1 Introduction

1.1 Purpose

[001] This Statement of Work (SOW) describes the requirements and activities to deliver the Future Land Command and Control (FLC2) System.

[002] The purpose of this Contract is to buy and implement the best available Commercial-Off-The-Shelf (COTS) software product.

[003] Project DEMETER is the name given to this project. It is the responsibility of the contractor to integrate DEMETER within the NATO Enterprise, to migrate the data from the existing Land Command and Control Information Services (LC2IS) and to address the initial training aspects of the capability.

1.2 Background

[004] DEMETER was authorised under NSIP project 2021/0IS03211 and originates from the Capability Programme Plan 5A1201 “Future Land Command and Control Information Capability”.

[005] Currently, the NATO Land Command and Control requirements are supported by LC2IS. DEMETER is intended to replace LC2IS to provide an updated capability for Command and Control (C2) of NATO Land Forces at the Strategic and Operational levels, including provision of a Recognised Ground Picture, Enablement of Battlespace Management and exchange of information and knowledge across operational domains within the NATO Command Structure (NCS), NATO Force Structure (NFS) and NATO Nations.

1.3 Conventions and Interpretations

[006] The headings in this SOW are for ease of reference only and shall not affect its interpretation.

[007] In this SOW, unless the context otherwise requires:

(a) The term “Contract Award” (CAW) is the date of the last signature of the Contract by the Parties and the date the Contract enters into force;

(b) The term “Effective Date of Contract” (EDC) is the date for beginning the period of performance under the Contract;

(c) For this project EDC = CAW.

(d) A number in brackets [number] precedes each informational or context paragraph; a unique identifier, consisting of a prefix and number [SOW-number] precedes each requirement;

(e) Requirements are formulated using the form “shall” and are contractually binding. Context information supporting the requirements definition is provided using the form “will” and implies the intent or aim on the part of the Purchaser; the context forms one part with the requirements;

(f) Any phrase introduced by the words "including", "includes", "in particular", "for example" or similar, shall be construed as illustrative and without limitation to the generality of the related general words;

(g) Any reference made to a section or paragraph encompasses the referenced section or paragraph including all subordinate sections and paragraphs; and

(h) The convention used for dates (e.g. quoting dates of meetings) is day-month-year.

1.4 Scope of Work Overview

[008] This section provides a summary of the scope of work of this SOW. It is intended that project DEMETER will:

(1) Provide the software in support of NATO FLC2 operations. It will be used across the full spectrum of NATO operations and missions to support the C2 needs of the NCS across strategic and operational levels;
(2) Address initial training aspects of the capability with the provision of the training to the NATO trainers, support personnel and users; and
(3) Migrate from LC2IS to DEMETER through a detailed Transition Plan, including secure data migration.

[009] As shown in Figure 1.1, the main work will be organized in two work packages (WPs) i.e. WP1 and WP2. In addition, an optional WP3 is defined for adaptations with regard to interoperability and an optional WP4 for Contractor furnished maintenance and support services.

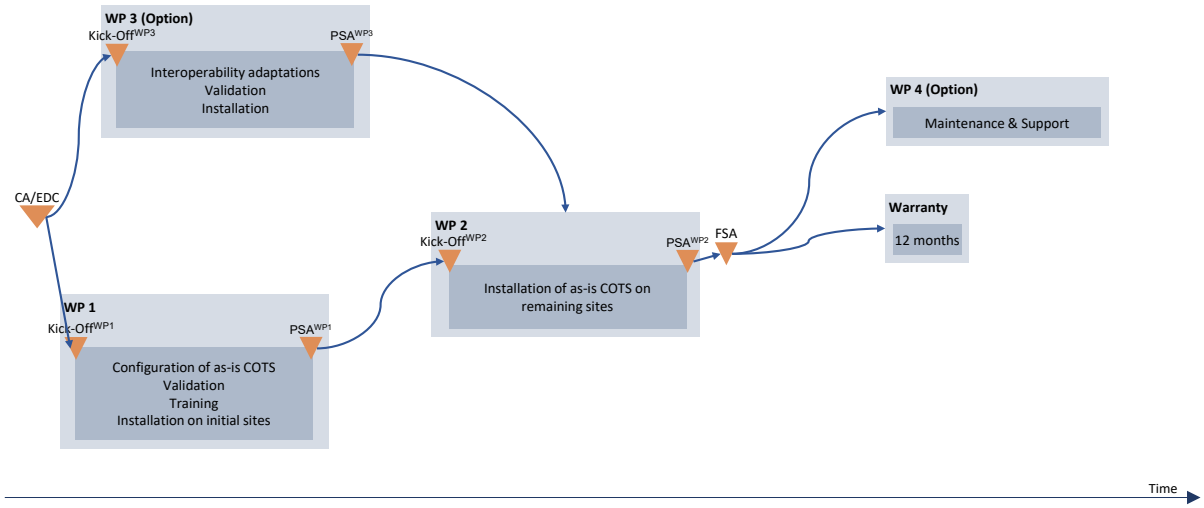

Figure 1.1 – Overview of Timelines and Stages

[010] Figure 1.2 illustrates the timelines of the Contract, the WPs and the major delivery milestones: Partial System Acceptance (PSA) for each of the WPs and Final System Acceptance (FSA).

[SOW-001] The Contractor shall deliver all supplies and services as specified in this SOW and as stated in the Schedule of Supplies and Services (SSS), with an associated expected delivery time. With the expected delivery time, it is assumed the Purchaser understands the difference between ‘delivered’ and ‘accepted’. The Contractor will need to incorporate within its schedules sufficient time i.e. a minimum of 15 business days, for the Purchaser to validate and accept each deliverable and milestone.

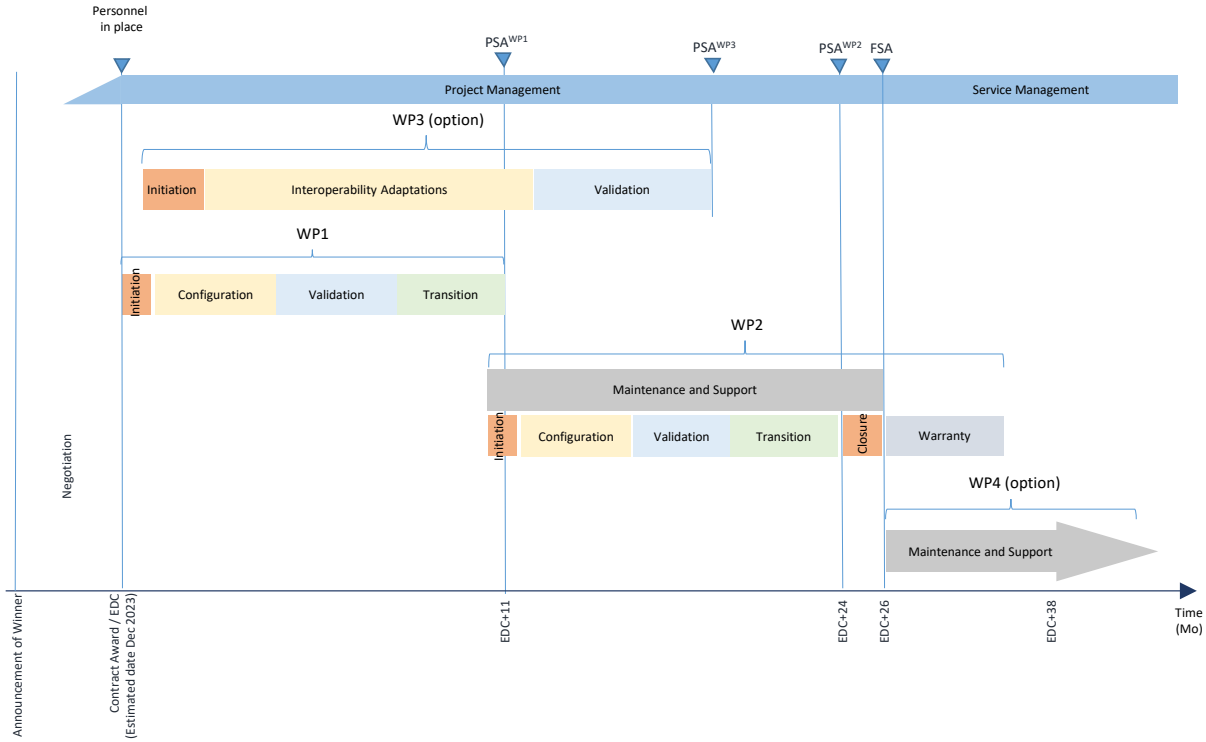

Figure 1.2 – DEMETER Life Cycle overview

[011] The project schedule as illustrated in Figure 1.2 is a proposed schedule, however the milestone dates are considered fixed dates.

[SOW-002] The Contractor shall deliver according to the SSS. The key project schedule constraints are listed in Table 1.1.

Table 1.1 – Key events and dates

Key event	**Schedule Date**
Training Materials accepted	Training Material Review (TMR) = EDC + 6 months
Acceptance of WP1	PSA^{WP1} = EDC + 11 months
Acceptance of WP2	PSA^{WP2} = EDC + 24 months
Acceptance of all project deliverables	FSA = EDC + 26 months
End of Warranty	FSA + 12 months

1.4.1 Work Package 1: Implement initial sites

[012] This WP covers the configuration and implementation of DEMETER in authorized locations (refer to Table 4.2) inclusive of licenses and all the required activities, such as tests, site surveys and deployments.

[013] This WP addresses initial training aspects of the capability with the provision of the training to the NATO trainers, support personnel and users.

[014] This WP includes the migration from LC2IS to DEMETER by preparing a detailed Transition Plan, including secure data migration.

[015] At successful completion of WP1, the PSA WP1 milestone is reached (PSA^{WP1}).

1.4.2 Work Package 2: Implement remaining sites

[016] This WP covers the configuration and implementation of DEMETER in the remaining authorized locations, inclusive of licenses, as well as all the required activities, such as tests, site surveys and deployments.

[017] This WP also includes (repeating) the migration from LC2IS to DEMETER.

[018] The Contractor will perform the maintenance and support of DEMETER and any follow-on deployed baseline releases or patches.

[019] At successful completion of this WP, the PSA WP2 milestone is reached (PSA^{WP2}).

[020] FSA will be granted when the Purchaser has verified completeness of the entire scope and has determined that it meets the contractually agreed scope. Subsequently, on successful achievement of the FSA, the warranty period will commence.

[021] Starting on the date of the FSA, the Contractor will provide one year warranty for all deliverables and services furnished under this Contract.

1.4.3 Work Package 3: Optional Interoperability Adaptations

[022] This optional WP will cover the specified interoperability requirements that require adaptations in order to fully meet the selection criteria.

[023] Also adaptations needed for other requirements are included in this WP.

[024] The adaptations in this WP will be deployed to production as part of WP2.

[025] Any additional costs when this WP is exercised should be included in WP3 and not in WP2.

[026] At successful completion of this WP the PSA WP3 milestone is reached (PSA^{WP3}).

[027] Refer to Annex B for the requested interfaces.

[028] Reserved.

1.4.4 Work Package 4: Optional Maintenance and Support Services

[029] The optional WP specifies the Contractor furnished services for the maintenance and support of DEMETER for ten years, starting from FSA with the first year being concurrent with the warranty period.

2 Purchaser's Responsibilities

[030] The Purchaser's project manager (PM) will act as the Purchaser's representative and will be the primary interface between the Contractor and Purchaser after CAW.

[031] The Purchaser's PM will be supported by specialists in certain areas (e.g. the technical lead) who may be delegated to act on the PM's behalf in their area of expertise.

2.1 Purchaser Furnished Property and Services

[032] The Purchaser will provide the Contractor with NATO documentation and references if such are required for the efforts under the Contract.

[033] The Purchaser will coordinate access to subject-matter experts (SMEs) and user communities.

[034] The Purchaser will coordinate access to NATO sites the Contractor will have to visit.

[035] The Purchaser will provide the Contractor with available technical descriptions of external NATO interfaces if such are required for the efforts under the Contract.

[036] The Purchaser will equip the Contractor with two NATO RΞSTRICTED (NR) laptops to be used for sharing of electronic material up to NR. For access to material of classification higher than NR, the Contractor will be required to visit one of the Purchaser's main facilities in order to be able to review the classified material required for the efforts under this Contract.

[037] The Purchaser will make available to the Contractor, by facilitating access at Purchaser facilities, the operational networks for deployment and if needed, for validation and training activities required under the Contract.

[038] The Purchaser will provide the Contractor with "NATO Software Factory DevSecOps" services, "NATO Software Factory" (NSF) in short, a cloud-sourced development, integration and test platform covering the entire application development lifecycle (see Section 2.2).

[039] The Purchaser will provide the Contractor for its project team a set of user accounts with access to the NSF and services furnished by the platform.

[040] The Purchaser will make available to the Contractor, by facilitating access at Purchaser facilities, the reference test environments for the deployment, integration testing and validation activities required under the Contract.

[041] The Purchaser will make available to Contractor, by facilitating access at Purchaser facilities, the integration testbed (ITB) facilities for deployment, integration testing and validation activities required under the Contract.

[042] The Purchaser will provide the Contractor with access to an NCI Agency approved integration platform (e.g. the Service Oriented Architecture and Identity Management (SOA-IdM) platform, see [SOA-IdM] or IntCore).

2.2 NATO Software Factory DevSecOps Services

[043] The NSF DevSecOps services offer a cloud-sourced development, integration and test platform covering the entire application development lifecycle.

[044] The platform makes use of standardized application development processes and common tooling. This approach supports the Purchaser's strategy in moving towards

an agile capability development approach embracing a high degree of componentization and reuse through services, with an improved return on investment.

[045] To ensure better coherency among the capabilities being developed and maintained within the NATO enterprise, the Purchaser is mandating the use of the NSF DevSecOps services. This approach will improve and tighten the collaboration between Purchaser and industry and ensures transparency of progress and quality throughout the development lifecycle, essential both to performance monitoring and quality assurance performed by the Purchaser.

[046] The NSF DevSecOps services are hosted in a secure public cloud and will be offered as Platform as a Service (PaaS) based on the Microsoft Azure DevOps platform. Therefore, the highest level of security classification that is allowed to be used on this platform is NATO UNCLASSIFIED.

[047] The NSF DevSecOps services will provide cloud services and a series of tools (toolchain) based on both Microsoft and Open-Source Stack (OSS) technology ecosystems. These include source code hosting, configuration management, build and continuous integration pipelines, (automated) testing, work item management, artefacts repository and collaboration space.

[048] The Purchaser furnished services part of the NSF is limited to the following:

(a) User accounts with access to the NSF:
- Basic Plus Profile for Microsoft Azure DevOps services and Test Plan access;
- NSF DevSecOps Security Services;
- NSF Microsoft Office 365 E1 license (Microsoft Office 365 online, Microsoft Teams for collaboration, Microsoft SharePoint for documentation management and collaboration);

(b) Git for source code control (for optional WP3);
(c) NSF Microsoft Azure Cloud services access (DevTestLabs, build server, integration platform); and
(d) Microsoft Azure Cloud Services costs.

It does not include:

(a) Development tools individual licenses (e.g. Microsoft Visual Studio).

3 General Requirements

[049] This section defines the general requirements of this SOW.

[050] The Purchaser's main facilities are at The Hague, Netherlands. Depending on the nature of the works, activities may need to be conducted at other facilities than the Purchaser's main facilities.

3.1 Communication

[SOW-003] The Contractor shall use the English language in all its communications relevant to this Contract, i.e. in conversations, meetings, workshops, emails, reports, etc.

3.2 Meetings

[051] The term meetings includes workshops, formal reviews and validation activities.

[SOW-004] Meetings requiring in person attendance shall take place at one of the Purchaser's main facilities, with location at the discretion of the Purchaser. If circumstances of the meeting require, at the discretion of the Purchaser, the Contractor shall meet in person at other Purchaser's facilities.

[SOW-005] If meeting/conference rooms at the specified Purchaser facilities are not available in the timeframe required to support an in-person meeting, the Contractor shall:

(1) Reschedule the meeting to such time as meeting/conference rooms are available at the Purchaser's facilities, with no further adjustment to schedule or cost; or

(2) If the Contractor prefers the meeting to take place within the foreseen timeframe, provide suitable meeting/conference rooms (e.g. hotel meeting/conference rooms) for the meeting in close proximity of the Purchaser's facilities at no additional cost to the Purchaser; or

(3) Alternatively, if the Purchaser agrees, arrange to host the meeting at the Contractor's facilities. These meeting/conference rooms shall be provided at no additional cost to the Purchaser.

[SOW-006] For meetings taking place at the Contractor's facilities, the Contractor shall enable the Purchaser to participate in the meeting remotely using video conferencing technology (e.g. Microsoft Teams), if the purpose and circumstances of the meeting allow for or require remote participation.

[SOW-007] Unless specified otherwise, at least two (2) weeks prior to all meetings required under this Contract, the Contractor shall send an invitation, including agenda and objectives of the meeting.

[SOW-008] If any artefacts or deliverables are to be reviewed in preparation of the meeting, the Contractor shall provide these artefacts at least at least one (1) week for the Purchaser to review them and provide feedback to the Contractor.

[SOW-009] The Contractor shall record meeting minutes and provide the minutes to the Purchaser within three business days after the meeting.

[SOW-010] The Contractor shall meet with the Purchaser as required to discuss progress of work or any other matter relevant to this Contract.

3.3 Security Aspects

[052] Security aspects relevant to the Contractor's work are defined in the Contract Provisions. This section identifies additional security requirements related to the execution of the Contractor's work.

[SOW-011] All Contractors' personnel assigned to work under this Contract shall have a NATO SΞCRET (NS), or higher, security clearance throughout the period of performance of the Contract.

[SOW-012] The Contractor shall process all its personnel through NATO security at each of the Purchasers' facilities, adhering to the local procedures for clearances, to obtain unescorted access (unescorted security badges) for the duration of the on-site activities.

[SOW-013] The Contractor shall seek prior Purchaser approval for any service or deliverable planned to be produced and delivered with a security classification level higher than NATO UNCLASSIFIED (NU).

[SOW-014] The Contractor shall ensure secure transfer of any classified service and deliverable from the Contractor's facilities to the Purchaser's facilities.

[SOW-015] All information items are to be handled according to their security classification, in accordance with [AD-070-001].

3.4 Location of Performance

[SOW-016] The Contractor shall perform the main effort set forth in the Contract at the Contractor's facilities, unless specified otherwise or agreed by the Purchaser.

3.5 NATO Software Factory

[SOW-017] The Contractor shall use the NSF services furnished by the Purchaser (Section 2.1) in support of delivering all capabilities and services, under the Contract.

[SOW-018] The Contractor shall furnish its project team with capable physical workstations and enable connectivity and provide access for its project team to the NSF services from its facilities and from mobile workstations when project team members are away from the Contractor's facilities, e.g. on travel duty. Mobile devices, e.g. laptops, shall have full disk encryption enabled.

[SOW-019] The Contractor shall deliver to the Purchaser a named-list of its project team members, including their email addresses.

[053] When the Purchaser has received the named-list project team members from the Contractor, the Purchaser will create accounts for these project team members within the NSF. The NSF accounts for key personnel will be created upon confirmation of the Contractor's key personnel.

[SOW-020] The Contractor shall verify that its project team members have access to the NSF after having received their account information.

[SOW-021] The Contractor shall notify the Purchaser immediately of any changes in the Contractor's project team composition to allow the Purchaser to manage effectively and efficiently the NSF accounts assigned to Contractor's project team.

[SOW-022] The Contractor shall enable and maintain full traceability between contracted requirements, test cases, etc. within the NSF.

[SOW-023] The Contractor shall organize the engineering artefacts within the NSF in a structured and logical way as configuration items that will enable the Purchaser to quickly find any artefacts based on context (e.g. WP) and artefact type.

[SOW-024] The Contractor shall use the ticketing system on the NSF for tracking defects and issues.

[SOW-025] The Contractor shall ensure that all artefacts uploaded and all services delivered on the NSF are kept at NATO UNCLASSIFIED or lower security classification level.

[SOW-026] In case it would not be feasible to stay at NATO UNCLASSIFIED or lower security classification level on the NSF (e.g. not feasible to use declassified or mock data), the Contractor shall perform the work at a Contractor's furnished secure environment.

[054] As per Section 2.1, the Purchaser will furnish NSF accounts and Microsoft Azure Cloud Services.

[055] The Contractor may also propose additional services and tooling to be hosted on the NSF in addition to the services and tooling furnished by the Purchaser.

[SOW-027] The Contractor shall specify and dimension the number of NSF user accounts, the Microsoft Azure Cloud Services and additional tooling that are required throughout the period of performance of the Contract.

