach
11.	Updated risk assessment and mitigations in the Risk Register
12.	Active Change Request (CR)

Table 3: The SRR Entry Criteria

[SOW-38] *The Contractor SHALL perform a System Requirements Analysis Review (see Section 5.3: System Requirements Analysis and Review).*

[SOW-39] *The Contractor SHALL update the Change Proposal documentation (see 12.6 Engineering Change Proposals (ECP)).*

3.3.3. The achievement of SRR is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 4: The SRR Success Criteria

[SOW-40] *During the event the Contractor SHALL collect from the Purchaser assessment inputs based on Table 4: The SRR Success Criteria and upon conclusion of the SRR the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the SRR.*

Serial	Requirement
1.	The resulting overall baseline is reasonable, feasible, complete, responsive to the operational requirements, and is consistent with system requirements and available resources (cost, schedule, staff, etc.).
2.	The project utilizes a sound process for the allocation and control of requirements throughout all levels, and a plan has been defined to complete the definition activity within schedule constraints. Preliminary software development plan exists
3.	Requirements definition, is complete with respect to the Contractual SRS requirements, and interfaces with external entities and between major internal elements have been defined
4.	Requirements allocation and traceability of key driving requirements have been defined from Contractual SRS, down to SRS and lower level system elements.
5.	Preliminary System and element design approaches and operational concepts exist and are consistent with the SRS.
6.	The requirements, design approaches, and conceptual design will fulfil the mission needs within the estimated costs
7.	Preliminary approaches have been determined for how requirements will be tested, verified and validated down to the system element level

8.	All changes to SRA, SRS, SISRS are agreed, they are accepted to have sufficient detail to begin or continue with the system design and implementation work
9.	Major risks have been identified, and viable mitigation strategies have been defined. Steps to mitigate risks are identified in the Risk Register

Table 4: The SRR Success Criteria

[SOW-41] *The Contractor SHALL consider the SRR completed when the Purchaser and the Contractor have agreed to all necessary changes to the SRS such that the SRS is sufficient to begin or continue with the design and implementation work.*

3.4. Preliminary Design Review (PDR)

3.4.1. The Preliminary Design Review (PDR at EDC+3MO) demonstrates that the preliminary design meets all system requirements with acceptable risk and within the cost and schedule constraints and establishes the basis for proceeding with detailed design. It will show that the correct design option has been selected, interfaces have been identified, and verification methods have been described.

[SOW-42] *Review and acceptance of design documentation provided by the Contractor to the Purchaser does not imply Purchaser acceptance of the design. The Contractor SHALL be solely responsible to prove the design through the regime of testing set forth in the Contract and the Contractor SHALL be solely responsible in the event that the system proves deficient in meeting the SRS*

[SOW-43] *The Contractor SHALL perform a System Design as defined in section 5.4.4: Design Reviews, and the associated documentation SHALL have been approved by the Purchaser.*

[SOW-44] *The Contractor SHALL complete the site survey process as defined in SECTION 9: Site Surveys and deliver the associated reports for approval by the Purchaser for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) and SECTION 9: Site Surveys.*

[SOW-45] *The Contractor SHALL perform the Training Needs Analysis (TNA) for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) for approval by Purchaser, as defined in Section 6.6.2: Training Needs Analysis (TNA) - The Contractor SHALL ensure the Training Materials include how the Transition from one Release to the next release is realised and how to install, configure and maintain the Modified or new Component capability, including COTS components.*

[SOW-46] *The Contractor SHALL deliver the Training Plan that will cover all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) for approval by Purchaser, as defined in Section 6.6.3: Training Plan.*

[SOW-47] *The Contractor SHALL have delivered the System Implementation Plan (SIP) for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA) and Section 7.3: System Implementation Plan (SIP)) for approval by Purchaser.*

3.4.2. PDR Entry Criteria

[SOW-48] *In planning the PDR (EDC+3MO) meeting, the Contractor SHALL include Entry Criteria given in Table 5: The PDR Entry Criteria and make them available to the Purchaser at least two (2) weeks prior to the PDR*

Serial	Activities/Documents

1.	A preliminary PDR agenda
2.	Success Criteria (enhanced or adapted)
3.	Master Test Plan (MTP) (preliminary)
4.	Test Procedures/Test Cases (preliminary)
5.	System Design Specification (SDS) (preliminary)
6.	System Implementation Plan (SIP)
7.	Updated Security Risk Assessment Report (SRA-R)
8.	System Security Design Specification (SSDS) (preliminary)
9.	Requirements Traceability Matrix (RTM)
10.	Interface Control Description (ICD) (draft)
11.	Integrated Logistics Support Plan (ILSP) (draft)
12.	Updated Risk Register
13.	Active Change Requests

Table 5: The PDR Entry Criteria

3.4.3. The achievement of PDR is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 6: The PDR Success Criteria

[SOW-49] *During the event the Contractor SHALL collect from the Purchaser assessment inputs based on Table 6: The PDR Success Criteria and upon conclusion of the PDR (EDC+3MO) the Contractor SHALL produce a final report and make it available to the Purchaser at most (1) week after the PDR*

Serial	Requirement
1.	Agreement exists for the top-level requirements, including their verification and validation criteria, technical performance measures and any implementation constraints, and that these are finalised, stated clearly, and are consistent with the preliminary design
2.	The traceability of design artefacts to verifiable requirements is complete and proper or, if not, an adequate plan exists for timely resolution of open items. Design artefacts are traceable to the SRS.
3.	The preliminary design is expected to meet the requirements at an acceptable level of risk
4.	Definition of the technical interfaces is consistent with the overall technical maturity and proves an acceptable level of risk.
5.	Adequate technical interfaces are consistent with the overall technical maturity and provide an acceptable level of risk.
6.	Adequate technical margins exist with respect to technical performance measures
7.	The project and security risks are understood; plans, process and resources exist to effectively manage them. Steps to mitigate risks are identified in the Risk Register
8.	Major user interface features are reviewed and concept of interfaces are agreed.
9.	Non-functional requirements have been adequately addressed in preliminary designs.
10.	The system operational concept is technically sound, that it includes (where appropriate) human factors that apply, and that requirements for its execution are traceable

Table 6: The PDR Success Criteria

3.5. Critical Design Review (CDR)

3.5.1. The purpose of the Critical Design Review (CDR at EDC+6MO) is to demonstrate that the maturity of the design is appropriate to support proceeding with full scale software and hardware implementation, integration, verification, validation and operation and that the technical effort is on track to complete system development in order to meet the SRS requirements within the identified cost and schedule constraints. At CDR the final version for each component (software) and interfaces to be used in the FBL shall be fixed. The Contractor will plan the CDR at the completion of the system design phase and conduct the CDR at the Purchaser's facility.

3.5.2. CDR Entry Criteria

[SOW-50] *In planning the CDR meeting, the Contractor SHALL include Entry Criteria given in Table 7: The CDR Entry Criteria and make them available to the Purchaser at least two (2) weeks prior to the CDR (EDC+6MO)*

Serial	Activities/Documents
1.	A preliminary CDR agenda
2.	Success Criteria (enhanced or adapted)
3.	Successful completion of the PDR and responses has been made to all PDR open issues, or a timely closure plan exists for those remaining open.
4.	Master Test Plan (MTP) (final)
5.	Test Procedures/Test Cases (intermediate)
6.	Site Survey Reports
7.	Training Need Analysis (TNA)
8.	System Design Specification (SDS) (final)
9.	System Security Design Specification (SSDS) (final)
10.	Requirements Traceability Matrix (RTM) (update)
11.	Interface Control Description (ICD) (initial version)
12.	Integrated Logistics Support Plan (ILSP) (initial version)
13.	Updated Risk Register
14.	Active Change Requests

Table 7: The CDR Entry Criteria

[SOW-51] *The Contractor SHALL perform a Critical Design Review as defined in 5.4, and the associated documentation SHALL have been approved by the Purchaser.*

[SOW-52] *The Contractor SHALL complete the site survey process as defined in SECTION 9 and delivered the associated reports for approval by the Purchaser for all the sites that form part of PSA scope.*

[SOW-53] *The Contractor SHALL update the Training Needs Analysis (TNA) for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) for approval by Purchaser, as defined in Section 6.6.2 Training Needs Analysis (TNA) - The Contractor SHALL ensure the Training Materials include how the Transition from one Release to the next release is realised and how to securely install, configure and maintain the Modified or new Component capability, including COTS components.*

[SOW-54] *The CDR documentation and achievement of the CDR milestone are subject to the Purchaser approval. Unless otherwise approved by the Purchaser, the Contractor SHALL NOT proceed with the CDR stage without successful completion of the PDR (EDC+3MO) milestone.*

3.5.3. The achievement of CDR is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 8: The CDR Success Criteria

[SOW-55] *During the event the Contractor SHALL collect from the Purchaser assessment inputs based on Table 8: The CDR Success Criteria and upon conclusion of the CDR the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the CDR.*

Serial	Requirement
1.	The detailed design is expected to meet the requirements with adequate margins at an acceptable level of risk. System Element-level functionality, design and interfaces are defined
2.	Core Services integration (at Service-level and host environment-level) is defined.
3.	System security, including Technical Services access-control mechanisms, data protection, backup and recovery, audit, interconnection, and information exchange security in context of the Services breakdown are defined.
4.	High-level design of Information Entities is completed.
5.	ICDs and SIPs are appropriately matured to proceed with implementation, integration and test, and plans are in place to manage any open items. System-level and Service-level interfaces, including external Services interfaces are defined.
6.	High confidence exists in the CDR, and adequate documentation exists and/or will exist in a timely manner to allow proceeding with implementation, integration, and test. For any elements that require development, the development methodology and documentation approach are defined
7.	Overall system design and its interactions, Services, components and Human-Machine Interface and Human Factors justifications are defined.
8.	For COTS products, the intended product and version, and note if any modifications, adaptations, or additional elements (such as macros or plug-ins) are required. Open Source Software (OSS) are to be disclosed (for review of OSS conditions by the Purchaser).
9.	The verification and validation requirements and plans are complete.
10.	The testing approach is comprehensive, and the planning for system integration, test, and operation is sufficient to progress into the next phase. Sequence and scope of system tests of each Baseline and any requirements for Purchaser support and participation are defined.
11.	Adequate technical and programmatic margins and resources exist to complete the development within budget, schedule, and risk constraints.
12.	Risks are understood, and plans and resources exist to effectively manage them. Steps to mitigate risks are identified in the Risk Register
13.	Non-functional requirements have been adequately addressed in system and operational designs.

Table 8: The CDR Success Criteria

3.6. Factory Acceptance Test (FAT)

[SOW-56] *The Contractor SHALL have performed necessary activities and satisfied criteria for meeting FAT (EDC+9MO) milestones as defined in SECTION 8 and SHALL achieve Purchaser approval of the associated documentation.*

3.7. Acceptance of IEG-C security accreditation package

[SOW-57] *The milestone "Acceptance of IEG-C security accreditation package" will be achieved when NSAB approval is granted at EDC+13mo.*

[SOW-58] *The contractor SHALL deliver all documentation according to SECTION 10, 7 months in advance of the expected "Acceptance of IEG-C security accreditation package Milestone" in order to have NSAB approved deliverables before commencing WP 3 / Installation of gateways.*

3.8. System Integration Testing (SIT) + System Acceptance Testing (SAT) + User Acceptance Testing (UAT)

[SOW-59] *The Contractor SHALL have performed necessary activities and satisfied criteria for meeting SIT + SAT + UAT (EDC+17mo) milestones as defined in SECTION 8 and SHALL achieve Purchaser approval of the associated documentation.*

3.9. Deployment Authorization (DA)

3.9.1. Successful completion of RFC process is a prerequisite for adding the IEG-C to the AFPL, which is a pre-requisite for authorization to deploy the IEG-C on to NATO networks.

[SOW-60] *The Contractor SHALL comply with the decision of the Purchaser's CAB and only after CAB approval to deploy authorization is granted, the installation of the first site can be initiated based on the Purchaser approved Deployment Plan.*

[SOW-61] *The Contractor SHALL have handled any change to satisfy the security requirements.*

[SOW-62] *The Contractor SHALL have delivered the required training (including training for RAs operators) at agreed site(s), according to Training and the training plan approved by Purchaser.*

[SOW-63] *The Contractor SHALL have completed and received approval by the SAA of the Security Accreditation Documentation (see SECTION 10), including all the localised versions of documents (see 10.3), for all the (block of) site(s).*

[SOW-64] *The Contractor SHALL have completed the Site Acceptance Plan and have received the approval by the Purchaser.*

[SOW-65] *The Contractor SHALL have completed the Site Acceptance Test Cases and have received the approval by the Purchaser.*

[SOW-66] *The Contractor SHALL have completed the Operational System Acceptance (OSA) Plan and have received the approval by the Purchaser.*

[SOW-67] *The Contractor SHALL have completed the OSA Test Cases and have received the approval by the Purchaser*

[SOW-68] *The Contractor SHALL note that system implementation activities in the operational environment SHALL NOT start until the Deployment Authorization milestone is approved by the Purchaser.*

3.9.2. The achievement of DA is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 9 The DA Success Criteria

[SOW-69] *During the event the Contractor SHALL collect from the Purchaser assessment inputs based on Table 9 The DA Success Criteria and upon conclusion of the DA the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the DA.*

Serial	Requirement
1.	The IEG-C is added to the AFPL
2.	The IEG-C has obtained CAB approval
3.	Training for operators is completed
4.	High-level design of Information Entities is completed.
5.	Security Accreditation Documentation is approved by the Security Accreditation Authority
6.	The Site Acceptance Plan is approved by the Purchaser
7.	Site Acceptance Test Cases are approved by the Purchaser
8.	Operational System Acceptance (OSA) Plan are approved by the Purchaser
9.	OSA Test Cases are approved by the Purchaser

Table 9 The DA Success Criteria

3.10. Provisional System Acceptance (PSA)

3.10.1. The IEG-C will be considered as having achieved the PSA (EDC+20mo) milestone when all the relevant system prerequisites have been completed successfully and the first operational IEG-C Gateway is activated.

3.10.2. The criteria for achieving PSA are listed below:

[SOW-70] *The Contractor SHALL install, test and activate all the IEG-C components for the first operational IEG-C (IEG-C-02, see Annex B1, page 169) at SHAPE as described and defined in SECTION 6: Integrated LOGISTICS Support (ILS), SECTION 7: System Implementation and SECTION 8: Test, Verification, Validation (TVV).*

[SOW-71] *The Contractor SHALL have delivered all functionalities of IEG-C defined within Work Packages Scope (Annex B2)*

[SOW-72] *The Contractor SHALL have trained all required personnel according to Section 6.6: Training.*

[SOW-73] *The Contractor SHALL have provided reviewed and approved operational and maintenance documentation as described in Section 6.5 Technical Documentation and SECTION 15: Deliverables Outlines.*

[SOW-74] *The Contractor SHALL have satisfied the security requirements (see SECTION 10: Security).*

[SOW-75] *The Contractor SHALL have migrated on IEG-C all services required to support the information exchange requirements for the CIS interconnection.*

[SOW-76] *The Contractor SHALL ensure all performance and availability requirements specified in this SOW (Annex A, SRS) have been met.*

[SOW-77] *The Contractor SHALL have executed all activities required to have all IEG-C software components (including ITSM tools) on the AFPL (Approved Fielded Product List).*

[SOW-78] *The Contractor SHALL have supplied the spare parts and consumables.*

[SOW-79] *The Contractor SHALL have implemented and tested all Support Services and the ITSM Tools, covering the PSA Site (SHAPE), and obtained the Purchaser's approval.*

[SOW-80] *The Contractor SHALL have updated Product Baselines (PBL) and SHALL have provided the Operational Baseline (OBL) as described in SECTION 12: Configuration Management to reflect the actual PSA configuration*

[SOW-81] *The Contractor SHALL have provided the Configuration Management database (CMDB) in a format that is compatible with the Purchaser CMDB tools.*

[SOW-82] *The Contractor SHALL have performed the Physical Configuration Audit (PCA) and Functional Configuration Audit (FCA), provided the audit reports and completed the corrective actions as outlined in the reports.*

[SOW-83] *The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status "PASS", as described in [SOW-640] .*

3.10.3. It is important to note that PSA is not only dependent on compliance against testable requirements, but will require non-testable requirements to be met too.

[SOW-84] *The Contractor SHALL handle all observations and deficiencies from the Formal Test Phases following the Defect Management Process and SHALL satisfactory resolve them before awarding PSA.*

3.10.4. The Contractor SHALL have completed and received approval by the Security Accreditation Authority (SAA) of the Security Accreditation Documentation (see para: 10.3), including all the localised versions of documents, for the PSA Site (SHAPE).

3.10.5. First Site Acceptance

[SOW-85] *In addition to the requirements set below, the Contractor SHALL achieve, for the Mons site, the requirements as set below in 3.12 and SECTION 10: Security Accreditation.*

3.10.6. The achievement of PSA is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 10: PSA success criteria.

[SOW-86] *During the event the Contractor SHALL collect from the Purchaser assessment inputs based on Table 10: PSA success criteria and upon conclusion of the PSA the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the PSA.*

Serial	Requirement
1.	The IEG-C documentation is delivered and approved
2.	The IEG-C functionalities are delivered
3.	The IEG-C Training is completed
4.	Spare parts and consumables are delivered
5.	All IEG-C software components (including ITSM tools) are on the AFPL (Approved Fielded Product List)
6.	PBL and OBL are updated and the corresponding CMDB data provided to the Customer
7.	PCA and FCA reports are delivered and corrective actions completed

8.	Site Security Accreditation is approved by the Security Accreditation Authority
9.	The IEG-C is integrated with Core Services, Service Management and Monitoring
10.	IEG-C Services are migrated from the old IEG-C prototype in SHAPE to the new IEG-C-02
11.	Performance and Availability requirements set in Annex A of this SOW (SRS) are met
12.	The IEG-C-02 is installed, tested and activated

Table 10: PSA success criteria

3.11. Site Accreditation

Site accreditation is addressed in Section 10.1 and will apply to each site individually.

3.12. Site Acceptance

3.12.1. The following requirements will apply to each of the locations that will host an IEG-C.

3.12.2. The completion of acceptance all locations will mean the completion of the Site Acceptance milestone.

[SOW-87] *Between PSA and FSA milestones, the Contractor may propose an activation per site. In such a case, the Contractor SHALL comply with the requirements of this section in order to reach activation for a site.*

[SOW-88] *The Contractor SHALL meet all the PSA-related requirements.*

[SOW-89] *The Contractor SHALL have implemented the site in accordance with SECTION 6: Integrated LOGISTICS Support (ILS), SECTION 7: System Implementation SECTION 8: Test, Verification, Validation (TVV), SECTION 9: Site Surveys and SECTION 15: Deliverables Outlines SHALL have delivered the associated documentation.*

[SOW-90] *The Contractor SHALL have installed, tested and activated the IEG-C(s) at the site.*

[SOW-91] *The Contractor SHALL have migrated on IEG-C all services required to support the information exchange requirements for the CIS interconnection(s).*

[SOW-92] *All performance and availability requirements specified in this SOW SHALL have been met by the Contractor.*

[SOW-93] *The Contractor SHALL train all required personnel according to Section 6.6: Training.*

[SOW-94] *The Contractor SHALL have supplied the spare parts and consumables.*

[SOW-95] *The Support Services SHALL have been updated as required.*

[SOW-96] *The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status "PASS", as described in [SOW-640] .*

[SOW-97] *The Contractor SHALL have provided the Operational Baseline (OBL) as described in SECTION 12: Configuration Management to reflect the actual Site configuration.*

[SOW-98] *The Contractor SHALL complete and receive approval by the Security Accreditation Authority (SAA) of the Security Accreditation Documentation (see para: 10.3), including all the localised versions of documents, for the site.*

3.12.3. The SAA has issued the Statement of Accreditation for the interconnection via IEG-C at the site.

3.12.4. Site Activation Meetings

The achievement of Site Activation is subject to the Purchaser approval, in writing. Site Activation will be established at a meeting convened between the Contractor and the Purchaser for that purpose. At that meeting the Contractor will present to the Purchaser evidence that all conditions for Site Activation as described in Section 3.12 Site Acceptance and summarized in Table 11: Site Activation Criteria have been met.

Serial	Requirement
1.	PSA requirements are met
2.	The IEG-C gateways for the site are installed, tested and activated as per ILS and TVV requirements
3.	All deliverables are delivered
4.	All IEG-C Services are migrated
5.	Performance and Availability requirements set in Annex A of this SOW (SRS) are met
6.	The IEG-C Training is completed
7.	Spare parts and consumables for the site are delivered
8.	PBL and OBL are updated and the corresponding CMDB data provided to the Customer
9.	Site Security Accreditation is approved by the Security Accreditation Authority

Table 11: Site Activation Criteria

3.13. Operational Test and Evaluation (OT&E)

[SOW-99] *The Contractor SHALL conduct OT&E as defined in Sections SECTION 7 and SECTION 8.*

[SOW-100] *The Contractor SHALL have successfully implemented or achieved the Operational Acceptance Criteria (OAC) that apply to this SOW and have been included in Annex A (SRS).*

[SOW-101] *The Contractor SHALL note that the achievement of the OT&E milestone is subject to the Purchaser acceptance.*

3.14. Final System Acceptance (FSA)

3.14.1. FSA (EDC+27mo) is the act by which the Purchaser has evaluated and determined that the implemented IEG-C System meets the requirements of the Contract, and that the Contractor has fully delivered all requirements.

[SOW-102] *The Contractor SHALL meet all PSA milestone requirements (see par.3.10) as well as Site Activation milestone requirements (see par.3.13**)** for all the sites to be implemented under this contract.*

[SOW-103] *The Contractor SHALL execute all implementation activities according to SECTION 3 at all the sites to be implemented under this contract.*

[SOW-104] *The Contractor SHALL install the most recent version of implemented IEG-C.*

[SOW-105] *The Contractor SHALL fully implement the centralised management and control of the IEG-C according to the requirements specified in this SOW.*

[SOW-106] *The Contractor SHALL deliver a complete and updated set of documents (e.g. Functional Baseline, Product baseline, Operational baseline)*

[SOW-107] *The Contractor SHALL have provided the Configuration Management database (CMDB) in a format that is compatible with the Purchaser CMDB tools.*

[SOW-108] *The Contractor SHALL activate Support Services at all the FSA Sites.*

[SOW-109] *The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status "PASS".*

[SOW-110] *The Contractor SHALL complete and receive approval by the SAA of the Security Accreditation Documentation (para: 10.3), including all the localised versions of documents (para: 10.2: Security Accreditation Authority (SAA)), for all the FSA sites.*

3.14.2. The SAA has issued the Statements of Accreditation for the **IEG-C** at all the Sites.

[SOW-111] *The Contractor SHALL deliver all deliverables (SECTION 15), and conducted all activities, as specified in this Contract.*

[SOW-112] *The Contractor SHALL close to the satisfaction of the Purchaser all outstanding issues, failures, and deficiencies.*

3.14.3. Site FSA Meetings and Success Criteria

The achievement of FSA (EDC+27mo) is subject to Purchaser approval, in writing. Project FSA will be established at a meeting convened between the Contractor and the Purchaser for that purpose. At that meeting the Contractor shall present to the Purchaser evidence that all conditions for FSA, as described in 3.14.1 and summarized in Table 12: FSA Success Criteria, have been met.

[SOW-113] *During the event the Contractor SHALL collect from the Purchaser assessment inputs based on and upon conclusion of the FSA the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the FSA.*

Serial	Requirement
1.	PSA and OT&E milestones are achieved
2.	All the IEG-Cs in the scope of this SOW and listed in ANNEX B Implementation Scope are delivered and are operational
3.	All changes to IEG-C software components (including ITSM tools) are on the AFPL (Approved Fielded Product List)
4.	All site have the latest version of IEG-C system solution
5.	FBL, PBL and OBL are updated and the corresponding CMDB data provided to the Customer
6.	Site Security Accreditation for all FSA sites is approved by the Security Accreditation Authority
7.	IEG-C Services are migrated from the old IEG-C prototypes to the new IEG-C
8.	Performance and Availability requirements set in Annex A of this SOW (SRS) are met
9.	Test and Acceptance phases with Test Reports are provided to the Customer
10.	Legacy Gateways (WP3 and WP4 locations) have been decommissioned and removed

Table 1 FSA Success Criteria

SECTION 4 : PROJECT MANAGEMENT

4.1. Introduction

4.1.1. This section outlines the Project Management requirements for this Contract.

4.1.2. The Contractor's Project Management activity is viewed as a critical factor in the successful execution of the IEG-C Project.

[SOW-114] *The Contractor SHALL at all times ensure that:*

- *Adequate resources are applied to all activities undertaken under the contract;*
- *Milestones are identified and achieved in a timely manner;*
- *The project status information is comprehensively reported to the Purchaser in a timely manner;*
- *Configuration Management baselines are established and maintained throughout the project lifecycle;*
- *All risks (Purchaser and Contractor risks) to project achievement are identified and managed;*
- *Professional standards of project activities and deliverables through the application of QA techniques are applied;*
- *Due account is taken of Purchaser Furnished Information including Process Management Directives.*

4.1.3. The success of the IEG-C project depends upon a sound project management approach. Full and open communication between the Contractor and the Purchaser is an essential element of this approach.

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

[SOW-115] *The Contractor SHALL acknowledge email receipt and answer email received from NATO project team members (see para: 4.3 Project Management Organization) within 3 business days.*

4.1.5. Methodology

[SOW-116] *The Contractor SHALL use PRINCE2 or an equivalent PM standard for the direction, governance and management activities for the entire project. If an equivalent PM standard is used, the Contractor SHALL prove that it at minimum meets all requirements stated in this section.*

[SOW-117] *The Contractor SHALL be agile in the approach for any software development and configuration product delivery activities within each release and by doing so SHALL enable:*

- *All SOW requirements are met*
- *Detailed planning and progress tracking for the short horizon (time-boxed) activities*
- *Re-planning and reviewing activities at frequent intervals*
- *Product deliverables breakdown and continuous (re)prioritization*
- *Iterative development and incremental delivery via product releases*

- *Team collaboration, rich communication, self-organisation, transparency and customer-focus*
- *A test-driven approach utilising frequent and comprehensive testing activities using testing automation to the greatest possible extent (target 100%)*
- *Progress Reporting with Earned Value Management (EVM)*

[SOW-118] *The Contractor SHALL define and describe its implementation of the required PM approach so that at minimum it shows a clear and consistent exchange of information between the Project team and minimal duplication of information and project management activities. For example:*

[SOW-119] *The Contractor SHALL use Project Master Schedule (PMS; i.e., Gantt chart) for higher level project planning and milestones tracking but should be regularly fed by information from Product Delivery Reviews.*

[SOW-120] *The Contractor SHALL produce Project Status Report (PSR) that include inputs about delivery progress, issues and risks taken from Product Delivery Reviews and meeting.*

4.2. Project Implementation Plan (PIP)

[SOW-121] *The Contractor SHALL provide a Project Implementation Plan (PIP), which wil describe how the Contractor will implement the Project.*

4.2.1. The PIP shall be provided to the Purchaser for review and acceptance within four (4) weeks after Effective Date of Contract (EDC). The PIP will be reviewed by the Purchaser and comments submitted to the Contractor no later than five (5) working days after receipt. PIP final version will be provided to the Purchaser six (6) weeks after Effective Date of Contract (EDC).

4.2.2. The approval of the PIP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This approval in no way relieves the Contractor from its responsibilities to meet the requirements stated in this SoW.

4.2.3. The PIP shall be kept up to date throughout the project, and shall be subject of review at each Project Review Meeting (PRM), until and including Provisional System Acceptance (PSA (EDC+20mo)). The PIP will also identify the security accreditation process.

4.2.4. The PIP shall include the sections listed and described in 4.4 Project Management Documentation below:

4.3. Project Management Organisation

4.3.1. Project Governance

4.3.1.1. This project will be managed in accordance with the NCIA project management procedures, based on the Projects in Controlled Environments (PRINCE 2) methodology. The NCIA has established the Project Board representing, among others, the users and suppliers.

4.3.1.2. The NCI Agency Project Board is composed of the following.

4.3.1.2.1. Senior User: SHAPE J6 is the Senior User for this project. NCI Agency internal representation of the users is provided by NSIP section.

4.3.1.2.2. Senior Supplier: The Implementation Contractor is the Senior Supplier for this project and is responsible for delivering the required capability. NCIA Agency Internal Representation of the Supplier is provided by NCIA Agency Contracting as needed.

4.3.1.2.3. Executive: The NCI Agency Core Enterprise Services (CES) Service Line Chief is the Project Board Executive for this project.

4.3.1.2.4. NCI Agency Service Strategy will be part of the Project Board to assure technical conformity of the implementation and its architecture to the relevant NATO standards. Project assurance will be augmented by other NCIA entities as needed, including Chief Technical Officer and IV&V.

4.3.1.3. The NCIA Project Manager (PM) will report to the NCIA Project Executive in accordance with the Prince2 principles.

4.3.2. Overall Project Organisation

4.3.2.1. The Project Management Structure is shown in Figure 4 below

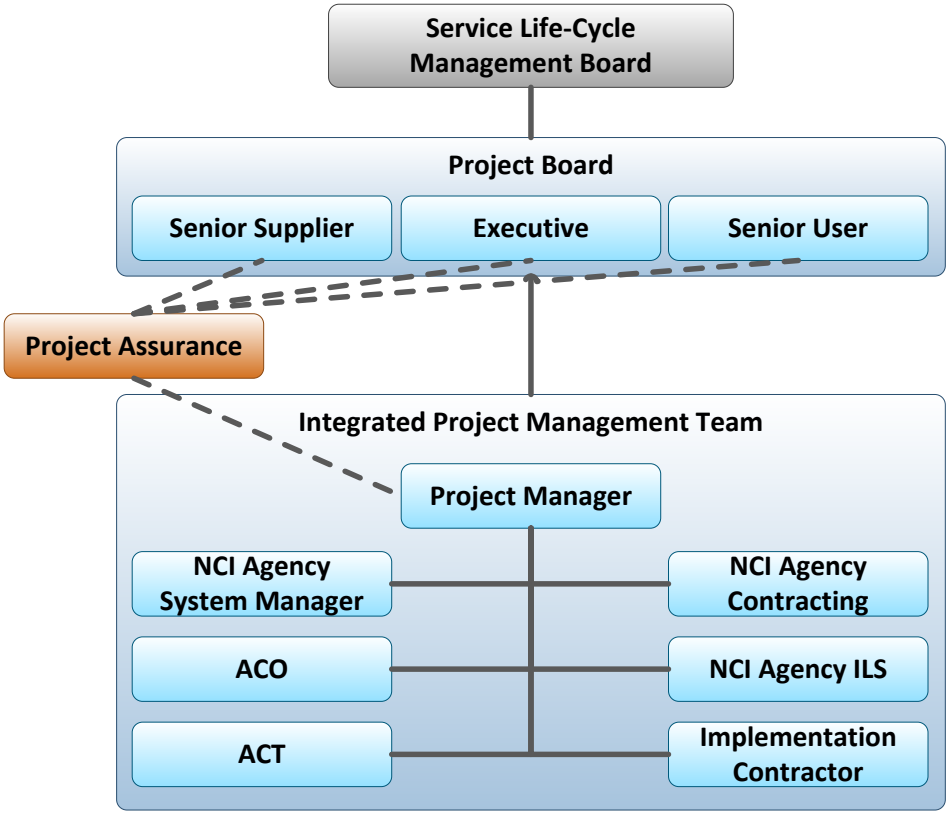


Figure 4: Project Management Structure

4.3.2.1.1. The Project board is accountable for the project success and has the authority to direct the project by making key decisions and exercising overall control. The Board manages by exception via reports provided by Project Managers and escalates as needed to the NCIA SLMB.

[SOW-122] *[Reserved].*

[SOW-123] *[Reserved].*

4.3.3. Purchaser Project Organisation and Responsibilities

4.3.3.1. The Purchaser Contracting Office (CO) will act as the Purchaser's representative and will be the primary interface between the Contractor and Purchaser after the EDC.

4.3.3.2. The Purchaser Project Manager will be supported by Subject Matter Experts (SME) in certain areas who may, from time to time, be delegated to act on the Purchaser Project Manager's behalf in their area of expertise.

4.3.3.3. The Purchaser Project Manager, the specialists, other team members, or any other NATO personnel are not allowed to make changes to the terms and conditions of the Contract. They may only provide the Purchaser's interpretation of technical matters.

4.3.3.4. All changes to the Contract will be made through the Purchaser's Contracting office only.

4.3.3.5. The Purchaser and Contractor Project Manager, the specialists, and the key Stakeholders representatives collectively form the IEG-C IPMT.

4.3.3.6. The Purchaser Project Manager chairs the IEG-C IPMT. The other participating members are the designated representatives of the stakeholders (key user representatives). All other members serve as advisory members.

4.3.3.7. The IPMT serves as the steering group or project board for the contractor's project and as the primary mechanism for monitoring project status, resolving issues or conflicts within the project, and advising the Purchaser Project Manager.

4.3.3.8. The IPMT also serves as the Purchaser's IEG-C Configuration Control Board (CCB), to which the following items may be submitted for baselining decision as required by the Purchaser:

a. PMP,
b. PMS (Project Master Schedule), for the first version and for all changes beyond tolerance available to the Purchaser Project Manager[5].
c. System Implementation Plan (SIP)
d. ILS Plan (ILSP)
e. Functional Baseline (FBL or "as required")
f. Allocated Baseline (ABL, or "as designed");
g. Product Baseline (PBL, or "as built")
h. Configuration Management Plan (CMP)
i. Quality Assurance Plan (QAP)

[5] The Purchaser Project Manager can, at his/her own discretion and without consulting the other IEG-C CCB members, approve changes to the PMS that do not affect other baselined documents, and/or do not incur additional costs, and/or do not bring the project beyond time tolerance available to him/her.

4.3.3.9. The Purchaser will also ensure its SMEs are available to engage in the role of Product Owners (PO). PO will represent the Purchaser's interests within Product Delivery Teams and will work to enable:

a. Detailed product requirements are well-defined, understood and prioritized for development

b. Product deliverables are reviewed, fitting the purpose and have been tested by the Contractor according to the agreed upon Test Plan

c. Communication, collaboration and feedback from other Purchaser representatives such as end user representatives and other SMEs

4.3.4. Contractor Organisation and Responsibilities

[SOW-124] *The Contractor SHALL identify all major Contractor organizational units and any Sub-Contractors involved in the implementation of the IEG-C and a description of the portion of the overall effort or deliverable item for which they are responsible.*

[SOW-125] *The Contractor SHALL establish and maintain a Project Management Office (PMO) to perform and manage all efforts necessary to discharge all his responsibilities under this Contract.*

[SOW-126] *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-127] *The Contractor SHALL designate one or more Senior Engineer(s) as Team Managers throughout the performance of the Contract. Team Manager SHALL design, coordinate and lead the process of product delivery within the defined Product Delivery Team(s) making sure product requirements are met within given timelines and quality criteria. Team manager organizes and facilitates all Product Delivery Meetings (PDM). Team manager SHALL report and take direction from the Contractor Project Manager. See SECTION 13 for labour category requirements.*

[SOW-128] *The Contractor SHALL designate a Field Engineer to serve as the Service Direction Manager throughout the performance of the Contract. See SECTION 13 for labour category requirements.*

[SOW-129] *The Contractor SHALL designate an Engineer to serve as QAM throughout the performance of the Contract until project completion. See SECTION 13 for labour category requirements.*

[SOW-130] *The Contractor SHALL designate a Senior Engineer to serve as ILS, Change and Configuration Manager throughout the performance of the Contract, including the Operation and Maintenance (O&M) Phase. See SECTION 13 for labour category requirements.*

[SOW-131] *In order to facilitate communication and effectiveness, the Contractor SHALL locate the Core Team (i.e., Project Manager and Technical Lead) close to the Purchaser premises.*

[SOW-132] *The Contractor's team SHALL be available during EU time zone working hours (8:30 - 17:30 Monday-Thursday, and 8:30 - 16:30 on Fridays).*

4.3.4.1. The following members of the Contractor PMO are Key Personnel for this project:

[SOW-133] *The Contractor SHALL designate a Project Manager (Contractor PM), who will direct and co-ordinate the activities of the Contractor's project team. The Project Manager SHALL be the Contractor's primary contact for the Purchaser Project Manager and SHALL conduct all major project design, test, and review meetings. See SECTION 13 for labour category requirements.*

[SOW-134] *The Contractor SHALL designate a Senior System Engineer as the Technical Lead throughout the performance of the Contract. The Technical Lead SHALL lead the analysis, design, integration, transition into operations and follow-on enhancement efforts of the Contractor. See SECTION 13 for labour category requirements.*

[SOW-135] *The Contractor SHALL designate a Senior Test Engineer to serve as the Test Director for all test activities conducted under this Contract. See SECTION 13 for labour category requirements.*

4.4. Project Management Documentation

4.4.1. For the purpose of this Contract, Deliverables are split into two categories:

a. Management products are all Contract Deliverables covered under the Project Management activities.

b. Specialist products are all other Deliverables in this Contract.