[SOW-028] The Contractor shall include the associated costs for the Microsoft Azure Cloud Services and tooling in its price estimation.

[SOW-029] The Contractor shall acquire/procure the necessary licenses/subscriptions for its project team members and maintain those licenses throughout the period of performance of the Contract.

[SOW-030] After Purchaser approval has been obtained for the additional services and tooling, the Contractor shall submit any NSF service request, including hosting of additional services and tooling on the platform, to the Purchaser, who will evaluate the request and, if approved, engage with the NSF service support team for implementation of the request.

[SOW-031] The Contractor shall implement and provision the support associated with these services and tooling throughout period of performance of the Contract.

3.6 Third-Party Software and Components

[056] DEMETER may use and integrate several COTS, non-commercial and open-source, i.e. free and open-source software (FOSS), components, libraries and packages. This includes the development environment, office and other specialised applications for use by the project team. This collection of software, components, libraries and packages, are referred to as third-party software and components.

[SOW-032] The Contractor shall only use components as described in [056] that are supportable and are admissible to the Agency Approved Software List (A2SL).

[057] The choice of third-party software and components should not limit the distribution or installation of DEMETER.

[SOW-033] The Contractor shall acquire/procure the required third-party software and component licenses/subscriptions and maintain those licenses throughout the period of performance of the Contract.

[SOW-034] The Contractor shall place all third-party software and components, including vendor-supplied documentation artefacts (e.g. manuals) under configuration control (refer to section 3.9).

[SOW-035] The Contractor shall use and integrate any updates (major, minor, patch releases) of any of the third-party software and components when these become available.

[SOW-036] The Contractor shall maintain a roadmap for the third-party software and components based on available information provided by vendors (e.g. anticipated or published release cycle) for at least the next three (3) years. The Contractor shall consult the Purchaser regarding the appropriate timeframe for inclusion of major versions and favour long-term support (LTS) releases when available. In addition, the Contractor shall adhere to the change management processes. Refer to section 3.8.4.4.

[SOW-037] Subject to Purchaser approval, the Contractor may propose the use and integration of new third-party software and components, for example to replace existing software or components, or to support the implementation of new requirements.

[SOW-038] The Contractor shall deliver the needed licenses and/or subscriptions as part of DEMETER and maintain those licenses/subscriptions throughout the period of performance of the Contract, meeting the following conditions:

(1) The Contractor shall deliver all third-party software and component licenses/subscriptions registered with the NCI Agency as license holder;
(2) The Contractor shall ensure that all upgrades, update and patch releases of the third-party software and components are included within the provided licenses/subscriptions;
(3) The Contractor shall deliver renewed/extended licenses/subscriptions of these third-party throughout the period of performance of the Contract; and
(4) The Contractor shall ensure that none of the third-party software and components have an additional run-time or per end-user/seat license-fee.

3.7 Project Management

[058] The objective of the Contractor's project management is to establish a project organization and guide the delivery of services and capabilities of this Contract through a controlled, well-managed, visible set of activities to achieve the desired outcomes. Wherever possible, the Contractor's project management should aim to eliminate problems and ensure that those problems that do occur are identified early, assessed accurately, and resolved quickly.

3.7.1 Project Organization and Management

[SOW-039] The Contractor shall establish and maintain a project organization to manage and deliver all services necessary to discharge of all its responsibilities set forth in the Contract.

[SOW-040] The Contractor shall establish a project management process using PRINCE2, or a similar and internationally recognized project management standard, and perform effective project management throughout the period of performance of the Contract.

3.7.2 Project Board

[059] A project board is formed by the Purchaser according to PRINCE2 principles and serves as the primary mechanism for monitoring project status, resolving issues or conflicts within the project, as well as advising the Purchaser's PM.

[060] The Purchaser's C2 Centre Chief chairs the project board in an "Executive" role.

[061] The Contractor will be considered a member of the project board as the "Senior Supplier" role.

[062] The user community (or representative) will be considered a member of the project board as the "Senior User" role.

[063] The other members (e.g. "Assurance") are designated representatives of the Purchaser.

[SOW-041] Depending on the context of the meeting, the Contractor will be invited and shall participate in the project board meeting.

3.7.3 Resources and Personnel

[SOW-042] The Contractor shall provide the necessary resources and personnel, appropriately skilled and experienced, to deliver the services and capabilities that meet the requirements set forth in the Contract.

[SOW-043] The Contractor shall take all reasonable steps to ensure continuity of resources and personnel assigned throughout the period of performance of the Contract.

[SOW-044] The Contractor's personnel shall be available to travel and may be required to perform duties (e.g. conduct preparations or perform upgrades) during weekends, official holidays, and after regular business hours as the Purchaser's operational or practical requirements necessitate.

[SOW-045] The Contractor personnel identified below shall be considered as key personnel in accordance with the Contract Special Provisions:

(1) Project Manager;
(2) Lead Instructor;
(3) Technical Lead; and
(4) Test Manager.

[SOW-046] The Contractor shall provide to the Purchaser an (updated) list of the key personnel and their resumes during Contract negotiations.

[SOW-047] The Contractor shall make available its key personnel for interviews with the Purchaser during Contract negotiations prior to CAW.

[064] CAW will only proceed when Contractor proposed key personnel has been assessed and considered acceptable by the Purchaser.

[SOW-048] The Contractor shall ensure that assigned key personnel is available from the CAW onwards.

[SOW-049] The Contractor shall make available replacement key personnel for interviews with the Purchaser from the moment the Contractor formally notifies the Purchaser of the replacement.

3.7.4 Key Personnel Qualifications

3.7.4.1 General

[SOW-050] All key personnel shall be proficient in the English language for effective verbal and written communication and for technical documentation.

3.7.4.2 Project Manager

[SOW-051] The Contractor shall designate a PM, who shall direct and co-ordinate the activities of the Contractor's project organization. Responsibilities include establishing project plans as well as their proper execution, coordinating with the project teams to ensure that all project requirements, deadlines and schedules are on track, submitting project deliverables, preparing status reports, and coordinating with Purchaser.

[SOW-052] The Contractor’s PM shall be prepared at all times to present and discuss the status of Contract activities with the Purchaser’s PM, Contracting Officer, or Technical Lead.

[SOW-053] The Contractor’s PM shall serve as point of contact for the Purchaser’s Independent Verification, Validation and Quality (IVVQ) Service Line.

[SOW-054] The Contractor’s PM shall meet the following minimum qualifications:
(1) Have a bachelor’s degree or equivalent;
(2) Have a formal certification through Project Management Institute, PRINCE2, or equivalent; and
(3) Have seven years of proven experience in managing projects similar to this project in technical and financial scope.

3.7.4.3 Lead Instructor

[SOW-055] The Contractor shall designate a Lead Instructor who shall be responsible for ensuring the integrity and quality of all training deliverables and training activities conducted under this Contract. The Lead Instructor shall have a leading role in delivering the training courses.

[SOW-056] The Contractor’s Lead Instructor shall meet the following minimum qualifications:
(1) Have a bachelor’s degree or equivalent;
(2) Have at least five years of experience in developing training materiel and two years of experience in leading training materiel development teams;
(3) Have at least five years of experience in instructing software applications;
(4) Have effective verbal and written communication skills, with ability to communicate direct feedback in a compelling way that empowers others;
(5) Have effective presentation skills, strong classroom-management skills and stage presence;
(6) Being able to relate the practical use of a software application to the applicable functional/operational context; and
(7) Desirable to have a military background and/or have experience in instructing military personnel (e.g. commissioned officers).

3.7.4.4 Technical Lead

[SOW-057] The Contractor shall designate a Technical Lead who shall be responsible for all technical aspects of the project, such as:
(1) The high-level structure of the COTS, its main components and their interfaces;
(2) The interactions of the COTS with external systems; and
(3) The configuration of the COTS to work on NATO networks.

[SOW-058] The Contractor's Technical Lead shall meet the following minimum qualifications:
(1) Have a master's degree in computer science, or related/equivalent studies;
(2) Have at least seven years of experience in leading technical roles in projects similar to this project in complexity and scope; and
(3) Understanding of the particular business domain.

3.7.4.5 Test Manager

[SOW-059] The Contractor shall designate a Test Manager who shall be responsible for planning and executing all test activities conducted under this Contract and shall manage the testing team.

[SOW-060] The Contractor's Test Manager shall meet the following minimum qualifications:
(1) Have a master's degree in computer science, or related/equivalent studies; and
(2) Have at least five years of experience as test manager/senior test engineer in projects similar to this project in complexity and scope.

3.7.5 Project Management Plan

[SOW-061] The Contractor shall deliver a Project Management Plan (PMP) compliant with Section 8.4, and document its project organization, project management processes and project execution and delivery approach.

[065] The acceptance of the PMP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the contractual obligations. This acceptance does not relieve the Contractor from its responsibilities to meet the requirements stated in the Contract. The requirements of the Contract supersede any statement in the PMP in case of any conflict, ambiguity or omission.

[SOW-062] The Contractor shall ensure the PMP remains current to reflect the actual state of the Contractor's organization, processes and efforts throughout the period of performance of the Contract.

[SOW-063] The Contractor shall deliver follow-on revisions (post the accepted baseline) of the PMP to the Purchaser for Purchaser assessment.

3.7.6 Risk Management

[SOW-064] The Contractor shall establish a risk management process and perform risk management throughout the period of performance of the Contract.

[SOW-065] The Contractor shall document its risk management process within the PMP.

[SOW-066] The Contractor shall document all risks to the project in the risk register as part of the risks, actions, issues, decisions (RAID) register (Section 8.5) and maintain the risk register to reflect the actual status of risks throughout the period of performance of the Contract.

[SOW-067] The Contractor shall periodically, at least once every three (3) months, conduct a risk assessment, deliver an updated risk register and report on any significant changes in the risks.

3.7.7 Issue Management

[066] Issue management is the process of identifying, tracking, analysing, reporting and resolving all project issues.

[SOW-068] The Contractor shall establish an issue management process and perform issue management throughout the period of performance of the Contract.

[SOW-069] The Contractor shall document its issue management process within the PMP.

[SOW-070] The Contractor shall document all project issues in the issue register as part of the RAID register (Section 8.5) and maintain the issue register to reflect the actual status of issues throughout the period of performance of the Contract.

3.7.8 Project Highlight Report and Project Checkpoint Review

[SOW-071] The Contractor shall provide, no later than the fifth working day of every 3rd month, a Project Highlight Report (PHR), see Section 8.6.

[SOW-072] The Contractor shall conduct Project Checkpoint Reviews (PCR) throughout the Contract period of performance. By default, the PCRs shall take place in the week after the delivery of the PHR.

3.8 Test, Verification, Validation and Assurance (TVVA)

[067] This section details the Test, Verification and Validation TV&V processes and requirements to be applied and performed under the Contract, which are required for the verification and validation of the requirements set forth under the Contract by the Purchaser.

[SOW-073] All Contract-related deliverables supplied by the Contractor under this contract shall be tested, verified and validated to ensure that they meet the requirements of the contract. Both fitness-for-use and fitness-for-purpose will be assessed using a quality based approach. Responsibility for each test, verification and validation activity is defined in this section.

[068] 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 Properties and Services.

[069] In this document, the term “deficiency” is considered to be an inadequacy or incompleteness process definition or execution, while the term “defect” is an error, a fault or a malfunction inside a Configuration Item.

[070] Requirements verification methods, as defined in [ISO/IEC/IEEE-29148], will be used in order to obtain evidence(s) that requirements have been fulfilled.

[SOW-074] For each requirement, the Contractor shall select a verification method, which shall be approved by the Purchaser.

[SOW-075] The Contractor shall use the Purchasers’ categorization nomenclature for all defects and non-compliances.

[SOW-076] 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.

[SOW-077] All TVVA material developed and used under this contract shall be delivered to the Purchaser, latest by FSA.

[SOW-078] Progress and result measurement shall be reported at agreed milestones and focused on items identified in the Master Test Plan (MTP).

3.8.1 TV&V activities

[SOW-079] The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities. This includes the development of all TV&V documentation required under the Contract, the conduct of all independent verification and validation as well as the evaluation and documentation of the results.

[SOW-080] All document-based deliverables shall be produced in a manner compliant with the templates provided by the Purchaser.

[SOW-081] The Contractor shall perform the verification activities for each iteration and for each target environment (Contractor and Purchaser).

[SOW-082] The Contractor shall perform verification to confirm that each element properly reflects the specified requirements, design, code, integration and documentation.

[SOW-083] The Contractor shall support Purchaser led Validation activities to confirm that the solution is fit for purpose.

[SOW-084] The Contractor shall be responsible for the planning, preparation, organization, execution and follow-up of all TV&V events.

[071] 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 TV&V events to witness and assist with these events, as well as IVVQ Test Engineers, and, for some events and at the Purchaser's discretion, a NATO Quality Assurance Representative.

[SOW-085] The Contractor shall demonstrate to the Purchaser that there is a Test Process in place for the Contract, supported by Contractor Quality Assurance (QA).

[SOW-086] The Contractor shall provide test data to support all TV&V activities.

[SOW-087] The Contractor shall follow the Purchaser defined TV&V processes as described in this SOW.

[SOW-088] If the Contractor wishes to propose a modification to the process, the proposal shall be approved by the Purchaser and documented accordingly.

[SOW-089] 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-090] All test, verification and validation material developed and used under the Contract shall be delivered to the Purchaser.

[072] The List of TV&V Phases table below, lists and describes the different TV&V phases and associated activities during the project execution. If deemed necessary, the project may split the test phases defined in the Table into multiple events.

[SOW-091] The Contractor shall appoint a Test Manager for the phases defined in the Table below. The Test Manager will work closely with the Purchaser's assigned TVV Manager and NATO Quality Assurance Representative (NQAR).

[SOW-092] The Purchaser will appoint TV&V Test Engineers and Subject Matter Experts (SME) for each test event.

[SOW-093] The Contractor shall use Key Performance Indicators (KPIs) to measure process execution and identify opportunities for quality improvement, provide solutions and update the plans, the achievement of defined objectives like coverage of risks, requirements, supported configurations, supported operational scenarios, etc.

[SOW-094] The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities defined in the Table below.

Table 3.1 – List of TV&V Phases

TV&V Phases	Scope	Purchaser Involvement
Factory Acceptance Phase	To verify that production units comply with the requirement/design specifications and assess whether production can start. Confirm that all required engineering-level testing activities have been completed in accordance with the requirements. Determine if project deliverables are ready for subsequent TV&V activities.	**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)
TV&V 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. Ensures quality criteria defined in figure 1 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.	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)

	System Acceptance Test (SAT) – Tests focused on ensuring compliance with the requirements outlined in the SoW. 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 TV&V 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)

[073] The Purchaser reserves the right to monitor and inspect the Contractor's TV&V activities to verify their compliance with the requirements set forth in this Contract.

[SOW-095] The Contractor shall only proceed to the next formal TV&V activity, after the successful completion of the previous TV&V activity and after the agreement/approval by the Purchaser.

3.8.2 Deliverable

[SOW-096] The Contractor shall provide a System Test Documentation Package, following documentation templates provided by the Purchaser, which is comprised of the following documents:

Table 3.2 - Test Documentation

Work Product Name	Sent to Purchaser
The Master Test Plan (MTP)	4 weeks after Contract award
Defect Reporting and Management Plan	4 weeks after Contract award
Event Test Plans for individual test events (ETP)	4 weeks before TV&V event

Work Product Name	Sent to Purchaser
The Security Test & Verification Plans (STVP)	as required per the NSAB
Any submitted test Waivers together with supporting material	4 weeks before TV&V event
The Test Cases/Scripts/Steps	4 weeks before TV&V event. First draft 4 weeks after Contract award
Status Reports	Periodically (to be defined in the MTP)
Test Completion Report	1 week after TV&V event
System under-test Documentation	2 weeks before TV&V event
The Requirements Traceability Matrix (RTM) updated with test-related information	First with MTP and update as required

[SOW-097] The following timeline indicates by when the deliverables need to be provided to the Purchaser (and approved by the Purchaser) for each Test Event (dates follow the timelines of the previous table):

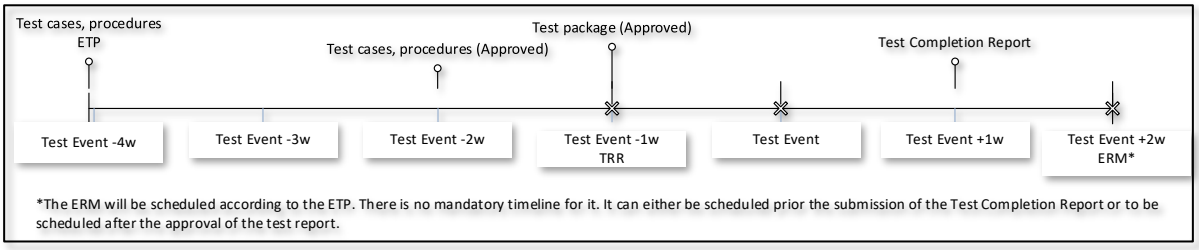

Figure 3.1 – Test Event timeline

[SOW-098] Modification of inaccurate or inadequate TV&V deliverables and any subsequent work arising as a result shall be carried out at the Contractor's expense.

[SOW-099] All TV&V materials developed and used under the Contract shall be delivered to the Purchaser.

[SOW-100] Templates provided by the Purchaser are to be utilized by the Contractor 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, it shall be approved by the Purchaser.

[074] All deliverables shall undergo as many review cycles are required, and have to be approved once all deficiencies have been corrected.

3.8.2.1 Master Test Plan

[SOW-101] The Contractor shall develop a Master Test Plan (MTP) document conforming to the specifications in section 8.7 and keep the MTP always up to date.

3.8.2.2 Test Cases and Test Procedures

[SOW-102] Any updates required from the execution of test cases during each phase shall be incorporated into the relevant test cases by the Contractor for use during independent verification, validation and acceptance. If only certain sections are

affected, then it shall be sufficient to up-date and re-issue those 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

[SOW-103] The Contractor shall submit the draft test cases for the TV&V event to the Purchaser for approval no later than four (4) weeks prior to the execution of the tests, unless differently stated in a work package. The Purchaser shall provide comments or approval within four (4) weeks of receipt. The Purchaser must have the final version of the test cases and Event Test Plan available one (1) week prior to the TRR for a specific TV&V event

[SOW-104] The Contractor shall develop test and use cases to verify and validate all requirements in the SoW, requirements specifications and final design. The test cases shall follow the template provided by the Purchaser

3.8.2.3 Event Test Plan (ETP)

[SOW-105] 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-106] The Contractor shall describe in the event test plan what training (if any) will be provided prior to formal TV&V events.

[SOW-107] The Contractor shall identify, in the ETP, which environment(s) to be used at each TV&V event and the responsibilities for configuration control, operation and maintenance of the environment.

[SOW-108] The ETP shall describe when an agreement shall be reached between the Contractor and the Purchaser on the defect categorization and defect priority of failures encountered, as well as a way forward (if either at the end of each day of a TV&V event or at the Event Review Meeting). If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Managers

3.8.2.4 Requirement Acceptance Criteria

[075] Requirement Acceptance criteria represent a condition that states whether the specified SRS requirements are fulfilled or not. Written in simple language, the Acceptance Criteria is complementary to each contractual requirement in the SRS and provides the basis of a shared understanding for what is to be delivered and what is required as objective evidence to assess that a requirement has been met. Acceptance Criteria for requirements with V&V Method of Test and Demonstration for instance can be written in "Given/When/Then" format. It is meant to provide a logical description which actions would lead to meeting the requirements. It is not meant to provide detailed input or physical description (as this is the actual Test Case/Script).

[SOW-109] The Contractor shall translate each requirement in the SRS, in an acceptance criteria that will clearly detail how the requirement will be fully met (clear pass/fail or yes/no outcome)

[SOW-110] The Contractor shall address the Purchaser's comments and update the Acceptance Criteria accordingly.

[SOW-111] The Acceptance Criteria shall be agreed by both Contractor and Purchaser prior to the creation of the Test Cases/ Scripts.

[SOW-112] The agreed Acceptance Criteria SHALL be translated into Test Cases to provide details of full requirements coverage

3.8.2.5 Requirements Traceability Matrix (RTM)

[SOW-113] The Contractor shall produce and maintain the Requirement Traceability Matrix (RTM), which includes all functional and non-functional requirements, to track the TV&V status of all requirements throughout the Contract execution (especially during the TV&V activities).The RTM shall also trace the requirements to the design. It shall also define how the requirements will be validated or verified at each of the TV&V activities:
(1) The verification method: Inspection, Analysis, Test or Demonstration
(2) Correspondent TV&V phase(s) for each requirement
(3) Coverage Status

[076] The Purchaser will review and approve the proposed RTM. In addition another document, called Operational Acceptance Traceability Matrix (OATM), shall be maintained by the Purchaser to trace the Operational Acceptance Criteria along the TVV activities execution.