4.4.2. The Project Overview management product, which shall provide an executive summary overview of the offered IEG-C.

[SOW-136] *The Contractor SHALL establish and maintain a Project Overview*

4.4.3. Product Breakdown Structure (PBS) and Product Flow Diagram (PFD)

[SOW-137] *The Contractor SHALL establish and maintain a PBS, which SHALL:*

- *Identify all products and shall distinguish between management products and specialist products.*
- *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 IEG-C System.*
- *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-138] *The Contractor SHALL establish and maintain a PFD, which SHALL sequence all products in their logical order of creation.*

4.4.3.1. The acceptance of the PBS and of the PFD by the Purchaser signifies only that the Purchaser agrees to the Contractor’s approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

4.4.4. The Project Management Plan management product, which clearly describes the implementation of the project.

[SOW-139] *The Contractor SHALL establish and maintain a PMP which shall describe how the Contractor will implement the totality of the project as specified in this SOW, including details of the project control that will be applied.*

[SOW-140] *The Contractor's PMP SHALL cover all aspects of the project implementation including its management structure and project management processes,*

personnel assignments, external relationships necessary to provide the capability as required by this Contract.

[SOW-141] *The Contractor's PMP SHALL be sufficiently detailed to ensure that the Purchaser is able to assess the Contractor plans with insight into the Contractor's plans, capabilities, and ability to satisfactorily implement the entire project in conformance with the requirements as specified in this SOW.*

[SOW-142] *The Contractor's PMP SHALL follow the outline recommended in this SOW (see SECTION 15.9).*

[SOW-143] *The Contractor's PMP SHALL be provided to the Purchaser for acceptance.*

4.4.5. Work Breakdown Structure (WBS)

4.4.5.1. The WBS is the basic structure for EVM data collection and reporting, and should be reflected in the detailed activities in the Project Master Schedule (PMS).

[SOW-144] *Contractor SHALL develop the Contractor WBS to the level needed for adequate management and control of the contractual effort. A single WBS should be used for planning, managing, and reporting.*

- *Contractor SHALL perform the contract technical effort using a guidelines-compliant EVM (EVM PMI standard) that correlates cost and schedule performance with technical progress.*
- *Progress and problems SHALL be presented and discussed in periodic program management reviews. Technical issues SHALL be covered in terms of performance goals, exit criteria, schedule progress, risk, and cost impact.*
- *The WBS SHALL include designation of critical subcontractors, by name, for EVM compliance and validation or flow down of EVM compliance to these subcontractors.*

4.4.6. Project Master Schedule (PMS)

[SOW-145] *The Contractor SHALL establish and maintain a PMS which SHALL be based on realistic time estimates, subject to Purchaser acceptance:*

- *Contain all Contract events and milestones*
- *Correlate with the products defined in the PBS and sequentially ordered in the PFD*
- *Incorporate the WBS*
- *Be provided in Microsoft Project format*
- *Identify the critical path for the overall project*
- *Identify the start and finish dates, duration, predecessors, constraints (as necessary) and the total slack of each task*
- *Identify key resources needed for each task completion*
- *Identify the main project milestones (see) and intermediate milestones as required*
- *Identify the "physical" progress for each task*
- *Identify the applicable baseline, and shall show progress against the baseline*
- *Minimise the use of constraints and absolute dates*

- *Provide network, milestone, Gantt and Tracking Gantt views*
- *Identify the main deliverables.*

[SOW-146] *The Contractor SHALL provide the PMS to the Purchaser for acceptance.*

[SOW-147] *The Contractor SHALL use the PBS, the WBS, the PFD and the PMS as the primary framework for Contract planning and reporting to the Purchaser.*

4.4.7. Risk Management Plan (RMP)

[SOW-148] *The Contractor SHALL establish and maintain a RMP which shall describe how the Contractor will implement the Risk Management process, with at least the following details:*

- *Overall Risk Management approach*
- *Key Risk Management processes*
- *Key Risk Categories*
- *Risk Prioritization Matrix*
- *Risk Management roles and responsibilities*
- *Risk Log template which shall at minimum follow the outline recommended in this SOW (see Section 15.2).*

4.5. Project Controls

4.5.1. Risk Management

[SOW-149] *The Contractor SHALL establish and maintain a Risk Management process for the project, described in the RMP, and compliant with [NCIA PDED 06.00.03, 2015] and NATO Risk Management Policy [AC/323-D(2018)0009].*

[SOW-150] *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-151] *The Contractor SHALL document and maintain status of all risks in the Risk Log (see 15.2) where he shall record and track all project risks regardless of their status.*

[SOW-152] *The Contractor SHALL update the project Risk Log at minimum on a monthly basis as an input for the Project Status Report (PSR).*

[SOW-153] *The Contractor SHALL add to the Risk Log additional risks identified by the Purchaser.*

[SOW-154] *Upon Purchaser request, the Contractor SHALL deliver the Risk Log to the Purchaser, throughout the duration of the Contract.*

4.5.2. Issue management

4.5.2.1. 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-155] *The Contractor SHALL establish and maintain a process for identifying, tracking, reviewing, reporting, and resolving all project issues.*

[SOW-156] *The Contractor SHALL describe the Issue Management Process in the CMP (see section 18.3).*

[SOW-157] *The Contractor SHALL develop and maintain an Issue Log (see Section 21.3) where he SHALL record and track all project issues regardless of their status.*

[SOW-158] *The Contractor SHALL include the Issue Log in the Configuration Management process and keep it under configuration control and in the Configuration Management Database (CMDB).*

[SOW-159] *The Contractor SHALL update Issue Log at minimum on a monthly basis as an input for the PSR.*

[SOW-160] *The Contractor SHALL add to the Issue Log additional issues identified by the Purchaser.*

[SOW-161] *Upon Purchaser request, the Contractor SHALL deliver the Issue Log to the Purchaser, throughout the duration of the Contract.*

4.5.3. Configuration management

4.5.3.1. The Contractor SHALL implement a Configuration Management plan to perform the Configuration Management functions as described in SECTION 12 of this SOW.

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

[SOW-162] *The Contractor SHALL implement a QA and QC plan as described in SECTION 17 SECTION 12 of this SOW.*

[SOW-163] *The Contractor SHALL deliver and maintain a Quality Assurance Plan as detailed in SECTION 11 of this SOW.*

4.5.5. Independent Verification & Validation (IV&V)

4.5.5.1. The Purchaser will be supported, quality monitored and reported, for corrective actions, by purchaser arranged IV&V services.

4.5.5.1.1. The IV&V services will entail the following activities:

a. Documentation assessment; this includes:
   i. System design documentation package assessment
   ii. Security documentation package assessment
   iii. Plans assessment
   iv. More generally assessment of project deliverables
b. Support to all types of tests. This includes:
   i. Attend and monitor the tests performed by the Contractor
   ii. Evaluate Contractor provided test plan, test procedures and reports
   iii. Provide independent reports
c. Testing. This includes the design and execution of independent tests, and the provision of the associated reports.
d. Monitor Contractor activities at Contractors' facilities
e. Attend any meeting as requested by the Purchaser

[SOW-164] *The Contractor SHALL fully support IV&V activities and in particular:*

- *Host inspection visits*

- *Make himself available for answering questions and furnishing information related to the project*
- *Allow inspection and monitoring of testing activities*
- *Allow inspection and monitoring of Contractor's processes applicable to this project*
- *Allow execution of independent testing activities.*

4.6. Project Management Communications

4.6.1. Project Status Report (PSR)

[SOW-165] *The Contractor SHALL provide, no later than the third working day of each month, a PSR. The Contractor's PSR SHALL be a monthly document to cover the previous month and include cumulative aspects of execution.*

[SOW-166] *The Contractor's PSR SHALL at minimum summarise completed, ongoing, and upcoming activities, as well as attached updated PMS as needed, Risk and Issue Log.*

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

[SOW-167] *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.*

4.6.2. Meetings

4.6.2.1. Except otherwise stated in the Contract, the following provisions shall apply to all meetings (including "attendance in person" meetings, video or tele conference meetings, reviews…) to be held under the Contract.

[SOW-168] *The Contractor SHALL take meeting minutes, submit them in draft version to the Purchaser for approval within 2 working days of the meeting. The minutes SHALL be submitted to an accelerated review cycle at Purchaser's discretion.*

[SOW-169] *The Contractor's representatives SHALL NOT regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract nor as a vehicle to alter the design or configuration of equipment or systems. The Contractor SHALL note that any such changes will only be made by authorised mechanisms as set forth in the Contract.*

[SOW-170] *The Contractor SHALL provide any documentation (even in draft format), that may be useful to the Purchaser in preparing for meetings and ensuring efficient discussions during the meetings no later than 2 working days before the meeting.*

4.6.2.2. Project Review Meetings (PRM)

[SOW-171] *The Contractor SHALL coordinate and hold PRM with the Purchaser at major milestones (listed in 3.1.2) throughout the Contract period of performance, as follows (-/+ 2 weeks around the date provided below):*

- *PRM#1 focused on IEG-C design at EDC+5*
- *PRM#2 focused on Factory Tests and Accreditation at EDC+9*

- *PRM#3 focused on Provisional System Acceptance and the IEG-C system going live*
- *PRM#4 focused on Final System acceptance and closing the project*

[SOW-172] *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-173] *At each PRM, the Contractor SHALL provide the status of all on-going tasks, the status of the Contract deliverables, identify any changes to the PMP, PMS, SIP, ILS Plan (ILSP), QAP, Issue Log, Change Requests document, Off-specifications document, baselines and Risk Log, and identify any problems.*

[SOW-174] *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.*

[SOW-175] *The Contractor SHALL provide minutes of the meeting. The minutes will include:*

- *Date, place, and time of the meeting:*
- *Purpose of the meeting;*
- *Name of participants;*
- *Approval of previous meeting's minutes and all resolutions;*
- *Record of principle points discussed, action taken, and decisions made*

4.6.2.3. The location of PRMs will in principle be at the Purchaser's premises in Mons (BEL) or in The Hague (NL) and when possible, they shall be scheduled with other project meetings. Attendance in person is preferred, but participation via video or telephone conference can be mutually agreed.

4.6.2.4. Product Delivery Meetings (PDM)

[SOW-176] *The Contractor SHALL organize PDMs.*

[SOW-177] *The Contractor's PDMs SHALL at minimum cover the following activities:*

- *Product Delivery Planning meeting with frequency of minimum 1 per month*
- *Product Delivery Review meeting with frequency of minimum 1 per month*
- *Product Delivery Progress Meeting with frequency of minimum every 2 working days*

[SOW-178] *The Contractor SHALL appoint his Team Manager or Tech Lead to organize all PDMs.*

4.6.2.5. Purchaser representative (Product Owner and/or Project Manager) will attend Product Delivery Planning and Review meetings and as needed also Product Delivery Progress Meetings.

[SOW-179] *The Contractor SHALL record all outputs from all PDMs in a product delivery toolset chosen, implemented and hosted by the Contractor.*

[SOW-180] *The Contractor SHALL ensure Purchasers access to the above-mentioned product delivery toolset.*

[SOW-181] *The Contractor SHALL report key outputs from PDMs such as delivery progress information (e.g., product backlog status, key test results, burn down / burnup*

charts) as well as key changes, issues and risks to the Contractor Project Manager who SHALL integrate that information in the PSR.

4.6.2.6. IPMT Meetings

4.6.2.6.1. Upon award of this Contract, the Contractor's Project Manager shall become an advisory member of the IEG-C IPMT.

[SOW-182] *The Contractor's Project Manager SHALL provide inputs to and attend IPMT meetings as requested by the Purchaser Project Manager.*

4.6.2.6.2. All IPMT meetings of the IEG-C will take place at the Purchaser premises (Brussels or Mons (Belgium) and/or The Hague – Netherlands).

4.6.2.7. Ad-hoc Security Working Group

4.6.2.7.1. The ad-hoc Security Working Group (with representatives from NATO SAAs and CISOA) can be established if certain security issues could not be solved via regular contacts between Purchased and Contractor SMEs.

[SOW-183] *For daily/regular contact the Contractor SHALL designate Security SMEs as points of contact for security accreditation and security-related issues.*

4.6.2.7.2. The Purchaser will host the Security Working Group Meetings.

4.6.2.8. Other Meetings

4.6.2.8.1. The Purchaser will host all other meetings agreed by both parties unless there is a specifically agreed need to review material, witness technical demonstrations, or perform any other activity outside of the Purchaser's premises as part of the meeting.

4.6.3. Project Website

[SOW-184] *The Contractor SHALL maintain a NATO RESTRICTED Project Portal (provided by the Purchaser) on which all relevant (classified up to and including NATO RESTRICTED) CO-14314-IEG-C project documentation and datasets shall be maintained. This Project Portal is created on the NATO RESTRICTED network at NCIA by the Purchaser, and will be accessed by the Contractor using the Purchaser provided REACH laptop(s) (See Annex B of the Contract Special Provisions) or any other approved device/mechanism for the exchange of NATO RESTRICTED information. Accreditation related documentation SHALL also be stored and referenced thereafter, in the NCIA Security Accreditation Portal.*

4.6.3.1. The Purchaser will provide the necessary access rights to the Contractor.

[SOW-185] *The Contractor SHALL maintain on this website all unclassified documents, as soon as they are submitted in draft version to the Purchaser. This includes all project deliverables, presentation materials from all meetings, as well as the Contract SOW and SRS, and all applicable documents. More generally, the website SHALL include any document as deemed necessary by the Purchaser.*

[SOW-186] *The Contractor SHALL identify all relevant classified documents on the Project Website, by title, unless a title itself is classified higher than NR and SHALL state from where the classified document can be obtained.*

4.6.3.2. The Purchaser is able to provide the Contractor with a capability (named "REACH") to exchange NATO RESTRICTED information over the Internet with the Purchaser.

4.6.4. Documentation Delivery and Review

[SOW-187] *The Contractor SHALL submit all documentation in electronic format to the Purchaser for review and comments as applicable.*

[SOW-188] *The Contractor SHALL NOT provide any Contractual documentation in a partial or gradual manner.*

[SOW-189] *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.*

4.6.4.1. Except otherwise stated for specific documents, the following provisions shall apply for any documentation to be provided by the Contractor under this Contract.

[SOW-190] *The Contractor SHALL provide a first version of each deliverable for Purchaser review. The first version SHALL be substantially complete and correct.*

4.6.4.2. 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-191] *The Contractor SHALL NOT rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.*

[SOW-192] *The Contractor SHALL resubmit the document as a revised version addressing the Purchaser's comments within two (2) weeks after receipt.*

4.6.4.3. 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-193] *The Contractor SHALL provide an updated version of the document within two weeks of receipt of the Purchaser's comments on the revised version.*

4.6.4.4. The above cycle shall continue until the document reach a quality level acceptable by the Purchaser, excluding security accreditation documentation for which NSAB approval will be required.

[SOW-194] *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.*

4.6.5. Co-ordination with other NATO projects

4.6.5.1. The NATO CIS environment will be under continual development by other NATO projects that are being implemented in parallel with the IEG-C Project.

4.6.5.2. The Purchaser will inform the Contractor and provide information concerning the operational environment that may emerge as a result of these projects.

[SOW-195] *The Contractor SHALL be able to adapt the IEG-C to accommodate this additional information.*

[SOW-196] *The Contractor SHALL incorporate in his activities the integration, performance, and schedule considerations related to the co-ordination of the IEG-C with the other Purchaser systems to be interfaced with it throughout the duration of the project.*

[SOW-197] *The Contractor SHALL identify any documents, meeting minutes, or other information from these projects required to maintain an effective co-ordination process.*

[SOW-198] *The Contractor SHALL include into Project Communication Plan (part of PMP) activities clearly identifying his proactive approach with regards to the coordination with other related NATO projects.*

4.6.6. Project-level communication

[SOW-199] *As a Project-level communication activity, the Contractor SHALL provide an IEG-C Information Sheet of maximum 2 pages providing an overview of the IEG-C system, its functions, external interfaces and major components, and its projected installation schedule.*

SECTION 5: SYSTEM ENGINEERING

5.1. General

5.1.1. This section outlines the System Engineering, Integration, Tests, and implementation of IEG-C Project.

[SOW-200] *The Contractor SHALL be responsible for the overall design, integration, obtaining security accreditation and system engineering of the IEG-C throughout the Contract period of performance.*

[SOW-201] *The Contractor SHALL develop the IEG-C System Design Specification (SDS) based on an analysis of the Purchaser's requirements.*

[SOW-202] *The Contractor SHALL integrate all necessary components to establish the IEG-C Product Baseline, and plan and execute a series of tests to confirm that this baseline meets its functional and non-functional requirements (portability, maintainability, security, reliability, usability, compatibility, performance, functional).*

[SOW-203] *The Contractor SHALL perform the activities described in this section considering that the IEG-C will integrate with a wide variety of NATO activities and systems (e.g., Core Services, Functional Area Services (FAS)).*

[SOW-204] *The Contractor SHALL be responsible for integration of the IEG-C System. This means both the integration of the various products that constitute the IEG-C System and the integration of the IEG-C System with other NATO systems.*

[SOW-205] *The Contractor SHALL make use of NCIA testbed (Annex B1) to perform the integration or more generally to conduct tests, and in particular the following Milestone events:*

- *Factory Acceptance Test (FAT at EDC+9MO) (see Section 3.5.4) at the Contractor premises if the contractor has chosen to develop on their own premises; or the Purchaser's Development and Integration Testing Environment (see Section 5.1.1.2) if the Contractor has chosen to develop on the Purchaser's Development and Integration Testing Environment.*
- *Integration and Interoperability tests (SIT milestone at EDC+17mo) related to the integration of the IEG-C system with other NATO systems, at the Purchaser's Development and Integration Testing Environment.*
- *System Acceptance Test (SAT) and User Acceptance Test (UAT) for the Formal Verification and Validation and the execution of tests in support of NATO's change process with the objective to achieve Deployment Authorization, at the NATO Enterprise Reference System (see Section 5.1.1.7).*

5.1.1.1. As an option, the Contractor may use the Purchaser's Development and Integration Test Environment for the development of the IEG-C, at Contractor's cost. The Development and Integration Test Environment makes the Purchaser's tool chain for development and testing available to the Contractor.

5.1.1.2. The Purchaser's Development and Integration Test Environment is a test environment configured to provide a representation of the target network/security domain. It will include the necessary configurations and interfacing systems and services to represent the live environment for test purposes. It will also include test harnesses and test data.

5.1.1.3. The IEG-C Integration Test System will be created based on the System Specifications provided by the Contractor but as a virtualized system and not necessarily reflect the same performance or storage capacity.

5.1.1.4. All hardware (server, storage, network elements and workstations) and Virtualisation Platform for the Development and Integration Test Environment will be provided by the Purchaser for the tests related to the integration of the IEG-C system with other NATO systems.

5.1.1.5. The Purchaser will prepare the Virtual Environment for the IEG-C Integration Test System on the Development and Integration Test Environment.

[SOW-206] *The Contractor SHALL deliver and install the IEG-C Integration Test System with all its components as defined in ANNEX B, in compliance with the processes described in SECTION 13 as a virtualized system and SHALL integrate it within the contractor provided Development and Integration Test Environment.*

[SOW-207] *The Contractor SHALL provide the operating systems and any other COTS software needed by the IEG-C Integration Test System with the necessary Original Equipment Manufacturer's manuals and licenses unless agreed to be provided by the Purchaser.*

[SOW-208] *The Contractor SHALL install the COTS software on the IEG-C Integration Test System and apply the necessary configuration.*

[SOW-209] *The Contractor SHALL implement a procedure to ensure that the IEG-C Integration Test System is representative of the actual operational system, in particular in terms of design and configuration, and software versions.*

[SOW-210] *The Contractor SHALL establish and update the IEG-C Integration Test System on the Purchaser prepared Development and Integration Test Environment prior to the relevant events.*

[SOW-211] *The Contractor SHALL update the IEG-C Integration Test System with each new release until FSA.*

[SOW-212] *The Contractor SHALL demonstrate how the Purchaser will have to make use of the IEG-C Integration Test System to adapt any existing software, scripts, reports etc. to changing requirements (this encompasses both development and testing activities).*

5.1.1.6. As an option, the Contractor can use their own data generators, to provide test feeds to the IEG-C Integration Test System.

5.1.1.7. The IEG-C Reference System is a reference system configured to provide a representation of the target network/security domain. It will include the necessary configurations and interfacing systems and services to represent the live environment for verification and validation purposes. It will also include test harnesses and test data.

5.1.1.8. All hardware (server, storage, network elements and workstations) for the virtualized elements of the IEG_C Reference System will be provided by the Purchaser for the tests related to the integration of the IEG-C system with other NATO systems.

[SOW-213] *The Contractor SHALL deliver hardware components for elements of the IEG-C Reference System that cannot be virtualized.*

5.1.1.9. The Purchaser will prepare the Virtual Environment for the IEG-C Reference System on the NATO Enterprise Reference System.

[SOW-214] *The Contractor SHALL deliver and install the IEG-C Reference System with all its components as defined in ANNEX B, in compliance with the processes described in SECTION 13, and SHALL integrate it within the Contractor provided NATO Enterprise Reference System.*

[SOW-215] *The Contractor SHALL provide the operating systems and any other COTS software needed by the IEG-C Reference System with the necessary Original Equipment Manufacturer's manuals and licenses unless agreed to be provided by the Purchaser.*

[SOW-216] *The Contractor SHALL install the COTS software on the IEG-C Reference System and apply the necessary configuration.*

[SOW-217] *The Contractor SHALL implement a procedure to ensure that the IEG-C Reference System is representative of the actual operational system, in particular in terms of design and configuration, performance, security settings, and software versions.*

[SOW-218] *The Contractor SHALL demonstrate how the Purchaser will have to make use of the IEG-C Reference System to adapt any existing software, scripts, reports etc. to changing requirements (this encompasses both development and testing activities).*

[SOW-219] *The Contractor SHALL establish and update the IEG-C Reference System on the Purchaser prepared Development and Integration Test Environment prior to the relevant events.*

[SOW-220] *The Contractor SHALL update the IEG-C Reference System with each new release until FSA.*

[SOW-221] *The Contractor SHALL deliver and activate the IEG-C Reference System. The Contractor SHALL deliver all documents as required in this section for the Reference System (e.g., SIP, accreditation documents, etc.).*

5.1.1.10. As an option, the Contractor can use their own data generators, to provide test feeds to the IEG-C Reference System. In this case, the Contractor shall deliver all documents as required in 3.5.3 for the Reference System (e.g., SIP, accreditation documents, etc.).

5.2. Orientation Workshop

[SOW-222] *The Contractor SHALL conduct a workshop (at a Purchaser-provided facility) to orient the IEG-C Platform Administrators and other stakeholders on the overall system design and capabilities. This workshop can be combined with the CDR. As part of this workshop, the Contractor SHALL:*

- *deliver overview briefings on the anticipated IEG-C system, and lead question and answer sessions with the attendees;*
- *provide visuals, models, demonstration as necessary;*
- *provide information about the anticipated IEG-C System Implementation;*
- *provide information about how the System Design fully meets the requirements specified in this SOW and SRS;*
- *provide an overall description of the external interfaces;*
- *provide an overall description of the ILS concept and strategy;*
- *Provide an overall description of Configuration Management and Quality concept and strategy.*

- *Collect any necessary information from the IEG-C Administrators, CIS Security Administrators and other stakeholders in order to perform the design activities. As required, the Contractor SHALL conduct further dialogue with the IEG-C Administrators, CIS Security Administrators and other stakeholders.*

[SOW-223] *The Contractor SHALL propose the event date minimum 2 months in advance to allow the coordination time with various stakeholders. The Contractor SHALL provide the proposed content for the workshop including schedule, coverage, content, presentation and the information for Purchaser approval minimum 4 weeks prior to the event.*

5.2.1. This workshop is a key meeting in the course of the Project. As any other meeting outcomes of such will be subject to the Purchaser Acceptance.

5.3. System Requirements Analysis and Review

5.3.1. Review of the requirements

[SOW-224] *The Contractor SHALL review the IEG-C SRS and all applicable documents, meet and communicate with NATO SMEs as necessary, and present its findings in terms of proposed changes to the SRS based on system cost, schedule, or performance impacts.*

[SOW-225] *The Contractor SHALL also identify any inconsistencies within the requirements. Any inconsistencies not identified by the requirements review will not be accepted later as the basis for a change with cost impact.*

[SOW-226] *The Contractor SHALL host and conduct a System Requirements Review (SRR at EDC+2MO) to present and discuss its findings and proposed changes to the requirement baseline for the design and integration of the IEG-C project. The purpose of this review is to agree upon the requirement baseline for the design and integration of the IEG-C system.*

[SOW-227] *The Contractor SHALL produce and provide a set of minutes that accurately reflect the discussions taken during the SSR meeting and provide them to the purchaser within 1 week of the meeting.*

5.3.2. Change Requests

[SOW-228] *Upon completion of the SRR, the Contractor SHALL identify any proposed changes to System Requirements Specification in the form of one or more Change Requests (i.e. ECPs). The Contractor SHALL address these Change Requests according to the processes implemented by the Contractor to meet the requirements of 12.6 and of 15.5 Change Request.*

5.3.2.1. The Purchaser will update and provide an updated Functional Baseline (FBL; see 18.2.2) as necessary to reflect the decision of the IEG-C CCB on these Change Requests.

[SOW-229] *The Contractor SHALL use the updated FBL as the basis for the IEG-C system design and subsequent activities.*

5.4. System Design

5.4.1. Design activities

[SOW-230] *The Contractor SHALL review the Purchaser-provided provided IEG-C Target Architecture [NCIA TR/2016/NSE010871/01, 2017].*

[SOW-231] *The Contractor SHALL consider this Target Architecture as a document for information which should be helpful to conduct its design activities. Therefore, the Contractor SHALL NOT consider the Target Architecture as a binding document.*

[SOW-232] *The Contractor SHALL conduct the necessary Design Activities and develop its own complete design of the IEG-C at the Preliminary and Critical levels, including all interfaces to other systems to meet the SRS.*

[SOW-233] *The Contractor SHALL keep the system design documentation package (including security accreditation documentation) up to date throughout project execution, in particular as a result from the site surveys and/or in order to obtain the security accreditation.*

[SOW-234] *The Contractor's IEG-C System Design SHALL cover all sites identified for this project.*

[SOW-235] *The Contractor's IEG-C architecture SHALL be designed so that it can be reused for other security classification levels (in any case, the system will be installed and operated at System High/NS mode of operation).*

[SOW-236] *The Contractor's IEG-C architecture SHALL be designed to be modular design, allowing for future extension and enhancements.*

[SOW-237] *The Contractor's IEG-C architecture SHALL be designed so that it can be reused in the deployed environment.*

[SOW-238] *The Contractor SHALL agree coding syntax(es) with the Purchaser during the Design Stage.*

[SOW-239] *The IEG-C Contractor SHALL ensure that the design is compliant with and covers the System Operations Processes.*

5.4.2. System Design Documentation Package

[SOW-240] *The Contractor SHALL establish, deliver and maintain the IEG-C System Design Documentation Package, comprising of:*

- *The System Design Specification (SDS),*
- *The Interface Control Document (ICD),*
- *The Security Accreditation Documentation Package*
- *The Master Test Plan (MTP), and*
- *The Requirements Traceability Matrix (RTM).*

[SOW-241] *The duration of the review cycle for the IEG-C System Design Documentation Package SHALL be 4 (four) weeks.*

[SOW-242] *The Contractor SHALL prove the design through the regime of testing set forth in the Contract and the Contractor SHALL be responsible in the event that the system proves deficient in meeting the Contractual requirements.*

[SOW-243] *As part of the Configuration Management activities, and like any other management product or specialist product, the Contractor SHALL update the System Design Documentation Package to reflect changes, at least at each of the following major milestones: a new design review, the start of a test phase, the completion of each tests activities, the start of the deployment, PSA, FSA.*

[SOW-244] *The Contractor SHALL ensure that in order to maintain clear consistency throughout all documents in the System Design Documentation Package, any update of any of the documents comprised in the System Design*

Documentation Package SHALL result in re-delivery of a new version of the complete System Design Documentation Package.

5.4.2.1. System Design Specification (SDS)

[SOW-245] *The Contractor's SHALL ensure the SDS describes the IEG-C System to a level of detail that is sufficient for the Purchaser to be able to understand how the requirements in the SRS and the security requirements (see ANNEX A) are implemented.*

[SOW-246] *In particular, the Contractor SHALL ensure IEG-C SDS addresses the IEG-C Operational Requirements (see SRS).*

[SOW-247] *The Contractor SHALL ensure the IEG-C SDS is developed as per the detailed contents indicated in section 15.6.*

5.4.2.1.1. Interface Control Document (ICD)

[SOW-248] *Reserved ~~The Contractor SHALL document, as specific annexes to the ICD:~~*

- *~~Each direct interface between the IEG-C and NEDS to include detailed descriptions of any "configuration settings" and agreements to enable synchronisation between IEG-C and NEDS.~~*
- *~~Each direct interface between the IEG-C and other systems (e.g., AIFS, E-NPKI)~~*
- *~~Each interface between the IEG-C subordinate or superior IEG-C components~~*
- *~~Each interface between the IEG-C and end-entity users and devices SHALL be documented~~*

[SOW-249] *Where work was conducted by the Contractor under this Contract to document the design of any system to be interfaced to the IEG-C project, Contractor SHALL ensure the results of that work are included in the relevant annex of the ICD.*

[SOW-250] *The Contractor SHALL develop the ICD in accordance with the template provided by the Purchaser.*

5.4.2.1.2. Security Accreditation Documentation Package

[SOW-251] *The Contractor SHALL ensure that the Security Accreditation Documentation Package comprises all documentation mentioned in Section 10.3.*

5.4.2.1.3. Requirements Traceability Matrix (RTM)

[SOW-252] *The Contractor SHALL develop and maintain a RTM that establishes a complete cross-reference between on the one hand the requirements stated in the SRS, System Security Requirements Statement (SSRS), and on the other hand the detailed contents of the SDS in terms of SDS statements and lowest-level CIs.*

5.4.2.1.3.1 The minimum contents of the RTM are listed in Section 8.3.5 Requirement Traceability Matrix RTM.

5.4.3. Disaster Recovery Plan (DRP) and Backup Plan

[SOW-253] *The Disaster Recovery Plan & Procedures and the Backup Plan & Procedures prepared by the Contractor SHALL address the best practices developed by the vendors of the system components, including security best practices.*

[SOW-254] *The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL address all possible scenarios and corresponding actions, including security.*

[SOW-255] *The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL align with the site-specific Disaster Recovery Plan & Procedures, including those defined in the ITM Joining Instructions.*

[SOW-256] *The Contractor SHALL ensure the Backup Plan & Procedures align with the site-specific Backup Plan & Procedures, including those defined in the ITM Joining Instructions.*

[SOW-257] *As a minimum, the Contractor SHALL ensure the Disaster Recovery Plan and Procedures address the following scenarios:*

- *Recovery of an entire IEG-C;*
- *Transfer of an IEG-C service from one platform to another.*
- *The Contractor SHALL define for every IEG-C component:*
- *Storage capacity for back up*
- *Type of storage to use*
- *Back up frequency*
- *Type of back up (full or incremental)*
- *Level of information to back up*

[SOW-258] *The Contractor SHALL ensure the Disaster Recovery Plans & Procedures clearly distinguish between service restoration and data restoration, and SHALL include a disaster recovery kit.*

[SOW-259] *The Contractor SHALL deliver the disaster recovery kit which SHALL contain distribution media for all software (including versions, upgrades/updates, patches and hot-fixes) to restore an IEG-C Element from "bare metal", in accordance with site-specific Disaster Recovery plans.*

[SOW-260] *The Contractor SHALL deliver the disaster recovery kit that includes a full, customized, installation plan that covers all steps (including Operation System (OS) installation) to build and configure each of the IEG-C components.*

[SOW-261] *The Contractor SHALL ensure that Volume Shadow copy service SHALL be used to optimize the backup/recovery process where appropriate.*

[SOW-262] *The Contractor SHALL ensure that disaster recovery and back-up procedures is included in the Technical Manuals and SHALL be a dedicated section of it.*

[SOW-263] *The Contractor SHALL ensure that disaster recovery Kit is analysed in terms of ILS resources and all the necessary resources and support needed for disaster recovery is produced as required in SECTION 6 : Integrated LOGISTICS Support (ILS) of this document.*

5.4.4. Design Reviews

[SOW-264] *The Contractor SHALL conduct Design Reviews, a Preliminary Design Review (PDR at EDC+3MO) and a Critical Design Review (CDR at EDC+6MO), to present the IEG-C Design Documentation Package. The Contractor SHALL include the following areas in the Design Review:*

- *IEG-C overall system architecture and interactions*
- *System functionality, modularity and interfaces, breakdown into lowest-level Configuration Items (CI; see section 12.4 for CIs identification)*

- *Off-the-shelf products to be used in the system: the Contractor SHALL identify the intended product and version, and note if any additional elements (such as macros or plug-ins) are required*
- *Interfaces with other relevant systems (i.e., with NEDS)*
- *System security design: Presentation of the Risk Assessment Methodology that the Contractor intends to use for the Project, Results of the Risk Analysis, Definition and implementation of the Security measures to counter the risks that will be identified in the Security Risk Assessment (SRA). This presentation SHALL be done as a separate item.*
- *Sequence and scope of system tests of the ABL and any requirements for Purchaser support and participation*
- *Any change request or off-specification*
- *Any changes to the PBS and PFD*
- *Any changes to the PMS*
- *Cost considerations*
- *Risk assessment of proposed changes and an update of the Risk Log and Issue Log*
- *RTM*
- *MTP traceable to system system/component requirements and acceptance criteria.*

[SOW-265] *The Contractor SHALL provide a Design Review Report for every Design review cycle.*

[SOW-266] *The Contractor SHALL update the Design Documentation Package as per the result of the Design Review.*

SECTION 6: INTEGRATED LOGISTICS SUPPORT (ILS)

6.1. General

6.1.1. This section outlines the supportability requirements of the project.

[SOW-267] *The Contractor SHALL identify in the PMS of the PMP the Contractor activities and milestones related to ILS.*

[SOW-268] *The Contractor SHALL use the [ALP 10-2016] and [AIA/ASD SX000i, 2016] specification as guidance when establishing and conducting the ILS Process (i.e. Integrated Logistics Support – ILS Process), in accordance with the requirements of the contract.*

[SOW-269] *The Contractor SHALL use [ADMP-1], [ADMP-2], [MIL-HDBK-338B], [MIL-HDBK-470A], [MIL-STD-1388-1A], [MIL-STD-1388-2B] and [ASD S3000L] as guidance when establishing and conducting the Logistic Support Analysis (LSA) programme, including the RAMT programme, in accordance with the requirements of the Contract.*

6.2. Integrated Logistics Support Plan (ILSP)

[SOW-270] *The Contractor SHALL provide and maintain an ILSP, tailored to the Project Program phases.*

[SOW-271] *The Contractor SHALL develop the ILSP in accordance with the requirements described in this section and cover all areas.*

6.2.1. The ILSP is a standalone Product Lifecycle documents that will survive the project after FSA. As such, these documents are not to be submitted as part of the PMP, but will be part of the Technical Proposal.