[SOW-114] The Contractor shall maintain the RTM updated during the project lifecycle.

[SOW-115] The RTM shall be provided and maintained, extend this matrix to the [SW Only] Development Baseline, [/SW Only], Product Baseline / As-Built configuration and the Master Test Plan (MTP) to ensure verification throughout the project.

[SOW-116] The RTM shall guarantee the two-way link between requirements (SRS) and technical specifications.

[SOW-117] 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 the MTP. A workflow for updating the RTM shall be proposed by the Contractor and approved by the Purchaser.

[SOW-118] The Contractor shall verify each requirement using a verification method as defined in Annex A. Selected verification method for each requirement is subject to Purchaser approval.

[SOW-119] If the verification method per requirement is not provided beforehand, the verification method shall be either test or demonstration. Any deviation to this requirement is subject to Purchaser approval.

3.8.2.6 Operational Acceptance Traceability Matrix

[077] Operational Acceptance is the formal process, and decision, with respect to confirming whether or not a system/project satisfies the operational requirements, user needs and is sustainable over the course of its expected life.

[078] An Operational Acceptance Criteria (OAC) is a requirement that a system, project, service, or capability must satisfy in order to be accepted by a user, customer or other authorized entity.

[SOW-120] The purchaser will provide a collection of Operational Acceptance Criteria in the SRS and in an Operational Acceptance Traceability Matrix (OATM).

[079] The process for updating the OATM will be provided by the Purchaser and coordinated with the Contractor.

[SOW-121] For each OAC in OATM, the Contractor shall provide a proposal of evidence for achievement of the OAC. The proposal shall be approved by the Purchaser.

[SOW-122] The Contractor shall provide the Purchaser with updates (via the tools) to the OATM during the execution of an event, and following the conclusion of each event defined in the MTP.

3.8.2.7 STVP

[SOW-123] The Contractor shall produce an STVP, to ensure that the Security testing, including verification of compliance with NATO CIS Security Regulations is applied. This is an integral part of the TV&V process.

[SOW-124] The STVP shall support the accreditation of the System Platform. This document shall be approved by NATO Office of Security.

3.8.2.8 Test Completion Report

[080] The Test Completion Report provides a summary of the testing performed during the Test Event.

[SOW-125] The Contractor shall provide, in the Test Completion Report, a log/record of the event, including but not limited to individual test results, defects found (with a way forward for the ones remaining open), requirement coverage (planned and executed), test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

[SOW-126] The Contractor shall provide Contractor’s provisions and strategy for building/maintaining of the Reference Environment in MTP

3.8.2.9 Tools

[SOW-127] The Contractor shall generate and deliver automated test procedures/cases compatible with Purchaser test management and automation tools.

[SOW-128] 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-129] Tools supporting requirements coverage, defect management and test management shall be selected and hosted by the Purchaser and used by the Contractor. For any internal work, the Contractor may use their own internal tools, but the tools used for the Contractor’s internal work shall be able to natively interface with the tools selected and hosted by the Purchaser in order to keep all TV&V related data for the project in the Purchaser tools.

3.8.3 TV&V Events and Results

[SOW-130] The Contractor shall conduct testing during the Project lifecycle compliant with the following requirements:

(1) 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
(2) The Contractor shall conduct all testing activities for any architectural changes.
(3) The Contractor shall support post go-live activities during the Operational Acceptance phase, to evaluate the project capability performance and establish benchmarks for future enhancements, including any changes made to fulfil the requirements.
(4) The Contractor shall provide status reports to the Purchaser regarding verification and validation activities during the planning/design and development phases, via the use of a dashboard report within the test management tool set and through meetings. The Contractor shall provide report(s) to the Purchaser following the completion of any TV&V event.
(5) Test results shall be recorded in the test management tool set. All results of all formal acceptance testing performed during a given day must be recorded in the test management tool. The Contractor shall provide these test results for any given day by the starting of the next business day (0800 AM), but as a minimum not later than 24 hours following the execution of any test.

[081] The Purchaser will approve the report and its findings within two business days

[082] Progress and results measurement shall be approved by the Purchaser and focused on KPIs.

3.8.3.1 Test Readiness Review (TRR)

[SOW-131] The Contractor shall conduct a Test Readiness Review (TRR) meeting at least one week prior to the events defined in the MTP. The TRR shall ensure that all entry criteria for the events have been met. Documentation that requires review by the Purchaser prior to a TRR, as defined in the Event Test Plan (ETP), shall be provided no less than 2 weeks prior to TRR.

[083] 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-132] The Contractor shall demonstrate that all the internal tests and dry runs are successful with test reports and results delivered to the Purchaser at least 2 weeks prior to start of any Contractual test activities.

[SOW-133] Formal acceptance testing, including installation testing, shall be performed always on an environment with the up to date security settings, latest approved patches and antivirus applied and on a solution that has followed the security guidelines and policies.

3.8.3.2 Event Review Meeting

[084] The start and/or ending of any test session shall be subject to the Purchaser approval. In the event that critical issues are encountered which impact the process of the testing or if the other functions depends on the failed test cases, the Purchaser has the right to

stop the testing for Contractor's investigation. The tests can only re-start if Purchaser agrees to continue testing from the point of failure or re-start testing from the beginning.

[SOW-134] The Contractor shall convene an Event Review Meeting (ERM) as defined in the ETP. The ERM shall ensure that the event results, defect categorization and a way forward to fixing the defects (if required) is agreed between the Contractor and the Purchaser. If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Managers.

3.8.3.3 TV&V Event

[085] An event starts with the Test Readiness Review (TRR) and finishes off with the Event Review Meeting (ERM).

[SOW-135] During formal TV&V phases, a daily progress debrief shall be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.

[SOW-136] For each TV&V event, the Contractor shall provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

[SOW-137] At the end of the project, the Contractor shall provide the final version of all artefacts (regardless of format) created during the execution of all TV&V activities.

3.8.3.4 Reference environments

[SOW-138] 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-139] The Contractor shall ensure that all test/reference environments are under proper configuration management, especially configuration control. The Configuration Management toolset and process shall be approved by the Purchaser.

[SOW-140] Formal verification and validation activities, including formal integration testing, shall be executed on the reference environment.

3.8.3.5 Test Waivers

[086] The Contractor may request a Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. The Purchaser, after review of test waivers and analysis of their impact, reserves the right to require test and certification of the modified equipment at no cost to the Purchaser. The Purchaser has the right to reject any test Waiver.

[SOW-141] In respect to a requested Test waiver, the Contractor shall certify that the test environment to be implemented is identical to that which was originally used for testing, or inform the Purchaser of design/construction changes which affect form, fit or function.

[SOW-142] The Contractor shall record and log all waiver requests along with their resolution submitted for the Purchaser's approval.

3.8.3.6 Failed Events

[SOW-143] In the event of failed TV&V event and the need to return to a site for re-testing; travel and per diem expenses of NATO personnel shall be borne by the Contractor

3.8.4 Test Types

[087] Depending on the WP certain test types are to be performed. Section 4 documents the required test types for each WP.

3.8.4.1 System Integration Testing

[088] The purpose of system integration testing (SIT) is to validate the baselines coexistence with other capabilities and services, and test the dependencies between them. With multiple integrated capabilities, assuming that each has already passed system testing, system integration testing proceeds to test the required interfaces and interactions.

[089] The Purchaser will observe the system integration testing and reserves the right to participate in executing test cases to confirm compliance and to conduct its own test case verification after demonstration of a test case by the Contractor.

[090] Coalition Interoperability Assurance and Validation (CIAV) testing will be part of the system integration testing phase.

[SOW-144] The Contractor shall perform a test readiness review prior to conducting system integration testing.

[SOW-145] The Contractor shall develop for test artefacts in coordination with Purchaser SMEs.

[SOW-146] The test cases shall be based on operationally realistic test scenarios, with representative test data in terms of structure, content and size to emulate real-word conditions.

[SOW-147] The test cases, supported by the test scenarios, shall cover all internal and external interfaces delivered by a baseline to verify and validate the interoperability between them.

[SOW-148] The Contractor shall plan, prepare, organise and conduct system integration testing for each baseline, which shall take place at one of the Purchaser's facilities, using a Purchaser-specified integration test bed or operating environment.

[SOW-149] The Contractor shall conduct system integration testing dry-runs with Purchaser SMEs, prior to conducting the system integration testing.

[SOW-150] The Contractor shall deliver an updated baseline release that incorporates defect corrections and the lessons-learned from the system integration testing.

3.8.4.2 Data Migration Testing

[091] The purpose of data migration testing (DMT) is to validate the proper migration of data from the legacy C2 system (LC2IS) to DEMETER.

[092] The Purchaser will observe the data migration testing and reserves the right to participate in executing test cases to confirm compliance and to conduct its own test case verification after demonstration of a test case by the Contractor.

[SOW-151] The Contractor shall perform a test readiness review prior to conducting data migration testing.

[SOW-152] The Contractor shall develop for test artefacts in coordination with Purchaser SMEs.

[SOW-153] The Contractor shall plan, prepare, organise and conduct data migration testing for WPs 1 and 2, which shall take place at one of the Purchaser's facilities, using a Purchaser-specified integration test bed or operating environment.

[SOW-154] The Contractor shall conduct data migration testing dry-runs with Purchaser SMEs, prior to conducting the data migration testing.

The Contractor shall deliver an updated baseline release that incorporates defect corrections and the lessons-learned from the system integration testing.

3.8.4.3 IVVQ

[093] IVVQ acts as a final verification of the required operational functionality as defined in the contracted requirements and proper functioning of the capability. It proves to the users that the capability is working according to their understanding of their own operational requirements and validates the fitness for purpose of the capabilities delivered.

[SOW-155] The Contractor shall plan, prepare, organise and conduct this test, which shall take place at one of the Purchaser's facilities.

[SOW-156] The Contractor shall develop test artefacts in coordination with Purchaser SMEs and representatives of the operational community.

[SOW-157] The test cases shall use operationally realistic test scenarios, with representative test data in terms of structure, content and size to emulate real-word conditions.

[SOW-158] The test cases, supported by the test scenarios, shall cover the scope delivered by a baseline to ensure that the requirements as contracted are met.

[SOW-159] The test cases, supported by the test scenarios shall be designed such that it enables IVVQ to validate the software acceptance criteria.

[SOW-160] The Contractor shall perform a test readiness review (see section prior to conducting IVVQ.

[SOW-161] IVVQ shall be conducted by representatives of the operational community, IVVQ and Purchaser SMEs; Contractor personnel shall support them.

3.8.4.4 CRQ Testing and Security Testing

[094] All software releases to be used on NATO networks will undergo a release management process, initiated by submitting a change request (CRQ), and will be subject to CRQ testing and Security testing.

[095] CRQ process guidance is included in NCI Agency technical instructions and standard operating procedures [NCIA-AI-23.02], [NCIA-SOP-06.03.05] and [NCIA-SOP-23.01]. The CRQ process also applies to patch and corrective baseline releases.

[096] The purpose of the IV&V testing is to demonstrate that the baseline release is compliant with the NATO network policies and meets the security requirements for use on NATO networks managed by the NCI Agency. The objective is to have the baseline release approved and included in the Agency Approved Software List (A2SL).

[097] The process of IV&V testing is anticipated to take 6-8 weeks from submitting the baseline change request.

[098] Independent security penetration testing will be conducted by the Purchaser as part of the A2SL admission process.

[SOW-162] The Contractor shall be responsible for successfully obtaining the A2SL approval allowing use of the baseline release on the NATO networks (NS, NR and NU).

[SOW-163] If any major software frameworks (operating system, database, or runtime environment) are added to the COTS at any point in time, the Contactor shall be responsible for obtaining separate approvals for addition to the A2SL of these frameworks.

[SOW-164] The Contractor shall cover all applicable threat types and corresponding security test cases (e.g. Unauthorized user/Fake identity/Password cracking; Cross-site scripting (XSS); Buffer overflows; URL manipulation; SQL injection; Denial of service) within its security testing. Refer to Annex A for further details.

[SOW-165] The Contractor shall support the Purchaser with submitting the CRQ to the CRQ Governance Board and deliver all required artefacts in support of the change request. These include:

(1) Release of the COTS, including third-party software as required;
(2) Standard operating procedures user manual;
(3) Installation and configuration manual;
(4) Maintenance and administration manual;
(5) Test reports;
(6) Release notes;
(7) Release and deployment plan; and
(8) Support plan.

[SOW-166] The Contractor shall use the latest Purchaser templates for request for changes and artefacts in support of it.

[SOW-167] In case third-party software is used for the baseline, the Contractor shall deliver the software, licences and warranty documentation to the Purchaser prior to the submission of the request for change.

[SOW-168] In order to allow deployment of a pre-release, for example for use during a workshop or user acceptance testing, the Contractor shall support the Purchaser with submitting the change request to the CRQ Governance Board for a limited authorization to operate (LATO) and deliver all required artefacts in support of the change request.

[SOW-169] The Contractor shall support, if necessary at Purchaser facilities, the IV&V testing, and security testing performed by the Purchaser for each release submitted through the CRQ process.

[SOW-170] In order to avoid delays in obtaining A2SL due to failure in testing or vulnerabilities, the Contractor shall prepare and support pre-testing of the baseline release.

[099] The Purchaser will provide the Contractor with a test report after conclusion of each test session, documenting the test results. Any failures and possible remedial actions will be indicated.

The Contractor shall resolve any discrepancies and vulnerabilities and support additional independent verification and validation testing required to verify these fixes.

3.8.4.5 Coalition Interoperability Assurance and Validation

[100] CIAV will be used in order to validate FMN compliance of DEMETER.

[SOW-171] The Contractor shall be responsible for obtaining FMN approval through CIAV test event(s). Refer to Annex A for further specifications.

3.8.4.6 Site Acceptance Testing

[101] The purpose of the site acceptance test (SiAT) is to validate the proper working of the system after installation on each site.

[102] Therefore, it is not the intention of the SiAT to repeat all tests already done.

[103] The Purchaser will observe the SiAT and reserves the right to participate in executing test cases to confirm compliance and to conduct its own test case verification after demonstration of a test case by the Contractor.

[104] Testing the COTS in an exercise will be part of the SiAT.

[SOW-172] The Contractor shall perform a test readiness review prior to conducting site acceptance testing.

[SOW-173] The Contractor shall develop for test artefacts in coordination with Purchaser SMEs.

[SOW-174] The test cases shall be based on operationally realistic test scenarios, with representative test data in terms of structure, content and size to emulate real-word conditions.

[SOW-175] The test cases, supported by the test scenarios, shall cover the main functions and interfaces of DEMETER to proof that the installation on site has been successful.

[SOW-176] The Contractor shall plan, prepare, organise and conduct site acceptance testing for each baseline, which shall take place at one of the Purchaser’s facilities, using a Purchaser-specified integration test bed or operating environment.

[SOW-177] The Contractor shall conduct site acceptance testing dry-runs with Purchaser SMEs, prior to conducting the site acceptance testing.

[SOW-178] The Contractor shall deliver an updated baseline release that incorporates defect corrections and the lessons-learned from the system integration testing.

3.9 Configuration Management

[SOW-179] The Contractor shall implement a configuration management process consistent with [ACMP-2100] and the additional guidelines from ACMP standards within [STANAG-4427] and [NCIA-AD-06.00.16].

[SOW-180] The Contractor shall deliver a Configuration Management Plan (CMP) compliant with Section 8.10, document its configuration management processes and describe how it intends to meet the configuration management requirements of the Contract.

[SOW-181] The CMP, when accepted, shall serve as a working document to plan, guide, and measure the configuration management process.

[SOW-182] The Contractor shall perform configuration management using the Azure DevOps tools furnished within the NSF. Any configuration management requirements that cannot be fulfilled due to limitations of the furnished Azure DevOps tools, shall be met by alternative means or tools by the Contractor with the approval of the Purchaser.

[SOW-183] The Contractor shall allow the Purchaser access these tools for viewing and extracting configuration information.

[SOW-184] The Contractor shall establish and maintain three (3) configuration baselines for each work package release (ref [NCIA-AD-06.00.16]), as follows:
(1) Functional Baseline (FBL or “as required”);
(2) Allocated Baseline (ABL or “as designed”);
(3) Product Baseline (PBL, or "as built”).
See Section 3.9.1 for specifications of the configuration baselines.

[SOW-185] The Contractor shall identify and define all top-level configuration items to be delivered under this Contract.

[SOW-186] The top-level configuration items shall be broken down into a tree/hierarchy of its parts and sub-parts consisting of deliverables, the relevant documentation of these deliverables, all dependent third-party components and libraries and respective documentation.

[SOW-187] The configuration items shall be organized around working and executable software units (i.e. applications or executable services) and each configuration item shall be assigned a unique identifier.

[SOW-188] The Contractor shall establish a Configuration Management Database (CMDB) that persists the configuration items attributes, (inter-) relationships, dependencies, and configuration baselines. The CMDB shall be maintained in sync with the NSF.

[SOW-189] The CMDB shall have support for tracing higher and subordinate configuration items using their identifiers or other attributes.

[SOW-190] The Contractor shall ensure that the configuration baselines and configuration items are persistently stored, maintained and managed throughout the period of performance of the Contract.

[SOW-191] It shall be possible from the CMDB, at any time, to generate Configuration Status Reports for any specified baseline where the report provides a full history on all configuration items in the baseline including information on changes, deviations, waivers, releases, etc.

[SOW-192] The CMDB and configuration management tools shall support generation of Configuration Status Accounting (CSA) reports in a readable and structured document format (Microsoft Excel or Word format).

[SOW-193] A baseline in the CMDB shall:
(1) Be defined by version controlled artefacts that all resides in the proper repositories in the NSF;
(2) Include any (off-the-shelf) software and (off-the-self) software license(s) where all software license(s) shall be registered with the NCI Agency as the end-user;
(3) Include all (supporting) documentation, e.g. off-the-shelf OEM manuals, operations and maintenance support documentation, training documentation, quality assurance documentation, security documentation, configuration management documentation, and warranty documentation.

[SOW-194] It shall be possible from the CMDB and configuration management tools to generate a package (as one or several electronic files) with all the artefacts included in a PBL release.

[SOW-195] The configuration management tools using the CMDB shall have support for comparison of baselines and precisely identify the changes to the individual items from one baseline to the other (including versions of third-party software components and libraries).

[SOW-196] The Contractor shall be responsible for the Configuration Status Accounting (CSA) and reporting for all configuration items.

[SOW-197] The Contractor shall perform Configuration Audits to check configuration items for compliance with their configuration documentation:
(1) Functional Configuration Audit (FCA) for which the inputs are the Functional Baseline, the Allocated Baseline and the Product Baseline. The output is the Audit Conformity Report.
(2) Physical Configuration Audit (PCA) for which the inputs are the Product Baseline and the Service Baseline. The output is the Audit Conformity Report.

[SOW-198] The Contractor shall invite the Purchaser's configuration management representative to the PCA and FCA with a minimum of two weeks' notice. When the Purchaser attends an audit, the Contractor shall answer any specific questions directed by the Purchaser's representatives, and shall record the minutes of the audit meeting.

[SOW-199] The Contractor shall solve any deficiencies found during the configuration management audits within the agreed timeframe and update the baseline accordingly.

[SOW-200] The Contractor's Product Baseline (PBL) version numbering strategy shall be compliant with [NCIA-AI-TECH-06.03.01].

3.9.1 Configuration Baselines

[SOW-201] Functional Baseline: The Functional Baseline (FBL) shall be derived from the software requirements specifications and shall be established at the successful completion and accepted incremental baseline allocation.

[SOW-202] Allocated Baseline: The Allocated Baseline (ABL) reflects the "as-designed" configuration of the system and its conformity to the Functional Baseline.

[SOW-203] Product Baseline: The PBL shall be established after successful completion of the incremental development phase. It shall contain all delivered configuration items that comprise the baseline. It reflects the “as-built” configuration of the system. Besides the product itself, the PBL shall comprise:

(1) System documentation artefacts, including the installation and configuration manual, maintenance and administration manual, coherent with the baseline release;
(2) User documentation artefacts, including online help, standard operating procedures manual and training materiel, coherent with the baseline release; and
(3) A product description document and the interface control document (ICD), coherent with the baseline release.

[SOW-204] Where incremental development with multiple deliveries approach is used (WP3), the Contractor shall establish the first PBL for the first released product, and the second PBL for the second release combining the first release functionalities with the additional ones.

3.9.2 Change Proposals

[105] In compliance with ACMP-2009, the Purchaser-led Change Control Board (CCB), will govern the configuration change process by reviewing and deciding on the Change Proposals. The relevant Contractor representatives will be invited to the CCB for consultation.

[106] Change Proposals are proposals for changes relevant to tasks, deliverables, requirements, processes, or any other term of the Contract, which are submitted in written form by the Contractor independently, or upon request from the Purchaser, when such changes are necessary in light of varied facts or circumstances, which prevent the execution of the Contract in its form.

[SOW-205] The Contractor shall prepare and submit change proposals to the CCB for approval that are compliant with the template provided in Annex D.1.

[SOW-206] When approved, the Contractor shall implement the change proposal.

[SOW-207] The Contractor shall place all submitted change proposals under configuration control.

3.9.3 Requesting Deviations/Waivers

[107] A Request for Deviation (RFD) is defined as "planned departure" from a specific requirement with "departure" defined as the "inability of a product to meet one of its functional performance or technical requirements".

[108] A Request for Waiver (RFW) is defined as "unplanned departure" from a specific requirement.

[SOW-208] When required, the Contractor shall prepare and submit request for deviations/request for waivers to the Purchaser for approval that is compliant with the template provided in Annex D.2.

[SOW-209] The Contractor shall submit permanent departures from contractual requirements by means of a change proposal rather than by request for deviation.

[SOW-210] The Contractor shall place all submitted RFDs/RFWs under configuration control.

3.10 Quality Assurance

[SOW-211] The Contractor shall establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the Contract's lifetime conform Section 8.11.

[SOW-212] The QA programme shall apply to both the contractual requirements and to the appropriate AQAPs which apply to the contract according to [STANAG-4107] to provide confidence in the Contractor's ability to deliver products that conform to the Contractual requirements.

[SOW-213] If any inconsistency exists between the SOW requirements and the references, the SOW requirements shall prevail.

[SOW-214] The Contractor‘s QA effort shall apply to all services and products (both management and specialist) to be provided under the Contract. This includes all hardware, software, firmware and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract (including deliverable and non-deliverable items like test and support hardware and software), without limitation.

[SOW-215] The Contractor‘s QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.

3.11 Defect Management Process

[SOW-216] The Contractor shall use the Purchasers' categorization nomenclature for all defects and non-compliances

[SOW-217] Should a failure occurs during a TV&V event/activity a defect shall be recorded in the Agency's' test management and defect management systems. Once the event has concluded, the defect shall be reviewed during the event review meeting to agree on the severity, priority and category. The event test report shall then report the disposition of all defects recorded during the event and the defect management system shall be updated accordingly. Classification shall follow the definitions in the table below:

Table 3.3 - Definitions for Defect Categorization

Attributes	Definition
Severity	The severity of a defect is the degree of impact that the failure has on the development or operation of a component, a system or a user function. The severity shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached, the Purchaser's PM will set the severity.
Priority	The priority of a defect defines the order in which defects shall be resolved. The priority of the defect shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached, the Purchase's PM will set the priority.

Category	The type of observation identified during the execution of a test case.

[109] For the independent penetration/security tests, the Purchaser will provide an approved list of defects along with their Test Report.

[110] An individual test will be a failure if a critical or major defect is discovered.

[111] The test will be repeated for all failures when the associated defects are fixed.

[112] The overall test event will fail if there is one or more Critical or Major defects discovered. The test event will pass if there are no Critical and Major defects.

[SOW-218] All defects shall be entered to the testing tool of preference and will be tracked through this tool. Failures shall also be recorded in the Quality Log.

[SOW-219] The Contractor shall include the failures in the Test Report (individually identified to ensure traceability and with sufficient detail to ensure reproducibility) and carry out a preliminary investigation to classify the severity of the failure as one of the levels shown in Table 3.4.

3.11.1.1 Severity

[SOW-220] According to their severity, defects shall be classified as one of the following in Table 3.4:

Table 3.4 – Classification of defects based on severity

LEVEL	IMPACT	WORK-AROUND AVAILABLE	DEFINITION
1	**CRITICAL**	No	***Causes all testing to be halted – top priority to fix. The test execution schedule is compromised.*** A critical failure for which an acceptable work around does not exist. The defect totally prevents the system from performing operational processes and/or causes unrecoverable data loss. Applies to conditions under which one or more components are inoperative and jeopardize the ability to continue using the system. This condition generally is characterized by a complete or catastrophic system failure and requires immediate restoration or correction.
2	**MAJOR**	Yes	***Causes one or more areas of functional testing to be halted but with some other functional areas tests unaffected.*** Test executed during this situation would likely require retesting when the blocking defect is fixed. The test execution schedule is likely to be compromised. A significant failure that causes severely impaired functions but does not prevent operational processing. Applies to conditions under which one or more components are partially inoperative, but are still usable by the users. A workaround might be available but it may require manual intervention.
3	**MODERATE**	Yes	***Causes tests of none, one or a few less significant functional areas to be halted until a fix is available. Most testing continues and the execution schedule is unlikely to be adversely impacted.***

			A functional failure that causes a specific aspect of the system to fail. There is a reasonably satisfactory work around which can be used during normal operations for a limited period of time. The system may be released provided the defect and work around is documented. Applies to conditions under which one or more components are usable with limited functions, but creates a manageable situation with respect to the normal operations. A work around is available and does not require any manual intervention.
4	**MINOR**	Yes	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.
5	**COSMETIC**	Yes	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.

3.11.1.2 Priority

[SOW-221] According to their priority, defects shall be classified as one of the following in the table below:

Table 3.5 - Priority Classes for Defect Classification

Priority	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.

3.11.1.3 Category

[SOW-222] According to their category, defects shall be classified with one of the values defined in the table below:

Table 3.6 - Defect 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 defects encountered in the system documentation (test cases, test procedures, RTM, test plan, manuals, design, procedures…).

Category	Description
Clarification	This category is used to record deficiencies encountered during the test execution, which must be clarified.
Waiver	This category is used to record when a waiver is required to address a specific observation or defects.

3.12 Audits

[113] The Purchaser reserves the right to perform reviews and quality audits at any of the Contractor facilities.

[114] Review and audit activities do not relieve the Contractor from any contractual quality responsibilities.

[SOW-223] The Contractor shall periodically, at least once a year, review the QA programme and audit it for adequacy, compliance and effectiveness.

[SOW-224] The Contractor shall make available to the Purchaser's QA personnel and auditors all information and artefacts deemed necessary to perform reviews and quality audits, on their own initiative or on request by the Purchaser.

[SOW-225] The Contractor shall fully support the Purchaser in performing reviews and quality audits at any of the Contractor facilities and activities and in particular:

(1) Make available the necessary Contractor personnel for coordination meetings prior, during and post quality audit inspection visits and for answering questions and furnishing information related to the Contract;
(2) Host inspection visits by Purchaser's QA personnel and auditors; and
(3) Allow the Purchaser's QA personnel and auditors to inspect and monitor the Contractor's processes applicable to this Contract.

4 Work Packages 1, 2 and 3: Delivery of DEMETER

4.1 Approach

[115] The required capabilities will be delivered in accordance with the contracted requirements.

[SOW-226] The Contractor shall be responsible for the deployment of DEMETER to the NATO operational networks and test and integration environments, and implement the capabilities throughout the NCS, under the supervision of and with support from the Purchaser.

[116] Successful conclusion of a WP is marked by the PSA of that WP.

[117] The transition phase will focus on ensuring an efficient migration from the existing Land C2 system to DEMETER, with continuity of service and minimal degradation of services during the transition.

[118] The PSA of WP2 will be followed by the closure phase during which the Purchaser will conduct the final validation of all deliverables and verify fulfilment of contractual obligations. The closure phase is concluded with the FSA, which also indicates the start of the one-year warranty period.

[SOW-227] Starting with the PSA of WP1, the Contractor shall be responsible for maintenance and support until FSA is achieved.

[119] After FSA, the Purchaser assumes full responsibility, with the exception of Contractor furnished maintenance and support services under warranty and during the optional maintenance and support services provided post FSA if the Purchaser decides to exercise the option.

[120] The sections below describe all activities and requirements for WPs 1, 2 and 3. If a section does not apply to any of these three WPs, it is indicated for which WP(s) it is applicable.

4.1.1 Work Package 1

[121] Figure 4.1 below represents the order of events for WP1.

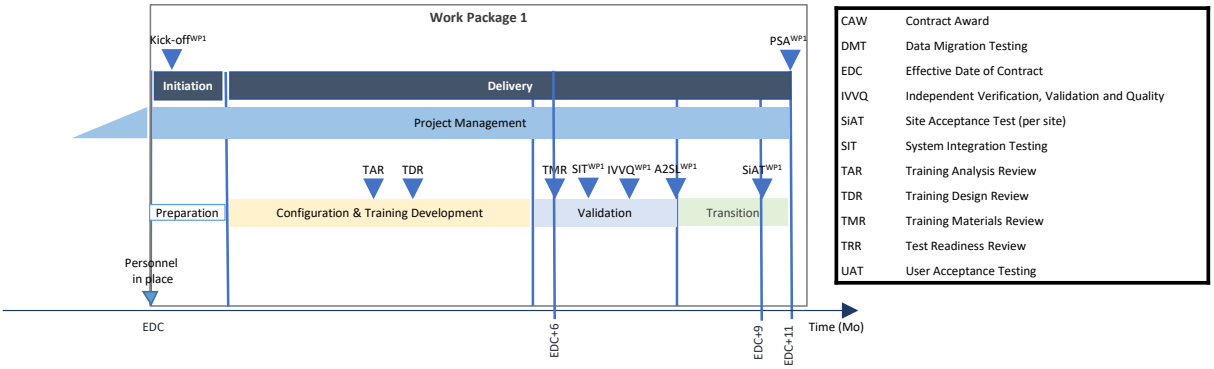

Figure 4.1 – WP1 Delivery of DEMETER to the initial sites and Training

[122] The configuration phase will be followed by a validation phase, starting with system integration testing, then the IVVQ and security testing prior to deploying the baseline to

the operational environment and the SiAT, which will be conducted in a NATO exercise.

[123] During the transition phase, the Contractor will also provide support and deliver training for the new capabilities to the different user communities after preparing/adapting the material in the previous phases.

4.1.2 Work Package 2

[124] WP2 will commence with an initiation phase and kick-off meeting as shown in Figure 4.2.

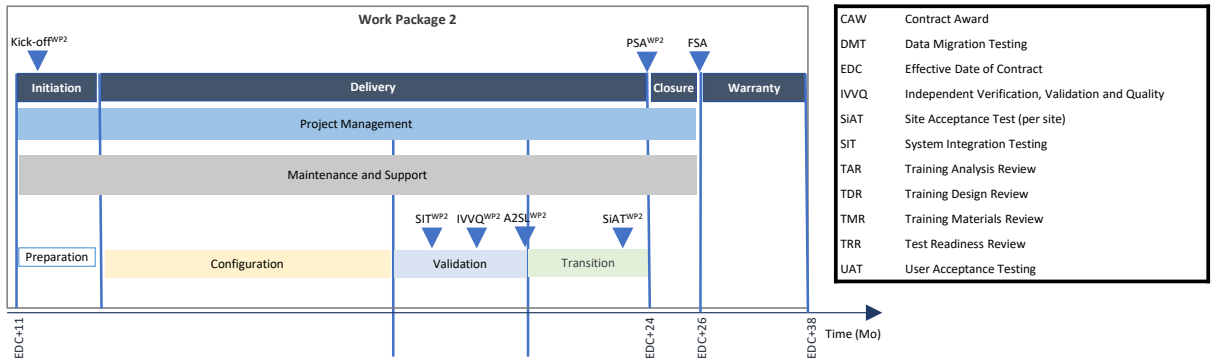

Figure 4.2 - WP2 Delivery of DEMETER to all remaining sites

[125] The Contractor will deliver maintenance and support on the licenses delivered in WP1.

[126] It is anticipated that a new version of the COTS will be available for WP2 and that interfaced systems may have changed. To cater for this, there will be a configuration phase, followed by a validation phase and a transition phase similar to WP1.

[127] The Contractor will deliver one year warranty starting at FSA.

4.1.3 Work Package 3

[128] Figure 4.3 illustrates the activities for the optional WP3.

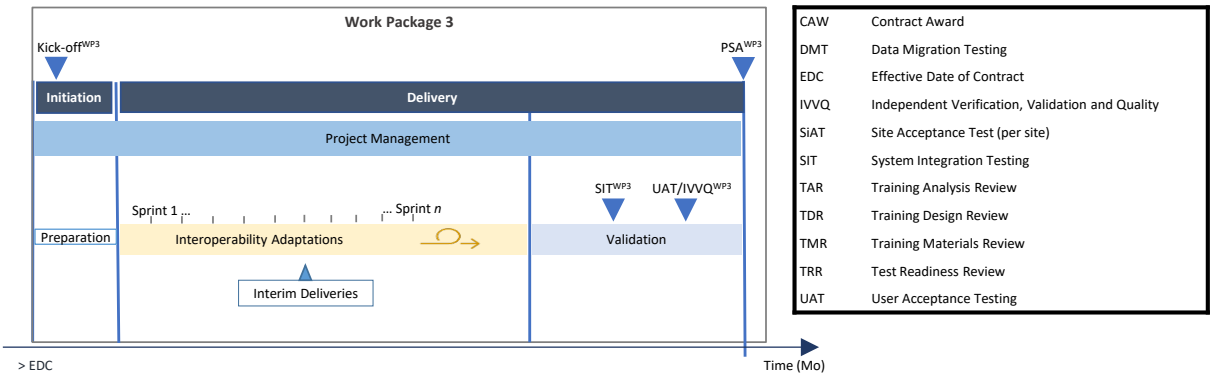

Figure 4.3 – WP3 Optional implementation of interoperability adaptations

[129] The delivery phase of WP3 consists of design and build of the interoperability and other adaptations, as well as a validation phase.

[130] The process for inclusion in the A2SL and deployment of the deliverables from WP3 will be part of WP2; the activities to be performed for this are included in the Validation

and Transition phases of WP2. Any additional costs related to WP3 must be included in the WP3 costing.

4.2 Initiation Phase

[131] The objective of the initiation phase is to start the work, to review the Contractor's approach and to make the necessary preparations for the next phase, including completion of knowledge transfer from the Purchaser to the Contractor as well as conducting site surveys of the sites involved.

[132] A kick-off meeting will be held at the start of the phase and this is where the Purchaser and Contractor Team review the Contractor's plans and approach to the development and delivery of the capabilities.

[133] Some of the goals associated with this phase are:
(a) Verify that the Contractor's project resources are assigned in line with defined qualification requirements and have completed the required knowledge transfer to start the work;
(b) Verify the Contractor's access to the NSF; and
(c) Validate the Contractor's proposed plans.

4.2.1 Kick-off Meeting

[SOW-228] For WP1, the Contractor's key personnel shall meet with the Purchaser's project team for a kick-off meeting within four weeks after CA.

[SOW-229] For WP2, the Contractor's key personnel shall meet with the Purchaser's project team for a kick-off meeting within one week after the start of the initiation phase of WP2.

[SOW-230] For WP3, the Contractor's key personnel shall meet with the Purchaser's project team for a kick-off meeting within one week after the start of the initiation phase of WP3.

[SOW-231] For WP1, the Contractor shall deliver to the Purchaser no later than two weeks prior to the start of the kick-off meeting the meeting invitation, including agenda and the following Contractor documentation:
(1) PMP, including PMS (Section 6.4);
(2) RAID Register, with populated Risk Register (Section 6.5);
(3) Deliverable Requirements Traceability Matrix (DRTM) (Section 8.13);
(4) Training Plan (Section 4.3.2.1);
(5) Configuration Management Plan (Section 6.6);
(6) Quality Plan (Section 8.11);
(7) Master Test Plan (Section 3.8.2.1); and
(8) Integrated Product Support Plan (Section 8.12).

[SOW-232] For WP2 and WP3, the Contractor shall deliver updated versions of abovementioned documents.

[SOW-233] During the kick-off meeting, the Contractor shall provide an introduction and present its PMP, its approach and schedule. The Contractor's presentation shall:
(1) Demonstrate that the schedule is realistic and that a team of skilled personnel has been allocated that matches the identified resource qualifications; and
(2) Demonstrate the initial DRTM.

[134] During the kick-off meeting, the Purchaser shall provide feedback to the Contractor on the provided information and the documentation submitted prior to the meeting. The agenda should include sufficient time to discuss each of the artefacts.

4.2.2 Site Surveys (WP1 and WP2)

[SOW-234] The Contractor shall conduct site surveys in order to gather all information needed for successful execution of this project.

[SOW-235] The Contractor shall prepare and deliver site survey reports, summarizing the conclusions of the surveys and highlighting any actions or support to be delivered by the Purchaser.

4.2.3 Entry and Exit Criteria

[SOW-236] The Contractor shall comply with the following entry criteria for the initiation phase:

(1) The Contractor has delivered to the Purchaser a named-list of project team members;
(2) Contractor resources and personnel are in place to commence the initiation phase;
(3) The Purchaser has no concerns with the key personnel and project team composition;
(4) The planned knowledge transfer to Contractor personnel during the ramp-up period has been completed; and
(5) The Contractor has delivered to the Purchaser no later than two (2) weeks prior to the start of the kick-off meeting, the meeting invitation and Contractor documentation.

[SOW-237] The Contractor shall comply with the following exit criteria for a successful conclusion of the initiation phase:

(1) The kick-off meeting has been held and the submitted meeting minutes are accepted by Purchaser;
(2) Contractor resources and personnel are in place to commence the next phase;
(3) The Purchaser comments/concerns regarding the plans and documentation have been addressed, there are no pending concerns and the documents have been baselined; and
(4) The Risk Register and the Issue Register, as part of the RAID Register are properly initialized with manageable risks and issues, and contains suitable mitigation/action plans. Action items and decisions have been recorded.

[135] If the Contractor fails to meet the exit criteria, then the Purchaser will not give the Contractor the permission to proceed.

4.3 Delivery Phase

[136] The delivery phase for WPs 1 and 2 consist of configuration, validation and transition phases.

[137] Training development and delivery is part of the delivery phase of WP1.

[138] The delivery phase for WP3 consists of the design and build of contracted interoperability adaptations on an NCI Agency approved integration platform (e.g. SOA-IdM or IntCore), other adaptations and validation.

[139] In order to conduct verification and validation activities, the Contractor will deploy, in coordination with the Purchaser, the configured DEMETER release onto the NATO test and integration environments and if needed to the NATO operational network (for sites see Section 4.3.5.1).

4.3.1 Configuration (WP1, WP2)

[140] Based on the results from the site surveys, the Contractor will configure the COTS to be able to work on the NATO Networks at the specified site(s).

[SOW-238] The Contractor shall configure and dry-run test DEMETER, implementing and satisfying the contracted requirements.

[141] There is a set of operational overlays that form the Recognised Ground Picture (RGP). These are LC2IS formatted data that require migration to DEMETER. Refer to [XSD-LC2IS] for the XSD of the overlays to be migrated.

[142] Also LC2IS users and roles need to be migrated.

[SOW-239] The Contractor shall design and develop migration scripts to migrate the following from the current Land C2 system to DEMETER:
(1) Overlays
(2) Users and roles

[SOW-240] The Contractor shall comply with the following entry criteria:
(1) The Contractor has concluded the previous phase successfully.

[SOW-241] The Contractor shall comply with the following exit criteria for a successful conclusion:
(1) The Contractor shall present the successful results of test dry-runs conducted by the Contractor.

4.3.2 Training (WP1)

[143] Accompanied with the deliveries of WP1, the Contractor will develop and provide training for users, support staff and trainers of the capabilities of new DEMETER application.

[144] Section 8.9.2 discusses training related definitions.

[SOW-242] The Contractor shall plan, execute and control the DEMETER Training Process as defined in [NATO-Bi-SC-DIR-075-007].

[SOW-243] The Contractor shall perform the Training Needs Analysis (TNA) to justify all the training activities for DEMETER.

[SOW-244] The Contractor shall apply the NATO Systems Approach to Training as defined in [NATO-Bi-SC-DIR-075-007]. The Contractor shall perform all required analysis, design, development, implementation and evaluation tasks according to the guidance provided in [NATO-Bi-SC-DIR-075-007].

[SOW-245] The Contractor shall provide DEMETER training for users, support staff and trainers (train the trainer) through a combination of face-to-face, live online, self-paced online, hybrid or blended learning in accordance with the Maintenance and Support Concept described in Section 8.12 and in line with [NATO-Bi-SC-DIR-075-007] and DEMETER specific training requirements

[SOW-246] The Contractor shall demonstrate that all required personnel has been trained in accordance with the training plan.