[SOW-272] *The Contractor SHALL detail in the ILSP how ILS will be designed, managed, procured and provided throughout the system lifetime.*

[SOW-273] *The Contractor SHALL provide an updated version of the ILSP to the Purchaser for each milestone for Purchaser acceptance.*

[SOW-274] *The Contractor SHALL cover the following sections at minimum including the processes to perform the related activities in ILSP:*

- *The Contractor's ILS organization, roles, responsibilities and procedures;*
- *Maintenance Concept (Maintenance Plan, detailed Maintenance Level definitions and tasks);*
- *Planning of supply support (System Inventory, Codification, Recommended Spare Parts and Consumables list);*
- *Design Influence*
    - *i. Reliability, Availability, Maintainability and Testability (RAMT) Programme planning, activities, processes (including testing);*
    - *ii. Logistics Support Analysis planning, activities and processes;*
    - *iii. Support Case planning, releases and processes.*
- *Support and Test Equipment Lists;*
- *Computer Resources (licences, SWDL etc.);*

- *Manpower and Personnel Requirements;*
- *Technical Documentation (organization, process, inputs, reviews, release schedule)*
- *Planning of packaging, handling, storage, and transportation (PHS&T);*
- *Planning of supply chain security.*
- *In-Service Support Plan (as an annex)*

6.2.2. The acceptance of the ILSP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

[SOW-275] *The Contractor SHALL maintain and update the ILSP as required to reflect changes in the Project Baselines, in the SOW, or in support arrangements for any IEG-C System CIs.*

[SOW-276] *The Contractor SHALL provide an In Service Support Plan (ISSP) as an annex to the ILSP and SHALL cover the following topics at minimum with practical instructions:*

- *the Contractor's Support organization, roles, responsibilities, processes and procedures (between PSA and FSA; and during warranty);*
- *description of the system of interest (SOI) in scope of integrated support,*
- *description of the integrated support concept, including the maintenance concept, warranty concept, customer support concept, service management & control concept including but not limited to the incident, problem management, release and deployment management, and configuration and change management;*
- *description of the parties involved, their responsibilities for the various levels of support (with indication of start and end dates), interfaces, response times and POC details;*
- *description and allocation of operation, SM&C and corrective and preventive maintenance tasks required to operate and maintain the system;*
- *description of the Sustainability measures (obsolescence management, failure reporting, performance monitoring, reliability and availability assessment and reporting);*
- *procedures to follow when any part of the system fails; response times for analyses and resolution by the Contractor,*
- *comprehensive lists of all available spares, consumables, software licenses (SWDL), support software tools, COTS documentation, technical documentation, training documentation and manuals.*

[SOW-277] *The Contractor SHALL provide the latest ISSP as part of PSA (EDC+20mo) and FSA (EDC+27mo) milestone achievement.*

6.3. Maintenance and Support concept

[SOW-278] *As an Annex of the ILSP and in accordance with SOW ANNEX F, the Contractor SHALL develop and maintain the IEG-C System Maintenance and Support Concept that defines the maintenance and support environment, constraints, locations, procedures, artefacts, organisation and personnel skills to maintain the Delivered baselines of the IEG-C Capability.*

[SOW-279] *The Contractor SHALL design/deliver the system/elements and the Operation/Support/Maintenance documentation, training, instructions, and resources (skills, tools/test equipment) in order to allow the Purchaser to fully operate the system, to perform Level 1, Level 2 and Level 3 Maintenance and Support from the Provisional Site Acceptance (PSA).*

[SOW-280] *Starting from PSA (EDC+20mo) and until FSA (EDC+27mo) with all the sites are completed; the Contractor SHALL be responsible for the Level 2, Level 3 and Level 4 maintenance and support activities in each activated site within the scope of the Initial Operational Support.*

[SOW-281] *Starting from FSA and until the end of warranty period, the Contractor's dedicated on-site interventions and/or off-site resolutions SHALL carry on all maintenance activities beyond Purchaser capabilities/skills (as per Maintenance Concept and Contractor delivered training and documentation) required to restore the System from a critical failure.*

[SOW-282] *The Contractor SHALL ensure the Maintenance and Support Concept fulfills the functional and non-functional Requirements of the IEG-C System.*

[SOW-283] *The Contractor SHALL ensure the Maintenance and Support Concept defines the Maintenance and Support tasks at any level of support and at any level of maintenance.*

[SOW-284] *The Contractor SHALL ensure the Maintenance and Support Concept defines the Delivered Baselines maintenance and supply flow amongst the various NATO locations, organisations, groups, and people.*

[SOW-285] *The Contractor SHALL ensure the Maintenance and Support Concept defines and describes the Maintenance and Support process interfaces to all other processes.*

[SOW-286] *The Contractor SHALL define the 2nd and 3rd Level Support process interfaces to the other processes, including the existing NCIA Service Desk (1st Level of Support).*

[SOW-287] *The Contractor SHALL ensure the Support process interface definition includes the input and output information, its structure, the communication path (i.e., Points of Contact (POC)), the time constraints for sending and receiving information, and quality criteria to evaluate the integrity of the interface. This SHALL Include the related ITIL Processes to be tailored and detailed for the purposes of IEG-C System Support Concept.*

[SOW-288] *At each Support and Maintenance Level, the Contractor SHALL ensure the Support Concept describes the support environment, constraints, locations, procedures, artefacts, organisation and personnel.*

[SOW-289] *The Contractor SHALL ensure the procedural description includes objective(s), triggering event(s), input(s), output(s), task(s), roles and responsibilities (Responsible, Accountable, Consulted and Informed (RACI) format), constraints, exceptional case(s), and tool(s) support.*

[SOW-290] *The Contractor SHALL ensure the IEG-C System ILSP is based on the established Support Concept, approved by the Purchaser before the CDR (EDC+6MO) milestone.*

6.4. Design Influence

6.4.1. Reliability, Availability, and Maintainability (RAM) Requirements

[SOW-291] *The Contractor SHALL develop its RAM Programme and perform the analysis based on the RAM metrics and requirements outlined in the SRS.*

[SOW-292] *The Contractor SHALL ensure the design of the system includes sufficient redundancy and other Reliability, Maintainability, Availability and Testability measures to ensure the RAM requirements in this Contract are achieved and attained at an optimal Total Cost of Ownership (TCO), minimising preventive maintenance, manpower requirement and usage of special-to-type tools and test equipment.*

[SOW-293] *The Contractor SHALL document in the Support Case such measures taken to ensure fulfilment of RAM requirements and optimisation of TCO.*

[SOW-294] *The Contractor SHALL ensure the RAM analysis clearly captures and displays the RAM characteristics of each main component, aggregated up to the level of sub-system, and subsequently the entire system. System breakdown in line with the configuration item structure SHALL be used as reference to perform the analysis.*

[SOW-295] *The Contractor SHALL ensure the RAM is used to calculate and predict intrinsic availability and operational availability, as defined in SRS, for each type of subsystem, each type of node and each type of end-to-end connection.*

[SOW-296] *The Contractor SHALL ensure the RAM analysis includes the reliability prediction based on the proposed design solution and created RBDs, as well as the reliability allocation model to include to trigger the design changes*

[SOW-297] *The Contractor SHALL ensure the RAM analysis includes Failure Modes, Effects and Criticality Analysis (FMECA) in accordance with MIL-STD-1629A.*

[SOW-298] *The Contractor SHALL ensure that the first issue RAM analysis is performed and delivered before PDR (EDC+3MO) , updated before CDR and finally accepted at CDR (EDC+6MO), to include all relevant data to demonstrate compliance with the SRS and SOW requirements. The Contractor SHALL document such data in the Support Case as outlined below.*

6.4.2. Logistics Support Analysis (LSA)

[SOW-299] *The Contractor SHALL conduct a Logistic Support Analysis (LSA) Process, tailored to support the specific scope of the System operation activities.*

[SOW-300] *The Contractor's LSA analysis SHALL include, as a minimum:*

- *Task Analysis for identification of operational tasks, Service Management and Control (SMC) tasks; and administration and maintenance tasks (corrective, preventive, adaptive)*
- *Level of Repair Analysis (LORA) to determine the correct level of Support/Maintenance needed to perform each Operational and Maintenance task*
- *Planning and execution of the O&M Procedures Verification Test with references to the Master Test Plan.*
- *Total Cost of Ownership Analysis, which SHALL include the warranty cost and all the operational costs and all the maintenance cost for all the support and Maintenance levels for at least 5 years after FSA*
- *Obsolescence Analysis and Management for each software and hardware CI from end of sales, end of production and end of support perspective. .*

[SOW-301] *The Contractor's analysis SHALL contain also the list of procedures needed to configure the capability for mission and/or exercise environment.*

[SOW-302] *The Contractor SHALL ensure that Operation tasks are identified through analysis of the functional and non-functional requirements of the new system taking into account mission scenarios and conditions under which the system will be operated.*

[SOW-303] *The Contractor SHALL ensure the analysis examines each system function allocated to personnel and determines what operator tasks are involved in the performance of each system function.*

[SOW-304] *The Contractor SHALL ensure that maintenance tasks are identified using the RAM data and results.*

[SOW-305] *The Contractor SHALL ensure the SMC tasks are identified through analysis of all functions related to customer support and SMC.*

[SOW-306] *For each task in Task Analysis, the Contractor SHALL determine the properties and physical resources required to execute the task. For that purpose, each task SHALL be analysed to identify and capture:*

- *The support level to be assigned;*
- *Location/ facility involved;*
- *Personnel skills required;*
- *Roles (as they are assigned in Purchaser's maintenance and support organization);*
- *Task duration and frequency, reusing Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) data available;*
- *Manpower required.*

[SOW-307] *For each task, the Contractor SHALL perform a cost calculation based on the properties and physical resource requirements of each task.*

[SOW-308] *The Contractor SHALL ensure the cost calculation provides an estimated annual cost for each task.*

[SOW-309] *The Contractor SHALL ensure the data and results of the Task Analysis are used as input to the development of technical publication (all manuals at any level of maintenance) and the development of training material.*

6.4.3. Support Case

[SOW-310] *The Contractor SHALL document the LSA and RAM process, resourcing and organization, inputs, outputs, methodology, and timelines within ILSP.*

[SOW-311] *The Contractor SHALL develop and maintain the necessary Support Cases in which all LSA and RAM activities SHALL be documented, which include:*

- *System description and breakdown down to lowest level of maintenance significant items (I.e. LRUs, SRUs) and in accordance with the CI structure and identifications*
- *All COTS equipment datasheets, clearly indicating the reliability and maintainability characteristics which will be used as input for LSA and RAM.*

- *Availability, Reliability, and Maintainability analysis modelling, calculations and results (complete set of Reliability Block Diagrams (RBDs), FMECA including a list of critical items);*
- *Spare part calculations and modelling,*
- *Recommended Items List (RIL) including spares, consumables, tools and test equipment with rationale and justifications,*
- *The complete data for LSA activities and results,*
- *The complete data set of the Task Analysis, including listings of all operation tasks, SMC tasks, administrative tasks, corrective maintenance tasks and preventive maintenance tasks;*
- *References to the Master Test Plan and other relevant testing documentation for RAM requirements verification and validation;*
- *The results of the Disaster Recovery Logistic Analysis.*
- *The results from the O&M Procedures Verification Test;*
- *The Total Cost of Ownership Analysis results*
- *The Obsolescence Analysis results*

[SOW-312] *The Contractor SHALL ensure its Support Case forms a body of evidence, providing sufficient credibility that all LSA and RAM requirements outlined in SOW 6.4.1 and 6.4.2, and SRS have been met and providing credibility to the data used and the results achieved in all calculations and models.*

[SOW-313] *The Contractor SHALL ensure its Support Case provides rationale and justifications for all data and formulas used in any of the calculations and models.*

[SOW-314] *The Contractor SHALL ensure that the first issue of Support Case is delivered before PDR (EDC+3MO) encompassing all the design details up to the PDR milestone, updated before CDR and accepted at CDR (EDC+6MO), to include all relevant data to demonstrate compliance with the SRS and SOW requirements.*

6.5. Technical Documentation

[SOW-315] *The Contractor SHALL provide all the technical documentation for IEG-C System.*

[SOW-316] *The Contractor SHALL ensure all the Technical Documentation is kept updated and under configuration control for the entire life cycle of the system.*

[SOW-317] *The Contractor SHALL ensure the information contained in each technical documentation is coherent with the operational configuration deployed, i.e., OBL.*

6.5.1. This SOW specifies the format for each type of technical documentation.

[SOW-318] *The Contractor SHALL ensure the technical documentation consists (as a minimum) of:*

- *Training documentation*
- *Operation and User Manuals*
- *Maintenance Manual (including administration manuals)*
- *OEM Manuals for Commercial-Off-The-Shelf (COTS) products*

- *As-Built Documentation*
- *Other project documentation as required in this SOW.*

[SOW-319] *The Contractor SHALL ensure the all activities, milestones and actors associated with the development of technical documentation are described in the ILSP.*

[SOW-320] *The Contractor SHALL ensure all technical documentation SHALL be provided in the English language.*

[SOW-321] *The Contractor SHALL provide technical documentation as required in the various Sections of this SOW.*

[SOW-322] *The Contractor SHALL ensure the Classification of Technical documentation is at the lowest level possible.*

[SOW-323] *The Contractor SHALL ensure the all documents, however short, identify the complete name and version of the software they refer to, originator, date of production, the type of document, and Configuration Management information of the document itself.*

[SOW-324] *The Contractor SHALL ensure the all documents also contain a list of those CIs (title and version identifier) that the document or parts thereof refer to.*

[SOW-325] *The Contractor SHALL submit all final and accepted versions of documentation deliverables in electronic format, as Portable Document Format (PDF).*

[SOW-326] *The Contractor SHALL submit documentation, intended for review by the Purchaser, with each modification identified through the change tracking feature or otherwise marked.*

[SOW-327] *The Contractor SHALL submit documentation, intended for review by the Purchaser, in electronic format.*

[SOW-328] *The manuals SHALL supplement the COTS O&M documentation the Contactor SHALL provide with the IEG-C System.*

[SOW-329] *The Contractor SHALL capture and document lessons learned during the System development and the System Installation.*

[SOW-330] *If activated, the Contractor SHALL provide updated technical documentation in accordance with Section 6.5 to cover the changes for each optional site and service outlined in the SSS.*

6.5.2. Operation and User Manuals

[SOW-331] *The Contractor SHALL develop, provide and maintain the System Operation Manual (SOM).*

[SOW-332] *The Contractor SHALL provide an Operation Manual that describes the complete system by the explanation of functional blocks and CIs (HW, SW).*

[SOW-333] *The Contractor SHALL provide an Operation Manual that defines the in-depth, step-by-step procedure how to operate the system and how to perform Level 1 maintenance tasks.*

[SOW-334] *The Contractor's SOM SHALL include all the possible system operations in order to safely operate and use the capability.*

[SOW-335] *The Contractor SHALL ensure the operation described in the Manual is an outcome of the Operation and maintenance Task Analysis as described in this SOW.*

[SOW-336] *The Contractor SHALL ensure that each and every procedure include as a minimum the following information:*

- *Location/facility involved (if the operation is performed remotely, it has to be specified);*
- *Personnel skills required;*
- *Task duration and frequency, reusing MTBF and MTTR data available;*
- *Manpower required;*
- *Tools and special tools required (if any);*
- *The steps needed to perform the operation.*

6.5.3. Maintenance and Administration Manuals.

[SOW-337] *The Contractor SHALL develop, provide and maintain the System Maintenance and Administration Manual.*

[SOW-338] *The Contractor SHALL ensure the Maintenance Manual contains all possible Scheduled and Unscheduled maintenance procedures and all possible Administration procedures as requested in this SOW.*

[SOW-339] *The Contractor SHALL ensure the Maintenance Manual contains a full illustrated product breakdown list. The Contractor SHALL ensure that all CIs and all items required for maintenance are included in this full product breakdown list.*

[SOW-340] *The Contractor's Maintenance Manual SHALL provide functional descriptions and specifications, with appropriate drawings, of the mechanical, electrical, and electronic assemblies, sub-assemblies, physical and logical components, configuration files and interfaces that comprise the system.*

[SOW-341] *The Contractor's Maintenance Manual SHALL provide information, illustrations, and procedures required for: deployment, installation, configuration, provisioning, disaster recovery, backup/restore, BIT/condition monitoring, fault finding and fault isolation/ troubleshooting techniques, test remove/ replace; and check out of each hardware and software item with relevant safety instructions.*

[SOW-342] *The Contractor's Maintenance Manual SHALL provide description of all the configuration settings for the modules, services and components/ how configuring the logging and uses of performance counters/ where finding the log files/ the different categories of logging/ the different performance counter categories.*

[SOW-343] *The Contractor's Maintenance Manual SHALL provide the description for the usage of all third-party applications needed to configure, manage and maintain the system.*

[SOW-344] *The Contractor's Maintenance Manual SHALL provide the descriptions of all indicators, switches, switch positions, and displays.*

[SOW-345] *The Contractor's Maintenance Manual SHALL define the in-depth, step-by-step procedure how to perform the 1st, 2nd and 3rd level corrective and preventive maintenance tasks and SM&C tasks.*

[SOW-346] *The Contractor's Maintenance Manual SHALL include a maintenance plan to cover all the preventive maintenance activities based on the operational time or calendar time as applicable.*

[SOW-347] *The Contractor SHALL ensure the Procedures contained in the manuals are an outcome of the O&M Task analysis requested in Section 11.5.2.*

[SOW-348] *The Contractor SHALL ensure the manual includes an annex with troubleshooting information that provides breakdowns of actions to be performed to solve a full range of (potential) problems or provide workarounds (Problem Management).*

[SOW-349] *The Contractor SHALL ensure the manual contains all possible configuration information and settings.*

[SOW-350] *In case Software Identifier (SWID) tags cannot be automatically installed by software installers (e.g., legacy or third party software), the Contractor SHALL include in installation documentation descriptions of the process to manually install SWID tags.*

[SOW-351] *The Contractor SHALL ensure the manual contains all possible information on the use and locations of Log Files.*

[SOW-352] *The Contractor SHALL ensure that each and every procedure include as a minimum the following information:*

- *The support level to be assigned;*
- *Location/facility involved (if the operation is performed remotely, it has to be specified);*
- *Personnel skills required;*
- *Task duration and frequency (if applicable), reusing MTBF and MTTR data available;*
- *Manpower required;*
- *Tools, test equipment and special tools required (if any);*
- *The steps needed to perform the procedure.*

6.5.4. OEM Manuals for Commercial Off the Shelf (COTS) product

[SOW-353] *The Contractor SHALL provide OEM manuals for all Commercial Off-the-Shelf (COTS) hardware and software installed.*

[SOW-354] *The Contractor SHALL be responsible to keep the COTS OEM manual under configuration control and to assure that all the COTS OEM Manuals will be always coherent with the operation configuration deployed, i.e., OBL.*

[SOW-355] *The Contractor SHALL assure that all the possible information needed to configure, operate, manage and maintain the COTS product will be in the User Manual and in the Maintenance Manual if they are no in the COTS OEM manuals.*

6.5.5. As-Built Documents

[SOW-356] *The Contractor SHALL provide as-built installation drawings, which reflect the complete installation conducted by the Contractor for each site.*

[SOW-357] *The Contractor SHALL ensure that all as as-built drawings SHALL comprise:*

- *Layout Plans showing the locations of all Contractor installed assets;*
- *Cabling Plans showing all Contractor installed cabling, per security classification, clearly identifying the location and labelling of each cable, together with the terminations at both ends and the use of the cable;*
- *Rack Layout Plans for all Contractor installed racks;*

- *System Configuration Plan showing all installed assets with all their interfaces and interconnections, both internal and external.*

[SOW-358] *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 material.*

[SOW-359] *The Contractor SHALL ensure that all as-built drawings representing technical networking and service configuration diagrams use layered views, as follows:*

- *One layer SHALL be created for the physical view, covering hardware, ports and cable-connections (including also signal flow, electrical power and grounding);*
- *One layer for the logical view, covering VLANs, virtual servers, logical links;*
- *One layer for the addressing and routing information;*
- *Service view schematics.*

6.5.6. Other Project Documentation

[SOW-360] *The Contractor SHALL ensure all Other Project Documentation respects the general requirement about publications in this SOW (SOW 11.6.12; SOW 11.6.13 as a minimum).*

6.5.7. Publication Criteria

[SOW-361] *The Contractor SHALL prepare and submit for approval a set of business rules which explain the harmonization criteria of all the technical documentation in terms of fonts, numbering, bullet points and all the publication rules to be used for the complete set of documentation. The business rules will be applicable for both Paper and electronic publication.*

[SOW-362] *The Contractor SHALL ensure all Manuals are printable if required and therefore the page format SHALL be A4, printable in loose-leaf form, and possible to be presented bound in stiff backed covers with 4-ringed binders which permit the removal and insertion of individual pages and drawings.*

[SOW-363] *The Contractor SHALL ensure each page contains the appropriate NATO classification of the manual at the top and bottom of each page.*

[SOW-364] *The Contractor SHALL ensure all pages containing drawings and schematic diagrams are of the same size as other pages of the manuals.*

[SOW-365] *The Contractor SHALL place the appropriate security classification in the identification block of each drawing.*

[SOW-366] *The Contractor SHALL deliver soft copies of any composed or compiled documentation in Compact Disc Read-Only Memory (CD-ROM) or digital versatile disc (DVD) format.*

[SOW-367] *The Contractor SHALL ensure all documentation delivered in this Contract is compatible with Microsoft Office Professional and Adobe PDF.*

[SOW-368] *The Contractor SHALL deliver O&M Manuals in Microsoft Office Professional or PDF format, if available. If not available in this format, another common format may be accepted. If the commercial documentation is not available in CD-ROM, another form of electronic media is acceptable with the prior authorization of the Purchaser PM.*

[SOW-369] *The Contractor SHALL ensure the physical support of electronic, optical or soft copies of documents display the highest level of the classification of their contents.*

[SOW-370] *The Contractor SHALL ensure the Header and/or Title of the directory structure of documentation provided in soft copy format bears a reminder of the highest classification level of its contents.*

[SOW-371] *For ease of handling, the Contractor SHALL separate unclassified from classified documentation and provided it on separate CD-ROMs or DVDs.*

6.5.8. Amendments to documentation

[SOW-372] *The Contractor SHALL be the responsible authority for the issue, control, and distribution of amendments to delivered documentation in the format provided for the associated equipment or system until expiration of the warranty period.*

6.5.9. Manual Issuing Schedule

6.5.9.1. Releases of manuals are described in Section 9.6.4.

[SOW-373] *The Contractor SHALL test and validate the procedures and resources described in the technical manuals.*

[SOW-374] *The Contractor SHALL provide all the technical documentation at least 12 weeks prior to the final delivery dates outlined in SSS to enable the Purchaser to perform a detailed review as the content matures and leave sufficient time for the updates resulted by the review. The Contractor SHALL include the documentation release plan within the first version of ILSP for approval, to provide Purchaser enough visibility for the schedule.*

[SOW-375] *Not later than one (1) month prior to the delivery of the IEG-C at the first location, the Contractor SHALL submit a copy of the final technical and training publications to the Purchaser for review.*

[SOW-376] *The Contractor SHALL ensure any resulting recommended changes, corrections and/or additions submitted by the Purchaser are incorporated by the Contractor in the final version.*

[SOW-377] *The Contractor SHALL provide the final versions of each Technical Publication, and Training Material in the requisite number of copies within four (4) weeks of FSA.*

[SOW-378] *Until the expiration of the warranty, the Contractor SHALL remain responsible for any changes to the manuals and training material required as a result of any omission or inaccuracy discovered in use or, whenever changes/modifications in equipment or spare parts are made under the Contractor's responsibility.*

[SOW-379] *The Contractor SHALL deliver two copies on CD-ROM of the IEG-C Operations Manuals for each of the sites, plus two copies for the NCI Agency.*

[SOW-380] *In addition to the "Manual Issuing schedule", the Contractor SHALL update all Manuals as needed throughout this contract.*

6.6. Training

6.6.1. General Requirements:

[SOW-381] *The Contractor SHALL provide all training modules and courses required to enable all initially assigned Purchaser personnel to operate and maintain the system at Level 1, 2 and 3. The Contractor SHALL ensure all activities, milestones and actors associated with IEG-C System Training are guided by the Training Plan.*

[SOW-382] *The Contractor SHALL design, develop and deliver minimum the following trainings;*

- *System operations training*
- *System maintenance training*
- *Guard administration training*
- *Other administration trainings (e.g. SMC, Security) identified during TNA*
- *Train the Trainer (TtT) trainings*
- *Test Crew trainings*
- *Transition Training (in each site).*

[SOW-383] *The Contractor SHALL design, develop, deliver and maintain the following types of training:*

- *Classroom Training (for operators, system administrators, guard administrators, engineers)*
- *On the Job Training (for operators, system administrators, guard administrators, engineers)*
- *Computer Based Training (CBT) modules for self-paced individual learning, compatible with the NCIA Learning Management System (only for NU).*

[SOW-384] *As part of the system implementation the Contractor SHALL provide on-site training to all support staff designated by the Site POC and on all tasks required to operate, maintain and recover the IEG-C System.*

[SOW-385] *As part of the training process the Contractor SHALL provide the on-site training course (operators, ~~and~~ administrators/maintainers and trainers) for a maximum number of two sessions in Mons for each type of training as outlined in [SOW-384], or another site designated by the Purchaser or an online course. The Contractor SHALL provide the Site Transition Training in each installation site both for operation and Level 1 maintenance, as applicable.*

[SOW-386] *The Contractor SHALL provide each training session for a maximum of 12 persons per session.*

[SOW-387] *The Contractor SHALL use the Training Needs Analysis (TNA) to refine the number of training sessions needed for each role.*

[SOW-388] *The Contractor SHALL deliver any additional training sessions that may be deemed necessary after completion of TNA at no additional cost to the Purchaser.*

[SOW-389] *As part of the training process the Contractor SHALL provide Train the Trainer courses for a minimum of 5 instructors designated by the Purchaser.*

[SOW-390] *The Contractor SHALL provide Training and all related training documentation in the English language.*

[SOW-391] *The Contractor SHALL complete Training Courses before the PSA (EDC+20mo) milestone, with the exception of the Test Crew trainings which the Contractor SHALL provide before the official test events start.*

6.6.1.1. The Purchaser will provide the following basic facilities: room, power supply, tables, chairs, network connectivity.

[SOW-392] *The Contractor SHALL provide all other facilities, services and equipment (including servers and workstations for students and teachers, network equipment, all required software, etc.) necessary to carry out the On-Site Training activities.*

[SOW-393] *The Contractor SHALL identify the eventual prerequisite of the personnel for training participation as part of the TNA.*

[SOW-394] *The Contractor SHALL train the Reference and Testing Facility staff to operate the Reference and Testing Facility, through attending a short, informal, on-site training course that the Contractor SHALL prepare, organise and lead.*

[SOW-395] *The Contractor SHALL provide training for all releases of the project.*

[SOW-396] *The Contractor SHALL ensure the Training Materials include how the Transition from one Release to the next release is realised and how to install, configure and maintain the Modified or new Component capability, including COTS components.*

[SOW-397] *If activated, the Contractor SHALL provide all training related services and deliverables in accordance with Section 6.6 for each optional site and service outlined in the SSS.*

6.6.2. Training Needs Analysis (TNA)

[SOW-398] *The Contractor SHALL base the Training Process and Procedures on the results of the Contractor's TNA.*

[SOW-399] *The Contractor SHALL detail its approach and planning on how the TNA process will be performed and managed within its Training Plan.*

[SOW-400] *The Contractor SHALL conduct a TNA in accordance with the [BiSC D-075-007, 2015]. The TNA SHALL include (as a minimum):*

- *A Target Audience Analysis*
- *A Performance Gap Analysis*
- *A Difficulty, Importance and Frequency (DIF) Analysis;*
- *A Training Delivery Options Analysis*

[SOW-401] *The Contractor SHALL base the TNA on the tasks resulting from Task Analysis carried out as part of the LSA Process and on the possible gaps highlighted during the site surveys (so called Target Audience Analysis).*

[SOW-402] *The Contractor SHALL ensure the TNA considers all staff roles involved in IEG-C System operation, administration, maintenance and support at all levels as they are assigned within Purchaser organization. For this purpose, the Contractor SHALL use the roles identified under training requirements as baseline and finalize the list of the roles as part of TNA and based on Purchaser input.*

[SOW-403] *The Contractor SHALL perform the TNA and create the courses as applicable for different types of administrators, operators, maintenance, and support personnel as they are assigned within Purchaser organization.*

[SOW-404] *The Contractor SHALL deliver a TNA Report that captures the results of the TNA for Purchaser approval. The TNA report SHALL include the following:*

- *A description of the TNA approach and activities*
- *An account of the operation, support, corrective and preventive maintenance tasks considered in the TNA*
- *The results of the Target Audience Analysis, the Performance Gap Analysis the DIF Analysis and the Training Options Analysis*
- *The final list of Performance Objectives in the form of Table 2 of Annex H of [BiSC D-075-007, 2015].*

- *The final list of Learning Objectives in accordance with Annex G of [BiSC D-075-007, 2015].*
- *One or more Course Control Document II – Course Proposals in accordance with Annex L of [BiSC D-075-007, 2015] as summaries of the proposed E&IT solutions*

6.6.3. Training Plan

[SOW-405] *The Contractor SHALL develop and provide an IEG-C System Training Plan. The Training Plan SHALL be updated to address the results of the TNA.*

[SOW-406] *The Contractor SHALL develop and provide a Training Plan that describes how it will meet the Training requirements outlined in the contract and found after the TNA for initial and follow-on training.*

[SOW-407] *The Contractor SHALL develop and provide a Training Plan that describes the quality management process for training.*

[SOW-408] *The Contractor SHALL develop and provide a Training Plan that addresses all stages of training development, delivery, and support covered under this Contract.*

[SOW-409] *The Contractor SHALL develop and provide a Training Plan that describes in a coherent way how training will be designed, developed, delivered, and maintained throughout the life of the IEG-C System.*

[SOW-410] *The Contractor SHALL develop and provide a Training Plan that includes training design documentation using the Course Control Document III – Programme of Classes template provided in [BiSC D-075-007, 2015] Annex R-4.*

[SOW-411] *The Contractor's Training Plan SHALL take the TNA results into consideration, and based on the TNA results it SHALL propose the specific courses for all maintenance levels and operation.*

[SOW-412] *The Contractor's Training Plan SHALL propose the different training types (classroom, on the job training, train the trainer and CBTs) for each course for Purchaser approval.*

[SOW-413] *The Contractor SHALL describe in this plan the approach to training, milestones, organization and resource requirements, management structure, interrelationships and other tasks related for training development.*

[SOW-414] *The Contractor SHALL develop and provide a Training Plan that describes the training documentation for each course including but not limited to the syllabuses, schedules, course prerequisites (both for attendees and physical resources), course descriptions and training materials, method of evaluations and instructors.*

[SOW-415] *The Contractor SHALL recommend in this plan the mode(s) of training (e.g., formal classroom, individual computer-based, on-the-job, commercial or a combination) and the rationale for these recommendations for each type of training (User , Administrator, etc.).*

[SOW-416] *The Contractor SHALL develop and provide a Training Plan that describes the transition training process.*

[SOW-417] *The Contractor SHALL develop and provide a Training Plan that describes the support to be provided by the Purchaser (manpower, services, and material).*

[SOW-418] *The Contractor SHALL deliver a Training Plan that describes the basic physical classroom and infrastructure required to perform the training in Purchaser locations.*

6.6.4. E-Learning Training / Computer Based Training (CBT)

[SOW-419] *The Contractor SHALL prepare all e-learning training material in compliance with the Sharable Content Object Reference Model (SCORM) edition 2004.*

6.6.4.1. All e-learning material prepared by the contractor should be compatible and deliverable on the NATO Advanced Distributed Learning (ADL) platform.

[SOW-420] *The Contractor SHALL produce CBT/E-Learning material that complements the IEG-C classroom training by defining and explaining key concepts and terminology of the operational processes as incorporated into IEG-C features and functions.*

[SOW-421] *The Contractor SHALL produce a CBT/E-Learning Package that allows modifications by the Purchaser to reflect changes in the training concept and/or content without any additional cost to NATO.*

[SOW-422] *The Contractor SHALL produce a CBT/E-Learning Package to provide the system administrators with a generic view of the system functionalities, operational aspects, troubleshooting and maintenance.*

6.6.5. Training Materials

[SOW-423] *The Contractor SHALL provide all the appropriate training documentation to support the Purchaser Personnel to test, operate and maintain the IEG-C System and its support equipment.*

[SOW-424] *Each training course material SHALL be provided for Purchaser review minimum 8 weeks before the start of the training courses.*

[SOW-425] *The Contractor SHALL generate the following Training Material:*

- *Training syllabus,*
- *Student manual*
- *Instructor guide and material*
- *Learning guide*
- *Quick reference card*
- *Upon completion, a training certificate*
- *Course evaluation feedback form*
- *Performance support materials to support users after the training during their work, with the following characteristics: 'bite-sized' learning chunks (maximum 5 minutes of learning time), designed to model or explain concrete tasks.*

[SOW-426] *The Contractor SHALL ensure the Training documentation conforms to the standards outlined in the training Section of the SOW and SRS.*

[SOW-427] *The Contractor SHALL ensure the Training documentation (Including the E-Learning Material) is developed in accordance with the results of the TNA.*

[SOW-428] *The Contractor SHALL ensure the training materials for the IEG-C System-specific courses provide all the information required to conduct the courses and maintain the training materials.*

[SOW-429] *The Contractor SHALL ensure the materials follow an existing instructional methodology that links training objectives with course structure, instructional techniques, course content, and assessment tools.*

[SOW-430] *For the development of training material, the Contractor SHALL reuse existing COTS documentation and manuals to the maximum extent possible.*

[SOW-431] *The Contractor SHALL ensure all course content is referenced to commercial or Contractor-developed documentation -- preferably user or technical manuals -- that describe the subject matter and are available on-site to students after course completion.*

[SOW-432] *The Contractor SHALL ensure the hands-on exercises included in the Training Process incorporate all IEG-C System implementation activities at a site.*

[SOW-433] *The Contractor SHALL ensure that the IEG-C System Training Materials are all provided in the UK English language. It may be assumed that all Purchasers personnel selected to attend the courses will meet the minimum Standardised Language Proficiency (SLP) of 3232 in English as specified in [STANAG 6001, 2014].*

[SOW-434] *The Contractor SHALL include, in the Training presentation materials, all slides or other information to be presented by the instructor during the course.*

[SOW-435] *The Contractor SHALL include, a Training Syllabus containing the following elements:*

- *Course title,*
- *Course description,*
- *Learning objectives, as identified in the TNA and confirmed in the Training Plan,*
- *Entry profile,*
- *Concepts, Functions and Features presented in the course,*
- *Instructional methodologies to be employed in the delivery of the course,*
- *In-class assignments or laboratories,*
- *Evaluation tools,*
- *Performance standards.*

[SOW-436] *The Contractor SHALL develop and provide a Student Handbook for each course.*

[SOW-437] *The Contractor SHALL develop and provide a Student Handbook that provides the student with necessary information on all lesson objectives and contents, guidance for all learning activities and cross-references to assist the students in achieving the course objectives.*

[SOW-438] *The Contractor SHALL ensure that the Student Manuals take into account results from the DIF analysis and SHALL enable students to perform their major tasks.*

[SOW-439] *The Contractor SHALL ensure the System Operations training provides all necessary information, description and operational tasks to enable the Purchaser operators to use and perform the Level 1 maintenance activities.*

[SOW-440] *The Contractor SHALL ensure the Test Crew training provides all necessary information for the system specifications, testing environment, tools and test*

procedures for Purchaser test crew to be able to support the test activities. This training SHALL not exceed 4 hours in total with maximum of 12 participants.