[SOW-247] The Contractor shall be able to design, develop, deliver and perform the following types of training:
(1) Face-to-face;
(2) Live online;
(3) Self-paced online;
(4) Hybrid Learning; and
(5) Blended Learning
The exact distribution and weight of the different training methodologies shall be proposed based on the TNA results for Purchaser approval, and updated as requested by the Purchaser.

[SOW-248] The Training Courses shall utilise a combination of lecture and hands-on exercises to ensure students completing a course can perform to the level agreed to in the Training Plan.

[145] The Purchaser will provide if required the following basic facilities: rooms, power supply, tables, chairs, network connectivity.

[SOW-249] 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 Training activities.

[SOW-250] The Training Courses shall be provided on the training version of the databases, without interference to operational activities.

[SOW-251] The DEMETER Training Courses shall provide training for the various categories of roles based on the TNA or specific direction from the Purchaser.

[SOW-252] The Contractor shall develop and maintain a Training Plan and associated materials and activities as defined in the next sections.

4.3.2.1 Training Plan

[SOW-253] The Contractor shall develop and maintain the DEMETER Training Plan as described in Section 8.8.

[SOW-254] The Training Plan shall be updated as required accordingly with the TNA development and finalization.

[146] The acceptance of the Training Plan 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-255] The Contractor's Training Plan shall guide all the activities, milestones and actors associated with the Training of DEMETER.

4.3.2.2 Training Need Analysis

[SOW-256] The Purchaser will establish a Training Needs Analysis Working Group (TNA WG) to which the Contractor shall appoint his own personnel with the appropriate subject matter expertise. The TNA WG shall conduct assigned TNA tasks in line

with [NATO-Bi-SC-DIR-075-007]. The TNA tasks for the TNA WG shall include as a minimum:
(1) Target Audience Analysis;
(2) Task Analysis;
(3) Development of performance and Learning objectives; and
(4) Training Strategy proposal.

[SOW-257] The Training design shall be based on the results of the TNA to be performed by the TNA WG.

[SOW-258] The TNA WG shall identify the required prerequisites for training participants, as part of the TNA.

[SOW-259] The TNA WG shall base the scope, delivery methods, and duration of DEMETER training and materials on the TNA. The contractor shall update the Training Plan based on the results of the TNA.

[SOW-260] The Contractor shall provide its organization, methodology and procedures within the Training Plan for Purchaser approval. This shall include the details for the planning and execution of Task Analysis, Difficulty, Importance and Frequency (DIF), GAP, user engagement methods (e.g. surveys, questionnaires, working groups etc.) and other activities as applicable.

4.3.2.2.1 Target Audience Analysis

[SOW-261] The Contractor shall conduct a Target Audience Analysis in accordance with [NATO-Bi-SC-DIR-075-007], utilizing any information already determined by the Purchaser Training Staff and produce a summary population table.

[SOW-262] The Contractor shall assess the current skills of operational staff that will use/operate DEMETER and the importance and difficulty of tasks via discussions with Purchaser-identified experts.

4.3.2.2.2 Task Analysis

[SOW-263] The Contractor shall conduct a Task Analysis in accordance with [NATO-Bi-SC-DIR-075-007], to identify and list all user/operator and maintenance tasks for each system, subsystem and integrated system and to provide a structured and sequenced diagram of performance statements including specific tasks, subtasks and supporting task elements.

[SOW-264] The Task Analysis shall include identified roles of users who will use DEMETER to accomplish their tasks.

[SOW-265] The Task Analysis shall include a DIF Analysis to determine the priority and training effort to be applied to the Performance Objectives (PO).

[SOW-266] The DIF analysis shall identify the difficulty and importance of each major task to be performed by each category of roles and the frequency with which the task will be performed.

[SOW-267] The Task Analysis shall refine a prior developed (as part of a Training Requirements Analysis (TRA) Report), or perform a new Performance Gap Analysis to assess the gap between the current skills of the target audience and the tasks they will be expected to perform in the use and support of the system, in order to determine which performance gaps can be addressed by training.

4.3.2.2.3 Performance Objectives

4.3.2.2.4 The contractor shall develop Performance Objectives for those tasks for which trainable performance gaps have been determined and document them in accordance with Annex J of [NATO-Bi-SC-DIR-075-007].

4.3.2.2.5 The contractor shall document the results of the analysis in the Course Control Document II (CCD II) - Course Proposal in accordance with [NATO-Bi-SC-DIR-075-007], Chapter 5 and Annex L.

4.3.2.2.6 Training Strategy

[SOW-268] The Contractor shall develop a Training Strategy for each course as identified as a requirement and document them in accordance with [NATO-Bi-SC-DIR-075-007], Chapter 5. The Training Strategy shall address how the DEMETER training requirements will likely be resolved, including an estimate of the duration for a course and the annual production, and identification of the proposed learning environment, e.g. face-to-face, live online, self-paced, hybrid or blended learning.

[SOW-269] The contractor shall document the results of this analysis in CCDs I & II - Course Proposal in accordance with [NATO-Bi-SC-DIR-075-007], Chapter 5 and Annex L.

4.3.2.2.7 TNA Initial Report

[SOW-270] The Contractor shall deliver an initial TNA Report in accordance with [NATO-Bi-SC-DIR-075-007], which shall include the following:

(1) A description of the TNA approach and activities conducted during the TNA workshops;
(2) User engagement (methodology, timelines based on the TNA development, inputs and output expected from the users, questionnaires, surveys etc.);
(3) An account of the Task Analysis performed;
(4) The results of the Performance Gap Analysis, Task Analysis, DIF Analysis, Target Audience Analysis (including the identification of student prerequisites);
(5) The list of POs; and
(6) Training strategy selected for all courses identified as requirement.

4.3.2.2.8 Instructional Analysis

[SOW-271] The contractor shall conduct an Instructional Analysis in accordance with Bi-SC DIR 75-7, Chapter 6 that includes but is not limited to, the following activities:

(1) Identify the main teaching points associated with enabling elements by breaking out the skills and knowledge into sub-components in order to achieve the Performance Objectives identified;
(2) Identify all components and sub-components of the tasks that make up the performance objective, including supporting skills and knowledge elements as well as other attributes, such as attitudes; and
(3) Identify the main points (the teaching points) associated with the supporting (enabling) elements.

4.3.2.2.9 Enabling/Learning Objectives

[SOW-272] The contractor shall take all the Performance Objectives that require Education and Individual Training (E&IT) and create a list of Enabling/Learning Objectives (ELO) in accordance with [NATO-Bi-SC-DIR-075-007], Chapter 6 and Annex N.

4.3.2.2.10 Training Assessment and Evaluation

[SOW-273] The Contractor shall propose assessment and evaluation methodology to the purchaser as part of the Training Plan.

[SOW-274] The contractor shall develop an assessment plan structured according to the template provided in Bi-SC DIR 75-7, Table 6-2 that specifies how achievement of the POs will be assessed and how the student progress based on the assessment of the ELOs will be monitored.

[SOW-275] The Contractor's Training Assessment methodology shall be based on [NATO-Bi-SC-DIR-075-007] sections 7-6, 7-7 and [ASOP 07.01.25] for assessment approaches and instruments and include:
(1) Examination methodologies and certification;
(2) Minimum score to achieve for successfully passing the course;
(3) A pass/fail policy, based on results of achievement tests;
(4) Test/retest policies;
(5) Course(s) to be done to get the certification for each role; and
(6) Description of Role’s certification process.

[SOW-276] The Contractor shall ensure that each student is instructed at the end of each course (residential or Computer Based Training (CBT)) to complete and return the course evaluation feedback form provided as part of the training course.

4.3.2.2.11 Instructional Strategies

[SOW-277] The contractor shall define instructional strategies in accordance with the guidance provided in [NATO-Bi-SC-DIR-075-007], Chapter 6, by identifying and selecting:
(1) Instructional methods such as demonstration-performance, case studies or lectures;
(2) Training Materials; and
(3) Learning environment e.g., face-to-face, live online, self-paced, hybrid or blended learning.

[SOW-278] The contractor shall formulate a proposal for instructional strategy based on the selected instructional methods, media and the learning environment in accordance with [NATO-Bi-SC-DIR-075-007], Chapter 6.

[SOW-279] The contractor shall document the CCD III - Programme of Classes in accordance with [NATO-Bi-SC-DIR-075-007], Chapter 5 and Annex R to define the training solution which shall include the ELO and provide the details supporting the overall instructional strategy including the final structure of the content, teaching points, the instructional method, the time allocated to complete the ELO and student assessment details.

4.3.2.3 TNA Final Report

[SOW-280] The Contractor shall deliver a TNA Report (TNA-R) in accordance with [NATO-Bi-SC-DIR-075-007], that shall include the following:
(1) A description of the TNA approach and activities;

(2) An account of the Task Analysis performed;
(3) The results of the Performance Gap Analysis, Task Analysis, DIF Analysis, Target Audience Analysis, and the Instructional Strategy Analysis;
(4) The final list of Performance Objectives (POs);
(5) The final list of Enabling/Learning Objectives (ELOs); and
(6) The List of Teaching Points developed for each ELO Training Materials.

[SOW-281] The Contractor shall provide all the appropriate training documentation to train the Purchaser support personnel to test, operate and maintain DEMETER and its support equipment.

[SOW-282] Based on the outcome of the TNA Final Report, the following Training Materials as required shall be generated by the Contractor.
(1) Training Syllabus;
(2) Student Manuals and Handouts;
(3) Instructor Guides;
(4) Master Lesson Plans;
(5) Training Presentations;
(6) Training Scenarios;
(7) Training Database;
(8) Training Certificate;
(9) Course evaluation feedback form;
(10) Quick Reference Guides;
(11) Frequently Asked Questions (FAQ);
(12) Introductory Video;
(13) Lesson exercises/quizzes/exams with answer sheets;
(14) Training System installation and configuration procedures;
(15) Question database and sample tests;
(16) Self-paced online learning content (eLearning/micro-learning); and
(17) Training aids of all types including real equipment, references and job aids.

[SOW-283] The Contractor's Training Materials for the DEMETER courses shall provide all the information required to conduct the courses and maintain the Training Materials.

[SOW-284] The Training Materials shall be developed in accordance with the results of the TNA.

[SOW-285] The Purchaser will provide comments to improve the Training Materials. The Contractor shall implement the changes directed by the Purchaser and provide updated Training Materials as part of reviews.

4.3.2.4 eLearning – Micro-Learning

[SOW-286] The Contractor shall develop a set of self-paced online learning modules in the form of eLearning and micro-learning as identified in the Training Plan to enable end users and self-service users to perform the tasks associated with their roles.

[SOW-287] The eLearning/micro-learning shall be provided for baseline numbers, and then updated until FSA.

[SOW-288] The eLearning/micro-learning shall complement the Face-to-Face training by defining and explaining the key concepts and terminology of DEMETER, and by providing additional practice opportunities.

[SOW-289] All eLearning Training Materials shall be prepared in compliance with the Sharable Content Object Reference Model (SCORM) Edition 2004.

[SOW-290] The eLearning Package shall allow modifications by the Purchaser to reflect changes in the training concept and/or content without any additional cost to NATO.

[SOW-291] The Contractor shall provide to Purchaser, all the eLearning assets including the SCORM packages, source code files, graphic and multimedia assets.

[SOW-292] The eLearning package shall be user transparent, efficient and integrating the specific features for instructor and student without requiring special training in authoring systems technology or help from SMEs.

[SOW-293] The contractor shall provide performance support materials (micro-learning) to support users after the training during their work, with the following characteristics: bite-sized learning chunks designed to model or explain concrete tasks, ideally embedded in-application performance support, including a search function to make all performance supporting materials findable at the point of need.

4.3.2.5 Training Delivery

[SOW-294] The Contractor shall plan, prepare and deliver the training modules and training courses in a physical classroom at Purchaser designated facilities.

[SOW-295] The Contractor shall coordinate with Purchaser the requirements and availability of training facilities at the Purchaser's facilities no later than three (3) months prior to the planned training.

[SOW-296] The Contractor shall prepare and deliver the invitations for the training no later than three months prior to the planned training.

[SOW-297] The Contractor shall provide each course participant with a copy of the student manual; other (student) materiel physical or electronically as required by the course.

[SOW-298] The duration, locations and number of sessions shall be agreed upon in the Training Plan and should be sufficient to cover all users in all roles as described in Table 4.1.

[147] The Purchaser may decide unilaterally to decrease or increase the number of iterations per training course, which will result in a decrease or increase of the price based on the price per course as specified in the bidding sheets and the number of courses.

Table 4.1 – Number of iterations for the DEMETER initial training

Course Type	**Max # of seats per iteration**	**# of iterations Training**
User courses	12	25
Functional Administrator courses	6	5
System Admin courses	6	3
Train the trainer courses	10	1

[SOW-299] The Contractor shall submit to the Purchaser a Training Course Evaluation Report (TCER) for each training. The TCER shall contain the following:
(1) Student attendance and performance record;
(2) Consolidated student feedback from feedback forms;

(3) Problems encountered (if any);
(4) Actions taken or recommended; and
(5) Suggested follow-up actions.

[SOW-300] The Contractor shall, as directed by the Purchaser's Project Manager, revise the Training Materials for each course to reflect instructors' and consolidated student feedback from the initial session of each course.

[SOW-301] The Contractor shall produce Training Certificates for each training session and student in accordance with NCI Academy Standard Operating Procedure [ASOP-07.01.25] NCI Academy Grading and Assessment. The certificates shall be delivered not later than two (2) weeks following the completion of the training.

4.3.2.6 Hand-over to the Purchaser

[SOW-302] Accompanied with the delivery of WP1, the Contractor shall deliver the associated complete set of training materiel to the Purchaser.

[SOW-303] As part of the hand-over process, the Contractor shall train the Purchaser trainers to allow Purchaser instructors to deliver all training courses.

4.3.2.7 Training Analysis Review (TAR)

[148] The purpose of the TAR is to conduct the initial TNA and develop Course Control Documents I & II of the courses identified proposed as training solutions. TAR shall be in line with [NATO-Bi-SC-DIR-075-007].

[SOW-304] The Contractor shall provide the deliverables listed below for TAR:
(1) The initial version TNA Report; and
(2) Course Control Documents I & II for the proposed training solutions.

[SOW-305] The Contractor shall comply with the following entry criteria to enter this milestone:
(1) The Contractor has delivered the required deliverables; and
(2) The Purchaser has reviewed all deliverables.

[SOW-306] The Contractor shall comply with the following exit criteria for a successful conclusion of this milestone:
(1) The Purchaser has approved the content; and
(2) The Purchaser has verified that the deliverables are in line with [NATO-Bi-SC-DIR-075-007].

4.3.2.8 Training Design Review (TDR)

[149] The purpose of the TDR is to design the training solutions which are the outcome of TAR.

[SOW-307] The Contractor shall provide the deliverables listed below for TDR:
(1) Course Control Documents III for the proposed training solutions updated with the scope of the baseline;
(2) The final version TNA Report; and
(3) Updated Training Plan.

[SOW-308] The Contractor shall comply with the following entry criteria to enter this milestone:
(1) TAR has been successful;
(2) The Contractor has delivered the required deliverables; and

(3) The Purchaser has reviewed all deliverables.

[SOW-309] The Contractor shall comply with the following exit criteria for a successful conclusion of this milestone:
(1) The Purchaser has approved the content; and
(2) The Purchaser has verified that the deliverables are in line with [NATO-Bi-SC-DIR-075-007].

4.3.2.9 Training Material Review (TMR)

[150] The purpose of the TMR is to develop the material in support of the training solutions.

[SOW-310] The Contractor shall provide the Training Materials deliverables as listed in Section 3.7.6 for each course.

[SOW-311] The Contractor shall comply with the following entry criteria to enter this milestone:
(1) TDR has been successful;
(2) The Contractor has delivered the required deliverables; and
(3) The Purchaser has reviewed all deliverables.

[SOW-312] The Contractor shall comply with the following exit criteria for a successful conclusion of this milestone:
(1) The Purchaser has approved the content; and
(2) The Purchaser has verified that the deliverables are in line with [NATO-Bi-SC-DIR-075-007].

4.3.3 Interoperability Adaptations (WP3)

[151] Intention of this phase is to develop the interoperability adaptations on an NCI Agency approved integration platform (e.g. SOA-IdM or IntCore).

[SOW-313] The Contractor shall design and build interoperability adaptations on an NCI Agency approved integration platform (e.g. SOA-IdM or IntCore) based on interfaces defined in Annex B as well as other adaptations.

[SOW-314] The Contractor shall use an iterative development approach.

[SOW-315] The Contractor shall break up the iterative development phase into a sequence of sprints.

[152] Each consecutive sprint shall implement a new scope of requirements and consolidate it with the resulting capabilities from the previous sprint. The aim will be to deliver a “shippable capability” (i.e. a working piece of software that is ready to be deployed and thus include documentation and other relevant support artefacts) at the end of each time-boxed sprint.

[153] The Purchaser may define the priority of the work to be delivered in this WP.

[SOW-316] The Contractor shall follow the priorities as defined by the Purchaser and include all activities required for requirements analysis, design, development, integration, testing, documentation, etc. within the scope of a single sprint in order to deliver a shippable capability at the end of each time-boxed sprint.

4.3.4 Validation

[154] The validation phase for each of the WPs consists of system integration testing (SIT) which will be combined with CIAV, IVVQ testing and the CRQ/Security tests prior to deployment in the operational environment and the SiAT, which may be combined with one or several NATO exercise(s). Also participation in NATO exercises such as Coalition Warrior Interoperability Exercise (CWIX) may be required.

[155] As Figure 4.4 illustrates, the testing will follow a sequence of formal verification and validation activities, either led and performed or supported by the Contractor.

[156] The Purchaser reserves the right to develop additional test cases and conduct its own independent testing.

[SOW-317] The Contractor shall lead, perform and support the activities as illustrated in Figure 4.4, Figure 4.5 and Figure 4.6.