[SOW-441] *The Contractor SHALL ensure the Transition Training provides all necessary information for on-site (i.e. local maintenance and support personnel) Purchaser personnel to understand the system and its components, installation, connections and wirings, system components, preventive maintenance tasks, system shut-down and restart, disaster recovery, corrective maintenance tasks (e.g. troubleshooting, removal/replacement, software installation), and configuration system back-up procedures,. This training SHALL aim to enable the on-site transition to operations for each site, and therefore it may have certain commonalities with the 'Systems Operations' and 'System Administration and Maintenance' training.*

[SOW-442] *The Contractor SHALL ensure the System Administration and Maintenance Training provides as a minimum the following training on the capability (up to Level 2 and Level 3):*

- *How to install, configure and maintain the capability, including COTS components.*
- *How to maintain the Capability and how to use the logging and performance counters provided by the Capability. It includes as a minimum:*
- *All the configuration settings for the Capability modules, services and components*
- *How to configure the logging and uses of performance counters*
- *Where to find the log files*
- *The different categories of logging*
- *The different performance counter categories*
- *SMC procedures*
- *How to troubleshoot the system, including actions to solve a full range of (potential) problems or provide workarounds.*
- *How to manage database information, including database tables, triggers and stored procedures.*
- *How perform back-up and restore procedures.*
- *How to maintain the CMDB,*

[SOW-443] *The Contractor SHALL provide an Instructor's Guide for each training course. It SHALL contain all necessary information to prepare and conduct lessons and to evaluate students, including exercises, quizzes, and examinations and their corresponding answer sheets.*

[SOW-444] *The Contractor SHALL ensure the training materials also provide notes to instructors to assist in conducting the lecture or exercise. The Contractor SHALL provide the Presentation materials in Microsoft PowerPoint.*

[SOW-445] *The Contractor SHALL ensure the IEG-C capability Instructor Guide details the sequence of course instruction, providing references to the applicable training presentation materials, assignments and laboratories, evaluation tools and answer keys, Student Manual, and the Capability on-line help function. Within the Instructor Guide, the Contractor SHALL also include:*

- *Materials for in-class assignments and laboratories.*

- *Sample evaluation tools and answer keys.*
- *Training System installation and configuration procedures.*
- *The Contractor SHALL create and submit a summary of the recommended Training Materials, aids and equipment.*

6.6.6. Training Assessment and Evaluation

[SOW-446] *The Contractor SHALL propose an assessment and evaluation methodology to the Purchaser as part of the Training Plan.*

[SOW-447] *The Contractor SHALL base the Training Assessment methodology on Sections 7-6 and 7-7 of [BiSC D-075-007, 2015] for assessment approaches and instruments and include as a minimum:*

- *Examination methodologies and certification*
- *Minimum score to achieve for successfully passing the course*
- *Course(s) to be done to get the certification for each role*
- *Description of Role's certification process.*

[SOW-448] *The Contractor SHALL ensure that each student is instructed at the end of each course or use of a Computer Based Training (CBT) to complete and return the course evaluation feedback form provided as part of the training course or E-Learning product.*

[SOW-449] *The Contractor SHALL consolidate and forward student feedback to the Purchaser following each training course in the form of a Training Evaluation Report. The report SHALL also recommend changes and improvements to the training plan based on the consolidated student feedback.*

[SOW-450] *In the report, the Contractor SHALL also address student attendance, problems encountered and actions taken to resolve the problems.*

[SOW-451] *The Contractor SHALL revise/refine and reissue course material and CBT products to reflect the consolidated student feedback and proposed improvements in the training evaluation report.*

[SOW-452] *The Contractor SHALL produce Training Certificates for each training session and student.*

[SOW-453] *The Contractor SHALL deliver Training Certificates later than two weeks following the completion of training.*

6.7. Supply Support

6.7.1. System Inventory

[SOW-454] *The Contractor SHALL provide the Purchaser's ILS POC with a System Inventory in electronic Microsoft Excel format at least 15 (fifteen) working days before the first delivery of equipment.*

[SOW-455] *The Contractor SHALL ensure the System Inventory is site-specific and includes all items furnished under this Contract, as follows:*

- *All main equipment – i.e. all CIS items, both COTS and Developed, down to replaceable item level, hierarchically listed conform configuration item decomposition, including groups and assemblies; all installed hardware, such as equipment racks; all LRU interconnecting equipment when they are special-to-type (e.g. special-to-type cables);*

- *All ancillary equipment – i.e. all secondary items not essential to the functioning of the system, but deemed essential to the operation of the system, such as an all-weather canopy or a tool box;*
- *All support equipment – i.e. all tools, test equipment and PHS&T equipment;*
- *All Purchaser Furnished Equipment (PFE);*
- *All Purchaser and Contractor provided software;*
- *All spare parts, to include all spares, repair parts, and consumables, separated into technical and non-technical consumables;*
- *All documentation, such as manuals, handbooks and drawings; and*
- *All training materials.*

[SOW-456] *The Contractor SHALL use the inventory template provided the Purchaser to develop and submit the System Inventory. This template will be provided by the Purchaser after Contract Award.*

[SOW-457] *The Contractor SHALL provide the tempest specific part information additionally in the Inventory List for the tempested items.*

[SOW-458] *The Contractor SHALL note that the depth and content of the Inventory List will be subject to Purchaser Approval.*

6.7.2. Codification

[SOW-459] *On the basis that an adequate manufacturer's identification numbering system is in place, NATO codification (the request and assignment of NATO Stock Codes – NSN) are not be required. In all other cases, the Contractor SHALL note that NATO codification is required and SHALL support the NATO codification process in accordance with the requirements of AcodP-1 and the requirements of the STANAGs referenced and included in AcodP-1, i.e. STANAG 3150, STANAG 3151, STANAG 4177, STANAG 4199 and STANAG 4438.*

6.7.3. Labelling

[SOW-460] *The Contractor SHALL label all equipment in compliance with the Purchaser regulation and guidance, such that they contain at least the Contractor/OEM's name, identification, part number and serial number to ensure proper and quick identification of equipment down to the LRU level.*

[SOW-461] *The Contractor SHALL provide the details of the labelling approach in the CM Plan for Purchaser approval. The Contractor SHALL provide its labelling for the items that are configured and/or modified after procurement from the OEM. For these items, the Contractor SHALL assign a P/N for that specific configuration. The format and content of the labelling SHALL be provided to the Purchaser for*

[SOW-462] *The Contractor SHALL ensure that Labelling is accomplished in a manner that will not adversely affect the life and utility of the assembly or module. Whenever practicable, the Contractor SHALL ensure the label is located in such a manner as to allow it to be visible after installation.*

[SOW-463] *The Contractor SHALL ensure that Markings are as permanent as the normal life expectancy of the material on which it is applied and that legibility for identification purposes is maintained throughout each item's life expectancy.*

[SOW-464] *The Contractor SHALL ensure markings are capable of withstanding the same environmental tests required of the part and any other tests specified for the*

label itself. When possible, letters, numerals, and other characters SHALL be of such a size as to be clearly legible.

[SOW-465] *The Contractor SHALL cause all labelling and marking to be in the English language.*

[SOW-466] *The Contractor SHALL ensure nameplates are attached to all major units of the system. Nameplates SHALL be in the English language with non-erasable letters/ numbers, clearly identifying the unit (unit designator); location code; as well as the Contractor or OEM CAGE code, part number and serial number. These plates SHALL be properly attached in a prominent position on each major unit to enable reading and control with easy access when installed. For the items requiring special handling and/or lifting up with additional tools due to heavy weight or high volume (dimensions), special plates including the weight, dimensions and lifting points information SHALL be provided on the items. Also these items SHALL have the adequate provisioning points to enable such special handling and lifting conditions.*

[SOW-467] *The Contractor SHALL ensure all delivered equipment labels contain a machine-readable code (e.g., barcode) compliant with ~~[STANAG 4329] and [AAP-44(A)]~~AITP-09 and in accordance with the NATO coding scheme, which will be provided by the Purchaser at the request of the Contractor. In case NATO asset labels are provided by the Purchaser, the Contractor SHALL apply those labels in addition to the Contractor's labelling.*

[SOW-468] *The Contractor SHALL utilize these machine readable codes during the project to ensure that the following activities are carried out as efficiently as possible:*

- *inventory checking;*
- *codification, when required;*
- *configuration auditing;*
- *equipment PHS&T;*
- *equipment delivery, placement and acceptance;*
- *Maintenance.*

6.7.4. Initial Provisioning

[SOW-469] *The Contractor SHALL provide a single, fully detailed, site-specific and priced Recommended Spare parts List (RSPL) that SHALL detail comprehensively all spare parts, tools, test equipment, and consumables required to operate and maintain the system at all levels of support, and in accordance with the RAMT requirements specified in the Contract, no later than 8 weeks before PSA (EDC+20mo) meeting.*

[SOW-470] *The Contractor SHALL ensure the RSPL separately lists L1/2/3 (LRUs) items and L4 items (SRUs).*

[SOW-471] *The Contractor SHALL note that the RSPL will be used by the Purchaser to evaluate the support concept and initial provisioning of Contractor-provided spares.*

[SOW-472] *The Contractor SHALL ensure the RSPL includes the following items:*

- *Spare LRUs;*
- *Spare special-to-type LRU interconnecting equipment;*
- *Spare ancillaries;*

- *Support equipment, such as tools, test equipment and PHS&T equipment;*
- *Repair parts;*
- *Technical and non-technical consumables.*

[SOW-473] *The Contractor SHALL ensure the RSPL includes the following data elements:*

- *Nomenclature;*
- *Contractor/OEM CAGE code, part number and serial number;*
- *Mean Time Between Failures (MTBF) – when applicable;*
- *Indication Repairable (ND) or Non-Repairable (XB);*
- *Turn Around Time (when repairable), lead time (new items);*
- *Population, by system, site and total;*
- *Recommended quantity;*
- *Indication SPOF or part of a redundant array;*
- *Unit price (including warranty and PHS&T) and minimum order quantity;*
- *Unit repair cost (for repairable items; including warranty and PHS&T);*

[SOW-474] *The Contractor SHALL provide a set of spares calculated with 98% confidence level (site level) and assumption of continuous operation for a year.*

[SOW-475] *The Contractor SHALL provide the spare part calculations as a part of the Support Case.*

[SOW-476] *The Contractor SHALL also provide the technical consumables (filters, batteries, etc.) for preventive maintenance that will be enough for approximately a year after FSA. The shelf life of these consumables SHALL be long enough to be usable until the end of first year from FSA.*

[SOW-477] *The Contractor SHALL deliver the set of the spares and consumables before PSA (EDC+20mo).*

[SOW-478] *The Contractor SHALL provide all tools and test equipment required to perform L1/2/3 maintenance, as identified in the RSPL.*

[SOW-479] *Procurement and replenishment of L1/2/3 spare parts, including PHS&T, SHALL be the responsibility of the Contractor as per the Contract until FSA. Procurement, provisioning and replenishment of technical and non-technical consumables SHALL also be the responsibility of the Contractor.*

6.7.5. Software Delivery

[SOW-480] *The Contractor SHALL provide a detailed Software Distribution List (SWDL), which SHALL detail comprehensively all Computer Software Configuration Items (CSCI) and associated software, firmware or feature/performance licenses provided under this Contract. The SWDL SHALL include, the following data elements:*

1) *CSCI identification number;*
2) *nomenclature;*
3) *version number;*
4) *license key (if applicable);*
5) *license renewal date (if applicable);*

6) *warranty expiration date;*

7) *date of distribution;*

8) *distribution location (geographically);*

9) *distribution target (server); and*

10) *Owner.*

[SOW-481] *The Contractor SHALL make sure that all licenses are originally registered with the Purchaser as end-user.*

6.8. Packaging, Handling, Storage, Transportation (PHST)

6.8.1. Packaging

[SOW-482] *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-483] *Any special packaging materials required for the shipment of items SHALL be provided by the Contractor at no extra cost to the Purchaser.*

[SOW-484] *The packages, palettes and/or containers in which supplies are transported SHALL, in addition to normal mercantile marking, show on a separate nameplate the name of this project, contract number and shipping address.*

[SOW-485] *In the case of dangerous goods and goods requiring export licenses, the Contractor SHALL ensure that all required forms and certificates are provided and that all regulations for such goods are followed.*

[SOW-486] *For the purpose of transportation, all supplies SHALL be packaged to withstand the shipping hazards applicable to the chosen mode of transportation. Any special packaging materials required SHALL be provided by the Contractor and disposed of by the Contractor after unpacking, insofar as the packaging is not retained with the system (e.g. for storage of spares or return of failed equipment).*

[SOW-487] *The Contractor SHALL provide a confirmation of delivery to the Purchaser's ILS POC within two weeks after each shipment. This confirmation SHALL summarize the supplies delivered, state the date of delivery, and provide a scan of the signature of the Purchaser POC on-site, receiving the supplies.*

[SOW-488] *The Contractor SHALL be responsible of removal and disposal of all packaging material after installation in each site.*

[SOW-489] *The Contractor SHALL produce and provide packing lists that accompany each shipment, which will include the following:*

- *The Purchaser's contract number*
- *The NATO project number*
- *Names and addresses of the Contractor and the Purchaser;*
- *Names and addresses of the Carrier, Consignor and Consignee (if different from Contractor or Purchaser)*
- *Final destination address and POC;*
- *Method of shipment*

- *For each item shipped: Contract Line Item Number (CLIN) number as per the SSS; nomenclature; part number; serial number; and quantity*
- *For each box, pallet and container: box/pallet/container identification number and number of boxes/pallets/containers; weight; dimensions.*

[SOW-490] *The Contractor SHALL ensure that two copies of the packing lists are fastened in a weather-proof, sealed envelope on the outside of each box, palette and/ or container, and one packing list put inside each container/box.*

6.8.2. Handling and Storage

[SOW-491] *The Contractor SHALL be responsible for all handling and storage of equipment, packages, boxes and containers during the project.*

[SOW-492] *The Contractor SHALL also be responsible for organising and operating any handling equipment and storage facilities required.*

[SOW-493] *The Contractor SHALL arrange all that is necessary to access the sites where equipment is handled or stored.*

[SOW-494] *In the case of dangerous goods and goods requiring export licenses, the Contractor SHALL ensure that all required forms and certificates are provided and that all Host Nation regulations for such goods are followed. The Contractor SHALL provide a list of such equipment.*

6.8.3. Transportation

[SOW-495] *The Contractor SHALL be responsible for transportation and delivery of all equipment furnished under this Contract from its site in a NATO nation to its respective implementation destination as outlined in Annex B1.*

[SOW-496] *Ten (10) working days before each shipment of supplies, the Contractor SHALL provide the Purchaser with a Notice of Shipment comprising the following details:*

- *Shipment Date;*
- *Purchaser Contract Number;*
- *CLIN;*
- *Consignor's and Consignee's name and address;*
- *Number of Packages/Containers;*
- *Gross weight;*
- *Final/Partial Shipment;*
- *Mode of Shipment (e.g., road…);*
- *Number of 302 Forms used.*

[SOW-497] *The Contractor SHALL be responsible for any insurance covering these shipments.*

[SOW-498] *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 Purchaser. However, if there are any special packaging requirements and materials required for the shipment, the Contractor SHALL be responsible providing the guidance and the special packaging material. Additionally, any export/import regulations and requirements SHALL be specified and directed by the Contractor.*

[SOW-499] *At the Purchaser designated staging area, the Contractor SHALL unload the equipment and move the equipment to its final destination for installation. The Contractor may use any support equipment provided by the Purchaser, but remains responsible for requesting, organizing and using any support equipment required to offload and move equipment to its final destination. If such support equipment is not available on-site, then the Contractor SHALL be the ultimate responsible to arrange such equipment with the shipment.*

6.8.3.1. All packages, boxes will be inspected visually by the Purchaser's POC at final destination to ensure that no damage has occurred during transport and that all packages, boxes and containers detailed in the packing list have been accounted for. The Purchaser will in no case open any package.

6.8.4. Customs

[SOW-500] *The Contractor SHALL be responsible for customs clearance of all shipments into the destination countries. It is the Contractor's responsibility to take into account delays at customs. He SHALL therefore consider eventual delays and arrange for shipment in time. Under no circumstances can the Purchaser be held responsible for delays incurred, even when utilising Purchaser provided Customs Form 302.*

[SOW-501] *Prior to a shipment by the Contractor, the Purchaser will upon request issue a Customs form 302, which in some cases may facilitate the duty free import/export of goods. The Contractor SHALL be responsible for requesting the issue of a form 302 at least 10 (ten) working days prior to shipment. The request for a Form 302 SHALL be included with the Notice of Shipment and 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. The original 302 forms SHALL accompany the shipment and therefore no fax or electronic copy will be used, nor provided to the Contractor.*

[SOW-502] *If a country refuses to accept the Form 302 and requires the payment of customs duties, the Contractor SHALL pay these customs duties and the Purchaser SHALL reimburse the Contractor at actual cost against presentation of pertinent supporting documents. 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.*

[SOW-503] *The Contractor SHALL be responsible for managing and performing all activities that is necessary to obtain export licenses for the goods requiring such licenses.*

[SOW-504] *The Contractor SHALL provide a detailed list of the equipment requiring export licenses. The Contractor SHALL provide the necessary procedures that needs to be applied for items to be relocated for repair or any other purposes.*

6.9. Initial Operational Support

[SOW-505] *The Contractor SHALL perform all the maintenance and support activities (Level 2, 3, and Level 4) starting with activation of the Reference Environment until the successful completion of PSA (EDC+20mo) milestone.*

[SOW-506] *The following criteria SHALL be met to achieve FSA:*

- *In case of a critical failure in Reference Environment effecting the continuity of the operation, the Contractor SHALL restore the system maximum within 1 business day.*
- *In case of a non-critical failure not effecting the operation, the Contractor SHALL fix the failure within 3 business days.*

[SOW-507] *The Contractor SHALL apply the formal Change Management process for the fixes requiring the change of the approved baseline.*

[SOW-508] *Starting from PSA (EDC+20mo) and until FSA (EDC+27mo) when all the site acceptance activities are completed; the Contractor SHALL be responsible for the Level 2, Level 3 and Level 4 maintenance and support activities in each activated site within the scope of the Initial Operational Support.*

[SOW-509] *In case of a critical failure in the systems effecting the continuity of the operation, the Contractor SHALL restore the system maximum within 3 business days. In case of a non-critical failure not effecting the operation, the Contractor SHALL fix the failure within 10 business days.*

[SOW-510] *The Contractor SHALL provide support that includes, but is not limited to, Level 2 maintenance that will focus on using Built-In Test Equipment (BITE), standard tools and test equipment, on-equipment, day-to-day corrective and preventive maintenance. This SHALL include replacement of LRU's, manual reconfiguration and adjustments, detailed baseline inspections and checkouts, fault identification and isolation, problem management, limited calibrations, and minor equipment repairs.*

[SOW-511] *The Contractor SHALL provide support that includes, but is not limited to, the Level 3 maintenance and support will constitute the engineering level. It SHALL include in-depth testing, problem and modification analysis, release management, complex repairs and replacements, node and mission configuration(if applicable), calibration, scheduled servicing, overhaul and rebuild, implementation of major and/or critical changes, baseline restoration, post-maintenance review, supply support and PHS&T.*

[SOW-512] *The Contractor SHALL provide support that includes the Level 4 maintenance that involves standard warranty type services for repair or replacement of the items.*

[SOW-513] *If activated by the Purchaser, the Contractor SHALL extend the operational support period as options outlined in SSS.*

6.10. Warranty

[SOW-514] *The Contractor SHALL warrant that all equipment and software furnished under this Contract and all installation work performed under this Contract conform to the requirements and is free of any defect in material, code or workmanship for a period starting at date of FSA to date of FSA plus one (1) year.*

[SOW-515] *The Contractor SHALL support the system as part of the project implementation scope from the first site activation until FSA (EDC+27mo) milestone is successfully completed. During this period, the Contractor SHALL provide on-site and off-site maintenance and support services as required.*

[SOW-516] *The Contractor SHALL fix/repair/replace all items received as per his internal procedures with the highest priority allocated. The Contractor SHALL provide the repaired/replacement item within maximum 20 business days after the Purchaser has provided the failure notification in written.*

[SOW-517] *The Contractor SHALL acknowledge and propose a corrective action for the failed components within two business days after the initiation of the warranty request. In the case of a failure could not be identified to an LRU level and/or could not be isolated within 3 business day (starting with the warranty request) even with on-call assistance from the Contractor, the Contractor SHALL dispatch a field engineer to provide a solution on-site.*

[SOW-518] *The Contractor SHALL provide a specific Customer POC for all warranty and support requests. The Contractor SHALL detail all the warranty and support requirements in its ISSP including the roles and responsibilities.*

[SOW-519] *The Contractor SHALL be responsible for the provision of any alternative or superseding items, should the original part be no longer available, ensuring compliance with the original design and System provided by this Contract. However, in such cases the Contractor SHALL propose the original alternative item for the Purchaser approval. The alternative item SHALL conform with all the specified quality requirements within the scope of the contract and standards.*

[SOW-520] *The Contractor SHALL provide a Technical Assistance to the Purchaser or his representatives during the warranty period. Technical assistance information details SHALL be indicated in the ISSP.*

[SOW-521] *The Technical Assistance SHALL provide on-call and/or on-site support in English for requests that correspond to information demands limited to the perimeter of delivered products, evolution proposals, problem reports, or any information needed by the Purchaser or its representatives, which are not included in the supplied technical documentation.*

[SOW-522] *If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any supplies, the Contractor SHALL coordinate with the Purchaser and promptly correct the defect.*

[SOW-523] *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.*

[SOW-524] *The Contractor SHALL replace any such defect storage devices with new storage devices at no additional cost to the Purchaser.*

[SOW-525] *The Contractor SHALL be responsible for the provision of any alternative or superseding items, should the original part be no longer available, ensuring compliance with the original design provided by this Contract.*

[SOW-526] *During the warranty period, the Contractor SHALL be responsible for supplying all COTS hardware and software upgrades and updates.*

[SOW-527] *The Contractor SHALL make the availability of COTS hardware and software upgrades and updates known to the Purchaser and, if proposed for introduction by the Contractor for whatever reason, including any corrective action for an identified fault, SHALL always be subject to Purchaser approval.*

6.10.1. The Contractor will not be responsible for the correction of defects in Purchaser furnished property, except for defects in installation, unless the Contractor performs, or is obligated to perform, any modifications or other work on such property.

6.10.2. As an option the Purchaser can request additional warranty under the same conditions on a yearly basis.

6.11. Disposal of Equipment

6.11.1. It is the aim of this project to remove all legacy gateways. The deactivation and removal of legacy equipment, both in case of installation of new gateways to replace a prototype gateway or in the scope of WP4 of this SOW (for locations that are not receiving a new gateway) will be the responsibility of the Contractor.

6.11.2. The disposal of the aforementioned legacy equipment will be the responsibility of NATO, in compliance with applicable policy.

6.11.3. Removal activities will begin only after the Purchaser has authorized them, as some legacy IEG-C services may still be required to run concurrently with the new services.

[SOW-528] *The Contractor SHALL request formal authorization from the Purchaser to proceed with deactivation and removal of legacy equipment.*

[SOW-529] *The Contractor SHALL be responsible for the removal of the items from the installation facilities as required, and SHALL hand-over such devices to the Purchaser in local Purchaser warehouse.*

[SOW-530] *The Contractor SHALL work with local site personnel to ensure the controlled removal and disposal, unless otherwise specified by the Purchaser.*

SECTION 7: SYSTEM IMPLEMENTATION

7.1. General

7.1.1. Throughout the whole system implementation activities the Purchaser will retain all administrator privileges on existing systems (e.g., Enterprise Administrator, Domain Administrator) which will therefore not be granted to the Contractor.

7.1.2. The Purchaser reserves the right to suspend the Contractor's installation and/or or activation work for up to ten (10) working days to avoid interfering with or disrupting a critical operational event.

[SOW-531] *The Contractor SHALL ensure the overall implementation at the sites respects the achievement of milestones as described in SECTION 3.*

[SOW-532] *The Contractor SHALL execute implementation activities in several steps:*

- *The Contractor SHALL conduct complementary site surveys in addition to the ones conducted under pilot release – see 13.2*
- *The Contractor SHALL update and deliver the SIP – see 13.3*
- *The Contractor SHALL conduct site preparation activities – see 13.4*
- *The Contractor SHALL conduct site installation and activation activities – see 13.5.*

7.2. Site surveys

[SOW-533] *The Contractor SHALL conduct site surveys at all the sites related to the Site Activation and FSA milestones, and which are part of the contract (i.e., data centre sites, and additional options which have been activated under the contract; see SECTION 3).*

[SOW-534] *The Contractor SHALL follow the site survey process as described in SECTION 9: Site Surveys*

[SOW-535] *The Contractor SHALL adjust the activities and deliverables to the results of the site surveys.*

7.3. System Implementation Plan (SIP)

[SOW-536] *The Contractor SHALL propose, for Purchaser approval, the implementation sequence of sites implemented at PSA in the System Implementation Plan (SIP) (see ANNEX B).*

[SOW-537] *The Contractor SHALL produce and deliver a SIP that at least meet all contents requirements as laid out in section 15.11.*

7.3.1. The acceptance of the SIP by the Purchaser signifies only that the Purchaser agrees to the Contractor’s approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

[SOW-538] *The Contractor SHALL coordinate the installation and activation dates reflected in the SIP with the Purchaser and the Site POCs to accommodate site-specific requirements, exercises, holiday periods, and other considerations. Any such dates and any revision of these dates SHALL be coordinated with the Purchaser and the relevant sites at least four weeks before the start of the relevant activities.*

7.4. Preparations for Installation

[SOW-539] *The Contractor SHALL provide each site POC, with a copy to the Purchaser Project Manager, with a draft list of hardware and software to be shipped, and a list of Contractor's personnel together with a copy of each person's Personnel Security Clearance (PSC) for those who will be involved in site installation and activation work.*

[SOW-540] *The Contractor SHALL monitor the progress of any required Site facilities preparations, and the progress of any required provision of input by the Purchaser and the Site, to ensure timeliness and quality of the preparatory work required from the Purchaser.*

[SOW-541] *The Contractor SHALL ensure that anything that may delay installation is brought to the attention of the Purchaser Project Manager promptly.*

[SOW-542] *The Contractor SHALL prepare and conduct a Site Verification Survey no later than two months prior to installation activities at the site. The purpose of this Site Verification Survey is to verify that the information provided by the site is still valid, and to perform any necessary updates to the system implementation documentation. The Contractor may recommend to the Purchaser that certain Site Verification Survey(s) are not warranted, which the Purchaser may accept or reject.*

[SOW-543] *The Contractor SHALL issue the updated SIP immediately after the Site Verification Survey and no later than two weeks before the Site installation.*

7.5. Site Installation and Activation

[SOW-544] *The Contractor SHALL produce a Site Activation/ Acceptance Plan in coordination with the Purchaser.*

[SOW-545] *The Contractor SHALL perform site installation and activation at any site, which comprises the following activities:*

- *Perform site installation of any IEG-C elements (Hardware, Software), including establishment of network connectivity between all required components.*
- *Perform site activation.*
- *Execute all activities related to security accreditation.*
- *Execute Physical Configuration Audit (PCA).*
- *Deliver all documentation associated to site installation and activation.*

7.5.1. Site Installation

[SOW-546] *The Contractor SHALL coordinate the start date of the planned installation no later than three weeks before that start date.*

[SOW-547] *Throughout all Site installation activities the Contractor SHALL hold a daily meeting with the site POC to agree on the work to be conducted during the day.*

[SOW-548] *Although the Purchaser will provide the facilities in which the IEG-C will be installed and the external systems to which it will be interfaced, the Contractor SHALL be responsible for timely and complete delivery and installation of all relevant supplies.*

[SOW-549] *The Contractor SHALL ensure that the equipment to be installed in any of the relevant site facilities (as identified by the site during the site survey) has been*

tested and certified to operate at the "facility's zone level". The Contractor SHALL provide relevant evidence to the site before installing any IEG-C piece of equipment.

[SOW-550] *The Contractor SHALL unpack all IEG-C equipment at the installation location and dispose of packing materials as directed by the Purchaser's Site POC.*

[SOW-551] *The Contractor SHALL install all equipment in accordance with the applicable document indicated in [NCIA AI TECH 06.03.01, 2015].*

[SOW-552] *The Contractor SHALL connect all equipment to electrical power and communications interfaces provided by the Purchaser.*

[SOW-553] *The Contractor SHALL turn on all equipment and configure hardware and software settings to match the PBL and site infrastructure configuration.*

7.5.2. Site activation

7.5.2.1. The purpose of site activation is to ensure that all IEG-C components installed at that site are ready for operational use and meet SRS requirements, for both Technical Services and User Services.

[SOW-554] *The Contractor SHALL perform site activation activities locally at the site.*

[SOW-555] *The Contractor SHALL ensure that none of the site activation activities have any impact on the NATO Staff Users' desktop applications, except for some authorised potential and limited outages.*

7.5.2.2. Site Activation Tests

[SOW-556] *The Contractor SHALL conduct the site activation tests.*

7.5.2.2.1. The Purchaser reserves the right to observe the site activation tests and to have the Contractor perform additional tests in order to demonstrate that the system is meeting the contractual requirements.

7.5.2.2.2. The completion of Site Activation testing will be subject to the Purchaser's confirmation that all Site Activation tests at a site have been completed successfully.

[SOW-557] *For that purpose, The Contractor SHALL provide a Site Activation Test Report for each site.*

7.5.2.2.3. Site Activation tests on operational sites

[SOW-558] *The Contractor SHALL execute Site Activation tests on the operational sites that demonstrate that the equipment installed so far (i.e., both on the individual site and system-wide if other sites have already been installed) provides the Contractual functionality and performance level, including all interfaces with all internal and external system, including administration requirements, and is ready for operational use.*

[SOW-559] *The Contractor SHALL carry out the site activation tests for a maximum of one week at each site, exclusive of any preparation time.*

7.5.3. Local Security Accreditation activities

7.5.3.1. As part of the local security accreditation, some security documents need to be modified to align with the local security requirements and environment. Additionally, any security tests are to be performed on the local IEG-C component.

7.5.3.2. Security Operating Procedures (SecOPs)

[SOW-560] *For each of the sites where a component of the IEG-C system is to be installed and local management to be activated, the Contractor SHALL modify the approved generic SecOPs (see 16.1.3.8) to meet the requirements of the local site.*

[SOW-561] *The Contractor SHALL deliver and present the localised version of the IEG-C SecOPs to the local SAA for approval.*

[SOW-562] *The Contractor SHALL take into account any comments from the reviewers and Local SAA and SHALL update the document as many times as necessary in order to gain Local SAA approval of the IEG-C localised SecOPs for the site.*

7.5.3.3. Site Security Compliance Statement (SSCS)

[SOW-563] *For each site where a component of the IEG-C system is to be installed, the Contractor SHALL provide inputs to the local SSCS to meet the requirements of the local site.*

[SOW-564] *The Contractor SHALL deliver and present the proposed modifications of the SSCS to the local SAA for approval.*

[SOW-565] *The Contractor SHALL take into account any comments from the reviewers and Local SAA and SHALL update the proposal as many times as necessary in order to gain Local SAA approval of the IEG-C localised SSCS for the site.*

[SOW-566] *The Contractor SHALL support the local security staff in the completion of the SSCS.*

7.5.3.4. Security Test and verification Plan (STVP)

[SOW-567] *For each of the sites where a component of the IEG-C system is to be installed, the Contractor SHALL modify the approved generic STVP to meet the requirements of the local site.*

[SOW-568] *The Contractor SHALL deliver and present the localised version of the STVP to the local SAA for approval.*

[SOW-569] *The Contractor SHALL take into account any comments from the reviewers and Local SAA and SHALL update the document as many times as necessary in order to gain Local SAA approval of the IEG-C localised STVP for the site.*

[SOW-570] *The Contractor SHALL support the NCI Agency in the execution of the STVP.*

7.5.4. Physical Configuration Audit (PCA)

[SOW-571] *The Contractor SHALL schedule and perform the PCA with the Purchaser ILS POC.*

[SOW-572] *The Contractor SHALL co-ordinate the PCA with the Purchaser's ILS POC.*

[SOW-573] *The Contractor SHALL produce and deliver a PCA Report.*

[SOW-574] *The Contractor SHALL perform the corrective actions as outlined in the PCA Report.*

7.5.5. Documentation

[SOW-575] *The Contractor SHALL deliver to the sites all documentation that is required for system implementation and operation.*

[SOW-576] *The Contractor SHALL update the documentation delivered at the sites to accommodate any site-specific changes and/or configurations.*

[SOW-577] *Upon completion of site implementation work, the Contractor SHALL provide the Purchaser with a copy of the site installation and activation checklist and resolve any discrepancies identified.*

[SOW-578] *The Contractor SHALL keep the Documentation under configuration control, as per section 18.11.*

7.6. Service Implementation Period

7.6.1. The Implementation period is defined as the time duration from CAW until Contract FSA. The Contractor will implement and deliver the following predefined Support Functions during these Milestones.

Support Function	Start	End	Responsibility
IT-Operation	PSA	FSA	Initial IT-Operation will be provided by the Implementation Contractor, incl. transfer to the NCI Agency.
Customer Support	PSA	FSA	All Levels of Customer Support will be provided by the Implementation Contractor, incl. transfer to the NCI Agency.
Maintenance	PSA	FSA	All Levels of Maintenance will be provided by the Implementation Contractor, incl. Transfer of 1st, 2nd, and 3rd Level Maintenance to the NCI Agency.
SMC	PSA	FSA	Initial IT-Service Management will be provided by the Implementation Contractor incl. transfer to the NCI Agency.
Configuration Management	CAW	FSA	All Support Functions will be provided by the Implementation Contractor incl. transfer to NCI Agency.
Quality Assurance			
Logistics Support			
Training.			

Table 13: Support during Milestones

SECTION 8: TEST, VERIFICATION, VALIDATION (TVV)

8.1. Introduction

8.1.1. This section details the Test, Verification, Validation (TVV) processes and requirements to be applied and performed under this Contract, which are required for the verification and validation of the requirements set forth under this Contract by the Purchaser.

8.1.2. All deliverables supplied by the Contractor under this contract shall 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.

8.1.3. The verification and validation approach will not only involve delivered equipment, but also interfaces and interoperability with existing NATO and/or national equipment, here considered as Purchaser Furnished Equipment (PFE).

8.1.4. The verification and validation of PFE is out of the scope of this document and the contract.

8.1.5. The IEG-C requires a set of TVV activities to verify its compliance with the Contractual requirements set forth in the SOW and in the SRS (Annex to the SOW).

8.2. TVV activities

[SOW-579] *The Contractor SHALL classify and handle all information items used during the verification and validation activities according to their security classification. Guidance is provided in this SOW, under the security section.*

[SOW-580] *The Contractor SHALL have the overall responsibility for meeting the TVV requirements and conducting all related activities. This includes the development of all TVV documentation required under this Contract, the conduct of all test verification, validation and assurance events, and the evaluation and documentation of the results.*

[SOW-581] *All deliverables supplied by the Contractor under this contract SHALL be verified and validated to meet the requirements of this contract. All document-based deliverables SHALL be produced in a manner compliant with the templates provided by the Purchaser. In particular:*

- *The Contractor SHALL perform the verification activities within each Build Process;*
- *The Contractor SHALL perform verification to confirm that each element properly reflects the specified requirements, design, code, integration and documentation;*
- *The Contractor SHALL support Purchaser led Validation Activities to confirm that the solution is fit for purpose.*

[SOW-582] *The Contractor SHALL be responsible for the planning, execution and follow-up of all TVV events. 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 Subject Matter Expertise (SME) during all TVV events to witness and assist with these events.*

[SOW-583] *The Contractor SHALL demonstrate to the Purchaser that there is a verification and validation process in place for the project, supported by Contractor Quality Assurance (QA).*

[SOW-584] *Where requested by the Purchaser, the Contractor SHALL provide test data to support all TVV activities.*

[SOW-585] *The Contractor SHALL strictly follow the TVV processes (described in the latest version of the TV&V Process Definition and Execution Document (PDED) provided by the purchaser). When Contractor would like to propose a modification, it SHALL be subject to approval by the Purchaser.*

[SOW-586] *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-587] *All test, verification and validation material developed and used under this contract SHALL be delivered to the Purchaser.*

[SOW-588] *The Contractor SHALL provide an overall project Test Director for the phases defined in Table 14: List of TVV Phases, who will work closely with the Purchaser's assigned TVV Manager and NATO Quality Assurance Representative (NQAR). Table 14: defines the test phases considered. If deemed necessary, IEG-C project may split the test phases defined in Table 14: into multiple events.*

8.2.1. The Purchaser will provide subject matter experts (SME) during each test event, as well as TVV Test Engineers and an NQAR.

[SOW-589] *The Contractor SHALL use Key Performance Indicators (KPIs) to 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-590] *The Contractor SHALL have the overall responsibility for meeting the TVV requirements and conducting all related activities defined in Table. Each phase may have one or more events to complete the full scope.*

TVV Phases	Scope	Purchaser Involvement
Engineering Phase	Internal contractor activities executed during development phase of the system to ensure the system/software conforms to their design specifications.	**Review**: Test Reports for Unit, Integration and System tests
Qualification Phase	Activities executed to verify the design and manufacturing process, ensure the system meets necessary design requirements, and provide a baseline for subsequent acceptance tests. *Possible activities:* *TEMPEST Testing* *Electro-Magnetic Compatibility (EMC) Testing* *General Environmental Testing* *Water/Dust Ingress Testing*	**Review**: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects. **Participate**: Test Readiness Review (TRR), Test Execution, Event Review Meeting (ERM)

TVV Phases	Scope	Purchaser Involvement
	Operational Robustness Testing *Mechanical Environmental Testing* *Environmental Control Testing* *Biological & Chemical Testing* *Transportation Testing* *Physical Functional System Testing* *Product Safety Testing* *User Interface Testing* *Component Testing* *Interface Testing* *Security Testing* *Integration Testing (internal to the project deliverables)*	
Factory Acceptance Phase	To verify that production units comply with the requirement/design specifications and production can start. Confirm that all required engineering-level testing activities have been completed in accordance with the SOW. Determine if project deliverables are ready for independent verification, validation and acceptance	**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)
TVV Assessment Phase	Independent assessment performed with Purchaser and led by Contractor to determine whether or not a system satisfies user needs, functionality, requirements, and user workflow processes etc. before it gets into operation. To ensure verification of quality criteria defined in Figure 5: Product Quality Criteria for the following tests: - **System Integration Test (SIT**) – Requirements based testing, focused on verifying integration of the different components together and with any external interface as defined by the SOW - **User Acceptance Test (UAT)** – Scenario based testing, focused on validating the system as per user needs. - **Security Tests** – Tests focused on ensuring the security criteria are met. - **System Acceptance Test (SAT)** – Tests focused on ensuring compliance with the requirements outlined in the SOW.	**Review**: Event Test Plan, Security Test and Verification 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)

TVV Phases	Scope	Purchaser Involvement
	- **RFC Evaluation** – Review by Agency Change Managers and execution of any additional evaluation as requested by Change Managers. Under normal circumstances, all required inputs are generated from TVV activities	
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. Migration related tests are also covered under this tests. This includes integration with PFE.	**Review**: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects **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 Security Accreditation Documentation Package. Ensure end to end delivered system works as expected and can interoperate with other Purchaser equipment	**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 14: List of TVV Phases

8.2.2. The Purchaser reserves the right to monitor and inspect the Contractor's TVV activities to verify their compliance with the requirements set forth in this Contract.