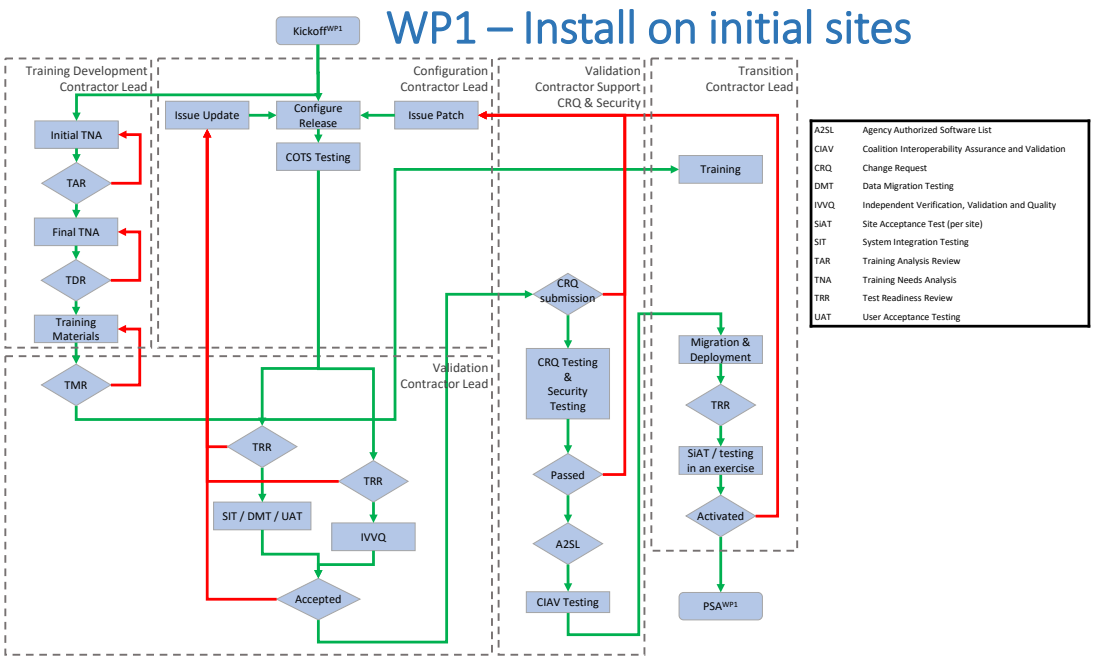

Figure 4.4 - Testing, Verification and Validation Process for WP1

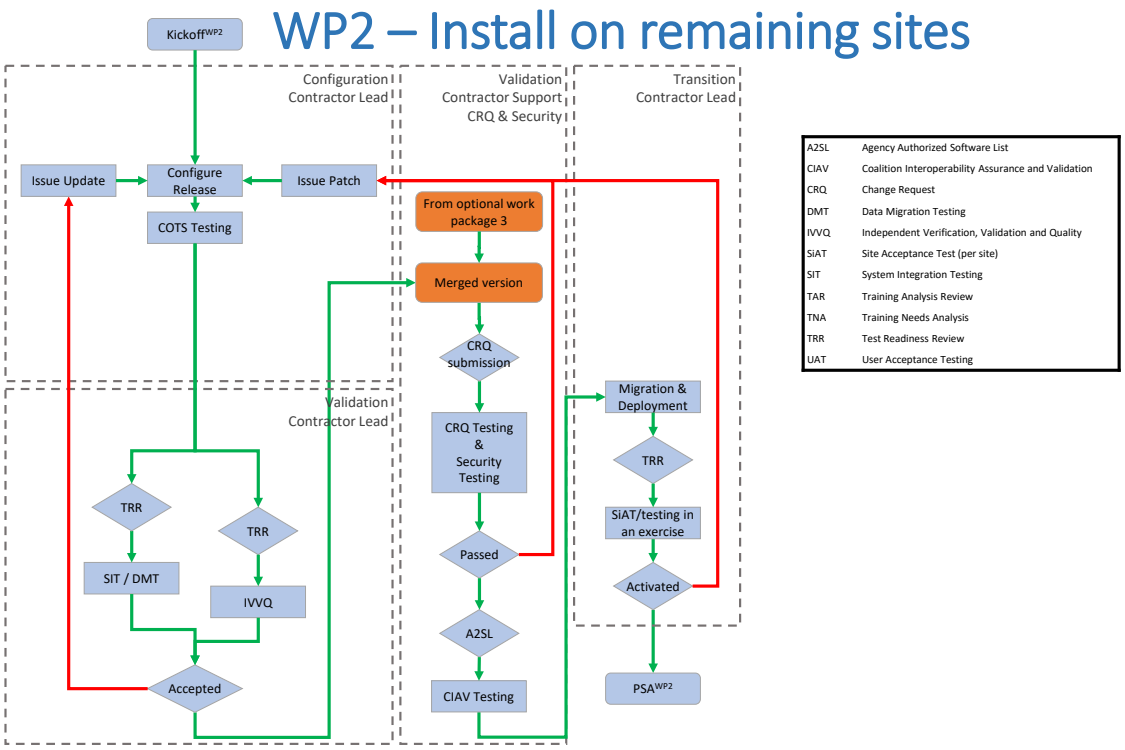

Figure 4.5 – Testing, Verification and Validation Process for WP2

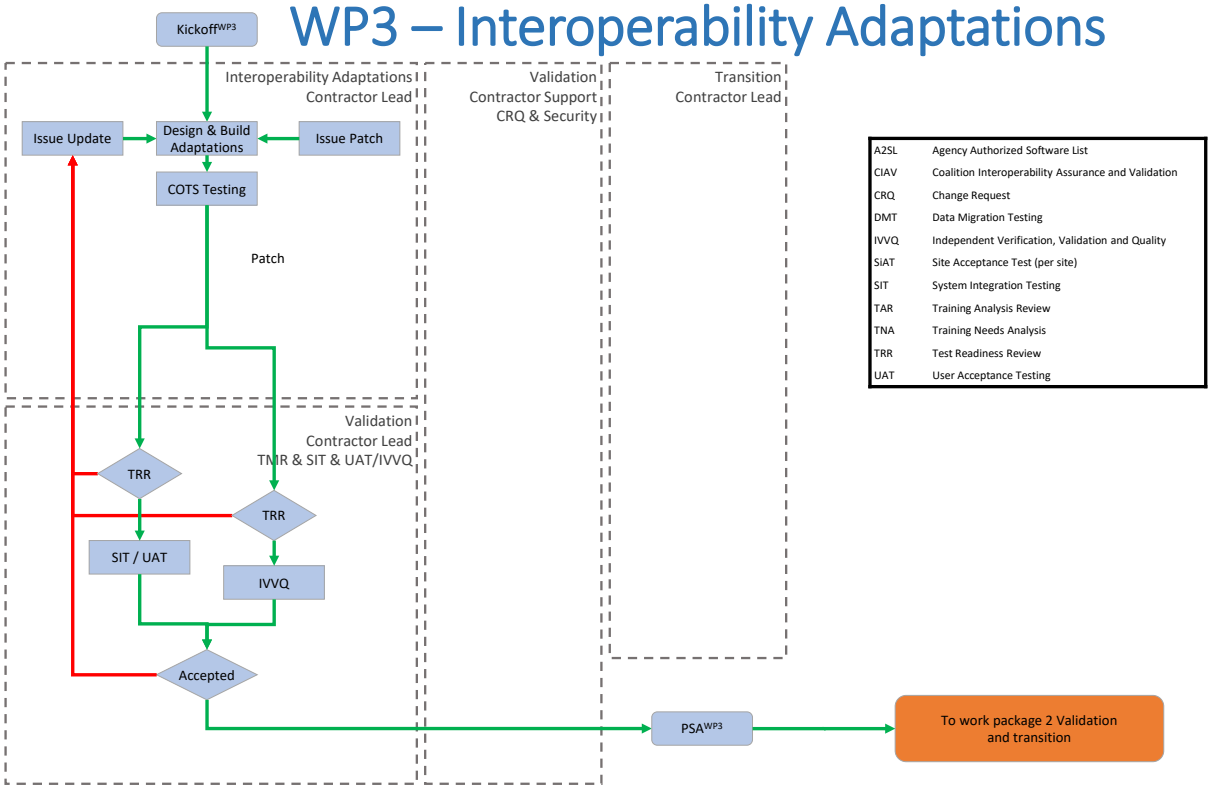

Figure 4.6 – Testing, Verification and Validation Process for WP3

4.3.4.1 Entry and Exit Criteria

[SOW-318] The Contractor shall comply with the following entry criteria for the validation phase:

(1) The Contractor has concluded the previous phase successfully.

[SOW-319] The Contractor shall comply with the following exit criteria for a successful conclusion of the validation phase:

(1) The Contractor has successfully conducted the training material review (only applies to WP1);
(2) The Contractor has successfully conducted the system integration testing with no remaining critical defects and 4 or less high defects;
(3) The Contractor has successfully conducted the user acceptance testing / IVVQ with no remaining critical defects and 4 or less high defects;
(4) The Contractor has successfully passed the CRQ and security testing and the baseline release is on the A2SL;
(5) The Contractor has delivered a release build, including source code (for WP3 only), any third-party software, licences and warranty documentation. This shall include any third-party software and components as per Section 3.6;
(6) The documentation artefacts supporting the CRQ have been reviewed and accepted by the Purchaser;
(7) The Contractor has delivered revisions of the system documentation artefacts including the installation and configuration manual, maintenance and administration manual, coherent with the baseline release that have been reviewed and accepted by the Purchaser;
(8) The Contractor has delivered revisions of the user documentation artefacts, including online help and standard operating procedures manual, coherent with the baseline release that have been reviewed and accepted by the Purchaser;
(9) The Contractor has delivered the product description and interface control document (ICD) coherent with the baseline release that have been reviewed and accepted by the Purchaser;
(10) The Contractor has delivered meeting reports of meetings held during this phase; and
(11) The Contractor has delivered test reports of the test activities conducted during this phase.

4.3.5 Transition

[157] Following successful completion of the validation phase, the transition phase will commence. The objective of the transition phase is to deploy the approved baseline release onto the NATO operational network, training platform, and relevant test and reference environments, and deliver training and support.

[158] The transition phase, and thus the WP, will be concluded with a PSA once all services and deliverables have been delivered and accepted by the Purchaser.

4.3.5.1 Deployment

[159] The deployment, i.e. installation, migration and activation, of a baseline release on the NATO operational networks, training platform, (integration) test beds and reference environments will be the responsibility of the Contractor, supervised by the Purchaser.

[160] Back-end deployments are required in the datacentres in Mons, Belgium and Lago Patria, Italy, as well as on the enhanced node in Izmir, Turkey and must be accessible from all NATO locations.

Table 4.2 - Overview Operational Sites, Reference Environment and Testbeds

Back-end installation locations	**WP1**	**WP2**
Operational		
Datacentre Mons, BEL		x
Datacentre Lago Patria, ITA		x
Enhanced node: Izmir, TUR	x	x
Deployable CIS in Europe		x
Exercises		
Joint Force Training Centre, Bydgoszcz, POL		x
Joint Warfare Centre, Stavanger, NOR		x
Testing		
NCI Agency Support and Reference Environment, The Hague, NLD	x	x
NCI Agency Bi-SC AIS IVVQ Testbed, The Hague, NLD	x	x
NCI Agency NSF, The Hague, NLD	x	x
End user operational locations accessing DEMETER	**WP1**	**WP2**
Land Command Izmir	x	x
HQ JFC Naples, ITA	x	x
HQ JFC Brunssum, NLD		x
HQ JFC Norfolk, USA		x
SHAPE Mons, BEL		x

[SOW-320] The Contractor shall ensure that the deployment of an instance of a baseline release includes:

(1) Installation of the baseline release;
(2) Integrate the newly installed operational baseline with the available core and other functional services as defined in the selection criteria;
(3) Migrate the existing data and users to the newly installed operational baseline; and
(4) Activate the newly installed operational baseline and verify the correct installation and configuration (site acceptance testing).

[SOW-321] The Contractor shall deploy an instance of each release submitted for IV&V (CRQ process) to the Bi-SC AIS IVVQ Test Bed from the Purchaser's facilities. These deployments could be conducted remotely if agreed with by the Purchaser.

[SOW-322] The Contractor shall deploy an instance of each release for system integration testing activities to the NCI Agency Support and Reference Environment from the Purchaser's facilities.

[SOW-323] The Contractor shall deploy an instance of each release to the NCI Agency Support and Reference Environment, from the Purchaser's facilities. These deployments could be conducted remotely if agreed with by the Purchaser.

[SOW-324] The Contractor shall deploy instances of limited approval (LATO) baseline releases to the NATO operational network from the Purchaser's facilities for user

acceptance testing and training as required throughout the period of performance of the Contract.

[SOW-325] The Contractor shall deploy and activate multiple instances of an approved baseline release (up to four: operational instance, exercise instance, training instance and test instance) to the NATO operational network for the operational sites listed in Table 4.2. In general, the deployment shall be conducted from the Purchaser's facilities. Specific components, e.g. Desktop Client (if applicable), may require local support on each site.

[SOW-326] The Contractor shall be responsible for ensuring that the deployed instances are installed and correctly configured, fully functional and accessible across the NATO network domain, i.e. from all connected sites (Table 4.2), with satisfying performance as specified in the contracted requirements.

[SOW-327] The Contractor shall deploy and activate an instance of an approved baseline release to the NCI Agency Support and Reference Environment from the Purchaser's facilities.

[SOW-328] The Contractor shall coordinate the deployment sequence and timeframes with the Purchaser and site POCs to accommodate for specific requirements, exercises, holiday periods and other considerations.

[SOW-329] The Contractor shall deliver a deployment report for each deployment, documenting deployment specific details of the activities conducted and results of the activation tests performed.

[SOW-330] In case issues or defects are discovered during the transition, the Contractor shall deliver an updated baseline release or patch to resolve the issue/defect and support the request for change process to obtain approval.

4.3.5.1.1 Release and Deployment Plan

[SOW-331] The Contractor shall deliver a Release and Deployment Plan (RDP) in accordance with section 8.8.

4.3.5.2 Partial System Acceptance

[161] Each WP will be concluded with a PSA, which will be granted when the Purchaser has verified completeness of the entire delivery and has determined that it meets the requirements of the Contract.

[SOW-332] The Contractor shall develop and deliver a PSA report, which shall reference relevant Contract Line Identification Numbers (CLINs) and includes:
(1) Traceability of the delivered and deployed baseline(s) and artefacts;
(2) Traceability of services delivered;
(3) Deliverable requirements traceability matrix, including completion status; and
(4) Overview of outstanding non-critical defects with a correction action plan for addressing these defects.

[SOW-333] The Contractor shall request PSA in writing to the Purchaser, supported by a PSA report and meeting invitation.

[SOW-334] The Contractor's personnel shall meet with the Purchaser's project team for a PSA meeting. At the discretion of the Purchaser, meeting by video conference may also be acceptable.

[SOW-335] During the meeting, the Contractor shall include in its presentation:
(1) An overview of the key dates of the Contract, amendments and engineering change proposals;
(2) A summary of the scope, with overview of main deliverables and services delivered, highlights and main achievements;
(3) Key dates of project milestones and acceptance;
(4) Invoicing log, including listing outstanding payments;
(5) Outstanding CLINs delivered to be formally accepted; and
(6) Defect correction action plan and approach to maintenance and support services to be furnished until FSA.

[SOW-336] The Contractor shall prepare and deliver a written report of the meeting in the form of meeting minutes that shall be reviewed and signed by the representatives of the Contractor and Purchaser respectively.

4.3.5.3 Maintenance and Support

[SOW-337] On passing PSA of WP1 until successfully achieving FSA, the Contractor shall provide maintenance and in-service support, service released or patches in accordance with the provisions stipulated in Section 5.3.

4.3.5.4 Entry and Exit Criteria

[SOW-338] The Contractor shall comply with the following entry criteria for the transition phase:
(1) The Contractor has concluded the previous phase successfully;
(2) The Contractor has coordinated the provision of training at the Purchaser's facilities (WP1); and
(3) The Contractor has delivered and sent the invitation for the training to be delivered (WP1).

[SOW-339] The Contractor shall comply with the following exit criteria for a successful conclusion of the transition phase:
(1) The Contractor has completed the deployment of multiple instances of the baseline releases on the NATO operational network and the instances are fully functional and operational;
(2) The Contractor has completed the deployment of multiple instances of the baseline releases to the NCI Agency Support and Reference Environment and the reference and test beds and the instances are fully functional and operational;
(3) The Contractor has delivered deployment reports for each deployment;
(4) The Contractor has resolved all critical and high severity defects discovered during this phase and provided updated baseline releases, as required;
(5) The Contractor has delivered revisions of the system documentation artefacts including the installation and configuration manual, maintenance and administration manual, coherent with the baseline release that have been reviewed and accepted by the Purchaser;
(6) The Contractor has delivered revisions of the documentation, coherent with the baseline release that have been reviewed and accepted by the Purchaser;
(7) The Contractor has completed the delivery of training (WP1);
(8) The Contractor has delivered training course evaluation reports of all training courses conducted during this phase (WP1);

(9) The Contractor has incorporated feedback and lessons-learned in the training scenarios and training packages and has delivered an updated version (WP1);
(10) The Contractor has delivered meeting reports of meetings held during this phase;
(11) The Purchaser has verified completeness of the entire delivery and has determined that it meets the requirements of the Contract;
(12) The Purchaser comments/concerns regarding the defect correction action plan and approach to maintenance and in-service support to be provided until FSA have been addressed;
(13) The PSA meeting has been held and the submitted meeting minutes are accepted by Purchaser; and
(14) The PSA has been granted.

4.4 Closure Phase

[SOW-340] The objective of the closure phase is for the Purchaser to conduct the final validation of all deliverables, confirming complete hand-over, and verify that all contractual requirements (except warranty) have been met by the Contractor.

[SOW-341] FSA will be granted when the Purchaser has verified completeness of the entire delivery and has determined that it meets the requirements of the Contract. Subsequently, on successful achievement of the FSA, the warranty period will commence.

[SOW-342] The Contractor shall develop and deliver a FSA report, which shall reference relevant CLINs and includes:
(1) Traceability of delivered and deployed baselines and associated artefacts;
(2) Traceability of any other artefact delivered;
(3) Traceability of services delivered;
(4) Updated deliverable requirements traceability matrix, including completions status; and
(5) Overview of outstanding non-critical defects with a correction action plan for addressing these defects under warranty.

4.4.1 Close-out Meeting

[SOW-343] The Contractor shall request FSA in writing to the Purchaser, supported by a FSA report and close-out meeting invitation.

[SOW-344] The Contractor’s personnel shall meet with the Purchaser’s project team for a close-out meeting. At the discretion of the Purchaser, meeting by video conference may also be acceptable.

[SOW-345] During the close-out meeting, the Contractor shall include in its presentation:
(1) An overview of the key dates of the contract, amendments and engineering change proposals;
(2) A summary of the scope, with overview of main deliverables and services delivered, highlights and main achievements;
(3) Key dates of project milestones and acceptance;
(4) Invoicing log, including listing outstanding payments;
(5) Outstanding CLINs delivered to be formally accepted; and
(6) Defect correction action plan and approach to maintenance and in-service support to be provided during the warranty period.

[SOW-346] The Contractor shall prepare and deliver a written report of the close-out meeting in the form of meeting minutes that shall be reviewed and signed by the representatives of the Contractor and Purchaser respectively.

4.4.2 Entry and Exit Criteria

[SOW-347] The Contractor shall comply with the following entry criteria for the closure phase:

(1) The Contractor has concluded the previous phase successfully;
(2) The Contractor has verified and confirmed hand-over of all deliverables under this Contract;
(3) The Contractor has delivered the FSA report and is requesting FSA; and
(4) The Contractor has delivered the Certificate of Conformity.

[SOW-348] The Contractor shall comply with the following exit criteria for a successful conclusion of the closure phase:

(1) The Purchaser has assessed completeness of the entire delivery and has determined that it meets the requirements of the Contract;
(2) The Purchaser comments/concerns regarding the defect correction action plan and approach to maintenance and in-service support to be furnished during the warranty period have been addressed;
(3) The close-out meeting has been held and the submitted meeting minutes are accepted by Purchaser; and
(4) The FSA has been granted.

5 Integrated Product Support

5.1 General

[SOW-349] The Contractor shall establish an integrated product support (IPS) process, using the [ALP-10] or [ASD/AIA SX000i] specification as guidance, and perform IPS throughout the period of performance of the Contract.

[SOW-350] The Contractor shall align delivery of all IPS related deliverables and services with the incremental delivery approach of the Contract.

5.2 Integrated Product Support Plan

[SOW-351] The Contractor shall deliver an integrated product support plan (IPSP) compliant with Section 8.12, and document its IPS process tailored to the Contract, including activities and milestones to deliver integrated product support deliverables and services.

[SOW-352] The Contractor shall document the planned maintenance and support activities in the IPSP, based on the definitions, concepts and requirement set forth in the Contract.

[162] The in-service support plan documents the schedule, organization and resources of support during the in-service phase (from the first baseline release until FSA, during warranty and during the optional maintenance and support furnished post the warranty period), considering the maintenance and support definitions and concept.

[SOW-353] The Contractor shall deliver an in-service support plan (ISSP) as an annex to the IPSP compliant with Section 8.12.1.

5.3 Maintenance and Support

5.3.1 Definitions

[163] The support concept is the set of activities and processes in charge of managing the various levels of support and to escalate the problem to the appropriate level in accordance with the defined responsibilities.

[164] It is based on the incident management process defined in ISO/IEC 20000, the Information Technology Infrastructure Library (ITIL) framework, software supportability concept of [ASD-S3000L]/[ASD-AIA-SX000i] or equivalent.

[165] Support Level: the extent of technical assistance provided for an information technology capability to its users. The service management is divided into three different levels of service, which interface each other to activate the proper level of support appropriate for the type of incident that occurred or the request that has been made in accordance with the event happened on the system.

[166] First Level Support: implements the incident management process in accordance with the 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 (incident or service\change request), performs an initial assessment and distributes it to the predefined actors to solve it.

[167] Second Level Support: implements the problem management process in accordance with the ITIL framework or equivalent. The problem management process receives the trouble tickets from the service desk and performs the following tasks (not limited to):
(a) (Re-)evaluation of trouble ticket 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 configuration item releases);
(e) Create problem analysis report and change request including schedule of implementation, and synchronization with the baseline maintenance process;
(f) Presentation of the problem analysis report and change requests to the change control board (CCB) for approval;
(g) Monitor and control the approved change request during implementation;
(h) Trigger third level support and/or third level maintenance process to implement the change request, in case the incident cannot be solved at second level; and
(i) Perform the post-change request implementation review.

[168] Third Level Support: implements the deployment and release management process in accordance with the ITIL framework or equivalent. The deployment and release management process receives the approved change request from the second level support and performs the following tasks (not limited to):
(a) Activating third level maintenance when new solutions shall be developed;
(b) Development of the solution (i.e. new configuration item fix, repair, replacement, patch, or release);
(c) Testing of the solution (i.e. issue/defect replication testing, regression testing);
(d) Update of baseline content and status;
(e) Submit the solution for IV&V testing;
(f) Release of the solution; and
(g) Delivery and deployment of the solution.

[169] Maintenance Level: the echelon at which maintenance tasks are performed on an information technology capability. 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. For all maintenance levels it is intended that:
(a) All proactive maintenance tasks are defined in the maintenance and administration manual (Section 8.16) and scheduled in the maintenance plan; and
(b) Reactive maintenance activities are triggered by reported incidents, or service/change requests.