[SOW-591] *The Contractor SHALL only proceed to the next formal TVV activity, after the successful completion of the previous TVV activity and after the agreement/approval by the Purchaser.*

8.3. Deliverables

[SOW-592] *The Contractor SHALL provide a System Test Documentation Package, following documentation templates provided by the Purchaser, that is comprised of the following documents in Table 15: Test Documentation:*

Work Product Name	First Draft	Sent to Review/Approve
The Master Test Plan (MTP)	*During Bid*	*4 weeks after contract award*

Work Product Name	First Draft	Sent to Review/Approve
Defect Reporting and Management Plan	*During Bid*	*4 weeks after contract award*
Event Test Plans for individual test events (ETP)	*During Bid (example)*	*4 weeks before TVV event*
The Security Test & Verification Plans (STVP)	*During Bid (sample procedures related to SISRS)*	*as required per the NSAB*
Security Implementation Verification Procedures (SIVP)		*4 weeks before TVV event*
Any submitted test Waivers together with supporting material		*4 weeks before TVV event*
The Test Cases/Scripts/Steps	*During Bid (example)*	*4 weeks before TVV event. First draft 4 weeks after contract award*
Status Reports		*Periodically (to be defined in the MTP)*
Test Completion Report		*1 week after TVV event*
System under-test Documentation		*2 weeks before TVV event*
The Requirements Traceability Matrix (RTM) updated with test-related information	*During Bid*	*First with MTP and update per test event*

Table 15: Test Documentation

[SOW-593] *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.*

[SOW-594] *The Contractor SHALL note that modification of inaccurate or inadequate TVV deliverables and any subsequent work arising as a result SHALL be carried out at the Contractor's expense.*

[SOW-595] *The Contractor SHALL deliver to the Purchaser all TVV materials developed and used under this contract.*

[SOW-596] *The Contractor SHALL utilise templates provided by the Purchaser as structure guides and for the content the Purchaser expects to be detailed. If the Contractor would like to propose a modification of the templates, the Contractor SHALL first obtain approval by the Purchaser.*

[SOW-597] *The contractor SHALL complete as many deliverable review cycles s required, until all deficiencies have been corrected.*

8.3.1. Master Test Plan (MTP)

[SOW-598] *The Contractor SHALL identify and describe in the Master Test Plan (MTP) which best practices and international standards will be applied and how.*

[SOW-599] *The Contractor SHALL produce a Master Test Plan (MTP) to address the plans for each TVV activities listed in this document. The Purchaser will monitor and inspect the Contractor's MTP activities to ensure compliance.*

[SOW-600] *The Contractor SHALL keep the MTP always up to date.*

[SOW-601] *The Contractor SHALL describe how the Quality Based Testing is addressed and implemented in the MTP. Figure 5: Product Quality Criteria is based on ISO 25010 and should be used as product quality criteria model.*

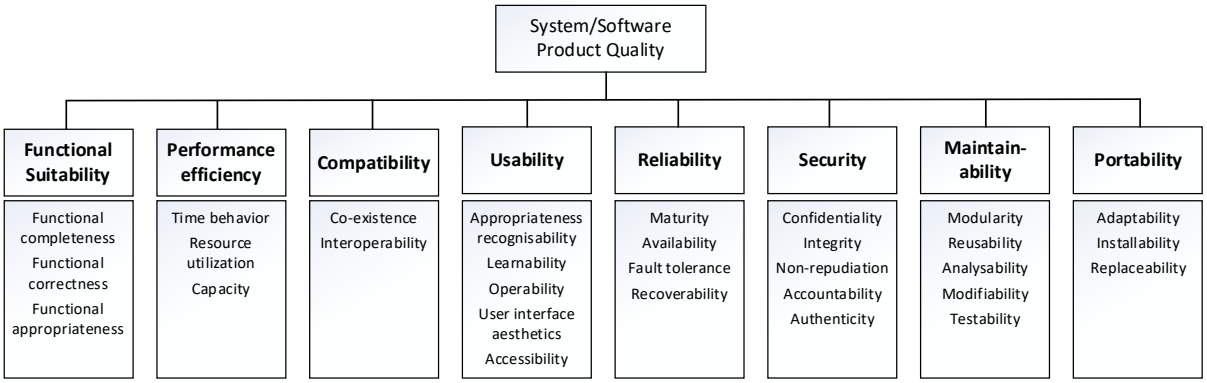


Figure 1: Product Quality Criteria

[SOW-602] *The Contractor SHALL describe all formal TVV activities in the MTP with a testing methodology and strategy that fit the development methodology chosen by the project.*

[SOW-603] *The Contractor SHALL propose a testing methodology that describes the method of achieving all the test phases, defined in Table 14: List of TVV Phases successfully.*

[SOW-604] *The Contractor SHALL describe in the MTP how the following objectives will be met:*

- *Compliance with the requirements of the Contract*
- *Verification that the design produces the capability required*
- *Compatibility among internal system components*
- *Compliance with the SRS requirements*
- *Compliance with external system interfaces and/or systems*
- *Confidence that system defects are detected early and tracked through to correction, including re-test and regression approach*
- *Compliance with Purchaser policy and guidance (i.e. security regulations, etc.)*
- *Operational readiness and suitability*
- *Product Quality Criteria (Figure 5: Product Quality Criteria)*

[SOW-605] *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-606] *The Contractor SHALL describe in the MTP "Entry and "Exit" criteria for each of the formal TVV events. The Contractor SHALL seek approval of all criteria related to an event not later than the TRR of the event.*

[SOW-607] *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-608] *Together with the MTP, the Contractor SHALL provide a defect reporting and management process to be applied during the TVV activities in Table 14.*

[SOW-609] *The Contractor SHALL describe how defects/non-conformances encountered during TVV events will be reported, managed and remedied.*

[SOW-610] *The MTP SHALL include the Contractor's approach to Test Reviews including Test Readiness Reviews (TRR) and Event Review Meetings (ERM) for each TVV event.*

[SOW-611] *The Contractor SHALL provide Contractor's provisions and strategy for building/maintaining of the Reference Environment in the MTP.*

8.3.2. Test Cases and Test Procedures

[SOW-612] *The Contractor SHALL develop test and use cases to verify and validate all requirements in the SOW, requirements specifications (SRS) and final design. The test cases SHALL follow the template provided by the Purchaser.*

[SOW-613] *The Contractor developed Test Case/Procedures SHALL clearly describe all the test steps that meet or demonstrate Purchaser's requirements with an expected Test Result and pass/fail result.*

[SOW-614] *The Contractor SHALL develop test cases and steps for each of the contractual test activities following each type of quality criteria. The Contractor SHALL ensure full test coverage based on a risk analysis and submit them for the Purchaser's review and approval.*

[SOW-615] *The Contractor SHALL use test tools for development of Test Cases and procedures. Whatever Test tool is used by the Contractor, the output format SHALL fully be compatible, transferrable and usable with the Purchaser's tools.*

[SOW-616] *The Purchaser will review and provide comments to the Contractor delivered Test Cases, Test Procedures and Test Steps within 4 weeks of receipt. The Contractor SHALL allow a4 week review cycle by the Purchaser for subsequent versions.*

[SOW-617] *All the Contractor developed Test Cases, Test Procedures and Test Steps SHALL be approved by the Purchaser prior to their execution.*

[SOW-618] *If the Contractor produced Test Cases, Test Procedures and Test Steps are not approved by the Purchaser, the execution of relevant testing SHALL be adjusted or delayed accordingly until approved by the Purchaser.*

[SOW-619] *The Contractor must deliver to the purchaser the final version of the test cases and Event Test Plan available one (1) week prior to the TRR for a specific TVV event*

[SOW-620] *The Contractor SHALL incorporate into the relevant test cases any updates required from the execution of test cases during each phase 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 section 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*

8.3.3. Event Test Plan (ETP)

[SOW-621] *The Contractor SHALL create an Event Test Plan (ETP) per each event detailing all the information required for that event. The ETP SHALL follow the template provided by the Purchaser.*

[SOW-622] *The Contractor SHALL describe in the event test plan what training (if any) will be provided prior to formal TVV events.*

[SOW-623] *The Contractor SHALL identify, in the ETP, which environment(s) to be used at each TVV event and the responsibilities for configuration control, operation and maintenance of the environment*

[SOW-624] *The Contractor SHALL ensure the ETP describes when an agreement is 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 TVV event or at the Event Review Meeting). If agreement is not reached, the Contractor SHALL escalate disputed items to the Purchaser's and Contractors' Project Managers*

8.3.4. Test Reports

[SOW-625] *The Contractor SHALL record the results for each test called for in the Test Plan in a Test Log (also known as Test Execution Log).*

[SOW-626] *The Contractor SHALL ensure the test report follows the template provided by the Purchaser, including a cover sheet that clearly shows how many tests passed, failed, or were not run.*

[SOW-627] *The Contractor SHALL ensure the test report indicates the result of the test cases execution.*

[SOW-628] *Where the Purchaser or his representative has witnessed the testing, appropriate annotations SHALL be made on each page of the test results to ensure that the test report is a true record of test activities and results as witnessed by the Purchaser, and the whole test report SHALL be signed by the Contractor representative and by the Purchaser representative on completion of that testing.*

8.3.5. Requirement Traceability Matrix RTM

[SOW-629] *The Contractor SHALL produce and maintain the Requirement Traceability Matrix (RTM), which includes all functional and non-functional requirements (respecting Purchaser's provided requirement IDs), to track the TVV status of all requirements throughout the Contract execution (especially during the TVV activities).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 TVV activities:*

- *The verification method: Inspection, Analysis, Test or Demonstration*
- *Correspondent TVV phase(s) for each requirement*
- *Correspondent Test procedure*
- *Coverage Status*
- *Product release*
- *Identify if covered by COTS, or custom development*
- *Identify any Off-specifications associated with the requirement.*
- *Identify test(s) or test waiver(s) on the basis of which the requirement was demonstrated.*
- *Identify associated problem report for failed requirements*

[SOW-630] *The Purchaser will review and approve the proposed RTM.*

[SOW-631] *The Contractor SHALL maintain the RTM updated during the project lifecycle.*

[SOW-632] *The Contractor SHALL provide the Purchaser with updates (via the tools) to the RTM daily during the execution of an event, and following the conclusion of each event defined in Table 14: List of TVV Phases. A workflow for updating the RTM SHALL be proposed by the Contractor and approved by the Purchaser.*

[SOW-633] *The Contractor SHALL include in the RTM (and be able to differentiate from SRS requirements) the requirements derived from the gap analysis of the Operational Acceptance Criteria.*

8.3.6. STVP

[SOW-634] *The Contractor SHALL produce an STVP, to ensure that the Security testing, including verification of compliance with NATO CIS security regulations (in 2.1.1. Security Documents ~~Annex C~~ of the SOW) is applied. This is an integral part of the Independent Verification and Validation process.*

[SOW-635] *The STVP SHALL support the accreditation of the System Platform. This document SHALL be approved by Security Accreditation Authority (SAA) – Section 10.2.*

8.4. Tools

[SOW-636] *The Contractor SHALL generate and deliver automated test procedures/cases compatible with Purchaser test management and automation tools.*

[SOW-637] *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-638] *The Contractor SHALL use the tools supporting requirements coverage, defect management and test management selected and hosted by the purchaser. 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 TVV related data for the project in the purchaser tools.*

8.5. TVV Events and results

[SOW-639] *The Contractor SHALL conduct testing during the Project lifecycle compliant with the following requirements:*

[SOW-640] *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-641] *The Contractor SHALL conduct all testing activities for any architectural changes.*

[SOW-642] *The Contractor SHALL support post go-live activities during the Operational Acceptance phase, to evaluate the IEG-C capability performance and establish benchmarks for future enhancements, including any changes made to fulfil the requirements.*

[SOW-643] *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 TVV event. The Purchaser will approve the report and its findings within five business days.*

[SOW-644] *The Contractor SHALL report progress and result measurement and these SHALL be approved by the Purchaser based on KPIs.*

[SOW-645] *The Contractor SHALL record test results 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 start of the next business day (0800 AM), but as a minimum not later than 24 hours following the execution of any test.*

8.5.1. Test Readiness Review (TRR)

[SOW-646] *The Contractor SHALL conduct a Test Readiness Review (TRR) meeting at least one week prior to the events defined in Table 14: List of TVV Phases. 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-647] *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-648] *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.*

8.5.2. Event Review Meeting (ERM)

[SOW-649] *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 depend 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-650] *The Contractor SHALL convene an Event Review Meeting (ERM) as defined in the ETP and MTP. The ERM SHALL ensure that the event results, defect categorization and a way forward to fixing the defects (if required) is agreed upon the Contractor and the Purchaser as well as any other items identified in the exit criteria defined and agreed for the event. If agreement is not reached, the disputed items SHALL be escalated to the Purchaser's and Contractors' Project Managers. The exit criteria presented in the ERM may as well be utilized as success criteria.*

8.5.3. TVV Event

[SOW-651] *An event starts with the Test Readiness Review (TRR) and finishes off with the Event Review Meeting (ERM).*

[SOW-652] *During formal TVV 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-653] *For each TVV 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-654] *The Contractor shall correct and re-test all failures with severity "Critical" or "Major".*

[SOW-655] *The Contractor shall record the agreed action plan for failures with severity "Moderate", "Minor" and "Cosmetic".*

[SOW-656] *The Contractor shall fix and demonstrate that the recorded issues or faults are fixed and working correctly. The next contractual test activity shall not start until all the findings are fixed to the Purchaser's satisfaction.*

[SOW-657] *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 TVV activities.*

8.5.4. Reference environments

[SOW-658] *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 Reference Environment 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-659] *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.*

8.5.5. Waivers

[SOW-660] *The Contractor may request a Test Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. 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-661] *In respect to a requested waiver, the Contractor SHALL certify that the test environment to be implemented is identical to that which was originally used for testing, or advise the Purchaser of design/construction changes which affect form, fit or function.*

[SOW-662] *The Contractor SHALL record and log all waiver requests along with their resolution submitted for the Purchaser's approval.*

8.5.6. Failed events

[SOW-663] *In the event of failed TVV 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*

8.6. Test Defect Categorization

[SOW-664] *The Contractor SHALL use the Purchasers' categorization nomenclature for all defects and non-compliances*

[SOW-665] *Should a failure be identified during a TVV 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 Table 16: Definitions for Defect Categorization, Table 17: Classification of defects based on severity, Table 18 and Table 19: Deficiency Categories .*

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 16: Definitions for Defect Categorization

8.6.1. Severity

[SOW-666] *According to their severity, defects SHALL be classified as one of the following in Table 17: 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:

Severity	Definition
	* 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 17: Classification of defects based on severity

8.6.2. Priority

[SOW-667] *According to their priority, defects SHALL be classified as one of the following in Table 18: Priority Classes for Defect Classification:*

Priority Class	Description
Urgent	The defect SHALL be resolved as soon as possible. Required to complete independent verification and validation activities.
Medium	The defect SHALL be resolved in the normal course of development activities. It can wait until a new build or version is created.
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.

Table 18: Priority Classes for Defect Classification

8.6.3. Category

[SOW-668] *According to their category, deficiencies SHALL be classified as one of the following in Table 19: Deficiency 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) Engineering Change Proposal (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 deficiencies 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 deficiency.

Table 19: Deficiency Categories

SECTION 9: SITE SURVEYS

9.1. Introduction

9.1.1. The purpose of the Site Survey is to gather all information of interest in view of the preparation, installation, configuration, on-site testing and support. This section outlines the requirements applicable for site surveys.

[SOW-669] *The Contractor SHALL respect requirements below for every site survey.*

[SOW-670] *For each site survey, the Contractor SHALL conduct site survey preparatory work, visit each site subject to site survey, survey relevant facilities, interview site personnel, and collect data to support project activities.*

[SOW-671] *The Contractor SHALL ensure coherence between site survey results and project documentation (e.g., System Design Documentation Package, SIP) at any time. The Contractor SHALL update project documentation accordingly.*

9.1.2. Any long-lead item purchases or other financial obligations made by the Contractor following site surveys will not be claimed unless they are reflected in the baseline agreed to by the Purchaser at or after the Design Review.

9.2. Site Survey Preparatory work

9.2.1. Site Survey Work Book (SSWB)

[SOW-672] *The Contractor SHALL prepare a SSWB of checklists, fill-in forms, installation sketches, contact information, installation specifications, and site data to be collected by the Contractor during the site survey, and any other documentation required to perform site surveys.*

[SOW-673] *The Contractor SHALL make the SSWB available for Purchaser review and comment before the first site survey, and SHALL maintain and update as necessary during the site survey process.*

[SOW-674] *Upon acceptance of the SSWB by the Purchaser, the Contractor SHALL distribute the SSWB to the site(s) for preparation of the Site Surveys. This approach will enable a better preparation by the sites.*

9.2.2. Agenda

[SOW-675] *The Contractor's site survey(s) and installation sequence and dates reflected in the Project Implementation Plan SHALL be co-ordinated by the Contractor with the Purchaser and the Site POC to accommodate site-specific requirements, exercises, holiday periods, and other considerations.*

9.2.3. Introductory briefing

[SOW-676] *The Contractor SHALL prepare and provide an Introductory Briefing as an introduction to the IEG-C project, which will not assume other than basic knowledge of the project by the site personnel, covering at least:*

- *An outline of the system requirements,*
- *System functionalities,*
- *The sites to be implemented,*
- *The project timelines,*
- *The goals and objectives and agenda of the Site Survey process,*

- *The notional implementation identified for the surveyed site, to be refined through the Site Surveys activities.*

9.3. Survey of the site facilities

[SOW-677] *At the beginning of the site survey the Contractor SHALL provide a presentation to the local site personnel on the objectives and conduct of the site visit in the context of the overall IEG-C project.*

[SOW-678] *During the Site Surveys activities the Contractor SHALL determine the necessary installation preparations and support arrangements and collect all system implementation-relevant information. This SHALL include:*

- *Identification of the IEG-C IEG-C Administrators, CIS Security Administrators, Operators, and more generally all Points of Contact;*
- *Identification of existing business processes (for both physical access control and logical access control), and how those processes will integrate with IEG-C Capability.*
- *Identification of the system IEG-C will interface with, in accordance with the business processes and transition requirements from existing capabilities to the IEG-C Capability;*
- *Identification of the system that are not ready to be migrated to IEG-C;*
- *Analysis of the training needs (see also 11.7);*
- *Identification of any input (item of equipment, documentation, information) or work required from the Purchaser and from the Site with indication of suspense date;*
- *Identification of the facilities where the IEG-C will have to be installed, together with each facility's zone level (see [NCIA AI TECH 06.03.01, 2015]);*
- *Identification of any potential TEMPEST-related requirement for the IEG-C equipment(see [NCIA AI TECH 06.03.01, 2015]);*
- *List of all system CIs (nature and quantities) to be installed in the site*
- *Update of the user list (see ANNEX B)*
- *Identification of the tools, policies and procedures in use at Purchaser facilities, in order to determine the integration requirements with the ITSM tools.*

[SOW-679] *After the Site Survey the Contractor SHALL present to the Purchaser his site engineering and installation drawing(s) and identify actions and follow-on activities.*

9.4. Site specific-requirements

9.4.1. Notwithstanding the requirements related to storage and backup solutions, some Purchaser locations have site-specific equipment (e.g. specific brand names for servers), which may differ from the project baselines at a site, to reduce operations and maintenance costs or to use existing facilities in the most efficient manner.

[SOW-680] *The Contractor SHALL determine if site-specific equipment is required at a location as part of any Site Survey performed under this Contract.*

[SOW-681] *If site-specific equipment is required, the Contractor SHALL issue an Engineering Change Proposal (ECP).*

[SOW-682] *In the ECP, the Contractor SHALL identify any requirements of the IEG-C System Design Specification it believes will not be met due to differences between the site-specific equipment and the standard baseline.*

[SOW-683] *If these exceptions to the IEG- System Design Specification are accepted by the Purchaser and incorporated into the Contract as formal amendments, the Contractor is not required to demonstrate, as part of its Site Activation work, that the associated System Design Specification requirement has been met. In such a case, the Contractor SHALL update the System Design Specification to reflect site-specific situations.*

[SOW-684] *The Contractor SHALL identify all facilities support, including modifications or additions, required. After coordination with the Purchaser, this notification SHALL be in the form of a letter to the site POC, with a copy to the Purchaser, accompanied by engineering drawings, checklists, or any other supporting information. Facilities support issues that represent Medium or High risk items SHALL be reflected in the Risk Log.*

9.5. Outcomes

[SOW-685] *The Contractor SHALL produce and deliver a Site Survey Report for each site. detailing its findings from the site survey, identifying all required Purchaser and Contractor actions to prepare for, conduct, or support IEG-C installation and activation, and identifying the type of training courses required and the number of Purchaser staff to be trained for each course.*

[SOW-686] *The Contractor SHALL accurately and formally document the findings of the Site Survey and the preparatory work required from the Site.*

[SOW-687] *After the Site Survey the Contractor SHALL present to the Purchaser his site engineering and installation drawing(s) and identify actions and follow-on activities.*

[SOW-688] *The Contractor's Site Survey Reports SHALL be provided within one week after the respective Site Survey is completed.*

[SOW-689] *At minimum, the Site Survey Report SHALL include:*

Serial	Requirement
1	Installation & Activation: • Stakeholders communication • System installation requirements • Schedule of installation activities
2	Training requirements
3	Logistics • Available system location & and space • Technical infrastructure • Delivery details
4	Local Security Accreditation Authority documentation • Contact Details of security responsibilities • Interconnection details • Network diagrams
5	Register all findings that require modification of the site infrastructure or change of the agreed implementation scope. For each of the changes the Contractor SHALL produce a formal change proposal.
6	For each out of scope item that requires either technical support or procurement activity, the Contractor SHALL offer a proposal to the Purchaser with his recommended solution.
7	Site diagram that SHALL be used as the basis for the As Built Documentation and used in the installation of the site.

[SOW-690] *At the end of the site survey the Contractor SHALL provide an out brief on the outcome of the site survey and identify actions and follow-on activities.*

9.5.1. The Purchaser will provide the Contractor with the exact shipment addresses and NATO POC for subsequent equipment delivery.

SECTION 10: SECURITY ACCREDITATION

10.1. Introduction

10.1.1. The objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained through the life cycle of the CIS. The IEG-C must achieve security accreditation for it to be granted the authority to go live. To achieve this, the system will need to go through a Security Accreditation process and obtain the approval from Security Accreditation Authorities to use **IEG-C** to interconnect NATO networks/security domains in scope of this contract.

[SOW-691] *The Contractor SHALL demonstrate the IEG-C platform compliance with the NATO Security Policy and supporting directives and IEG-C security accreditation document set by obtaining the security accreditation of interconnections via the IEG-C installations.*

[SOW-692] *The Contractor SHALL be responsible to follow, implement and conform to the Pre-Accreditation Activities, and the Accreditation Process as defined and documented in [AC/35-D/2005-REV3] and Security Accreditation Plan (SAP) for IEG-C in order to obtain the required security accreditation statement(s) for the interconnections via IEG-C during each phase of the IEG-C project.*

[SOW-693] *The Contractor SHALL be required to carry out and meet the terms of the Security Accreditation Authority to perform any Post-Accreditation activities, such as periodic re-assessments of the security risks and periodic inspections up to the time of handover of the IEG-C to the CIS Provider (CISP).*

[SOW-694] *The Contractor SHALL obtain Approval for Testing (AfT) and/or Interim Security Accreditation (ISA) which are necessary during the stages of the implementation, tests and trials of the IEG-C project. This does not diminish the requirement for the Contractor to obtain the full Security Accreditation statement for each interconnection via IEG-C.*

10.2. Security Accreditation Authority (SAA)

10.2.1. The overall Security Accreditation Authority (SAA) for the IEG-C is the NATO CIS Security Accreditation Board (NSAB). Local SAA's will be involved in accreditation of the interconnection via IEG-C. Their role will be to ensure that IEG-C is implemented in accordance with the NSAB-approved security accreditation package for IEG-C and ensure that any agreed local (site specific) configurations are agreed and implemented in accordance with the local security regulations (e.g. [ACO 070-005]).

10.2.2. Coordination with the SAAs will be conducted by the Purchaser. The Contractor may be invited to provide briefings for the meetings with the SAAs.

[SOW-695] *The Contractor SHALL take action to follow, carry out the necessary work and to implement the advice, instructions and changes given by the SAA and local SAA's for the IEG-C.*

10.3. Security Accreditation Documentation

10.3.1. The achievement of the IEG-C security accreditation will require a prescribed set of security documentation to be produced, using security accreditation documentation templates. The templates will be made available to the Contractor after the Contract Award.

[SOW-696] *The Contractor SHALL produce security accreditation documentation and/or provide inputs to documents in support of the 3.7 Acceptance of IEG-C security*

accreditation package , as detailed in Security Accreditation Plan (SAP) for IEG-C

CIS Description
Security Accreditation Plan (SAP)
Security Risk Assessment (SRA) Report
Generic System Interconnection Security Requirements Statement (SISRS)
Security Operating Procedures (SecOPs)
Security Test and Validation Plan (STVP)

Table 20: IEG-C Accreditation Package

Statement of Compliance with IEG-C accreditation package
Security Test and Verification Report (STVR)

Table 21: Documentation for specific interconnection

[SOW-697] *The Contractor SHALL produce all security accreditation documentation or inputs to documents using security document templates provided by the Purchaser. These will be provided after the Contract Award.*

10.3.2. The documentation to be developed to support the IEG-C security accreditation process is listed in Security Accreditation Plan (SAP) for IEG-C.

10.3.3. The documentation set includes:

a. CIS description;

b. Security Accreditation Plan (SAP);

c. Security Risk Assessment (SRA) Report;

d. Generic System Interconnection Security Requirement Statement (SISRS) for IEG-C

e. Security Operating Procedures (SecOPs) for IEG-C administrators;

f. Security Test and Verification Plan (STVP);

g. Security Test and Verification Report (STVR) template;

h. Site-specific documentation:

- *Compliance Statement for interconnection(s) via locally installed IEG-C*
- *Local STVP (if required by the Local SAA, to address site-specific requirements); and*
- *Test Report based on STVR template (mandated for each site).*

10.3.4. Security Accreditation Plan (SAP) has been developed by the Purchaser and approved by the SAA. This document will be made available to the Contractor after the Contract Award. The SAP will be maintained by the Purchaser during the project life-cycle. Any SAP update will be presented to the SAA for its approval. Further security accreditation activities will be dependent on the decisions of the NSAB regarding the SAP.

[SOW-698] *The Contractor SHALL be responsible to implement the activities described in the SAP as approved by the SAA.*

10.3.5. Initial System Description for the IEG-C (Section 1.2 System Description) has been developed by the Purchaser. This document will be made available to the Contractor after the Contract Award. The System Description is the first document related to security accreditation to be updated after the Contract Award. It will contain all relevant information taken from the System Design Documentation Package and adapted to the SAA needs.

[SOW-699] *The Contractor SHALL update the initial CIS description document based on the System Description in Section 1.2 provided by the Purchaser, including all relevant information taken from the System Design Documentation Package and adapted to the SAA needs.*

[SOW-700] *The Contractor SHALL address Purchaser comments (including SAA comments) to achieve CIS description endorsement by the SAA.*

[SOW-701] *The Contractor SHALL maintain the CIS description during the project.*

10.3.6. Security Risk Assessments (SRAs) report will be produced by the Contractor, using SRA report template [SRA template]. Based on the results of the SRAs, the Contractor SHALL identify areas of the IEG-C requiring safeguards and countermeasures to comply with NATO Security Policy and supporting directives and [NS Reference Baseline]. The decision on specific security mechanisms will be based on evidence and results produced by the Security Risk Assessment.

[SOW-702] *The Contractor SHALL develop the SRA in accordance with Guidelines for Security Risk Management of CIS (Ref. [AC/35-D/1017-REV3]).*

[SOW-703] *The Contractor SHALL use the NATO template [SRA template] to document the results of the SRA.*

[SOW-704] *The Contractor SHALL identify areas of the IEG-C requiring safeguards and countermeasures to comply with NATO Security Policy and supporting directives and [NS Reference Baseline]. The decision on specific security mechanisms will be based on evidence and results produced by the Security Risk Assessment.*

[SOW-705] *The Contractor SHALL consider any change to be within the technical and financial scope of this Contract whenever the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components; no ECP SHALL be generated.*

[SOW-706] *The Contractor SHALL raise an ECP whenever the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand.*

[SOW-707] *The Contractor SHALL address Purchaser comments (including SAA comments) to achieve SRA report approval by the SAA.*

[SOW-708] *The Contractor SHALL maintain the SRA report during the project.*

10.3.7. Generic System Interconnection Security Requirements Statement (SISRS) for IEG-C will be developed, as directed by the SAA, defining the security requirements for interconnection via the IEG-C. The generic SISRS for IEG-C shall be approved by the SAA. The SISRS template will be provided by the Purchaser after the Contract Award.

[SOW-709] *The Contractor SHALL produce a generic System Interconnection Security Requirement Statement (SISRS) for IEG-C to include the minimum requirements mandated by NATO Security Policy and supporting directives and security measures to counter the risks identified in the IEG-C SRA.*

[SOW-710] *The Contractor SHALL produce the SISRS template for IEG-C using and following the guidance provided by the Purchaser.*

[SOW-711] *The Contractor SHALL ensure that each security requirement in the SISRS have a unique identifier which is crossed referenced to the security mechanism (Ref. [NS Reference Baseline]) addressing the requirement.*

[SOW-712] *The Contractor SHALL describe in detail possible information exchange scenarios and relevant security mechanisms implemented.*

[SOW-713] *The Contractor SHALL address Purchaser comments (including SAA comments) to achieve generic SISRS approval by the SAA.*

[SOW-714] *The Contractor SHALL maintain the generic SISRS during the project.*

10.3.8. Security Operating Procedures (SecOPs) for Gateway Services Section will be adapted to include the centralized management of the IEG-C. Existing SecOPs for Gateway Services Section will be made available to the Contractor after the Contract Award.

[SOW-715] *The Contractor SHALL produce specific procedures for centralized management of IEG-C and include them in IEG-C-specific section of the Security Operating Procedures (SecOPs) for Gateway Services Section.*

[SOW-716] *The Contractor SHALL address Purchaser comments (including SAA comments) to part of the SecOPs related to IEG-C.*

10.3.9. Security Test and Verification Plan (STVP) defines a set of test procedures to be executed to prove that the security mechanisms designed into the IEG-C to enforce the security requirements identified in the IEG-C SISRS. The STVP for IEG-C will be developed by Contractor. The Security Test and Verification Plan template [STVP template] will be made available to the Contractor after the Contract Award.

[SOW-717] *The Contractor SHALL produce the Security Test & Verification Plan (STVP) for the IEG-C using the NATO template [STVP template], defining the set of test procedures to prove that the security mechanisms designed into the **IEG-C** enforce the security requirements identified in the **IEG-C** SISRS. Each test procedure SHALL have unique ID and refer to at least one requirements from IEG-C SISRS and at least one Security Mechanism (from [NS Reference Baseline]).*

[SOW-718] *The Contractor SHALL provide traceability matrix to ensure every security test to be cross referenced to the corresponding security requirement from SISRS as well as to the tested security mechanisms.*

[SOW-719] *The Contractor SHALL ensure all security mechanisms of the IEG-C to be planned for testing.*

[SOW-720] *The Contractor SHALL address Purchaser comments (including SAA comments) to achieve STVP approval by the SAA.*

[SOW-721] *The Contractor SHALL maintain the STVP during the project.*

[SOW-722] *Where necessary due to local security requirements, the Contractor SHALL develop local version of STVP to address local security requirements (e.g. from [AD 070-005]).*

10.3.10. Security Test and Verification Report provides results of all security tests specified in the STVP. Security Test and Verification Report will be generated by Contractor. The Security Test and Verification Report template [STVR template] will be made available to the Contractor after the Contract Award.

[SOW-723] *For each IEG-C site, the Contractor SHALL execute security testing in accordance with STVP (or its local version, where relevant) and in coordination with the Purchaser.*

[SOW-724] *For each IEG-C site the Contractor SHALL generate a Security Test and Verification Report, containing results of all security tests specified in the STVP, using the STVR template.*

[SOW-725] *The Contractor SHALL ensure security test identifiers are preserved in the Report as defined in the STVP or relevant local STVP.*

10.3.11. IEG-C Compliance Statement is required for each of system interconnected between security domains served by IEG-C. The Statement of Compliance template for IEG-C will be developed by the Purchaser on basis of generic SISRS for IEG-C will be made available to the Contractor after IEG-C SISRS approval by the SAA.

[SOW-726] *The Contractor SHALL complete Statement of Compliance for each interconnection via IEG-C. The Statement of Compliance SHALL address local security requirements, where applicable.*

10.4. Security Documentation Review

10.4.1. All documents for security accreditation will be subject to Purchaser and SAA review and approval.

10.4.2. The Contractor should expect a number of review rounds per document before it will be approved, which makes security accreditation a lengthy process. Each review round may last 3 (three) months.

[SOW-727] *The Contractor SHALL ensure draft versions of security documents are provided by the PDR (EDC+3MO) and final versions by the CDR (EDC+6MO).*

[SOW-728] *The Contractor SHALL ensure implementation plans are flexible to take account of the time required for accreditation.*

10.5. Responsibilities

10.5.1. Table below summarizes responsibilities related development of each document required for security accreditation process.

10.5.2. Column “Baseline/Guidance” lists available templates, relevant NATO Security Directives and Guidance, and similar documentation existing NATO CIS which can be used as an example or initial input.

[SOW-729] *The Contractor SHALL undertake the work identified in the column ‘Contractor Responsibility’ in Table 22: Security Accreditation Documentation and Contractor Responsibility below:*

Document	Baseline/Guidance	Contractor Responsibility (*The Contractor SHALL* :)	Purchaser Responsibility
Generic documentation			
SAP	The SAP needs to be updated to the latest approved SAP template	Inform Purchaser about any expected changes in schedule of accreditation-related activities	Update SAP, when necessary Coordination with the SAA
CIS description	[IEG-C description]	Update CIS description Address Purchaser and SAA comments Maintain CIS description during project duration Achieve CIS description endorsement	Provide initial IEG-C description and guidance to the Contractor Review CIS description provided by the Contractor Coordination with the SAA Provide SAA comments to the Contractor
SRA Report	[AC/35-D/1017] [SRA template]	Conduct SRA Develop SRA report Address Purchaser and SAA comments Maintain SRA report during project duration	Provide guidance to the Contractor Provide SRA Report Template Review SRA Report provided by the Contractor Coordination with the SAA Provide SAA comments to the Contractor

Document	Baseline/Guidance	Contractor Responsibility (*The Contractor SHALL* :)	Purchaser Responsibility
		Achieve SRA approval by the SAA	
Generic SISRS for IEG-C	[AC/35-D/0030-REV5] [AC/322-D/0048-REV3] [NS Reference Baseline] [SISRS template]	Develop generic SISRS for IEG-C Address Purchaser and SAA comments Maintain generic SISRS during project duration Achieve generic SISRS for IEG-C approval by the SAA	Provide template and guidance to the Contractor Review generic SISRS for IEG-C provided by the Contractor Coordination with the SAA Provide SAA comments to the Contractor
SecOPs	GSS SecOPs	Develop procedures for centralized management of the IEG-C. Address Purchaser and SAA comments to IEG-C part of the SecOPs	Provide BPS SecOPs and guidance to the Contractor Review SecOPs provided by the Contractor Coordination with the SAA Provide SAA comments to the Contractor
STVP for IEG-C	[STVP template] [NS Reference Baseline]	Develop STVP (The STVP shall refer to generic SISRS for IEG-C and include traceability matrix) Address Purchaser and SAA comments Maintain generic STVP during project duration Achieve STVP approval by the SAA	Provide template and guidance to the Contractor Review STVP provided by the Contractor Coordination with the SAA Provide SAA comments to the Contractor
STVR for IEG-C Template	[STVR Template] [STVP for IEG-C]	Develop STVR template Address Purchaser comments	Provide STVR template and guidance to the Contractor

Document	Baseline/Guidance	Contractor Responsibility (*The Contractor SHALL* :)	Purchaser Responsibility
			Review STVR for IEG-C template provided by the Contractor
Statement of Compliance – to be done for each site where IEG-C is installed	[generic SISRS for IEG-C] [Statement of Compliance Template]	Complete Statement of compliance for each interconnection via IEG-C Include local security requirements, where applicable Address Purchaser and local SAA comments Achieve Statement of Compliance approval by the local SAA	Provide Statement of Compliance template and guidance to the Contractor Review SISRS provided by the Contractor Coordination with the local SAA Provide local SAA comments to the Contractor
Local STVP	[STVP for IEG-C]	Develop local STVP for IEG-C, where applicable (include testing of local security requirements) Address Purchaser and local SAA comments Achieve local STVP approval by the local SAA	Provide guidance to the Contractor Review STVP provided by the Contractor Coordination with the local SAA Provide local SAA comments to the Contractor
STVR (test report)	[STVR for IEG-C] [Local STVP]	Execute testing in accordance with STVP (or its local version) in coordination with the Purchaser Complete STVR	Provide guidance to the Contractor Cooperate/supervise with the Contractor during the testing Coordination with the SAA

Table 22: Security Accreditation Documentation and Contractor Responsibility

SECTION 11: QUALITY ASSURANCE

11.1. Definitions

11.1.1. Quality Assurance (QA) is a process and set of procedures intended to ensure that a product or service, during its definition, design and development phases will meet specified requirements.