[170] First Level Maintenance: this constitutes the very basic maintenance activities including the software failure recovery by simple diagnostics, as well as activating the second level of maintenance when it is needed. It includes the initial preventive maintenance procedures and any additional service/capability and/or site-specific procedures that are defined in the corresponding operations and maintenance manual. First level maintenance procedures do not require specialised tools and/or specialised personnel.

[171] Second Level Maintenance: this constitutes isolation and resolution of system-level maintenance and management of defect/bug reports and repair including the simple software customizations, software reloading/installation, execution of scripts, management of users/profiles usually performed by system administrators, activating

the third level of maintenance when it is needed. It includes the initial preventive maintenance procedures and any additional service/capability and/or site-specific procedures that are defined in the corresponding manual. Second level maintenance procedures do not require specialised tools.

[172] Third Level Maintenance: this constitutes activities that involve a change to the system baseline, such as software patches or new releases including the bug recording and reporting, advanced troubleshooting and configuration changes with the changing environment. It includes 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 baseline (adaptive maintenance) e.g. security patches, operating system upgrades, minor software configuration changes due to operational/interface needs and refactoring. It includes the initial preventive maintenance procedures and any additional procedures that are defined in the corresponding manual. Third level maintenance procedures often require specialised tools and/or Personnel such as software architects, programmers, advanced system administrators and specialists.

[173] Fourth Level Maintenance: this is the responsibility of the software original developer under warranty and through separate agreements post warranty. It is activated from the third level of maintenance and covers the four types of maintenance (corrective, adaptive, perfective and preventive maintenance) and change requests. It requires software maintenance, testing (both in simulated and emulated environments), patch creation, release and deployment services.

5.3.2 Maintenance and Support Concept

[174] The NCI Agency's service support team for DEMETER, or its mandated representatives or third parties, will be performing maintenance and support services in parallel with the Contractor.

[SOW-354] The Contractor shall support and collaborate with the NCI Agency's service support and maintenance team or its mandated representatives or third parties.

[SOW-355] The Contractor shall integrate any changes and modifications made by the NCI Agency's service support and maintenance team or its mandated representatives or third parties.

[SOW-356] The Contractor shall deliver a maintenance and support concept, i.e. a collection of processes that are designed to ensure the operational efficiency of the operational baseline, including:
(1) Processes and procedures;
(2) Maintenance and support tasks at all levels;
(3) Maintenance and support environment;
(4) Locations;
(5) Constraints;
(6) Organization and personnel skills; and
(7) Roles and responsibilities (responsible, accountable, consulted and informed, RACI).

[SOW-357] The maintenance and support concept shall refer to applicable requirements.

[SOW-358] The maintenance and support concept shall define the second and third level support process interfaces to the other processes, including the existing NCI

Agency Service Desk (first level support) and various NATO sites and organizations.

[SOW-359] The maintenance and support concept shall define the delivered baselines maintenance and support processes and flow amongst the various NATO facilities, organizations, groups, and people. This shall include the flow and interfaces between various maintenance and support levels.

[SOW-360] On passing PSA of WP1 until successfully achieving FSA, the Contractor shall provide in-service support and maintenance services for the first DEMETER baseline and any follow-on deployed baselines. This support shall include:
(1) Second and third level support; and
(2) Third and fourth level maintenance, including implementation of fixes to defects and subsequently produce emergency patches and minor updates in between baseline releases to ensure that the operational baselines running in production fulfils its availability requirements.

[SOW-361] The Contractor shall deliver the support and maintenance documentation artefacts, training, and resources in order to allow the Purchaser to fully operate the solution, to perform first, second and third level support and maintenance from PSA of the final baseline onwards.

[SOW-362] Starting from PSA of WP1, until the end of the warranty period, all maintenance activities beyond Purchaser capabilities/skills (as per maintenance concept and Contractor delivered training and documentation) required to restore operational baselines from a critical failure shall be performed by Contractor provisioned dedicated on-site interventions and/or off-site resolutions.

[SOW-363] The Contractor shall maintain and deliver renewed/extended licenses of the third-party software and components in accordance with Section 3.6 and ensure that these licenses cover the full period of performance.

[SOW-364] The Contractor shall monitor the availability of third-party software and component upgrades and patches in accordance with the requirements stipulated in Section 3.6.

[SOW-365] When agreed by the Purchaser, the Contractor shall introduce and integrate upgrades and patches of all third-party software and components in accordance with the requirements stipulated in Section 3.6.

[SOW-366] For any critical failure or defect that is beyond the capability of the Purchaser, the Contractor shall ensure system restoration within two (2) business days from the moment of Purchaser notification by providing workarounds; and within ten (10) days for critical defect fixing including the fault identification, software recoding, patch creation, software testing and delivery of the new patch release. Corrective baseline or patch releases shall be done quarterly for non-critical bugs.

5.4 Supply Support

5.4.1 System Inventory

[SOW-367] The Contractor shall provide the Purchaser's IPS point of contact with an inventory and distribution list (IDL), in electronic Microsoft Excel format at least fourteen (14) days before each baseline release.

[SOW-368] The inventory and distribution list shall be site-specific (as required) with reference to relevant CLIN, and shall include all deliverables furnished under this Contract, as follows:
(1) Date of distribution;
(2) All software artefacts, i.e. all software applications, components, tools, (if applicable), etc.;
(3) All hardware devices, if applicable;
(4) All licences, if applicable, including license key and renewal dates;
(5) All documentation artefacts, i.e. manuals, drawings, reports, etc.; and
(6) All training packages.

5.4.2 Packaging, Handling, Storage, Transportation

[SOW-369] The Contractor shall deliver all deliverables, including all spares and repaired goods, DDP (Delivery Duty Paid) Incoterms 2020 to the NATO destinations, at Contractor's expense. The Purchaser shall not be held liable for any storage, damage or any other charges involved in transportation prior to delivery at destination.

[SOW-370] The Contractor shall be responsible for the availability of proper storage facilities and availability of material handling equipment that may be required for the shipment at the destination.

[SOW-371] The Contactor shall liaise with the destination and coordinate availability of proper storage facilities and material handling equipment through the Purchaser's integrated product support officer.

[SOW-372] In case classified items need to be transported, the Contractor shall adhere to the regulations concerning transportation of classified materials.

[SOW-373] The Contractor shall be responsible for the transfer and delivery of installation packages of all software, firmware and modifications thereof provided under this Contract to the respective destination.

[SOW-374] In case electronic storage media (CD/DVD, USB storage device, etc.) is used to deliver or transfer deliverables, then the Contractor shall physically label this media with the contract information, CLIN, identification, release date and security classification. The label shall be durable and non-erasable to ensure proper identification is warranted at all times.

[SOW-375] Fourteen (14) days prior to the delivery of any shipment, the Contractor shall provide the Purchaser with a notice of shipment comprising the following details:
(1) Shipment date;
(2) Purchaser contract number;
(3) CLIN;
(4) Consignor's and consignee's name and address;
(5) Items description and quantity; and
(6) Number of 302 Forms used (if applicable).

5.4.3 Customs

[SOW-376] The Contractor shall be responsible for customs clearance and/or export licences of all deliveries into their destination countries.

[SOW-377] The Contractor's shall be responsible for taking into account the time needed at customs, including eventual delays in obtaining customs clearance, and arrange

for timely ship. The Purchaser shall not be held responsible for delays incurred, even when utilising Purchaser provided Customs Form 302 (if applicable).

6 Warranty

[SOW-378] The Contractor shall warrant that all deliverables and all services furnished under this Contract conform to the requirements and are free of any defect in code or workmanship for a period of one year starting at FSA.

[SOW-379] The Contractor shall integrate the provision of corrective maintenance within its warranty services.

[SOW-380] When, at any time before the end of the warranty period, the Contractor becomes aware that a defect exists in any of the deliverables or services furnished under this Contract, the Contractor shall coordinate with the Purchaser and promptly correct the defect in accordance with the warranty provisions.

[SOW-381] The Contractor shall correct all defects and deliver a corrective baseline release at the end of each quarter throughout the warranty period.

[SOW-382] At the end of the warranty period, the Contractor shall deliver a final baseline release including the fixes for all the remaining defects.

[SOW-383] In case of a critical defect, the Contractor shall deliver analysis of the defect to the Purchaser and deliver a workaround within maximum eight (8) business hours, and the fixed solution by means of a patch release within four (4) business days after the Contractor has become aware of the defect.

[SOW-384] The Contractor shall integrate the provision of on-site service support within its warranty services to be provided off-site from the Contractor's facilities, or on-site at the Purchaser facilities as required in case the issue cannot be resolved remotely or to support warranty releases and deployment and hand-over thereof. In case on-site support provision at the Purchaser facilities is required, the Contractor’s response time at Purchaser site shall be within two business days from the moment of Purchaser notification.

[SOW-385] The Contractor shall warrant all third-party software and components used during the warranty period. If required, the Contractor shall renew/extend the third-party software and component licences to cover the full warranty period.

[SOW-386] The Contractor shall monitor the availability of third-party software and component upgrades and patches in accordance with the requirements stipulated in Section 3.6.

[SOW-387] When agreed by the Purchaser, the Contractor shall introduce and integrate upgrades and patches of all third-party software and components in accordance with the requirements stipulated in Section 3.6.

[SOW-388] The Contractor shall ensure that the warranty conditions remain valid even if the software is relocated/redeployed to an equivalent platform while under warranty.

[SOW-389] The Contractor shall conduct testing and perform the configuration and change management processes for each patch and maintenance baseline release

[SOW-390] The Contractor shall support the change request process for each patch and corrective baseline release.

[SOW-391] The Contractor shall support the IV&V testing in accordance with Section 3.8.4.4.

[SOW-392] The Contractor shall support the Purchaser in assessing the impact of issues, defects and identification and proposing workarounds and a fixed solution.

[SOW-393] The Contractor shall detail all the warranty requirements in its in-service support plan, including the roles and responsibilities.

[SOW-394] The Contractor shall provide a specific point of contact for all warranty and support requests.

7 Work Package 4: Optional Maintenance and Support

[175] This optional WP describes the requirements for the continued annual Contractor furnished maintenance and support services to be exercises for up to ten (10) years post-FSA.

[SOW-395] On exercising this optional WP, the Contractor shall provide fourth level maintenance services (see Section 5.3) off-site from the Contractor's facilities where this support includes:

(1) Support to NCI Agency's second and third level support process with identification of the root cause of the issue (i.e. problem identification and analysis);
(2) In case of a critical defect, the Contractor shall deliver analysis of the defect to the Purchaser and deliver a workaround within maximum eight (8) business hours (8:00 – 18:00, Central European Time), and the fixed solution by means of a patch release within four (4) business days after the Contractor has become aware of the defect;
(3) Provide modification of the software to keep it usable in a changed or changing environment (adaptive maintenance). This includes moving from one hardware platform to another, updating infrastructure software and insertion of other software components developed by third-parties;
(4) Detect latent faults, analysing patterns and discover potential vulnerable areas in the software and provide preventive fixes (preventive maintenance);
(5) Support to testing and CRQ process in accordance with Section 3.8.4.4;
(6) Support the user acceptance testing in accordance with Section 3.8.4.3;
(7) Conduct testing and perform the configuration and change management processes for each patch and maintenance baseline release; and
(8) Support the release and transition process for each patch and maintenance baseline release.

[SOW-396] The Contractor shall integrate the provision of on-site service support within its maintenance services to be provided off-site from the Contractor's facilities, or on-site at the Purchaser facilities as required in case the issue cannot be resolved remotely or to support warranty releases and deployment and hand-over thereof. In case on-site support provision at the Purchaser facilities is required, the Contractor's response time at Purchaser site shall be within two business days from the moment of Purchaser notification.

[SOW-397] To enable the interfacing between DEMETER and other capabilities and services, the Contractor shall provide support to Purchaser or its contractors responsible for implementing such interfaces with DEMETER.

[SOW-398] The Contractor shall maintain and deliver renewed/extended licenses of the third-party software and components in accordance with Section 3.6 and ensure that these licenses cover the full period of performance.

[SOW-399] The Contractor shall monitor the availability of third-party software and component upgrades and patches in accordance with the requirements stipulated in Section 3.6.

[SOW-400] When agreed by the Purchaser, the Contractor shall introduce and integrate upgrades and patches of all third-party software and components in accordance with the requirements stipulated in Section 3.6.

8 Documentation Artefacts and Definitions

[176] This section covers the requirements for documentation artefacts to be delivered.

[SOW-401] For documentation artefacts that have not been specified in further detail under this Contract, the Contractor shall deliver a template with an outline of the relevant documentation artefact for Purchaser review and agreement prior to developing the documentation artefact.

[177] In case the Contractor deems necessary, and supported with proper justification, the Contractor may propose amendments to the outline and contents of documentation artefacts for Purchaser agreement.

8.1 Distribution

[SOW-402] The Contractor shall deliver all documentation artefacts in an electronic format, unless otherwise instructed, as follows:
(1) Documentation artefacts intended for review by the Purchaser shall be delivered in an editable (i.e. Microsoft Office) format; and
(2) Final versions of documentation artefacts shall be delivered in Adobe PDF format with OCR (Object Character Recognition) capability, together with the editable source file.

[SOW-403] The Contractor shall distribute all documentation artefacts, unless otherwise instructed, as follows:
(1) All documentation artefacts: to the Purchaser's PM;
(2) In case of technical documentation artefacts, i.e. design documentation, user stories, manuals, etc.: to the Purchaser's technical lead; and
(3) In case of contract documentation artefacts, including invoices, change requests, etc.: to the Purchaser's contracting officer, and if required by the Purchaser's contracting officer, an additional printed copy.

[SOW-404] The Contractor shall not include any statements limiting the rights to use or reproduce the documentation artefact delivered under this Contract. The Purchaser reserves the right to make additional copies of any documentation artefact delivered.

[SOW-405] The Contractor shall ensure that the Purchaser always has access to the latest version of any documentation artefact from the moment the documentation artefact comes into existence, i.e. use the NSF for production and configuration management platform.

[SOW-406] The Contractor shall maintain the documentation artefacts and keep them current throughout the period of performance of the Contract.

[SOW-407] The Contractor shall place the documentation artefacts under configuration control throughout the period of performance of the Contract.

8.2 Review and Updates

[178] The Purchaser will, when reviewing documentation artefacts, provide comments and suggest changes to the Contractor within two weeks of receipt of the documentation artefact. When the Purchaser requires more time to complete its review, the Purchaser will inform the Contractor.

[179] The Purchaser will reserve the right to return without further review a documentation artefact that shows significant deficiencies.

[SOW-408] All documentation artefacts shall be subject to Purchaser review and acceptance.

[SOW-409] The Contractor shall not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.

[SOW-410] In case the Contractor considers that the Purchaser's comments and suggestions require further clarification, the Contractor shall arrange for a meeting to address the items of concern.

[SOW-411] The Contractor shall submit revisions of documentation artefacts for review, addressing the Purchaser's comments and suggestions within two weeks after receipt of the Purchaser's feedback.

[SOW-412] The Contractor shall submit revision documentation artefacts for review with each modification identified through the "track changes" feature or otherwise being marked as change.

[SOW-413] In case there is a change to an already delivered artefact, the Contractor shall be responsible for updating all documentation artefacts pertaining to the specific delivered artefact where the documentation artefacts are affected by the change.

8.3 Standards and Conventions

[SOW-414] The Contractor shall deliver all documentation artefacts compliant with the standards and conventions of the sections below. Third-party software and component documentation artefacts, such as a vendor-supplied user manual, are exempt from these requirements and shall be delivered in the original, unaltered, format.

8.3.1 File Format

[180] The Purchaser's default software packages for managing documentation artefacts are:
(a) Microsoft Office Professional 2016 or later;
(b) Microsoft Project 2010;
(c) Microsoft DocFX;
(d) Adobe PDF Reader; and
(e) Microsoft Windows compatible Zip compression and packaging format.

[SOW-415] Documentation artefacts shall be delivered in a file format that is compatible with the Purchaser's default software packages.

[SOW-416] Documentation artefacts shall be delivered in a file format that is best suited for review and maintenance by the Purchaser. In general, the following guidelines apply:
(1) Microsoft Word shall be used for text documents;
(2) Microsoft Excel shall be used for tabular or matrix data;
(3) Microsoft Project shall be used for schedule; and
(4) Microsoft PowerPoint shall be used for briefings and presentations.

[SOW-417] Documentation artefacts shall adhere to the following filename convention [NU|NR]_[Name]_[vX.Y|].[filename extension] and the elements used in the filename convention shall be as follows:
(1) [NU|NR] is the classification of the file: NATO UNCLASSIFIED or NATO RΞSTRICTED. Note: Classified files shall not be stored within the NSF;

(2) [Name] is the Contractor proposed, Purchaser agreed designation of the documentation artefact;
(3) [vX.Y] is the version number in the range (v0.1, v0.2,…, v0.9, v0.10, v0.11,…) for drafts submitted to the customer, and with vX.0 only for the final deliverables; and
(4) [filename extension] is the standard filename extension. Note: large files or large file sets may be compressed using a standard zip-compatible format. In these cases, the ".zip" filename extension shall be used to indicate a compressed file format.

[SOW-418] The source files of documentation artefacts shall be stored and managed without version number in the filename. Only submitted and final versions shall have a version number and shall be stored separately from their source files.

8.3.2 Language, Style and Formatting Conventions

[SOW-419] Documentation artefacts shall be written in the English language.

[SOW-420] Documentation artefacts shall be written using standard English abbreviations only and the use of non-common English acronyms shall be avoided.

[SOW-421] The use of capitalization of words/terms within documentation artefacts beyond English spelling and grammar rules, shall be avoided.

[SOW-422] Documentation artefacts shall be written using the following number, date and time conventions:
(1) The convention to be used for numbers is for a comma to be the thousands separator and a period to be the decimal separator (e.g. 1,365,276.24);
(2) The convention to be used for dates (e.g. quoting dates of meetings) is in the order of day-month-year and not month-day-year; and
(3) The convention to be used for times shall be 24-hour clock format.

[SOW-423] Documentation artefacts shall be based on style templates, which shall be proposed by the Contractor and agreed by the Purchaser.

[SOW-424] Documentation artefacts shall adhere to the same presentation style (cover pages, headers, footers, headings and paragraphs, font types and sizes, etc.).

[SOW-425] The layout and make-up of documentation artefacts shall be suitable for electronic reading in PDF format.

[SOW-426] The documentation artefact cover page (or equivalent cover slide or cover sheet) shall identify:
(1) The document title, contract title, contract number, and originator;
(2) Configuration management information, version number, issue date and NCAGE, if applicable;
(3) The name and version number of the software it refers to, if applicable; and
(4) Classification within headers and footers with the highest classification of information contained in the entire document.

[SOW-427] Documentation artefacts shall contain a table of contents. It shall be noted that depending on the type of artefact, a table of contents might not be required. The exclusion of a table of contents shall be agreed by the Purchaser prior to developing the documentation artefact.

[SOW-428] Documentation artefacts shall use sans-serif fonts (e.g. Calibri, Arial, Helvetica, etc.), and obey the following principles:

(1) Headings shall be numbered and use bold font styles of sizes higher than the body text (the higher the heading in the document hierarchy, the larger the font size);
(2) No document shall use headings below level 6 (i.e. 1.1.1.2.3.1 Heading Text);
(3) Body text (under the headings) shall not use font sizes smaller than Calibri 12 pt. (or equivalent size if another font is selected);
(4) Any graphic material produced, including network diagrams, shall not use font sizes smaller than Calibri 10 (or equivalent size if another font is selected); and
(5) Larger font sizes than those specified above shall be selected if the corresponding text or drawing is to be reduced in size when embedded in the document, in order to guarantee that the PDF output keeps the font size as specified.

[SOW-429] Documentation artefacts developed in Microsoft Word shall be printable, if required, and therefore the page format shall be A4, printable in loose-leaf form.

[SOW-430] Where documentation artefacts contain many complex specialized or strongly domain oriented terminologies, these shall be defined in a glossary.

8.4 Project Management Plan

[SOW-431] The PMP shall describe the project organization and identify key personnel in the project organization, their qualifications, and their responsibilities.

[SOW-432] The PMP shall describe all aspects of the project implementation, including the Contractor's project management approach, project control processes, used standards, and external relationships necessary to provide the deliverables.

[SOW-433] The PMP shall describe personnel assignments with specification of the personnel target capacity required at Effective Date of Contract. Note: Target capacity is to be understood as full-time equivalent (FTE) by role/function, for example x FTE full-stack software developer; it is not needed to identify Contractor personnel by name, except for key personnel.