11.1.2. 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

11.1.3. Under this contract the QA process SHALL be intended as Quality assurance and Control Program. The term QA will include also the QC definition.

11.1.4. Certificate of Conformity (CoC) is a document, signed by the Supplier, which states that the product conforms with contractual requirements and regulations

11.1.5. The CoC, verifies the process quality-enabled items produced or shipped comply with test procedures and quality specifications prescribed by the customer. It presents data derived from quality management information.

11.2. Introduction

[SOW-730] *The Contractor SHALL establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the Contract's lifetime.*

[SOW-731] *The Contractor's QA effort SHALL apply to all services and all products (both management products and specialist products) to be provided by the Contractor under this contract (this includes all hardware and software – COTS as well as developed for this project – documentation and supplies that are designed, developed, acquired, maintained or used, including deliverable and non-deliverable items).*

[SOW-732] *The Contractor's QA effort 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 (both management products and specialist products), in accordance with the requirements of this Contract.*

11.3. Quality Assurance References

[SOW-733] *The Purchaser, in this contract, applies the NATO Standardisation Agreement, STANAG 4107 "Mutual Acceptance of Government Quality Assurance and usage of the Allied Quality Assurance Publications (AQAP)" (see 2.1.2) which the Contractor SHALL herewith accept and adhere to.*

11.4. Roles and Responsibilities

[SOW-734] *The Purchaser may delegate the Quality Assurance to the appropriate Government Quality Assurance Authority (GQAA) in accordance with STANAG 4107. The Purchaser, through its own Quality Assurance, however, will retain*

the overall supervisory and liaison authority concerning all Quality related matters, and, for this purpose, will use its own QA Personnel.

[SOW-735] *The term "NATO Quality Assurance Representative" (NQAR) SHALL apply to any of the Purchaser appointed Quality Assurance Representative, whether nominated by the GQAA or by Purchaser QA. During the entire contract implementation, the NQAR(s) within their own rights, defined in the contract applicable AQAPs, SHALL assure the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirement.*

[SOW-736] *The term "Contractor Quality Assurance Representative" (CQAR) SHALL apply to any of the Contractor appointed Quality Assurance Representative. That person SHALL be designated as the Contractor's QA Representative and point of contact for interface with and resolution of quality matters raised by the NCI Agency or his delegated NQAR and identified in the Quality Assurance Plan.*

[SOW-737] *The Contractor SHALL be responsible for controlling product quality and for offering to the NQAR(s) for acceptance only those supplies and services which conform to contractual requirements and, when required, for maintaining and furnishing objective evidence of this conformance.*

[SOW-738] *The NQAR(s) is (are) responsible for determining that contractual requirements have been complied with, prior to the acceptance of the services.*

[SOW-739] *The Contractor SHALL give written notice to the NQAR(s) at least four weeks in advance that the services are being presented for inspection, testing and acceptance. Testing SHALL only be permitted by using Purchaser approved test procedures and plans.*

11.5. Quality Management System (QMS)

[SOW-740] *The Contractor SHALL establish, document and maintain a Quality Management System in accordance with the requirements of ISO 9001:2015 or equivalent. The Purchaser SHALL be allowed to audit the QMS on request.*

[SOW-741] *The Contractor's and Sub-Contractor's QMS relevant to performance under this contract SHALL be subject to continuous review and surveillance by the cognizant NQAR(s).*

[SOW-742] *The Contractor SHALL include in orders placed with his 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. As required, STANAG 4107 SHALL be specified.*

[SOW-743] *The Contractor SHALL specify in each order placed with his sub-Contractor(s) and Supplier(s),the Purchaser's and his 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).*

11.6. The Quality Assurance Plan (QAP)

[SOW-744] *The Contractor's QA effort SHALL be described in detail in a Quality Assurance Plan (QAP), which SHALL clearly indicate the QA activities, responsibilities, and checks for the Contractor and any Sub-Contractors.*

[SOW-745] *All versions of the QAP SHALL be configuration controlled and provided to the Purchaser for acceptance.*

[SOW-746] *The acceptance of the QAP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.*

[SOW-747] *The Contractor SHALL review his QA programme periodically and audit it for adequacy, compliance and effectiveness.*

[SOW-748] *The Contractor SHALL ensure that all contractual requirements, including NATO supplements, are included in internal audits.*

[SOW-749] *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-750] *The Contractor SHALL include a risk management section within the QAP including the risks connected to the subcontractors of the Contractor.*

[SOW-751] *The Contractor SHALL agree to provide all necessary assistance to the NQAR.*

[SOW-752] *The Contractor SHALL make his quality records, and those of his subcontractors, available for evaluation by the NQAR throughout the duration of the Contract.*

[SOW-753] *The Contractor SHALL use the review processes described in the SECTION 12 Configuration Management Plan (CMP) to manage changes to the QAP.*

[SOW-754] *The Contractor SHALL update the document, as required, from the delivery date of the initial QAP through Final System Acceptance (FSA), under Configuration Management. The Contractor SHALL provide a copy of each new version of the QAP to the NQAR and the new version SHALL be approved by the Purchaser.*

11.7. Defects and Corrective Actions

[SOW-755] *If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any product already supplied to the Purchaser, the Contractor SHALL coordinate with the Purchaser and promptly correct the defect.*

[SOW-756] *The Contractor SHALL implement a quality/product assurance risk log/action tracking system, which identifies all the major/minor non conformity raised during the life cycle of this Contract.*

[SOW-757] *The Contractor, through its Corrective Action System, SHALL track all reported and recorded problems and deficiencies until their closure and clearance.*

[SOW-758] *The Contractor SHALL notify the Purchaser of proposed action, resulting from Review Output that will affect compliance with contractual requirements.*

[SOW-759] *The Contractor SHALL demonstrate that all the non-conformities are solved and all defects are closed before the product acceptance.*

[SOW-760] *The Contractor SHALL issue and implement documented procedures which identify, control and segregate all non-conforming products. Documented*

procedures for the disposition of non-conforming product are subject to approval by the Purchaser when it can be shown that they do not provide the necessary controls.

[SOW-761] *The Contractor SHALL notify the Purchaser of non-conformities and corrective actions required, unless otherwise agreed with the Purchaser.*

[SOW-762] *When the Contractor establishes that a subcontractor product is unsuitable for its intended use, he SHALL immediately report to and coordinate with the Purchaser the remedial actions to be taken.*

[SOW-763] *The Contractor SHALL ensure that only acceptable products passing all required quality gates/measures/checks, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.*

[SOW-764] *The Contractor SHALL document the Corrective Action System in the QAP.*

[SOW-765] *The Contractor SHALL describe the process used for defect management in the QAP.*

11.8. Certificate of Conformity (CoC)

11.8.1. The Contractor is solely responsible for the conformance to requirements, of products provided to the Purchaser.

[SOW-766] *The Contractor SHALL deliver all the CoCs for COTS software (including firmware) and hardware released by the COTS Vendors.*

11.8.2. The CoCs delivered by the Contractor will be part of the acceptance data package of the product.

[SOW-767] *The Contractor SHALL provide a CoC at release of product to the Purchaser unless otherwise instructed.*

11.9. Support Tools

[SOW-768] *The Contractor SHALL make all support tools available for demonstration to the NQAR, upon request.*

[SOW-769] *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.*

SECTION 12: CONFIGURATION MANAGEMENT

12.1. General

12.1.1. The Configuration Management process will enable the baselining of CIs into the Functional Baseline (FBL), Allocated Baseline (ABL) and Product Baseline (PBL) as defined in this section of the SOW and the maintenance of these baselines throughout the duration of the contract.

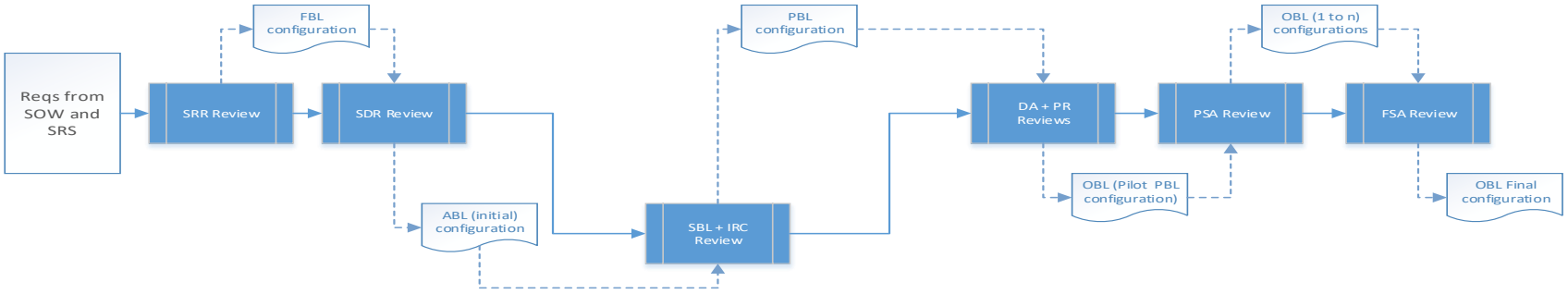
[SOW-770] *The Contractor SHALL implement a CM process as referred to in [STANAG 4427, 2014], [ACMP-2000, 2017], [ACMP 2009, 2017] and [ACMP-2100,2017] to carry out the Configuration Management functions as described in this SOW (configuration item identification, configuration control, configuration status accounting, and configuration audit and verification).*

[SOW-771] *The Contractor SHALL ensure that an effective Configuration Management organization is established to implement and manage the Configuration Management processes throughout the duration of this contract.*

[SOW-772] *The Contractor SHALL create and maintain four Configuration Baselines, as follows (see Figure 3). The Contractor shall create multiple instances of one type of the configuration baseline to adjust to the agile delivery approach, as required.*

- *Functional Baseline (FBL, or "as required"),*
- *Allocated Baseline (ABL, or "as designed"),*
- *Product Baseline (PBL, or "as built"),*
- *Operational Baseline (OBL, or "as delivered", or "as deployed").*

[SOW-773] *Under the CM program the Contractor SHALL maintain and update all project CIs as required by changes within the project or external to the project throughout the duration of the contract.*



1) SRR Review → FBL (as required)

2) SDR Review → ABL (as designed)

3) SBL Review(s) → PBL (as built)

4) DA+ PR Review(s) → OBL (as delivered) (Pilot Release)

5) PSA + FSA Reviews → OBL (as delivered) (Major/Final Release)

Product

Event

Legend:

SoW – Statement of Work
SRS – System Requirements Specification
SDR – System Requirements Review
FBL – Functional Baseline
ABL – Allocated Baseline
SBL – System Baseline Review
IRC – Internal Release Candidate
DA – Deployment Authorization
PR – Pilot Release Review
PBL – Product Baseline
PSA – Partial System Acceptance
OBL – Operational Baseline
FSA – Final System Acceptance

Figure 6: Configuration Baseline

12.2. Baselines

[SOW-774] *The Contractor SHALL ensure that all system configuration and baselines will be detailed in a System Version Definition Document (SVDD); see Section 15.7.*

12.2.1. Traceability

[SOW-775] *The Contractor SHALL ensure that there is full traceability through all baselines back to the functional baseline.*

[SOW-776] *The Contractor's developed baselines SHALL be encapsulated and maintained by the Contractor in a CM database (CMDB) established by the Contractor as specified under Configuration Management Tools.*

12.2.2. Functional Baseline (FBL)

12.2.2.1. The FBL is a set of documents that specifies the functional and non-functional requirements of a service or product and that is used as the approved basis for comparison.

[SOW-777] *The Contractor SHALL develop and derive the FBL from the IEG-C SRS and SHALL establish the FBL at the successful completion of the SRR (EDC+2MO) with the approved updated SRS.*

[SOW-778] *The Contractor SHALL maintain an up-to-date version of the Functional Baseline in the CMDB and ensure the relevant project documentation such as Requirements Traceability Matrix (RTM) is updated based on the approved FBL. The information SHALL be integrated into the NCI Agency DOORS database.*

12.2.3. Allocated Baseline (ABL)

12.2.3.1. The ABL is a set of documents that specifies the design of a service or product and is used as the approved basis for comparison.

[SOW-779] *The Contractor's developed design in the ABL SHALL meet the functional and non-functional requirements allocated in the FBL.*

[SOW-780] *The ABL set of documents and artefacts SHALL contain, but is not limited to, the following documents:*

- *System Design Specification*
- *Interface Control Document (ICD)*
- *The Test Specification*
- *Requirements Traceability Matrix*

[SOW-781] *The Contractor's initial ABL SHALL be established first at the successful completion of the PDR (EDC+3MO) and SHALL be finally accepted at the successful completion of CDR (EDC+6MO).*

[SOW-782] *The Contractor SHALL maintain and update the ABL configuration during the System Baseline Reviews (SBR).*

12.2.4. Product Baseline (PBL)

12.2.4.1. The PBL is a set of products and/or services, including supporting documents, which is used as the approved basis for comparison.

[SOW-783] *The Contractor SHALL ensure its PBL meets the functional and non-functional requirements allocated in the FBL and the design of the ABL.*

[SOW-784] *The Contractor SHALL ensure its PBL products are distinguished in documentation, software, hardware/equipment and services.*

[SOW-785] *The Contractor SHALL ensure the products of its PBL contain, but are not limited to, the following:*

- *Hardware components, including COTS,*
- *Software media, including COTS,*
- *Software license(s), including COTS.*

[SOW-786] *The Contractor SHALL ensure its PBL (supporting) documentation products contain, but are not limited to:*

- *As-built drawings,*
- *COTS O&M manuals,*
- *FBL documentation,*
- *ABL documentation,*
- *O&M manuals (custom),*
- *Inventory documentation (both for hardware and software products),*
- *Software Distribution list (SWDL),*
- *Training documentation,*
- *QA documentation,*
- *Security documentation,*
- *Configuration Management Database including the individual artefacts,*
- *Warranty documentation*
- *Requirements Traceability matrix.*

[SOW-787] *The Contractor SHALL include the SDS (including the RTM), the Test Plan, and any other documentation deemed appropriate by the Contractor, in accordance with provisions of IEEE 12207, to ensure requirements are reflected in the system during development and integration, can be demonstrated through a comprehensive set of tests, and can be delivered in the form of the Product Baseline.*

[SOW-788] *The IEG-C PBL SHALL be initially established before the testing events and SHALL be updated after the changes applied based on the outcomes of the testing events.*

[SOW-789] *The Contractor SHALL include in the PBL release package the following elements, as a minimum all items described in Table 23: Content for Product Baseline Release Package*

Serial	Requirement
1.	All required Hardware and Software CIs
2.	The source code of elements categorised as foreground knowledge, script, and configuration setting baseline, including the documentation for these items.
3.	The script and configuration setting baseline, including documentation for these items, for non-development software items (e.g., Microsoft Office).
4.	Release notes, which include a description of what is new or changed in each software module.
5.	List of open known problems and faults.
6.	The SRS and SDS versions against which the baseline has been developed.
7.	Interface Control Documents for all interfaces
8.	All design artefacts provided as part of the SDS, updated to reflect the PBL.
9.	Conversion programs and instructions.
10.	Plug-ins/add-ins, glue-code and interfaces.
11.	Parameter definitions.
12.	Initial data sets.
13.	On-line help files.
14.	Technical Documentation (i.e. operation and maintenance manuals)
15.	Training Documentation
16.	Test procedures and scripts for any automated tests, along with all source data for the manual and automated tests and including the documentation for these items.
17.	Test stub, along with test scenario and sample data to support the integration of IEG-C with other services.
18.	Copyright and license information.
19.	Instructions for system administration staff to follow to save the previously installed system baseline, to install the new baseline, and to recover the old baseline if the new baseline installation must be interrupted or aborted.
20.	Configuration files, and Installation scripts.
21.	Instructions on how to identify and report problems after acceptance.
22.	Instructions for the generation of new PBLs, distribution and installation of new software versions, and any test procedures and test cases necessary to verify the generated baseline before distribution.
23.	Additional documentation artefacts identified in the SRS.

Table 23: Content for Product Baseline Release Package

12.2.5. Operational Baseline (OBL)

[SOW-790] *The Contractor's developed OBL SHALL be initially established after successful completion of the PSA (EDC+20mo) and then finally established after successful completion of FSA. It reflects the "as-deployed" configuration of the system.*

[SOW-791] *The Contractor's OBL SHALL be established site-specific, as applicable.*

[SOW-792] *The Contractor's OBL SHALL contain, but is not limited to:*

- *All delivered software CI (i.e. CSCI, CSC, CSUs), including COTS;*
- *All delivered hardware CI (if any);*
- *All the Documentation that comprise the system and any subsequent releases;*

[SOW-793] *IEG-C Baselines SHALL be given a major release number and a minor release number comprising an X.X notation. The complete baseline identifier SHALL include the specific baseline identifier (i.e. FBL, ABL, PBL, and OBL), site identification (if applicable) and security domain difference (if applicable). Final numbering scheme for the baseline identification may be modified with Purchaser agreement, and it SHALL be proposed for Purchaser approval within the CM Plan.*

[SOW-794] *The Contractor SHALL update and re-release the PBL documentation outlined in Table 4, as required.*

12.3. Configuration Management Plan (CMP)

[SOW-795] *The Contractor SHALL provide a CMP tailored to the requirements of the proposed technical solution.*

[SOW-796] *The Contractor's CMP SHALL be structured as a living document subject to revisions and updates, as required.*

[SOW-797] *The Contractor SHALL place the plan under configuration control prior to its implementation and for the life of the Contract.*

12.3.1. The CMP is a Product Lifecycle document that will survive the project after FSA. As such, this documents are not to be submitted as part of the PMP, but will be part of the Technical Proposal.

[SOW-798] *In producing the CMP, the Contractor SHALL define the organisation and procedures used to configuration manage the functional and physical characteristics of CIs, including interfaces and configuration identification documents.*

[SOW-799] *The Contractor SHALL ensure that all required elements of CM are applied in such a manner as to provide a comprehensive CM process.*

[SOW-800] *The Contractor's CM Plan SHALL be compatible and consistent with all other plans, specifications, standards, documents and schedules.*

[SOW-801] *The Contractor SHALL propose in the CMP detailed configuration control procedures.*

[SOW-802] *All Contractor and Purchaser activities and milestones related to CM SHALL be identified and included in the PMS of the PMP.*

[SOW-803] *The Contractor SHALL establish and maintain product-based planning which SHALL include as a minimum:*

- *A product description of the final product of the project;*
- *A Project PBS;*
- *Product Descriptions of each product;*
- *A PFD.*

[SOW-804] *The Contractor's CM Plan SHALL address all disciplines within this Section and SHALL as a minimum include, but not be limited to the following Sections:*

- *Introduction;*
- *Organisation;*
- *Configuration Identification and Documentation;*
- *Configuration Control;*
- *Configuration Status Accounting;*
- *Configuration Audits;*
- *Configuration Management Database (CMDB);*
- *Configuration Management tools/Interface management.*

12.4. Configuration Item Identification and Documentation

[SOW-805] *The Contractor SHALL divide the products and specialist products into Configuration Items (CIs).*

[SOW-806] *The Contractor's CI structure SHALL show the relationships between the lower level Baselines and CIs.*

[SOW-807] *The Contractor SHALL propose appropriate CIs in the CM Plan including an explanation of the rational and criteria used in the selection process, based on the criteria for selection of CIs as detailed in [ACMP 2009, 2017].*

[SOW-808] *The Contractor's CIs SHALL be chosen in a way to assure visibility and ease of management throughout the development effort and the support to the OBL after acceptance.*

[SOW-809] *All Contractor's COTS, adapted, and developed software SHALL be designated as CIs.*

[SOW-810] *Where Contractor's COTS can be installed in a modular fashion, the description of the CI SHALL unambiguously identify the complete list of installed components.*

[SOW-811] *The Contractor SHALL designate as CIs all hardware elements (if any) down to the maintenance significant item level.*

12.4.1. Additional guidance about CI selection can be found in [ACMP 2009, 2017] and in [STANAG 4427, 2014].

12.4.2. The Purchaser reserves the right to modify the CI structure and attributes.

[SOW-812] *The Contractor SHALL ensure the level of granularity for the CI selection reaches at a minimum:*

- *Line Replaceable Units (LRUs) - Hardware CIs,;*
- *Software Assets and/or Firmware/Software CIs;*
- *All Maintenance Significant Items (MSI) lower than LRU level;*
- *Documentation delivered under this Contract - Documentation CIs;*

[SOW-813] *The Hardware CI attributes SHALL include, but is not limited to, the MDS information,(Optional);*

[SOW-814] *The Software CI attributes SHALL include, but is not limited to, the [ACMP 2009, 2017] definitions;*

[SOW-815] *Any Documentation CI that is not linked to a Software CI or Hardware CI (optional) SHALL include, but is not limited to, the Contract SSS attributes.*

12.5. Configuration Control

[SOW-816] *The Contractor SHALL be responsible for issuing in a timely manner all approved changes and revisions to the functional, development and PBL documents included in the Contract. This includes changes originated both by the Contractor and the Purchaser.*

[SOW-817] *Where a change affects more than one document, or affects documents previously approved and delivered, the Contractor SHALL ensure that the change is properly reflected in all baseline documents affected by that change.*

[SOW-818] *The Contractor SHALL appropriately reflect all design changes in the technical documentation by the issue of appropriate changes or revisions.*

[SOW-819] *The Contractor SHALL provide all such changes/revisions to the Purchaser.*

[SOW-820] *The Contractor SHALL be fully responsible for the Configuration Control of all baselines and CIs in accordance with [ACMP 2009, 2017] and [ACMP-2000, 2017].*

[SOW-821] *The Contractor SHALL define the responsibilities and procedures used within the Contractor's organization for configuration control of established CI, and for processing changes to these CI.*

[SOW-822] *The Contractor SHALL define the Configuration Baseline Change procedures and SHALL submit Notice of Revision or Request for Deviations (RFD) and Request for Waivers (RFW) when required and approved by the Purchaser.*

[SOW-823] *The Contractor SHALL provide read-only access to the Purchaser to audit and control its productions environments and configuration management tools (for software, documentation and hardware, if applicable).*

12.6. Engineering Change Proposals (ECP)

[SOW-824] *The Contractor SHALL process changes to the his developed baselined CIs as either Class I or Class II ECPs as defined in [ACMP 2009, 2017] and the change request requirements specified.*

[SOW-825] *The Contractor SHALL use the configuration control procedures specified in the CM Plan for the preparation, submission for approval implementation and handling of ECPs to baselined CIs.*

[SOW-826] *When submitting ECPs, the Contractor SHALL assign a priority rating of Emergency, Urgent or Routine Extensions to the target times for processing.*

[SOW-827] *Changes to baseline CIs SHALL be processed as either Class I or Class II ECPs as defined in [ACMP 2009, 2017].*

[SOW-828] *Class I ECPs SHALL have to be mutually agreed upon by the Contractor and Purchaser.*

[SOW-829] *Prior to implementation, all Class II ECPs SHALL be submitted by the Contractor to the Purchaser for review and classification concurrence.*

[SOW-830] *If the Purchaser's representative does not concur in the classification, Class I ECP procedures SHALL be applied by the Contractor and the ECP and then formally submitted to the Purchaser for approval or rejection.*

[SOW-831] *Extensions to the target times for processing Class I ECPs SHALL be mutually agreed upon by the Contractor and Purchaser.*

[SOW-832] *The Contractor SHALL not implement Class I ECPs before Purchaser approval.*

[SOW-833] *The Contractor SHALL reflect in the technical documentation all design changes appropriately by the issue of appropriate documentation revisions.*

[SOW-834] *The Contractor SHALL provide all supporting documentation and information to detail the impact of the change in design, specification, maintenance and support, documentation, cost, schedule, and security, as requested by the Purchaser.*

[SOW-835] *The Contractor SHALL propose in the CM Plan an ECP format based on the requirements in [ACMP 2009, 2017].*

[SOW-836] *The Contractor SHALL include in an ECP as a minimum, the following information:*

- *Reference Number;*
- *Requirement affected (using the outline numbering of the core SOW, or of Annex A);*
- *Nature of change;*
- *Rationale for the change;*
- *Impact of change;*
- *Description of how the change will be reflected in the delivered system's cost, schedule, and/or performance. This description SHALL include any trade-offs that SHALL be considered;*
- *Status;*

- *Priority.*

[SOW-837] *After the completion of Deployment Authorization (DA at EDC+20mo), the Contractor SHALL provide the ECP's for proposed changes which will also require the new approval for the DA. For that purpose, the Contractor SHALL provide all the information necessary and support the Purchaser Project Manager by any means to obtain the Deployment Authorization based on the proposed change and new baseline.*

12.7. Requests for Change (RFC)

12.7.1. The achievement of the Deployment Authorization (DA) milestone is subject to the Purchaser approval. This process will be triggered with a Request for Change (RFC) by the NATO assigned PM. The last Purchaser approved baseline for the RFC process will be used. The RFC will be submitted to the Purchaser's Change Advisory Board (CAB) for screening. The CAB will decide if further or other tests are required. If all the RFC required final documents are submitted and the production baseline is successfully tested by the Purchaser's internal test activities, the CAB may grant the approval to be deployed on NATO Operational targeted Networks. As part of this process the new baseline is incorporated into the relevant Approved Fielded Products List (AFPLs).

[SOW-838] *The Contractor SHALL comply and support Purchaser's internal Change Management Process in order to obtain the Deployment Authorization Approval through the Change Advisory Board (CAB).*

[SOW-839] *The Contractor SHALL support the Purchaser in preparing the Request For Change (RFC) to meet the requirements of the Purchaser's Change Evaluation process.*

[SOW-840] *The Contractor SHALL provide all necessary documentation and information for the successful completion of the Deployment Authorization.*

[SOW-841] *The contractor SHALL assist the Purchaser with the installation and configuration the system/application in accordance with the Contractor provided Installation and Configuration Manual(s).*

[SOW-842] *The Contractor SHALL conduct a Functional Configuration Audit (FCA) and deliver the associated FCA report*

[SOW-843] *After the successful testing of SIT/SAT/UAT and Security tests, the Contractor, through the NATO assigned PM, SHALL submit the baseline to the Purchaser IT Change Management process by submitting the RFC.*

[SOW-844] *The NATO assigned PM SHALL seek the authorization of deployment on the relevant targeted NATO networks. The Contractor SHALL provide the required final RFC documents (i.e. ECP and supporting documentation) described in SOW 12.6.*

[SOW-845] *The RFC SHALL be submitted to Purchaser's Change Advisory Board (CAB) for screening. The CAB SHALL decide if further or other tests are required. The latest Purchaser approved baseline for the RFC process SHALL be used.*

[SOW-846] *If the Contractor is produced a new build or baseline version the Contractor SHALL follow Purchaser's internal Change Management process and test activities as deemed necessary by the CAB.*

[SOW-847] *The Contractor SHALL note that system implementation activities in operational environment will not start until the DA milestone is approved by the Purchaser.*

[SOW-848] *The Contractor SHALL provide and update all related baseline documentation and traceability to reflect the modifications triggered by the change.*

12.7.2. The Purchaser will verify the Installation and Configuration Manual(s) and other delivered Documents as deemed necessary as part of the CAB approval process

12.7.3. The Purchaser has a right to perform any other tests as deemed necessary

12.7.4. The installation of new baseline will be performed by the Purchaser unless requested by the Purchaser to be installed by the Contractor and witnessed by the Purchaser.

[SOW-849] *The Contractor, if requested by the Purchaser SHALL install the new baseline or other instances of new baselines for Security and other Purchaser related tests.*

12.7.5. Release Package

12.7.5.1. A Release Package is a planned release of a product or product edition. The content of a Release Package is defined by the features and associated Requests for Change (RFC) that it implements.

[SOW-850] *The Contractor SHALL supply the documents in Final form listed in Table 24: System Submission Requirements Matrix (SSRM) for inclusion in the Purchaser Release Package for the RFC.*

		MAJOR / MINOR RELEASES	PATCH RELEASES
COMMON	A&T Portfolio	✓	✗
	Funding availability	✓	✓
	System Media	✓	✓
	Release information (Release Notes / Product Guide / Version Description document)	✓	✓
	Installation Instructions	✓	✓
	User Manual[6]	✓	✗

[6] User Manual is required for systems that have a human interface.

	Administration Manual[7]	✓	✗
	Security Settings[8]	✓	✗
	Support Plan	✓	✗
	Deployment Plan	✓	✓
	Design Description[9]	✓	✗
ADDITIONAL REQUIREMENTS FOR NOTS	Requirement Traceability Matrix	✓	✗
	Functional Test Report	✓	✗
	User Acceptance Test Report[10]	✓	✗
ADDITIONAL REQUIREMENTS FOR NEW SOFTWARE	CONOPS	✓	✗

Table 24: System Submission Requirements Matrix (SSRM)

12.8. Requests for Deviation (RFD) and Request for Waver (RFW)

[SOW-851] *If required, the Contractor SHALL prepare, handle, and submit for Purchaser's approval, RFDs and RFWs as defined in [ACMP 2009, 2017].*

---

[7] Administration Manual is only required if the deployment and maintenance of the release necessitates special administration operations.

[3] Security Settings are required when the target environment needs to be configured in accordance with Cyber Security requirements.

[4] Interface Design and Architecture Descriptions are required when the system interoperates with other systems.

[10] In case of Interim Approval request or customer feedback on UAT is available via other records or communication, User Acceptance Test (UAT) Report is not required upon submission.

[SOW-852] *The Contractor SHALL propose in the CM Plan a RFD and RFW format based on the requirements in [ACMP 2009, 2017].*

[SOW-853] *The Contractor SHALL be aware that permanent departures from a baseline SHALL be accomplished by ECP action rather than by RFD/RFW.*

12.9. Configuration Status Accounting (CSA)

[SOW-854] *The Contractor SHALL be fully responsible for the CSA for all CIs in accordance with [ACMP 2009, 2017].*

[SOW-855] *Contractor SHALL prepare and deliver the CSA reports for each milestone and as requested by the Purchaser.*

[SOW-856] *The Contractor SHALL propose the format of the CSA report in the CM Plan for Purchaser's approval.*

[SOW-857] *The Contractor SHALL deliver CSA reports to the Purchaser both as part of management and specialist products in this contract and also as standalone documents at the Purchaser's request.*

[SOW-858] *At the end of the Contract, the Contractor SHALL deliver a set of final CSA reports for each CI or set of CI's in both hard copy and in electronic media.*

12.10. Configuration Verification and Audits

[SOW-859] *Upon request from the Purchaser, the Contractor SHALL support configuration audits to demonstrate that the actual status of all CIs matches the authorised state of CIs as registered in the CSA reports according to [ACMP 2009, 2017].*

[SOW-860] *The Contractor SHALL support the FCA and PCA by providing the required Baseline Documentation and answering questions from the Purchaser's Auditor.*

[SOW-861] *The Contractor SHALL draft a Configuration Audit Report for the FCA and PCA that summarises the results for the Purchaser's approval.*

[SOW-862] *The Contractor SHALL solve any deficiencies found during the Configuration Management Audits within the agreed timeframe and update the baseline accordingly.*

[SOW-863] *The Contractor SHALL provide the initial version of his ABL and PBL to the Purchaser for acceptance.*

12.10.1. Upon Purchaser Acceptance, ABL and PBL will be placed under the control of the CCB.

12.10.2. The acceptance of the ABL and PBL by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

[SOW-864] *The Contractor SHALL keep the contents of the ABL and PBL under Configuration Control to reflect the progress of the project activities.*

12.11. Configuration Management Database and Software Versioning Tool

12.11.1. Configuration Management Database (CMDB)

[SOW-865] *The Contractor SHALL create and maintain a CMDB that persists the CIs attributes, (inter-) relationships, and Configuration Baselines.*

[SOW-866] *The Contractor SHALL create or use a COTS software to maintain the CMDB that persists the Configuration Items (CIs) attributes, (inter-) relationships and Configuration Baselines.*

[SOW-867] *The Contractor SHALL ensure that the Configuration Baselines and CIs are persistently stored, maintained and managed in the CMDB.*

[SOW-868] *The Contractor SHALL keep the CMDB consistent and updated. The Contractor SHALL keep the CMDB consistent and updated.*

[SOW-869] *The Contractor, through the CMDB, SHALL provide the ability to easily trace higher and subordinate CIs using CI identifiers or other CI attributes.*

[SOW-870] *The Contractor's CMDB SHALL be compliant with the Purchaser's IT Service Management (ITSM) Tools.*

12.11.2. Software Versioning Tool

[SOW-871] *The Contractor SHALL use a software source code version control program for any custom software development.*

[SOW-872] *Subject to approval of the Purchaser under the Technology Substitution clause, the Contractor SHALL establish and maintain the baselines referred to above using the latest commercial version of the version control/Configuration Management automated tool.*

[SOW-873] *The Contractor, through his provided version control/Configuration Management automated tool, SHALL include the capabilities for baselines management, source control versioning, configuration item identification, change request management, deficiency reporting management, and configuration status accounting.*

[SOW-874] *The Contractor SHALL provide the Purchaser read-only access to the version control/Configuration Management automated tool.*

[SOW-875] *The Contractor SHALL provide the ability for the Purchaser to access (read-only) the source code of the baseline via the version control/Configuration Management automated tool.*

[SOW-876] *The Contractor SHALL provide the version control/Configuration Management automated tool as part of the IEG-C Reference System to enable life-cycle Configuration Management.*

[SOW-877] *At the end of the contract, the Contractor SHALL transfer the current CMDB database to the Purchaser.*

12.12. **Configuration Identification and Documentation**

12.12.1. Configuration Identification

[SOW-878] *The Contractor SHALL establish a Configuration Identification System.*

[SOW-879] *The Contractor's, through his Configuration Identification System, SHALL identify all documents necessary to provide a full technical description of the*

characteristics of the Hardware and Software CIs that require control at the time each baseline is established.

[SOW-880] *The Contractor, through his Configuration Identification System, SHALL include the relevant deliverables in the contract.*

[SOW-881] *The Contractor SHALL provide a CI structure in a tree structure with the PBL being the top level CI.*

12.12.2. Documentation

[SOW-882] *The Contractor SHALL include detailed proposals for the documents that will comprise the above baselines in the CM Plan for approval by the Purchaser.*

[SOW-883] *At the end of the contract, the Contractor SHALL deliver the baseline documentation in a format which complies with SOW 11.6.12.*

[SOW-884] *As part of the CMDB, as specified under Configuration Management Tools, the Contractor SHALL transfer a copy of the current version of all baselines to the Purchaser at contract completion.*

[SOW-885] *The Contractor SHALL propose the documentation identification and version control system right after the Kick-off Meeting, before the release of the project documentation, for Purchaser approval. The identification SHALL include the project number, the document name and the version of the document. The versioning of the documentation SHALL be applied in a manner that major versions will be applied before each milestone or official delivery, and minor versions will be applied within the review cycles.*

SECTION 13: LABOUR CATEGORIES

13.1. General

13.1.1. This section outlines minimum educational and experience qualifications for Contractor key personnel assigned to this Contract.

[SOW-886] *All Contractor's IEG-C project key personnel SHALL demonstrate spoken and written fluency in English language, at a minimum of 4343 as defined in [STANAG 6001, 2014].*

[SOW-887] *All Contractor's IEG-C project key personnel SHALL have a current NS security clearance and maintain it throughout the lifecycle of the Contract. Contractor personnel who need System Administrator or Operator privileges when working on NATO SECRET systems SHALL be required to hold NATO CTS (Cosmic Top Secret) clearances.*

[SOW-888] *All Contractor's IEG-C project key personnel SHALL present references of successful project delivery and description of roles, responsibilities, activities executed, and SHALL include reachable points of contact for above.*

13.1.2. Substitution of experience or education is allowed as outlined in Table 19-1 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	Bachelors + 4 years of experience	8 years of relevant experience

Table 25: Experience / Education substitution

13.2. Management

13.2.1. Project Manager

13.2.1.1. Responsible for project management, performance and completion of tasks and deliveries. Establishes and monitors project plans and schedules and has full authority to allocate resources to insure that the established and agreed upon plans and schedules are met. Manages costs, technical work, project risks, quality, and corporate performance. Manages the development of designs and prototypes, test and acceptance criteria, and implementation plans. Establishes and maintains contact with Purchaser, subcontractors, and project team members. Provides administrative oversight, handles Contractual matters and serves as a liaison between the Purchaser and corporate management. Ensures that all activities conform to the terms and conditions of the Contract.

13.2.1.2. Education: University Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/ diplomas. Current Project Management certification (Prince2 Practitioner and/or Project Management Institute (PMI) Project Management Professional (PMP)). Current Information Technology Infrastructure Library (ITIL) Foundation Certificate.

13.2.1.3. Experience: At least ten (10) years of experience as an Information and Communications Technology (ICT) project manager. At least five (5) years of experience as the project manager for an effort of similar scope to the IEG-C project, preferably including the application of a formal project management methodology such as PRINCE2, supported by project references and description of role/responsibilities/activities executed.

13.3. Project Management Support

13.3.1. Project Control Analyst

13.3.1.1. Establishes and maintains project schedule and cost baseline and analyses risks and potential impacts. Prepares project highlight reports.

13.3.1.2. Education: Bachelor's degree.

13.3.1.3. Experience: At least three (3) years of experience in project scheduling, project control, or project monitoring and reporting.

13.3.2. Webmaster

13.3.2.1. Provides website construction and administration, develops connections between databases and web-based front ends. Generates technical reports and related documentation as required. Provides expertise in the development and maintenance of web sites. Provides training on the uploading of documents, creating pages, links and other web functions. Maintains access rights to pages on web. Maintains reports and statistics on utilisation of the Project Website.

13.3.2.2. Education: Associates degree or two years of technical training.

13.3.2.3. Experience: At least one (1) year of experience in website support and at least one year in website construction.

13.3.3. Contract Security Specialist

13.3.3.1. Provides support in areas directly pertinent to administration, supervision, and control of facility security in an industrial and/or government environment. Possesses a working knowledge of government and industrial security regulations.

13.3.3.2. Education: Bachelor's degree.

13.3.3.3. Experience: At least three (3) years of experience in Contract security administration.

13.4. Engineering and Technical

13.4.1. Senior Engineer

13.4.1.1. Performs complex engineering tasks and multiple tasks simultaneously. Assists with or plans major research and engineering tasks or programs of high complexity. Directs and co-ordinates all activities necessary to complete a major, complex engineering program or multiple smaller tasks or programs. Performs advanced engineering research, hardware or software development.

13.4.1.2. Education: Master's degree in engineering. ITIL Foundation and Service Transition certificates

13.4.1.3. Experience: At least seven (7) years in engineering positions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use. Member of recognised professional body.

13.4.2. Intermediate Engineer

13.4.2.1. Performs engineering tasks and additional duties as assigned. Assists higher level engineers with larger tasks. Manages or directs multiple engineering tasks, directing research and development activities as required. Performs advanced engineering applications programming and analysis for systems/equipment assigned.

13.4.2.2. Education: Bachelor's degree in engineering.

13.4.2.3. Experience: At least three (3) years of experience in engineering functions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use.

13.4.3. Junior Engineer

13.4.3.1. Performs engineering tasks under the direction of higher level engineers. Performs independent research, conducts studies and analysis, and participates in the design and development of complex systems.

13.4.3.2. Education: Bachelor's degree in engineering.

13.4.3.3. Experience: At least one (1) year of experience in engineering functions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use.

13.4.4. Senior Systems Engineer

13.4.4.1. Plans and co-ordinates engineering activities to meet SRS requirements. Provides comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance. Competent in technical disciplines as applied to government and commercial information and communications systems. Prepares trade-off studies and evaluations for vendor equipment. Recommends design changes/enhancements for improved system performance. Supervises the work of a design, integration, test, and implementation team. Analyses architectural options for performance and manageability.

13.4.4.2. Education: University Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/ diplomas. Current ITIL Foundation and Service Design certificates.

13.4.4.3. Experience: At least seven (7) years of experience in system design and integration. At least five (5) years in the design, integration, or implementation information systems, defence systems and large scale systems.

13.4.5. Intermediate Systems Engineer

13.4.5.1. Performs system engineering assignments in support of the analysis of complex system design, formulating requirements, developing alternative approaches, conduct of studies, and application of standards. May function as a member of an engineering team assigned responsibilities for specific task areas.

13.4.5.2. Education: Bachelor's degree in engineering or computer science.

13.4.5.3. Experience: At least three years of experience in system design and integration.

13.4.6. Junior Systems Engineer

13.4.6.1. Conducts research and application of system design principles for the design, development, implementation, or support as a member of assigned task staffing. Develops alternative solutions, concepts, or processes through research into assigned systems and components.

13.4.6.2. Education: Bachelor's degree in engineering or computer science.

13.4.6.3. Experience: At least one (1) year of experience in system design and integration.

13.4.7. Senior Communications Engineer

13.4.7.1. Performs communications system transition planning, engineering design for integration with processing systems, specification development, standards, interface design, testing, and the conduct of transmission and traffic studies.

13.4.7.2. Education: Master's degree in engineering.

13.4.7.3. Experience: At least seven (7) years of experience in the engineering of communications systems via all transmission media.

13.4.8. Intermediate Communications Engineer

13.4.8.1. Prepares communications systems designs and technical documentation, and other design criteria. Implements COTS and emerging communications systems and develops technical plans, documentation, and support.

13.4.8.2. Education: Bachelor's degree in engineering.

13.4.8.3. Experience: At least three (3) years of experience in the engineering of communications systems via all transmission media.

13.4.9. Junior Communications Engineer

13.4.9.1. Conducts engineering analysis, develops technical documentation, investigate communications requirements, formulates network interfaces, and assists in project/program execution.

13.4.9.2. Education: Bachelor's degree in engineering.

13.4.9.3. Experience: At least one (1) year of experience in the engineering of complex communications systems via all transmission media.

19.4.9bis Systems Integration Analyst

19.4.9bis.1 Develops and implements solutions using the optimal technology, capability, and interfaces Researches available tools and technologies to determine alternate technology solutions. Researches, implements, and supports multiple computing platforms, operating systems, processing environments, and telecommunications technologies. May conduct cost/benefit or feasibility analyses; perform capacity analyses and planning.

19.4.9bis.2 Education: Bachelor's degree in engineering or computer science.

19.4.9bis.3 Experience: At least seven (7) years of experience in the integration and implementation of information systems, defence systems, C2 systems, preferably in maritime domain.

13.4.10. Senior Software Programmer

13.4.10.1. Performs complex program development using standard and specialised languages to create special purpose software, modify existing programs, and enhance system efficiency and integrity. Translates detailed designs into software, tests, debugs, and refines software packages. Manages software development teams in modular development of complex applications. Provides technical direction to assigned programmers.

13.4.10.2. Education: Bachelor's degree in engineering or computer science.

13.4.10.3. Experience: At least seven (7) years of experience in the design, programming, and testing of applications software.

13.4.11. Intermediate Software Programmer

13.4.11.1. Analyses systems requirements and design specifications to develop block diagrams and logic flow charts. Translates detailed designs into computer software for specific applications. Prepares documentation, including program and user documentation.

13.4.11.2. Education: Bachelor's degree in engineering or computer science.

13.4.11.3. Experience: At least three (3) years of experience in the design, programming, and testing of applications software.

13.4.12. Junior Software Programmer

13.4.12.1. Performs programming tasks based upon specifications and flow diagrams. Translates concepts into program modules for testing, debugging, refinement, and integration with other modules. Prepares draft documentation including program and user documentation. Functions as a member of a software development team under the guidance of more experienced programmers.

13.4.12.2. Education: Bachelor’s degree in engineering or computer science.

13.4.12.3. Experience: At least one (1) year of experience in the design, programming, and testing of applications software.

13.4.13. System Support Engineer

13.4.13.1. Designs and integrates system support applications and protocols to meet system requirements. Analyses architectural options for performance and manageability. Analyses and designs implementations to meet specialised message formats or interfaces.

13.4.13.2. Education: Bachelor’s degree in engineering.

13.4.13.3. Experience: At least seven (7) years of experience in the design, integration, and implementation of information systems. At least three years of experience with Simple Network Management Protocol (SNMP) and system support applications.

13.4.14. Information Systems Security Engineer

13.4.14.1. Analyses and develops network systems and information security practices to include: operating systems, applications, Transmission Control Protocol (TCP)/Internet Protocol (IP), security architecture, multi-level security, intrusion detection, virus detection and control, PKI, vulnerability assessment. Documents findings and recommend changes in procedures, configuration, or design.

13.4.14.2. Education: Bachelor’s degree.

13.4.14.3. Experience: At least three (3) years of experience in information systems security. At least five years in information systems integration, implementation, or operation.

13.4.15. Information Systems Security Specialist

13.4.15.1. Provides support in implementing procedures and practices prescribed for safeguarding and control of an automated information system and the processing of classified information.

13.4.15.2. Education: Associates degree or two years of technical training.

13.4.15.3. Experience: At least two (2) years of experience as an Information Systems Security Officer for an operational system.

13.4.16. Field Engineer

13.4.16.1. Conducts site surveys, prepares implementation plans, prepares implementation procedures, supervises installation and activation, reports on installation status, manages repair and modifications to systems/equipment, performs field maintenance, and performs system configuration changes based upon approved specifications. Supervises provision of support to installed systems.

13.4.16.2. Education: Bachelor’s degree. ITIL Foundation and Service Operations certificates

13.4.16.3. Experience: At least five (5) years in the installation and support of information systems.

13.4.17. Senior Technician

13.4.17.1. Supervises technicians in the troubleshooting, repair, installation, training, integration, and upgrade of systems and equipment. Works closely with assigned engineers and systems personnel to support implementation and activation efforts.

13.4.17.2. Education: Associates degree.

13.4.17.3. Experience: At least seven (7) years of experience in the installation and maintenance of network and information systems.

13.4.18. Intermediate Technician

13.4.18.1. Performs troubleshooting, repair, refurbishment, and installation of systems and equipment. Performs factory or field testing of systems, development of maintenance or repair procedures, and supports installation teams in specific areas of expertise.

13.4.18.2. Education: Associates degree.

13.4.18.3. Experience: At least three (3) years of experience in the installation and maintenance of network and information systems.

13.4.19. Junior Technician

13.4.19.1. Performs troubleshooting, repair, and installation functions as assigned. May be assigned as technical support technician for specific systems or hardware. Performs factory or field testing and supports installation teams as assigned.

13.4.19.2. Education: Secondary school graduate with one year of technical training.

13.4.19.3. Experience: At least two (2) years of experience installing and maintaining network and information systems.

13.4.20. System Management Specialist

13.4.20.1. Analyses, develops, and maintains operational system configuration parameters. Establishes and implements system policy, procedures and standards, and ensures their conformance with system requirements. Ensures that security procedures are established and implemented. Provides technical assistance to operational, logistics, and system engineering staff.

13.4.20.2. Education: Bachelor’s degree and completion of a formal system administration or network management certification course.

13.4.20.3. Experience: At least three (3) years of experience in the administration of distributed information systems.

13.5. Testing

13.5.1. Senior Test Engineer

13.5.1.1. Directs test planning, design and tools selection. Establishes guidelines for test procedures and reports. Co-ordinates with Purchaser on test support requirements and manages Contractor test resources.

13.5.1.2. Education: Bachelor's degree in engineering.

13.5.1.3. Experience: Integration and testing engineering skills with five (5) years' experience as part of technical projects, supported by project reference and description of role / responsibilities / activities. Demonstration of practical experience in planning, conducting and assessing integration and testing activities in support of projects for at least equivalent to IEG-C for at least two (2) years, supported by project references and description of role/responsibilities/activities

13.5.2. (Deleted)

13.5.3. Intermediate Test Engineer

13.5.3.1. Designs and documents unit and application test plans. Transforms test plans into test cases and executes those cases. Supervises individual tests and prepares test reports.

13.5.3.2. Education: Bachelor's degree in engineering.

13.5.3.3. Experience: At least three (3) years of experience in the design and execution of information systems tests.

13.5.4. Junior Test Engineer

13.5.4.1. Performs testing activities under supervision of more experienced test personnel. Executes defined test cases and procedures. Collects and analyses test data; prepares test reports.

13.5.4.2. Education: Bachelor's degree in engineering.

13.5.4.3. Experience: At least one (1) year in the design and execution of information systems tests.

13.5.5. Test Technician

13.5.5.1. Provides installation and administration support to information system testing. Constructs and tests prototype equipment for electrical systems and components, consistent with engineering and other specifications. Executes tests and collects test data. Assists in preparing test reports.

13.5.5.2. Education: Associates degree or two years of technical training.

13.5.5.3. Experience: At least two (2) years of experience in the configuration and administration of information systems or test and measurement systems.

13.6. Implementation Support

13.6.1. Logistics Management Specialist

13.6.1.1. Provides support in the development of support documentation to include as a minimum, elements such as support equipment, technical orders, supply support and computer resources support, process of evolving and establishing maintenance/support concepts.

13.6.1.2. Education: Bachelor's degree.

13.6.1.3. Experience: At least seven years of experience in supply and support of information systems. At least three (3) years in support of distributed systems in more than one NATO nation.

13.6.2. Logistics Analyst

13.6.2.1. Creates and helps execute plans for the ILS of complex systems. Analyses adequacy and effectiveness of current and proposed logistics support provisions. Supervises the efforts of other logistics personnel in the execution of assigned tasks.

13.6.2.2. Education: Bachelor's degree.

13.6.2.3. Experience: At least three (3) years of experience in ILS planning and analysis.

13.6.3. Inventory Specialist

13.6.3.1. Creates and maintains an inventory control system. Tracks materials, coordinates shipping and receiving, and supervises packing operations.

13.6.3.2. Education: Associates degree.

13.6.3.3. Experience: At least three (3) years of experience in shipping, receiving, and inventory control.

13.6.4. Shipping and Receiving Clerk

13.6.4.1. Coordinates the shipping and receiving of materials. Tracks property using automated equipment. Performs and records materials inventory checks.

13.6.4.2. Education: Secondary school graduate.

13.6.4.3. Experience: At least three (3) years of experience in shipping and receiving.

13.6.5. Technical Writer

13.6.5.1. Develops, writes, and edits materials, briefs, proposals, instruction books, and related technical and administrative publications concerned with work methods and procedures for installation, operations and enhancement of equipment. Organises material and compiles writing assignments for clarity, conciseness, style, and terminology. Prepares and edits documentation incorporating information provided by

users, and technical and operations staff. Possesses a substantial knowledge of the capabilities of computer systems. Capable of writing, editing, and generating graphic presentations.

13.6.5.2. Education: Bachelor's degree.

13.6.5.3. Experience: At least three (3) years as a technical writer.

13.6.6. Senior Configuration Manager

13.6.6.1. Establishes and maintains a process for tracking the life cycle development of system design, integration, test, training, and support efforts. Maintains continuity of products while ensuring conformity to Purchaser requirements and commercial standards. Establishes configuration control forms and database.

13.6.6.2. Education: Bachelor's degree.

13.6.6.3. Experience: At least five (5) years of experience in specifying Configuration Management requirements, standards, and evaluation criteria in acquisition documents, and in performing configuration identification, control, status accounting, and audits. At least three years in computer and communication systems development, including physical and functional audits and software evaluation, testing and integration. At least two years of experience with application of Configuration Management tools.

13.6.7. Intermediate Configuration Manager

13.6.7.1. Maintains a process for tracking the life cycle development of system design, integration, test, training, and support efforts. Maintains continuity of products while ensuring conformity to Purchaser requirements and commercial standards. Maintains configuration control records and databases.

13.6.7.2. Education: Associates degree or two years of technical training.

13.6.7.3. Experience: At least three (3) years of experience in technical system Configuration Management. At least two years in communication and information systems development, including physical and functional audits and software evaluation, testing and integration.

13.6.8. Junior Configuration Manager

13.6.8.1. Prepares and coordinates change requests, configuration items, and configuration baselines. Maintains configuration control records and databases.

13.6.8.2. Education: Associates degree or one year of technical training.

13.6.8.3. Experience: At least one (1) year of experience in technical system configuration or document management.

13.6.9. Data Control Specialist

13.6.9.1. Performs assigned portions of managing the data input into complex information systems. Analyses and administers data for both the developing team and the customer. Handles daily administrative tasks, produces and edits technical reports

based on data system processing, monitors use of data and performs updates as required. Participates in all phases of system development with emphasis on the data collection, input, documentation, and acceptance phases. Designs and prepares technical reports and related documentation, and makes charts and graphs to record results.

13.6.9.2. Education: Associates degree.

13.6.9.3. Experience: At least three (3) years of experience in administration of Configuration Management or technical documentation.

13.6.10. Quality Assurance Manager (QAM)

13.6.10.1. Establishes and maintains process for evaluating software, hardware, and associated documentation. Determines the resources required for QC. Maintains the level of quality throughout the system life cycle. Develops project QA plan. Conducts formal and informal reviews at predetermined points throughout the system life cycle. Audit subcontractors, suppliers and outsource companies to ensure that appropriate standard practices are applied.

13.6.10.2. Education: Bachelor's degree.

13.6.10.3. Experience: At least seven (7) years working with QC methods and tools. At least four (4) years supporting system development and test projects.

13.6.11. Quality Assurance (QA) Specialist

13.6.11.1. Develops and implements quality standards. Reviews hardware, software, and documentation. Participates in formal and informal reviews to determine quality. Participates in the development of system QAPs. Examines and evaluates design, integration, and test processes and recommends enhancements and modifications.

13.6.11.2. Education: Bachelor's degree.

13.6.11.3. Experience: At least four (4) years of working with QC methods and tools.

13.7. Training Support

13.7.1. Instructional Systems Designer

13.7.1.1. Conducts the research, necessary to identify training needs based on performance objectives and existing skill sets; prepares training strategies and delivery methodology analyses; and prepares cost/benefit analyses for training facilities and deliverables. Develops training delivery plan, instructional guidelines, and performance standards and assessment mechanisms. Plans and directs the work of training material developers and coordinates activities with system development staff. Supervises the implementation and adaptation of training products to customer requirements.

13.7.1.2. Education: Bachelor's Degree.

13.7.1.3. Experience: At least three (3) years of experience in the design and development of training for information systems and defence systems using an Instructional Systems Design approach such as the Systems Approach to Training, Performance-Based Training, Analysis, Design, Development, Implementation, and Evaluation (ADDIE), or Criterion Referenced Instruction.

13.7.2. Senior Training Materials Developer

13.7.2.1. Conducts the research necessary to develop and revise training courses and prepares training plans. Develops instructor (course outline, background material, and training aids) and student materials (course manuals, workbooks, hand-outs, completion certificates, and course feedback forms). Trains personnel by conducting formal classroom courses, workshops, seminars, and/or computer based/computer-aided training. Provides daily supervision and direction to staff.

13.7.2.2. Education: Bachelor's Degree.

13.7.2.3. Experience: At least five (5) years in the preparation of technical training, including CBT materials.

13.7.3. Training Materials Developer

13.7.3.1. Conducts the research necessary to develop and revise training. Develops training materials (course outline, manuals, workbooks, hand-outs, completion certificates, and course feedback forms).

13.7.3.2. Education: Associates degree.

13.7.3.3. Experience: At least three (3) years of experience in the preparation of technical training materials.

13.7.4. CBT Developer

13.7.4.1. Uses CBT tool to design and implement course flowchart, text, animation, voice, and graphic displays.

13.7.4.2. Education: Bachelor's degree.

13.7.4.3. Experience: At least three (3) years of experience in the preparation of CBT courses.

13.7.5. Senior Instructor

13.7.5.1. Supervises trainers who conduct technical training classes. Conducts training classes. Works closely with Purchaser personnel to determine training and scheduling requirements. Develops and maintains training materials. Reviews and provides inputs for technical documentation.

13.7.5.2. Education: Bachelor Degree.

13.7.5.3. Experience: At least four (4) years of experience in systems administration or operation and at least four (4) years as technical training instructor in defence systems and maritime C2 systems.

13.7.6. Junior Instructor

13.7.6.1. Conducts technical training classes. Prepares and updates training documentation.

13.7.6.2. Education: Bachelor's Degree.

13.7.6.3. Experience: At least four (4) years of experience in systems administration or operation and at least two (2) years as technical training instructor.

13.8. Operational Support

13.8.1. System Administrator

13.8.1.1. Administers systems operations and configuration. Maintains user accounts and profiles. Performs system backup and restoration procedures. Troubleshoots operational problems. Coordinates system configuration and performance issues with central network support staff and Purchaser site personnel.

13.8.1.2. Education: Associates degree or two years of technical training.

13.8.1.3. Experience: At least one (1) year in systems administration of Windows Server 2012 systems. At least one (1) year in the administration and operation of an integration capability. At least one (1) year in the administration and operation of a virtualized environment.

13.8.2. Network Manager

13.8.2.1. Oversees administration and operation of network and service management applications. Develops and implements operating procedures. Administers upgrades to system support and network management components. Collects operational performance data and performs performance analysis.

13.8.2.2. Education: Associates degree.

13.8.2.3. Experience: At least two (2) years in administration and implementation of SNMP or other system support systems.

13.8.3. Database Administrator

13.8.3.1. Manages network-wide configuration databases. Develops and implements data synchronisation procedures and resolves database discrepancies. Maintains and publishes network configuration tables and indices. Designs and implements queries and other utilities. Ensures that Back-ups are scheduled and that the directory / database is restorable from them. Ensuring BC and DR preparedness is maintained.

13.8.3.2. Education: Associates degree.

13.8.3.3. Experience: At least two (2) years in database administration.

13.8.4. Operational Support Manager

13.8.4.1. Organises, directs and manages operational support activities. Analyses system performance data and prepares reports and assessments. Meets with Purchaser

personnel to coordinate support issues and coordinates with system deployment personnel on activation and cut-over. Ensures conformance with all requirements.

13.8.4.2. Education: Bachelor's degree.

13.8.4.3. Experience: At least five (5) years of experience in the administration and operation of a distributed information system.

SECTION 14: INTERFACES WITH OTHER PROJECTS / SYSTEMS

14.1. NS Domain (ITM)

14.1.1. The ITM project, which is the amalgamation of the three CP 9C0150 Projects: 0IS03091; 0IS03092, and 0IS03101, will transform the way IT services are provided to Users across the NATO enterprise, including the NATO Command Structure (NCS), the NATO Headquarters (NHQ) and NATO agencies.

14.1.2. The project will provide modern effective and cost-efficient Infrastructure as a Service (IaaS) supporting IT services at NS level on the ON domain. The project is, in effect, a hardware replacement and service consolidation project as it will maintain the existing NS AIS domain (or future ON – Operational Network at NS classification) at NATO military command structure HQs.

14.1.3. The architecture is based on various different types of implementation: Data Centres, Enhanced Nodes, and Standard Nodes. As for the Client Connectivity, ITM will support Thick Clients (Desktop/Laptop) and Thin Clients (Virtual Desktop Infrastructure).

14.2. MS Domain (x-FOR)

14.2.1. NATO implements 'mission' Secret domains in current operations and exercises in order to provide CIS access to non-NATO mission partners. Examples are the KFOR Secret domain supporting NATO-led operations in Kosovo, the EUFOR Secret domain supporting operations in Bosnia & Herzegovina and the Resolute Support domain supporting operations in Afghanistan. 'Mission' Secret domains are also established to support Exercises and are a central feature of NATO's 'Future Mission Network' concept.

14.3. Management Domain

14.3.1. The IEG-C system components will need to be managed from the Management domain already existing in Purchaser operations in addition to the Management tools which the Contractor will add. These components will include Servers, Switches, Firewalls Toolsets and any other appliance needed for the final IEG-C capability. The Management Consoles/Equipment that will host these toolsets will be provided as PFE to this contract.

[SOW-889] *The Contractor SHALL assist the Purchaser to configure existing Management Suites in Purchaser's toolset to integrate and manage IEG-C components, in consistence with the IEG-C system design and management.*

14.4. NCIA Cyber Monitoring Capability (former NCIRC)

14.4.1. The NATO Cyber Security Monitoring Capability involves capturing network traffic at key points in the global CIS infrastructure, and the collection of system logs, which can then be used to support cyber security incident analyses. In order to monitor the IEG-C and the traffic it mediates, probes will capture network packets at appropriate network interfaces connecting to the IEG-C, or within the IEG-C by software system agents installed at the components comprising the IEG-C. This traffic capture is transparent to the IEG-C.

14.4.2. The Contractor will assist the Purchaser or any other sub-contracted entity by the Purchaser to enact necessary changes and additions to the IEG-C Contractor's design and system, so that the aforementioned monitoring capability will integrate the IEG-C system like all other CIS equipment and systems operated by the Purchaser.

[SOW-890] *The Contractor SHALL assist the Purchaser to integrate the IEG-C system in the Purchaser's NATO Cyber Security Monitoring Capability.*

14.5. Mission Information Room

14.5.1. The 'Mission Information Room' (MIR) at SHAPE and JFC Naples allows HQ Staff access to a local extension of a 'mission' network and to the 'at risk' NATO Secret domain established for operations and exercise support. The MIR places this NATO Secret domain in the IEG-C DMZ.

SECTION 15: DELIVERABLES OUTLINES

15.1. General

15.1.1. This section describes the outline content of a subset of all deliverables (management products and specialist products) to be provided by the Contractor under this Contract.

15.2. Risk Log

[SOW-891] *The Contractor SHALL provide the Risk Log listing the risks, and indicating for each one the following information (but not limited to):*

- *Risk identifier: unique code to allow grouping of all information on this risk;*
- *Description: brief description of the risk;*
- *Risk category (e.g., management, technical, schedule, and cost risks);*
- *Impact: effect on the project if this risk were to occur;*
- *Probability: estimate of the likelihood of the risk occurring;*
- *Risk rating (High, Medium, Low);*
- *Proximity: how close in time is the risk likely to occur;*
- *Response strategy: avoidance, mitigation, acceptance, transference*
- *Response plan(s): what actions have been taken/will be taken to counter this risk;*
- *Owner: who has been appointed to keep an eye on this risk;*
- *Author: who submitted the risk;*
- *Date identified: when was the risk first identified;*
- *Date of last update: when was the status of this risk last checked;*
- *Status: e.g., closed, reducing, increasing, no change.*

15.3. Issue Log

[SOW-892] *The Contractor SHALL ensure that the Issue Log comprises the following information (but not limited to):*

- *Project Issue Number;*
- *Project Issue Type (ECP, Off-specification, general issue such as a question or a statement of concern);*
- *Author;*
- *Date identified;*
- *Date of last update;*
- *Description;*
- *Action item;*

- *Responsible person. (Individual in charge of the action item);*
- *Suspense date (Suspense date for the action item);*
- *Priority;*
- *Status.*

15.4. Project Status Report (PSR)

[SOW-893] *The Contractor SHALL ensure that the PSR summarises activities and progress, including (but not limited to):*

- *Changes in key Contractor personnel;*
- *Summary of Contract activities during the preceding month, including the status of current and pending activities;*
- *Progress of work and schedule status, highlighting any changes since the preceding report;*
- *EVM KPIs, including Planned Value, Earned Value, Actual Cost, Schedule Variance, Schedule Performance Index, Budget at Completion and Estimate at Completion.*
- *CSA report addressing all products in the Project Breakdown Structure;*
- *Issue Log;*
- *Change Requests status;*
- *Off-Specifications status;*
- *Risk Log;*
- *Test(s) conducted and results;*
- *Summary of any site surveys conducted;*
- *Plans for activities during the following reporting period;*
- *Provisional financial status and predicted expenditures.*

15.5. Change Request

[SOW-894] *The Contractor SHALL ensure that any Change Request will respect the requirements in SOW 12.7 Requests for Change (RFC).*

15.5.1. Change Request Document

[SOW-895] *The Contractor SHALL ensure that CR documentation includes:*

- *The list of all Change Requests processed since the start of the project, in a tabular form, indicating for each of them the date it was created and the current status;*
- *All Change Requests processed since the start of the project.*

15.6. System Design Specification (SDS)

[SOW-896] *The Contractor SHALL include, at a minimum, the following information in the SDS document:*

- *System Architecture*
- *The following Operational and Systems Views, as defined in the NATO Architecture Framework (NAF, [NAC AC/322-D(2007)0048, 2007]):*
- *NOV-1, High-Level Operational Concept Diagram;*
- *NSV-1 Systems Interface Description (Composition);*
- *NSV-1 System Interface Description (Intra System);*
- *NSV-1 System Interface Description (Inter System);*
- *NSV-2a: System Port Specification;*
- *NSV-4 System Functionality;*

[SOW-897] *The (minimum) information in the NAF views the Contractor SHALL supply is defined in Table 26 below.*

[SOW-898] *The NAF views SHALL be produced using applications compliant with NAF 4 and Archimate 3. If not, the Contractor SHALL ensure the exchange format SHALL be approved by the Purchaser upfront.*

[SOW-899] *Physical layout and operation principles of the IEG-C in the deployment sites (including the site of the IEG-C Reference System): identification of where the components will be installed, of how users (NATO Staff Users) will make use of the provided functionality, of how support staff (IEG-C Administrators will operate the system. This SHALL cover in particular how the IEG-C components SHALL integrate into the storage and backup solutions existing at the implementation sites.*

- *Results of the network simulation, showing the integration with the underlying network infrastructure, the mitigation of potential impact of the available bandwidth and of any latency;*
- *Replication, synchronisation and browsing protocols and flows;*
- *Proposed topology for the system;*
- *Routing, Transport, and connectivity to IEG-C components;*
- *Administration model design (Administrative groups and permissions, administrative roles, trust relationships between separate domains).*
- *Schema*
- *Attributes to which the NATO Staff Users have read-access.*
- *System Functionalities.*
- *Functional breakdown of the IEG-C system.*
- *Application Programming Interfaces (API) and libraries.*
- *System internal interfaces: Description of the interworking of all components to meet the system requirements (e.g., physical interfaces between components, data flows.)*

- *Performance Requirements: Performance requirements are defined in the SRS.*
- *Equipment*
- *Physical breakdown of the operational IEG-C system, of the Reference Test Bed, into hardware/software CIs (including the number of licenses for each software CI), with traceability to the functional breakdown.*
- *Identification of all COTS included in the system.*
- *CSA reports addressing all system CIs.*
- *All configuration information (parameters, settings, etc.) for all of the IEG-C components.*
- *Security*
- *Description of how the system complies with all security requirements.*

NAF view (subview)	Purpose	NAF objects to be used	NAF relationships to be used
NSV-1 (composition)	To show the different components of the envisaged IEG-C system	System	ResourceComposition (System->System)
NSV-1 (intra-system)	To identify the interactions between the different components of the IEG-C system. For each interaction applicable standards/formats/protocols need to be identified	System, DataElement, Standard/Protocol	ResourceInteraction (System->System), ConveyedElement (ResourceInteraction->DataElement) ConformsTo (ResourceInteraction->Standard/Protocol)
NSV-1 (inter-system)	To identify the interaction of the IEG-C system with other systems. This also incl. dependencies on hosting platforms. For each interaction applicable standards/formats/protocols need to be identified	System, DataElement, Standard/Protocol	ResourceInteraction (System->System), ConveyedElement (ResourceInteraction->DataElement) ConformsTo (ResourceInteraction->Standard/Protocol) ConformsTo (DataElement ->Standard/Protocol)
NSV-1 (deployment)	To show the deployment of components to locations (site-level). Note: this is a NAF extension	System, Location	RequiredLocation (System->Location)
NSV-2a (System port description) aka Interface Specification	To identify and specify each internal (i.e., between system components) and external (i.e., between IEG-C and other systems) interface.	System, System Port (aka interface), Protocol	Association (System->SystemPort), ImplementsProtocol (SystemPort->Protocol)
NSV-4 (system functionality)	To identify the functionality that each component provides. Each functional requirement must be traceable to a system function	System, SystemFunction, Requirement	FunctionProvision (System->SystemFunction), Satisfy (SystemFunction->Requirement)

Table 26: NAF Information Requirements

15.7. System Version Definition Document (SVDD)

[SOW-900] *The SVDD SHALL include the following:*

- *List of differences between this and the previous System version;*
- *List of capabilities of this System version;*
- *Guidelines on how to install this System version;*
- *Breakdown of the system into CIs and provision of accurate identification information for every CI.*

15.8. System Implementation Plan (SIP)

[SOW-901] *The Contractor SHALL submit to the Purchaser the SIP with the following information:*

- *The Contractor's approach to all system implementation tasks (including the sequence of activation of the sites to be implemented);*
- *The Contractor organisation and key personnel involved in system implementation;*
- *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;*
- *The schedule of all planned outages of any kind in the sites;*

[SOW-902] *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-903] *The installation plan, which SHALL specifically address:*

- *A general installation plan showing how the gradual installation and activation of the IEG-C will be carried out by the Contractor;*
- *The installation procedures, showing that those procedures will cause no or minimal disruption to the sites and to the User desktop applications;*
- *A site-specific design for each site;*
- *A detailed installation plan for each site;*
- *Site and system installation checklist;*
- *Site activation checklist;*
- *An Allocation Matrix showing the allocation of each system CIs (nature and quantities) to each site, and the number of users and support staff for each site;*
- *Any specific tools the Contractor intends to furnish and use during the site installation.*

[SOW-904] *The activation plan, which SHALL specifically address:*

- *The site activation activities;*

- *Any post-activation tasks;*
- *The "back-out" procedures. The back-out section to the SIP SHALL enable deactivation and/or removal of all installed IEG-C components and restoration of existing services without disruption of those services.*
- *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.*
- *The migration plan from existing gateways to IEG-C:*

[SOW-905] *The migration plan SHALL detail the migration activities. Schedule. Engineering activities for the migration of the existing gateways to IEG-C.*

[SOW-906] *The Contractor SHALL structure the SIP so that general implementation information is maintained in the body of the plan and site-specific details are kept as annexes.*

15.9. Project Management Plan (PMP)

[SOW-907] *The Contractor SHALL ensure that the PMP comprises at minimum of the following sections:*

- *An 'Organisation' section describing the Contractor's organisation for this project according to the requirements. This section SHALL include an organisational chart showing the members of the Contractor's Project Team (including the members of the Contractor PMO) and showing their respective responsibilities and authority. This section should also include proposed Project Communication Plan.*
- *A 'Project Planning' section describing the Contractor's processes supporting the development and maintenance of the PBS, PFD and PMS according to the requirements.*
- *A 'Risk management' section describing the Contractor's processes supporting Risk Management by the Contractor.*
- *A 'System Engineering' section describing the Contractor approach to these activities according to the requirements in SECTION 10.*
- *A 'System Implementation' section describing the Contractor approach to these activities according to the requirements in SECTION 13.*
- *An 'Operation and Maintenance' section describing the Contractor approach to these activities according to the requirements in SECTION 12.*
- *An "Operation and Maintenance" section describing the Contractor approach to these activities according to the requirements in Annex F: Annex F Maintenance and Support Concept (After FSA);*
- *A 'Testing' section describing the Contractor approach to these activities according to the requirements in SECTION 14.*

- *An "Earned Value Management Section" describing how the Contractor will assure EVM tracking and reporting.*

15.10. User and Maintenance Manuals

[SOW-908] *The Contractor SHALL develop all Technical Manuals compliant with the requirements in SOW 11.6.*

15.11. IEG-C Procedures and Work Instructions

[SOW-909] *The Contractor SHALL develop Standard Operating Procedures which detail the supporting processes described in ANNEX F.*

SECTION 16: OPTIONS

16.1. General

16.1.1. This section describes the options to be provided by the Contractor under this Contract, if these options are to be exercised by the Purchaser.

16.1.2. The optional gateways and respective locations are described in Annex B of this SOW.

16.1.3. WP 6 and WP 7 (paragraphs 16.2 and 16.3 respectively) are not optional and are included in the main scope of the project.

16.2. WP 6 Hardware

16.2.1. All required equipment will be identified and selected by the bidders to conform to SRS. The main reason is to achieve homogeneity in the Purchaser's installed hardware base.

16.2.2. This equipment in general involves Infrastructure hardware (processing, storage, networking), firewall and guard products. Lists will be finalized in the design phase, before the conclusion of the PDR at EDC+3[11].

16.2.3. The Contractor will include the costs of WP6 in the main Schedule of Supplies and Services.

[SOW-910] *The Contractor SHALL procure all hardware required for the completion of this project, as agreed during the PDR (EDC+3MO).*

16.3. WP 7 Cyber Security Monitoring (former NCIRC)

16.3.1. As described in paragraph 14.4 in this SOW, the IEG-C infrastructure will need to accommodate and integrate to NCIA's Cyber Security Monitoring capability systems and services. This integration will be performed by the Contractor or another sub-contracted entity.

16.3.2. The IEG-C contractor will be required to provide a costed, evaluated, delivery of the aforementioned activities and integration.

16.3.3. This integration will conform to the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017] and will comprise of the following activities:

16.3.3.1. Site Survey

16.3.3.2. Incorporation in IEG-C design

[11] PDR is not expected to change drastically the design submitted by the Contractor at Contract Award and so is not expected to have a cost impact to hardware acquisition.

16.3.3.3. Installation

16.3.3.4. Integration and testing Mandatory Sites and Management Suite

16.3.3.5. Integration and testing Optional Sites

16.3.3.6. Initial Operational Support

16.3.4. The aforementioned activities are described in detail in Annex H and they will be concluded in parallel with the other relevant project activities

[SOW-911] *The Contractor SHALL perform the activities of this Work Package. In particular:*

- *Surveys SHALL occur together with the main Site Surveys,*
- *incorporation in the IEG-C design SHALL occur before the PDR (EDC+3MO)*
- *Installation SHALL occur together the IEG-C equipment installations at various points in the project schedule (between the FAT at EDC+9MO and FSA at EDC+27MO).*
- *Integration and testing SHALL occur together with the other integration and testing activities as described in SECTION 7 : System Implementation and SECTION 8 : Test, Verification, Validation (TVV).*

16.4. WP 11 Hardware additional gateways

16.4.1. The same terms of paragraph 16.2 above will apply for the additional gateways referred to in paragraph 1.3.2 in this SOW.

16.5. WP 12 Additional gateways

16.5.1. This work package will contain all effort for the implementation of additional gateways referred to in paragraph 1.3.2 in this SOW. In general, all conditions in this SOW will also apply as for the mandatory gateways. The beginning date and duration of activities for this WP will be agreed together with the Purchaser and may be concurrent to WP3.

ANNEX A System Requirements Specification (SRS)

The SRS is a separate document that will be attached as Annex A

ANNEX B Implementation Scope

B.1. List of sites

Site ID	Geographic Location	Name of the Site	IEG-C ID	Operational use/network	Remarks
Mandatory Sites					
1	Mons, Belgium	SHAPE	IEG-C-01	Reference System & Management Facility	
			IEG-C-02	NATO Response Force (NRF)	
			IEG-C-03	Very high-readiness Joint Task Force (VJTF)	
			IEG-C-04	Exercise 1	
2	Stavanger, Norway	JWC	IEG-C-05	Exercise 2	
			IEG-C-06	Exercise 3	
3	Strasbourg, France	EUROCORPS	IEG-C-07	EUROCORPS	
4	Innsworth, UK	Allied Rapid Response Corps (ARRC)	IEG-C-08	ARRC	
5	Lago Patria, Italy	Joint Force Command (JFC), Naples	IEG-C-09	Active Endeavour	
			IEG-C-10	NRF Standby	
6	Bydgoszcz, Poland	Joint Force Training Centre (JFTC)	IEG-C-11	Exercise 4	
Optional Sites					
7	The Hague and/or NCIA Software Factory	NCIA Testbed	IEG-C-12	Integration Network Environment	
8	HQ Kabul, AFG		IEG-C-13	Resolute Support (option)	
9	Pristina, KSV	KFOR (option)	IEG-C-14	KFOR (option)	
10	Sarajevo, BiH	EUFOR (option)	IEG-C-15	EUFOR (option)	
-	Lago Patria, Italy	Joint Force Command (JFC), Naples	IEG-C-16	Ocean Shield (option)	
			IEG-C-17	Resolute Support (option)	
11	NATO flag ship	NATO flag ship	IEG-C-18	Afloat Command Platform (option)	

Table Annex B-16: Site Type and Location

B.2. Work Package Scope

B.2.1. Generalities

The purpose of this part of Annex B to the Statement of Work (SOW) is to describe the scope of work in terms of Contract Work Packages. This SOW is part of capability development activities under Project Serial 0IS03102 of Capability Package 9C0150 and for reference purposes it will follow the WP numbering of those activities. The sections below will give the relationships between these activities, their authorizations and the internal dependencies.

The list of Work Packages authorised under 0IS03102 is listed in Table Annex B-16. WP 1, 5 and 8-10 are not part of this SOW.

Number	Work Package
WP 2.1	Achieve FAT
WP 2.2	Installation of the Reference System
WP 2.3	Integration into NATO Enterprise
WP 3	Installation of Mandatory Gateways
WP 4	Decommissioning Legacy Gateways
WP 6	Hardware Purchase
WP 7	Cyber Security Monitoring Capability (former NCIRC)
WP 11	Hardware Purchase Optional Gateways (PFE)
WP 12	Installation of Optional Gateways

Table Annex B-16: List of Work Packages

Each Work Package defined in this document has the following structure:

- General
- Work Package Dates
- Work Package Activities
- Milestones (indicated as Months after Contract – MAC)

Work Packages 2.2 and 3 will have in addition options that will be defined

B.2.2. Work Package 2

B.2.2.1. General

Work Package 2 has been split in three subpackages and those include the

a. WP 2.1 Initial desing and build of the first gateway on the Contractor's testbed to reach satisfactory Factory Acceptance Test (FAT at EDC+9MO)
b. WP 2.2 Provision of a Reference System to NCIA
c. WP 2.3 Integration in NATO Enterprise and Provision of a Central Management Solution

B.2.2.2. **Work Package Dates**

a. Work Package 2 will start at EDC.
b. Work Package 2 will end at EDC + 13 months

B.2.2.3. **Work Package Activities**

The contractor shall perform the following reviews:

a. System Requirements Review
b. Preliminary Design Review
c. Critical Design Review

The contractor shall have reached FAT by the end of this Work Package and the Acceptance of the IEG-C Security Accreditation Package shall be achieved.

B.2.2.4. **Milestones**

Milestone Description	MAC	Remark
System Requirements Review	2	
Preliminary Design Review	3	
Critical Design Review	6	
Factory Acceptance Test	9	
System Integration Testing	~~13~~17	
Acceptance IEG-C Accreditation Package	~~13~~20	

B.2.3. **Work Package 3**

B.2.3.1. **General**

Work Package 3 includes the installation of gateways at the authorised sites including Initial Support up to FSA

B.2.3.2. **Work Package Dates**

a. Work Package 3 will start at EDC + 13 months
b. Work Package 3 will end at EDC + 27 months

B.2.3.3. **Work Package Activities**

The contractor shall prepare, execute and monitor

a. The deployment Authorization
b. The Provisional System Acceptance
c. The Site(s) Acceptance Testing
d. The Operational Test and Evaluation

B.2.3.4. **Milestones**

Milestone Description	MAC	Remark
Deployment Authorization	~~17~~20	
Provisional System Acceptance	20	
Site(s) Acceptance Accreditation	25	
Site(s) Acceptance Testing	25	
Operational Test and Evaluation	26	
FSA	27	

B.2.4. **Work Package 4**

B.2.4.1. **General**

Work Package 4 provides the additional decommissioning of legacy gateways on 3 sites that will not receive new ones from this project:

a. NDOG in SHAPE
b. F5 in Eggermond
c. F5 in Castlegate

B.2.4.2. **Work Package Dates**

a. Work Package 4 may start as soon as the first site has been accepted and the Purchaser has provided authorization
b. Work Package 4 will end after WP3

B.2.4.3. **Work Package Activities**

The contractor shall prepare, execute and monitor

a. The dismantling of the gateways at the sites mentioned in Par B.2.4.1 and this according to the policies and directives of the Purchaser.

B.2.4.4. **Milestones**

No specific milestones are defined, but WP4 will be concluded up to 4 months after FSA.

Annex C Purchaser Furnished Equipment (PFE) and services

C.1. Hardware

The contractor will determine what equipment will be required to conform to SRS and in general to fulfil the goal of this project. The customer has provided in Appendix D “Purchaser Furnished Equipment Detailed Specifications” of the SRS, equipment lists that the contractor shall use as a starting point to choose hardware for the IEG-C system.

The aforementioned equipment lists in general include End User equipment, Servers, Storage, Firewalls, Guards, Racks and Switches .

Lists will be finalized in the design phase before PDR+3.

C.2. Virtualized Environment

In regard to the optional NCIA Test Bed system requested in Annex B1 above, it is the customer’s intention to utilize a Virtualized Software Development environment based on Azure. When and if this option is exercised, this platform will be provided to the Contractor as PFE. This Test Bed will be used to provide IEG-C services to other developing projects of the customer and it will be at the NATO Unclassified level.

If it is not possible to use such an environment to host an IEG-C, the contractor will notify the customer before the PDR (EDC+3MO) and an alternative solution will be commonly sought.

The Contractor can however request to create a development environment for their own use during the development phase, instead of creating and using their own environment in their premises, so as to facilitate transition to test. This service however is not part of this contract and if requested will be mutually agreed during pre-contract discussions.

C.3. Software Licenses

The purchaser's Enterprise License Agreement (ELA) shall be used by the contractor for the following products:

- All Microsoft products, including OS Server, Workstations, SCOM, RDP etc.
- McAfee
- VMWare
- Adobe
- Oracle

C.4. REACH Laptop(s)

The Purchaser will provide to the Contractor NR classified laptop(s), otherwise called REACH, in order to facilitate classified at the NATO Restricted level communication, coordination between the teams, raising ITSM tickets and maintenance of the Puchaser’s project portal as defined in 4.6.3.

Details for the delivery of these laptop(s) (including licenses and user credentials) will be agreed right after EDC so that they are active before the first PRM (at EDC+5w).

Annex D Acronyms

Acronym	Description
A	
ABL	Allocated Baseline
ACMP	Allied Communication Management Plan
ACO	Allied Command Operations
ACP	Allied Communication Publication
ACT	Allied Command Transformation
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
ADDS	Active Directory Domain Services
AFPL	Approved Fielded Products List
AIA	Authority Information Access
AIFS	Allied Information Flow System
AIG	Address Indicator Group
AIMS	AIFS Integrated Message System
AirC2IS	Air Functional Services
AIS	Automated Information System
AL	Address List
AMSG	Allied Military Security Guideline
AOM	Alliance Operations and Missions
API	Application Programming Interface
ARH	Allied Replication Hub
ARO	Authorised Release Officer
ASM	Abbreviated Service Message
ATO	Approval to Operate
AV	Anti-Virus
AVC	Advanced Video Coding
B	
Bi-SC	Bi-Strategic Commands
BLAT	Baseline Acceptance Test
BMD	Ballistic Missile Defense
BPD	Boundary Protection Device
BPS	Boundary Protection Service
C	
C2	Command and Control
C3	Consultation, Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAB	Change Advisory Board
CAD	Collective Address Directory

Acronym	Description
CAW	Contract Award
CBT	Computer Based Training
CC	Common Criteria
CCB	Configuration Control Board
CCEB	Combined Communications Electronics Board
CD-ROM	Compact Disc Read Only Memory
CDP	CRL Distribution Point
CDR	Critical Design Review
CES	Core Enterprise Services
CFI	Connected Forces Initiative
CIS	Communication and Information Systems
CI	Configuration Item
CIP	Content Inspection Policy
CIPE	Content Inspection Policy Enforcement
CLI	Command Line Interface
CLIN	Contract Line Item Number
CMP	Configuration Management Plan
CMS	Configuration Management System
CMS	Cryptographic Message Syntax
CN	Common Name
CoC	Certificate of Conformity
COI	Community of Interest
COMCEN	Communication Centre
CONOPS	Concept of Operations
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
CP	Capability Package
CPU	Central Processing Unit
CQAR	Contractor Quality Assurance Representative
CRL	Certificate Revocation List
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
CSR	Certificate Signing Request
CSV	Comma-Separated Values
D	
DA	Deployment Authorization
DAP	Directory Access Protocol
DBMS	Database Management System
DC	Domain Controller
DCIS	Deployable Communication Information Services

Acronym	Description
DDoS	Distributed Denial of Service
DI	Developmental Items
DIF	Difficulty, Importance and Frequency
DIT	Directory Information Tree
DL	Distribution List
DMZ	De-Militarized Zone
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Service
DS	Directory Service
DSA	Directory Service Agent
DVD	Digital Versatile Disc
E	
EAL	Evaluation Assurance Level
EAPC	Euro-Atlantic Partnership Council
ECP	Engineering Change Proposal
EDC	Effective Date of Contract
EE	End Entity
EMS	Enterprise Management System
E-NPKI	Enterprise NATO Public Key Infrastructure
EOC	Essential Operational Capabilities
EPO	e-Policy Orchestrator
ERM	Event Review Meeting
ESS	Enhanced Security Services for S/MIME
ETP	Event Test Plan
EVM	Earned Value Management
F	
FAQ	Frequently Asked Question
FBL	Functional Baseline
FCA	Functional Configuration Audit
FFT	Friendly Force Tracking
FOC	Final Operational Capability
FQDN	Fully Qualified Domain Name
FSA	Final System Acceptance
FT	Factory Testing
FTE	Full Time Equivalent
FTP	File Transfer Protocol
G	
GbE	Gigabit Ethernet
GIF	Graphics Interchange Format

Acronym	Description
GIS	Geographic Information Systems
GFE	Government Furnished Equipment
GMT	Greenwich Mean Time
GA	Gateway Administrator
GO	Gateway Operator
GSSAPI	Generic Security Services Application Program Interface
GQAR	Government Quality Assurance Representative
GUI	Graphics Unit Interface
H	
HIDS	Host-based Intrusion Detection System
HL	High Low
HQ	Headquarters
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
I	
IAM	Identity and Access Management
ICD	Interface Control Document
ICT	Information and Communications Technology
IdM	Identity Management
IE	Internet Explorer
IEC	International Electrotechnical Commission
IEG	Information Exchange Gateway
IEG-C	Information Exchange Gateway – Scenario C
IEG-FS	Information Exchange Gateway Functional Services
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
IFB	Invitation for Bid
IFP	Information Flow Control Policy
IIS	Internet Information Services
ILS	Integrated Logistics Support
ILSP	Integrated Logistics Support Plan
INTEL	Intelligence
INTEL FS	Intelligence Functional Service
IOR	Interoperability Requirements
IOS	Initial Operational Support
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPMT	Integrated Project Management Team
IRC	Internal Release Candidate
ISA	Interim Security Accreditation

Acronym	Description
ISAF	International Security Assistance Force
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITM	IT Modernization
ITSM	IT Service Management
ITU-T	International Telecommunication Union
IV&V	Independent Verification and Validation
J	
JC2IS	Joint C2 Functional Services
JCOP	Joint Operational Picture
JFC	Joint Force Command
JFTC	Joint Force Training Centre
JPEG	Joint Photographic Experts Group
K	
KVM	Keyboard Video Mouse
JWC	Joint Warfare Centre
KPI	Key Performance Indicator
L	
LAC	Logical Access Control
LACS	Logical Access Control System
LAN	Local Area Network
LC2IS	Land Functional Services
LDAP	Lightweight Directory Access Protocol
LH	Low High
LOG FS	Logistics Functional Services
LOGA	Log Aggregator
LORA	Level of Repair Analysis
LSA	Logistics Support Analysis
M	
MARCOM	Allied Maritime Command
MaxTTR	Maximum Time To Repair
MCCIS	Maritime Functional Services
MCF	Main Computing Facilities
MDS	Material Datasheet
MDT	Mean Down Time
MG	Mail Guard
MHTML	MIME Encapsulated HTML
MIL-STD	Military Standard
MIME	Multi-Purpose Internet Mail Extensions

Acronym	Description
MM	Military Message
MMHS	Military Message Handling System
MN	Mission Network
MOD	Ministry of Defence
MPEG	Moving Picture Experts Group
MPIF	Metadata Policy Information File
MS	Mission Secret
MSO	Message Service Operator
MTBCF	Mean Time Between Critical Failures
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenance
MTP	Master Test Plan
MTTD	Mean Time To Diagnose
MTTR	Mean Time To Repair
MTTRSy	Mean Time to Restore (the System)
N	
NAF	NATO Architecture Framework
NAP	Network Access Protection
NAR	NATO Architecture Repository
NASIS	NATO Subject Indicator System
NAS	Network Attached Storage
NATO	North Atlantic Treaty Organisation
NCC	NCI Agency Control Centre
NCCIS	NATO Command, Control and Information System
NCIA	NATO Communication & Information Agency
NCIRC	NATO Computer Response Capability
NCIS	NATO Communications and Information Systems School
NCMS	NATO Core Metadata Specification
NCOP	NATO Common Operational Picture
NCI	NATO Communications Infrastructure
NCS	NATO Command Structure
NCSC	NATO Cyber Security Centre
NDI	Non-Developmental Items
NEDS	NATO Enterprise Directory Service
NEID	NATO Enterprise ID
NFR	Non-Functional Requirements
NGCS	NATO General Purposes Segment Communications System
NGO	Non-Governmental Organisation
NIAP	National Information Assurance Partnership
NIC	Network Interface Controller

Acronym	Description
NICE	(military-grade) NATO IP cryptographic equipment
NISP	NATO Interoperability Standards and Profiles
NNCS	NATO Network Control System
NNEC	NATO Network Enabled Capability
NNHQ	New NATO Headquarter
NOS	NATO Office of Security
NOV	NATO Operational View (ref. NAF V3)
NPKI	NATO Public Key Infrastructure
NQAR	National Quality Assurance Representative
NR	NATO RESTRICTED
NS	NATO SECRET
NU	NATO UNCLASSIFIED
NSA	National Security Authority
NSAB	NATO CIS Security Accreditation Board
NSON	NATO SECRET Operational Network
NSV	NATO System View (ref. NAF V3)
NSWAN	NATO SECRET WAN
NTP	Network Time Protocol
O	
O	Organization
O/R	Originator / Recipient
O&M	Operation and Maintenance
OAC	Operational Acceptance Criteria
OASIS	Organization for the Advancement of Structured Information Standards
OBL	Operational Baseline
OCSP	On-line Certificate Status Protocol
OCF	Online Computer Forensics
OEM	Original Equipment Manufacturer
OID	Object Identifier
OLA	Organizational Level Agreement
ON	Operational Network
OSA	Operational System Acceptance
OSATP	Operational System Acceptance Test Plan
OSS	Open-Source Software
ON	Operational Network
ORs	Off-specification Reports
OS	Operating System
OSP	Organizational Security Policies
OU	Organizational Unit
OVA	Online Vulnerability Assessment

Acronym	Description
P	
PAC	Physical Access Control
PACS	Physical Access Control System
PBL	Product Baseline
PBN	Protected Business Network
PBNE	Protected Business Network Environment
PBS	Product Breakdown Structure
PCA	Physical Configuration Audit
PDF	Portable Document Format
PDM	Product Delivery Meeting
PDR	Provisional Design Review
PFD	Product Flow Diagram
PFE	Purchaser Furnished Equipment
PfP	Partnership for Peace
PHST	Packaging, Handling, Storage, Transportation
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PLAD	Plain Language Address
PMIC	Programme Management and Integration Capability
PMO	Project Management Office
PMP	Project Management Plan
PMP	Project Management Professional (PMI Certification)
PMS	Project Master Schedule
PNG	Portable Network Graphics
POC	Point of Contact
PP	Protection Profile
PR	Pilot Release
PRM	Project Review Meeting
PSA	Provisional System Acceptance
PSC	Personnel Security Clearance
PSR	Project Status Report
PTP	Project Test Plan
PTS	Project Test Strategy
Q	
QA	Quality Assurance
QAM	Quality Assurance Manager
QAP	Quality Assurance Plan
QAR	Quality Assurance Representative
QOS	Quality of Service

Acronym	Description
R	
RA	Registration Authority
RACI	Responsible, Accountable, Consulted and Informed
RAM	Reliability, Availability, and Maintainability
RCCMD	Remote Console Command
RDP	Remote Desktop Protocol
RFC	Request for Change
RFC	Request for Comment
RFD	Request for Deviation
RFQ	Request For Quote
RFW	Request for Waiver
RI	Routing Indicator
RMP	Risk Management Plan
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RS	Resolute Support
RS	Release Server
RSA	Rivest, Shamir, and Adelman
RTF	Rich Text Format
RTM	Requirements Traceability Matrix
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTT	Round Trip Time
S	
S/MIME	Secure / Multi-Purpose Internet Mail Extensions
SA	IEG-C System Administrator
SAA	Security Accreditation Authority
SAN	Storage Area Network
SAP	Security Accreditation Plan
SAP	Site Activation Plan
SAT	Site Acceptance Testing
SBR	System Baseline Review
SBT	Service-based Testing
SCCM	System Centre Configuration Manager
SCOM	System Centre Operations Manager
SDS	System Design Specification
SDR	System Design Review
SecOPs	Security Operating Procedures
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement

Acronym	Description
SHAPE	Supreme Headquarters Allied Powers Europe
SI	Signal Instructions
SIC	Subject Indicator Code
SIP	System Implementation Plan
SIP	Service Interface Profile
SISRS	System Interconnection Security Requirements Statement
SIT	System Integration Test
SIVP	System Implementation Verification Procedures
SLA	Service Level Agreement
SLP	Standardised Language Proficiency
SMA	Signal Message Address
SMC	Service Management and Control
SME	Subject Matter Expert
SMP	System Management Plan
SMS	System Management Server
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service Operation Centre
SOM	System Operation Manual
SOW	Statement of Work
SPIF	Security Policy Information File
SQL	Structured Query Language
SRA	Security Risk Assessment
SRR	System Requirements Review
SRS	System Requirements Specification
SSCS	Site Security Compliance Statement
SSH	Secure SHell
SSL	Secure Sockets Layer
SSRS	System Security Requirements Statement
SSS	Schedule of Supplies and Services
SSWB	Site Survey Work Book
STANAG	Standards NATO Agreement
STR	System Test Review
STVP	Security Test and Verification Plan
STVR	Security Test and Verification Report
SUS	System Usability Scale
SVG	Scalable Vector Graphics
SWDL	Software Distribution List

Acronym	Description
SWID	Software Identifier
T	
TA	Target Architecture
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDL	Tactical Data Link
TEMPEST	TEMPorary Emanation ansd Spurious Transmission
TIFF	Tag Image File Format
TLS	Transport Layer Security
TNA	Training Needs Analysis
TOE	Target of Evaluation
TOPFAS	Planning Functional Services
TRR	Test Readiness Review
TSF	TOE Security Functionality
TTR	Time To Repair
U	
UA	User Agent
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time Coordinated
V	
VOE	Verifiable Objective Evidence
VLAN	Virtual LAN
W	
W3C	World Wide Web Consortium
WAN	Wide Area Network
WG	Web Guard
WSDL	Web Services Description Language
WSUS	Windows Server Update Services
X	
XML	Extensible Mark-up Language
XMPP	eXtensible Messaging and Presence Protocol
XSD	XML Schema Definition
XSL	eXtensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Transformations
XSS	Cross-Site Scripting
xFOR	KFOR, SFOR or any other NATO operation

Acronym	Description
Y	
Z	
Z	ZULU
ZULU	Universal Time Coordinated (UTC)

Annex E Glossary

Term	Definition
C3 Taxonomy	It is an effort leading to: •Support delivery of coherent C3 capabilities to NATO •Provide a common taxonomy to improve communication across planning domains and organisations •Provide a framework for multinational capability development •Provide a framework to support interoperability •Facilitates the practical implementation of NNEC •Save money by encouraging re-use •Support deliverable, product, program & project management •Support C3 governance Through the definition of classes of CIS capabilities arranged in a hierarchical structure organised by supertype-subtype relationships.
Commercial Off-the-Shelf (COTS)	Any item that is priced and available for purchase and delivery from a commercial firm can be considered Commercial Off-the-Shelf (COTS). A COTS product is one that is used "as-is." COTS products are designed to be easily installed and to interoperate with existing system components. Almost all hardware and software bought by the average computer user fits into the COTS category: computers, monitors, printers, cables, operating systems, office product suites, word processing, and e-mail programs are among the myriad examples.
Configuration Item	A Configuration Item is a hardware, firmware, or software component, or combination thereof, that satisfies an end use function and is designated for separate configuration management.
Fire and forget	Fire and forget is an attribute of the Military Messaging service. It can be described as the ability of the system to monitor military messages from the moment they are sent, throughout their journey to the recipient. Moreover, fire and forget generates alerts to an operator if the message has not reached the recipient within the set pre-defined time period. At the moment, within AIFS, the fire and forget function is accomplished by Communication Centre (COMCEN) operators through both technology and procedures.
High Grade Messaging	A High Grade Messaging Service is the mechanism for exchanging critical information and official correspondence throughout Defence Organizations and with its partners, in a manner optimised to meet stringent requirements for assurance of delivery, survivability, reliability, ease of use, security, integrity, non-repudiation and archiving commensurate with a general purpose service.
ITM	The name of the project that is delivering the new core NATO architecture for platform hosted Virtualised capabilities, reusing core NATO network infrastructures.
Metadata	METADATA is "data about data". The term is ambiguous, as it is used for two fundamentally different concepts (types). Structural metadata is about the design and specification of data structures and is more properly called "data about the containers of data"; descriptive

Term	Definition
	metadata, on the other hand, is about individual instances of application data, the data content. Metadata is traditionally in the card catalogues of libraries. As information has become increasingly digital, metadata are also used to describe digital data using metadata standards specific to a particular discipline. By describing the contents and context of data files, the usefulness of the original data/files is greatly increased. For example, a webpage may include metadata specifying what language it is written in, what tools were used to create it, and where to go for more on the subject, allowing browsers to automatically improve the experience of users. Wikipedia encourages the use of metadata by asking editors to add category names to articles, and to include information with citations such as title, source and access date. The main purpose of metadata is to facilitate in the discovery of relevant information, more often classified as resource discovery. Metadata also helps organize electronic resources, provide digital identification, and helps support archiving and preservation of the resource. Metadata assists in resource discovery by "allowing resources to be found by relevant criteria, identifying resources, bringing similar resources together, distinguishing dissimilar resources, and giving location information.
Milestones	Major decision points that separate the phases of a project implementation.
Military Messaging Service	The Military Messaging Services provide a reliable, store and forward message transfer service for both users and applications in support of organizational messaging (messaging between organizations and organizational units). The service supports different qualities of service for different message priorities (e.g., expediting higher priority messages, timing out higher priority messages more quickly) to honour the precedence of the military messages. The Military Message Transfer Service supports a range of elements of service including access management, alternate recipients, conversion prohibition, deferred delivery, delivery notification, distribution list expansion, latest delivery, and message security labelling. [As defined by C3 Taxonomy]
Military Messaging Application	The Military Messaging Application provides users with the capability to create, receive, and manage military messages. The application allows the assignment of different qualities of service for different message priorities (e.g., expediting higher priority messages, timing out higher priority messages more quickly) to honour the precedence of the military messages. The Military Messaging Application allows the user to define a range of elements of service (EoS) including alternate recipients, conversion prohibition, deferred delivery, delivery notification, distribution list expansion, latest delivery, and message security labelling. [As defined by C3 Taxonomy]
Risk	A measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints. Risks have three components: a future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential

Term	Definition
	consequence from occurring; a probability (or likelihood) assessed at the present time of that future root cause occurring; and a consequence (or effect) of that future occurrence. Information system-related security risks are those that arise from the loss of confidentiality, integrity, or availability of information or information systems
Risk Analysis	The process of examining each identified program and process risk, isolating the cause, and determining the impact. Risk impact is defined in terms of its probability of occurrences, its consequences, and its relationship to other risk areas or processes. Consequences are typically identified and analysed in terms of performance, schedule, and cost.
System	Any organised assembly of resources and procedures united and regulated by interaction or interdependence to perform a set of specific functions.
Virtualised Technologies	Virtualisation describes a technology in which an application, guest operating system or data storage is abstracted away from the true underlying hardware or software. A key use of virtualization technology is server virtualization, which uses a software layer called a hypervisor to emulate the underlying hardware. Thus allowing for greater flexibility, control and isolation by removing the dependency on any specific hardware platform.

Annex F Maintenance and Support Concept (After FSA)

F.1. Introduction

The Maintenance Process shall ensure the maintainability of the configuration baselines. The Baseline Maintenance Process implements modifications to be made either proactively or reactively to the PBL to correct faults and/or deficiencies, to improve performance or other PBL attributes, or adapt the PBL/OBL to a modified environment. The maintenance concept is based on the incident management concept and each and any maintenance and support level could be managed by a different organization during the Life Cycle of the project. The responsibility of each level, in accordance to the life cycle of the project will be part of the Contract. The Baseline Maintenance process is decomposed into 1st, 2nd, 3rd and 4th Level Maintenance tasks.

The maintenance concept includes the following activities:

a. The Maintenance of all the CIs and all related items,

b. The execution of all the required preventive and corrective maintenance activities for all the system and its subsystems for each level,

c. The allocation of the Maintenance tasks to the respective maintenance levels and the related organisation.

F.2. Definition

Level of Support: Level of support indicates a specific extent of technical assistance in the total range of assistance that is provided by an information technology product to its customer. The Service management is divided in three different level of service, which interface each other, in order to activate the proper level of maintenance in accordance with the event (incident) happened on the system.

Level of Maintenance: are various echelons at which maintenance tasks are performed on systems and equipment. The levels are distinguished by the relative sophistication of skills, facilities and equipment available at them. Thus, although typically associated with specific organizations and/or geographic locations, in their purest form, the individual maintenance levels denote differences in inherent complexity of maintenance capability.

F.3. Support Concept

The Support concept is the set of activities and processes in charge of managing the various level of maintenance and to escalate the problem to the appropriate level in accordance with the defined responsibilities.

It uses a systematic approach, to minimize the logistic delay and assure the maximum level of Service and Operation availability.

It is based on the Incident management process defined in ISO/IEC 20000 and ITIL framework or equivalent.

The Service management is divided into three different levels of service that interface each other to activate the proper level of maintenance in accordance with a system event.

The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.

The process of Support/Maintenance and the escalation process between the various levels is shown in the following figure:

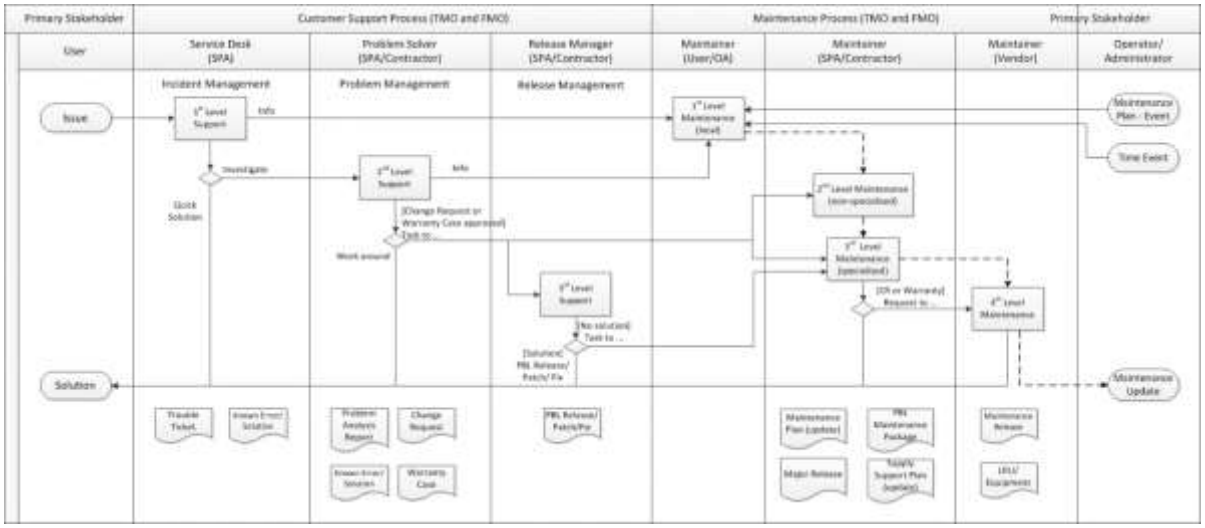


Figure 2: Support and Maintenance Concept Process

First Level Support Process

The 1st Level Support Process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket, TT), performs an initial assessment and distributes it to the predefined actors to solve it

Second Level Support Process

The 2nd Level Support Process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

The Problem Management process receives the TT from the Service Desk and performs the following tasks (not limited to):

a. (Re-)evaluation of TT category, criticality and priority,
b. Identification of the root cause of the issue (e.g., by issue replication testing),
c. Identification of workarounds,
d. Identification and initial planning of possible short, medium and long-term solutions (e.g., workarounds, patches, or new baseline or CI releases),
e. Create Problem Analysis Report and Change Request incl. schedule of implementation, and synchronization with the Baseline Maintenance process;
f. Presentation of the Problem Analysis Report and CR to the CCB for approval,
g. Monitor and Control the approved CR during implementation,
h. Trigger 3rd Level Support and/or 3rd Level Maintenance process to implement the CR, in case the incident cannot be solved at 2nd level;
i. Perform the post- CR implementation review.

Third Level Support Process

The 3rd Level Support Process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

The Deployment and Release Management process receives the approved Change Request from the 2nd Level Support and performs the following tasks (not limited to):

a. Release of the solution (release unit/record)
b. Development of the solution (e.g., new CI Fix, Repair, Replacement, Patch, or Release),
c. Testing of the solution (e.g., Regression testing, issue/deficiency replication testing),
d. Update of baseline content and status,
e. Delivery and deployment of the solution.

F.4. Maintenance Concept

The Maintenance Concept is the set of activities and processes in charge of restoring the system functionality in the shortest time possible.

The Maintenance shall be provided in a proactive and reactive manner by the Service Provider.

All proactive Maintenance tasks are defined in the Service/Capability and Site specific O&M Manuals (What) and corresponding Procedures (How) and scheduled in the Maintenance Plan.

Reactive Maintenance activities are triggered by Incident and Change Requests coming either from the Service Customer via the Customer Support Services or from the OEM/Vendor

First Level of Maintenance

It is responsible for the very basic maintenance activities. It is responsible to activate the second level of maintenance when it is needed.

It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding O&M Manual. All 1st Level Maintenance procedures do not require specialised tools and/or specialized personnel.

Second Level of Maintenance

It is responsible of isolation and resolution of system-level maintenance and management of deficiency reports and repair. It is responsible to activate the third level of maintenance when it is needed.

It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. All 2nd Level Maintenance procedures do not require specialised tools and/or specialized personnel.

Third Level of Maintenance

It is responsible of any support that involves a change to the system baseline, such as software patches or new releases. It is responsible of specialised hardware repair, if applicable. Third level maintenance is activated by third level support and can be initiated either to define the solution to a problem (corrective maintenance) or to maintain up to date software configuration (adaptive maintenance following changes to the underpinning hardware, firmware and software environment) e.g. security patches, operating system upgrades, minor software configuration changes due to operational/interface needs.

It implement the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. 3rd Level Maintenance procedures can require specialised tools and/or Personnel.

Fourth Level of Maintenance

It is the responsibility of the hardware vendor or the software original developer. It is activated from the 3rd level of maintenance only when it is needed.

Annex G Independent Verification and Validation Templates

In this annex are attached the templates which will be utilized during the contract execution and they are referred to in the main body of this SOW. These templates are evolving and are provided here for indication and estimation of effort only. Definite versions will be communicated and incorporated before Contract Signature. These templates will also be provided electronically.

Test Plan template

Test Case Specification Template

Test Completion Report Template

Project Master Test Plan Template

Test Readiness Review -Checklist

Project Requirements Traceability Matrix Template

Annex H NCIA monitoring capability systems and services

H1. The integration between IEG-C infrastructure (systems and software) and NCIA's monitoring capability systems and services will conform to the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017]

H2. This integration comprises the following activities and corresponding roles and responsibilities for the Contractor and the Purchaser:

Activity	Contractor	Purchaser
Site survey	Develop and provide site survey workbooks (with appropriate detail)	Validate and approve site survey workbooks
	Execute surveys: On each site the requirements of the NCSC Enclaves must be covered (e.g. requirements on connectivity between IEG-C and NCSC Enclaves)	Guide and validate surveys
Design	Draft and propose a design of the integration of the IEG-C with the NCSC monitoring capability • Include the physical, hardware and software interfaces in the design. • Address the aspect of scaleability of the design, taking into account: • The number of events per second that will be consumed by the NCSC monitoring capability upon deployment of the IEG-C and as expected in the future. • Impact on NCSC back-end systems and services (CSOC).	Provide information, review and approve the design
Identify necessary changes and updates to existing NCSC monitoring capability systems and services	Based on the site surveys and design, identify necessary changes and updates to NCSC monitoring capability systems and services and NSCN enclaves (also referred to as "NCIRC enclaves"). • Include consideration of module additions, component capacity changes, configuration changes etc. • Ensure proposed changes are aligned with the existing solution in terms of choice of equipment and vendors.	Review and approve the changes

Install components	Enable network connectivity between IEG-C and the NCSC monitoring capability. Install (software) agents on IEG-C components as required	Provide support and oversight to installation process, and perform CSOC-configuration as required
Configure monitoring components and IEG-C systems	In the event additional hardware components are procured, perform basic configuration based on NCSC guidance so that central management of these components by NCSC becomes possible	Provide supporting information (e.g. IP-addresses)
	Perform configuration of IEG-C components in accordance with the Purchaser's Guidance	Provide guidance and validate configuration
Migrate configurations of existing systems/solutions	Provide support to NCSC team to migrate and update necessary configurations within the NCSC enclave	Review existing system configurations, develop migration plan, and perform migration
Plan and execute test activities	Prepare test plan and procedures in accordance with the other test activities within the scope of this project	Review and approve test plan
	Execute test activities and document results	Provide oversight and validate results
Document the IEG-C monitoring solution as built	Prepare documentation	Validate and approve documentation
Provide training	Provide training material on the part of the IEG-C monitoring solution, which is not covered by the existing NCSC monitoring capability	Review and approve material
	Provide training to Purchaser (NCSC)	Participate and validate
Handover IEG-C monitoring solution	Finalize handover requirements regarding the part of the IEG-C monitoring solution, which is not covered by the existing NCSC monitoring capability	Review, validate and take over

Table 27