[SOW-434] The PMP shall specify and dimension the number of NSF user accounts, the Microsoft Azure Cloud Services and additional tooling that are required throughout the period of performance of the Contract (see Section 3.5).

[SOW-435] The PMP shall describe the Contractors' approach for establishing the project organization, bringing the project team at target capacity, and conducting knowledge build-up and preparations. The approach shall include justifications and identify assumptions and constraints in order for the Purchaser to assess the feasibility of the approach.

[SOW-436] The PMP shall identify all major Contractor operating entities and any Subcontractors involved in the work and describe the portion of the overall effort and deliverables allocated to them.

[SOW-437] The PMP shall describe how the various project management processes (quality management, configuration management, risk management, issue management, etc.) are integrated, either via a tool set and/or internal project management practices.

[SOW-438] The PMP shall describe the Contractor's and Subcontractors' approach to security management, including personnel and facility security.

[SOW-439] The PMP shall identify assumptions and constraints.

[SOW-440] The PMP shall describe methodology used for cost and schedule estimation.

[SOW-441] The PMP shall include a product breakdown structure (PBS) identifying all services and deliverables, with reference to the CLINs for traceability.

[SOW-442] The PMP shall include a PMS (see 8.4.1) as an annex.

[SOW-443] The PMP shall define all major milestones and major activities, all expected Purchaser involvements and all expected purchaser furnished property and services and associated timelines.

[SOW-444] The PMP shall be sufficiently detailed to ensure that the Purchaser is able to assess the Contractor plans, capabilities, and ability to satisfactorily implement the entire scope in conformance with the requirements of the Contract.

[SOW-445] Each revision of the PMP shall be accompanied by a summary of the changes together with impact statement for Purchaser assessment.

8.4.1 Project Master Schedule

[SOW-446] The PMS shall define all major milestones and major activities, with reference to the element of the product breakdown structure, the breakdown and durations of each activity, and the Contract end date.

[SOW-447] The PMS shall specify a level-of-effort (LOE) in number of person-days for each of the activities/deliverables.

[SOW-448] The PMS shall include a Gantt chart where the start and finish dates of the WPs and phases are depicted, and it shall from this schedule be possible to identify the timeframe when a specific deliverable is planned to be delivered.

[SOW-449] The PMS shall include all major milestones, phases and activities within a WP, including:
(1) CAW and EDC (note: for this project CAW=EDC);
(2) Phase start and finish dates;
(3) All contract milestones, including product or sub-product delivery timelines;
(4) All major milestones and activities;
(5) Other milestones and activities that requiring Purchaser and/or user involvement; and
(6) All sprints, including planning and review meetings.

[SOW-450] The PMS shall depict the sequence, start and finish dates, durations, and relationships among milestones and activities.

8.5 Risks, Actions, Issues, Decisions Register

[SOW-451] The RAID register shall be used to record and track all project risks, action items, issues and decisions.

[SOW-452] The RAID register shall be exportable to Microsoft Excel.

8.5.1 Risk Register

[SOW-453] The Risk Register within the RAID register shall list all project risks and for each risk indicate the following information (but not limited to):
(1) Risk identifier: unique code to allow grouping of all information on this risk;

(2) Risk category (e.g. management, technical, schedule, quality and cost risks);
(3) Description: brief description of the risk pointing on the uncertain event (risk), and its cause or causes;
(4) Impact: description of the effect on the project if this risk were to occur;
(5) Impact assessment: estimate the impact of the risk using five (5) level scale
(6) Probability: estimate of the likelihood of the risk occurring using five (5) level scale;
(7) Risk rating (High, Medium, Low);
(8) Proximity: how close in time is the risk likely to occur;
(9) Response strategy: avoidance, mitigation, acceptance, transference;
(10) Response plan(s): what actions have been taken/will be taken to counter this risk;
(11) Owner: who has been appointed to keep an eye on this risk;
(12) Status: e.g. closed, reducing, increasing, no change;
(13) Date of last update: when was the status of this risk last reviewed;
(14) Originator: who submitted the risk; and
(15) Date identified: when was the risk first identified.

8.5.2 Action Register

[SOW-454] The Action Register within the RAID register shall list all action items, and for each action item indicate the following information (but not limited to):
(1) Action identifier: unique identifier of the action item;
(2) Description: brief description of the action item;
(3) Owner: who is responsible for the action item;
(4) Date identified: when was the action item was raised;
(5) Due date: when the action item is expected to be completed;
(6) Status: e.g. open, closed, obsolete; and
(7) Date status update: when the action item's status changed.

8.5.3 Issue Register

[SOW-455] The Issue Register within the RAID register shall list all issues that require formal management by the project and for each issue indicate the following information (but not limited to):
(1) Issue identifier: unique identifier of the issue;
(2) Issue type (request for change, project issue, problem or concern);
(3) Description: brief description of the issue and its impact;
(4) Severity: Statement of the severity of the issue;
(5) Owner: who is responsible to deal with the issue;
(6) Date raised: when was the issue first raised/encountered;
(7) Originator: who identified the issue;
(8) Status: e.g. closed, reducing, increasing, no change; and
(9) Date status update: when the issue's status changed.

8.5.4 Decision Register

[SOW-456] The Decision Register with in the RAID register shall list all taken decisions and for each decision indicate the following information (but not limited to):
(1) Decision identifier: unique identifier of the decision;
(2) Description: brief description of the decision;
(3) Date approved: when was the decision taken approved; and

(4) Approved by: reference to the Purchaser's approver.

[SOW-457] All decisions entered on the register shall be submitted for Purchaser approval and the status shown on the register.

8.6 Project Highlight Report

[SOW-458] The Contractor's PHR shall include at least:

(1) Summary of contract activities during the preceding period, including the status of current and pending activities;
(2) Progress of work and schedule status against the PMS, highlighting any changes since the preceding report;
(3) Status of action items and decisions;
(4) Description of any identified problems, anomalies and high risk areas with proposed solutions and corrective actions;
(5) Test(s) conducted and their results;
(6) Provisional financial status and predicted invoices;
(7) Changes in key Contractor personnel, as approved by the Purchaser;
(8) Summary of Change Requests requested, recommended or approved;
(9) Summary of any analysis conducted; and
(10) Plans and dates for activities during the next reporting period.

8.7 Master Test Plan

[SOW-459] The Contractor shall identify and describe in the MTP which best practices and international standards will be applied and how.

[SOW-460] The Contractor shall produce a Master Test Plan (MTP) to address the plans for each TV&V activities listed in this document. The Purchaser will monitor and inspect the Contractor's MTP activities to ensure compliance.

[SOW-461] The Contractor shall describe how the Quality Based Testing is addressed and implemented in the MTP. Figure Product Quality Criteria is based on ISO 25010 and should be used as product quality criteria model.

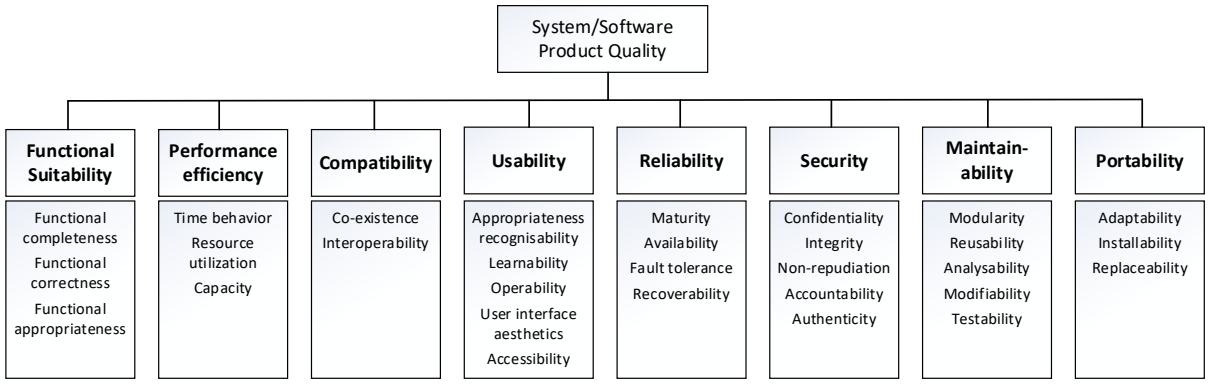

Figure 8.1 - Product Quality Criteria

[SOW-462] The Contractor shall describe all formal TV&V activities in the MTP with a testing methodology and strategy that fit the development methodology chosen by the project.

[SOW-463] The Contractor proposed testing methodology shall describe the method of achieving all the test phases successfully.

[SOW-464] The Contractor shall describe in the MTP how the following objectives will be met:
(1) Compliance with the requirements of the Contract;
(2) Verification that the design produces the capability required
(3) Compatibility among internal system components
(4) Compliance with external system interfaces and/or systems
(5) Compliance with the SRS requirements
(6) Confidence that system defects are detected early and tracked through to correction, including re-test and regression approach
(7) Compliance with Purchaser policy and guidance (i.e. security regulations, etc.)
(8) Operational readiness and suitability
(9) Product Quality Criteria (Figure 8.1)
(10) Identify which platform(s) to be used for the test events and the responsibilities for operation and maintenance of the environment.

[SOW-465] The Contractor shall describe in the MTP the Contractor's test organization and its relationship with the Contractor's Project Management Office and Quality Assurance (QA) functions.

[SOW-466] The Contractor shall describe in the MTP "Entry", and "Exit" criteria for each of the formal TV&V events. The Contractor shall seek approval of all criteria related to an event not later than the Test Readiness Review (TRR) meeting of the event.

[SOW-467] The Contractor shall provide the schedule in the MTP location and scope for all the events to be run, specifying to which phase they belong, and for the provision of the test related deliverables and detail the conduct of testing. When the Contractor identifies that multiple events are required for a phase, this shall also be specified in the MTP.

[SOW-468] Together with the MTP, the Contractor shall provide a defect reporting and management process to be applied during the TV&V activities.

[SOW-469] The Contractor shall describe how defects/non-conformances encountered during TV&V events will be reported, managed and remedied

The MTP shall include the Contractor's approach to Test Reviews including Test Readiness Reviews and Event Review Meetings for each TV&V event.

8.8 Release and Deployment Plan

[SOW-470] The RDP shall document the Contractor's approach to all deployment and activation tasks, and describe (key) personnel involved and how it intends to meet the deployment and activation requirements of the Contract.

[SOW-471] The RDP shall detail the overall schedule of deployment and activation activities, including required off-site and on-site preparations, baseline installation and configuration activities, data migration activities, and activation activities.

[SOW-472] The RDP shall cover the deployment of each baseline release of each module and include an agreed process for transitioning from the current baseline to the newly installed baseline.

[SOW-473] The RDP shall include “back-out” procedures for deactivating and removing the newly installed baseline and restoring existing services if any part of the new baseline is found to be interfering with the operation of other Purchaser capabilities.

[SOW-474] The RDP shall include activation test procedures and test cases that verify that the newly baseline has been installed and configured correctly and is fully functional, including the interfaces to/with external capabilities and services.

8.9 Training

8.9.1 Training Plan

[SOW-475] The Contractor’s Training Plan shall describe in a coherent way how training will be developed, delivered, and maintained throughout the life of the capability.

[SOW-476] As a minimum, the Training Plan shall cover the following:

(1) Summary of the Training Program scope (product, user types, baselines and the contractual scope);
(2) Training Organization;
(3) Training Methodology and Planning:
    (a) Analysis
    (b) Design
    (c) Development
    (d) Conduct
    (e) Evaluation
(4) Approach to TNA;
(5) Training delivery Student pre-requisites for each role:
    (a) Training courses
    (b) Training schedule (in line with PMS)
    (c) Training facilities
(6) Training courses development:
    (a) Training materials
    (b) Updating Training Materials
(7) Course quality assessment and evaluation.

[SOW-477] The Training Plan shall describe the training documentation for each course, including but not limited to the course plans, time schedules, and instructors in addition to CCD III.

[SOW-478] The Training Plan shall describe the quality management process for training.

[SOW-479] The Training Plan shall propose a training schedule, in relation to the overall Contract schedule.

[SOW-480] The Contractor shall recommend in this plan the delivery types of training (i.e. face-to-face, live online, self-paced online, hybrid or blended learning) and the rationale for those recommendations for each type of training (User, Administrator, train the trainer, etc.).

[SOW-481] The Training Plan shall describe the process for student assessment and Training Evaluation.

8.9.2 Definitions

8.9.2.1 Training Delivery Types

[181] Face-to-face learning: Students and instructor are physically present in the same training facilities at the same time (synchronously).

[182] Live online learning: Students and instructor are in different geographical locations, and they connect to the same digital training environment at the same time (synchronously). Live online was previously known as Remote Delivery.

[183] Self-paced online learning: Learning activity that is not led by an instructor where students access online learning materials individually, at a time of their own choosing, (asynchronously) and from any geographical location. They spend as much time on the training activity as they choose or is required. Self-paced online learning can range from full modules of several hours of training time (eLearning) to 'micro-learning' that only covers a few minutes of focused instruction or performance support.

[184] Hybrid learning: The instructor is physically present in one of the training facilities, together with a number of students. In addition, there are students in other geographical locations who connect virtually to the same physical classroom, at the same time (synchronously).

[185] Blended learning: Multiple delivery types are used within the bounds of achieving the same course objectives, most commonly using self-paced online as a precursor to live online, Mobile Training Team (MTT), or face-to-face.

8.9.2.2 Training Materials definitions

[186] Training Syllabus: Training Syllabus consists of the following elements:
(a) Course title;
(b) Course description;
(c) Learning objectives, as identified in the TNA;
(d) Instructional methodologies to be employed in the delivery of the course;
(e) Total number of instructional hours;
(f) In-class assignments or laboratories;
(g) Evaluation tools; and
(h) Performance standards.

[187] Student Manuals: Student Manuals are reference handbooks to be used and retained by the students. The Student Manual describes the concepts, functions, and features presented in the course, including links or references to the relevant documentation included in the system.

[188] Handouts: Handouts are additional aids that can supplement the student manuals when covering areas identified as difficult and/or particularly important. Handouts cover alternative approaches and provide realistic examples of task execution.

[189] Instructor Guides: Instructor guides are the procedures and specific instructions for use by the instructors during the planning, preparation, execution as well as close out of specific training activities. The Instructor Guide is best structured as a series of outline lessons, providing key points for the instructor to stress, some sample questions to ask, appropriate times to inject student progress tests and practical exercises, other instructional tips, and any activity aiding student learning of the related training objective.

[190] Master Lesson Plans: Master lesson plans are generally used to provide detailed guidance and the required supporting materials (e.g., electronic presentations) in order to minimize the preparation time for the instructor cadre.

[191] Training Presentations: Training presentations reflect the Course Lesson Plan and include all of slides for delivery of the course content.

8.9.2.3 Additional terms and definitions

[192] eLearning: Self-paced online learning, covering a complete or partial course.

[193] Micro-learning: Self-paced online learning that focuses on one or two learning objectives, and usually covers a few minutes of focused instruction or performance support.

[194] Online tutorial: Online manuals or online help e.g. in pdf format. These are systems related documents and are not part of the training.

[195] TNA: a series of activities within the Global Programming – Development Methodology which results with a set of Education and Training (E&T) solutions that satisfy a Requirements Package. This defines the objectives required to eliminate gaps and the necessary plans which result in the delivery of E&T solutions.

[196] Course Control Documents (CCDs): A set of documents used to define a NATO E&IT solution based on an E&IT requirement. Alternative formats include: Programme of Instruction, Qualification Standard, Training Plan, Curriculum and Syllabus.

[197] NCI Agency Learning Management System (LMS): The LMS managed by NCI Academy. LMS is used to host the SCORM compliant eLearning content.

8.10 Configuration Management Plan

[SOW-482] The CMP shall comply with the requirements and the format defined within [ACMP-2009-SRD-41].

[SOW-483] The Contractor shall analyse the Purchaser's configuration management procedures and tools, and incorporate those in the software configuration management process.

[SOW-484] The CMP shall define software configuration management process of the functional and physical characteristics of the configuration items, including interfaces and configuration identification documentation.

[SOW-485] In preparing the CMP the Contractor shall:

(1) Ensure that all required elements of configuration management are documented in such a manner as to provide a comprehensive configuration management program;

(2) Identify the means by which continuity of effort and understanding is achieved between the Contractor (prime) and its Subcontractors, if any, and between the project manager and the configuration manager, and internally within the organization, for the allocated configuration items, integrating, interfacing or otherwise related configuration items, supplier organizations, test and evaluation activities, and managers; and

(3) Establish his internal configuration management requirements for the Contract.

[SOW-486] The CMP shall identify explicitly any format and content requirements in [ACMP-2009-SRD-41] deemed by the Contractor to be not applicable for the Contract.

The relevant sections shall be marked not applicable (N/A) followed by a short justification why the requirement is considered not applicable. Note: Requirements in [ACMP-2009-SRD-41] that are readily expected to be declared N/A for a software acquisition are found in:
(1) Paragraph 3.2.1 - Hardware Configuration Item Identification;
(2) Paragraph 3.7 - Drawing library; and
(3) Paragraph 5.1.3 - Interface Control Working Group.

[SOW-487] The CMP shall define the configuration management organization including the configuration manager role and any other supporting configuration management personnel.

[SOW-488] The CMP shall be tailored, specifically addressing how configuration management shall be performed using an incremental delivery approach and iterative development process and integrate with NSF.

[SOW-489] The CMP shall identify the alternative means and tools proposed by the Purchaser beyond the Azure DevOps tools furnished by the NSF in order to meet the configuration management requirements.

[SOW-490] The CMP shall identify and define all top-level configuration items to be delivered under this Contract and where these top-level configuration items are traced to deliverables as defined in the product breakdown structure and SSS.

[SOW-491] As per requirements specified in Section 3.9, the CPM shall include the definitions of:
(1) The types of configuration baselines; and
(2) Configuration Status Accounting (CSA), Functional and Physical Configuration Audits, by specifying the inputs, outputs, timing and the resources.

[SOW-492] The CMP shall define the template for engineering change proposals (ECP), which as a minimum shall include the elements specified by the template in Annex D.1.

[SOW-493] The CMP shall define the template for RFD /RFW, which as a minimum shall include the elements specified by the template in Annex D.2.

8.11 Quality

8.11.1 Definitions

[198] Unless otherwise specified in the SOW, [STANAG-4107] and underpinning AQAPs, [ISO-9000:2015], PRINCE2 and ITIL definitions shall apply.

[199] QA is a process and set of procedures intended to ensure that a product or service, during its definition, design, development, test and deployment phases will meet specified requirements.

[200] 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.

[201] Under the Contract, the terms “QA process” will also include Quality Control process.

[202] A “project document” is a document developed and maintained to help in the management of the project. Typically the plans (amongst which, the Quality Assurance Plan (QAP)) are project documents.

[203] The term "NATO Quality Assurance Representative" (NQAR) shall apply to any of the Purchaser appointed Quality Assurance Representative.

[204] The term "Contractor Quality Assurance Representative" (CQAR) shall apply to any of the Contractor appointed Quality Assurance Representative.

8.11.2 Roles and responsibilities

[205] During the entire Contract implementation, the NQAR(s) assures the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirements. The Purchaser, through its NQAR(s), is the authority concerning all Quality related matters.

[SOW-494] The Contractor shall be responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the life-cycle of the Contract.

[SOW-495] The CQAR shall be accountable for the provision of the QA Plan and the compliance to the defined QA process.

[SOW-496] The CQAR(s) shall define the major quality checkpoints that will be implemented while executing the project and the quality process to be used at each checkpoint.

[SOW-497] The CQAR(s) shall be responsible for assessing that the Contractual requirements have been complied with, prior proposing the Contractual services and products.

[SOW-498] The CQAR shall report to a distinct manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.

[SOW-499] The CQAR shall be the point of contact for interface with and resolution of quality matters raised by the NCI Agency or its delegated NQAR.

[SOW-500] The Contractor shall support any NCI Agency or its delegated NQAR activity focused on monitoring Contractor activities at Contractor’s facilities or other sites related to the development, testing and implementation. In particular, the Contractor shall:

(1) Make himself/herself available to answer questions and provide information related to the project;
(2) Allow the Purchaser representatives to inspect and monitor testing activities, and management, technical and quality processes applicable to the project; and
(3) Transfer to the Purchaser representatives all information deemed necessary to perform the QA activities, on his/her own initiative or on request by the Purchaser representative.

[SOW-501] The Contractor shall ensure that CQAR(s) have the required qualifications, knowledge, skills, ability, practical experience and training for performing their tasks.

[SOW-502] The CQAR(s) shall have sufficient responsibility, resources, authority and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective actions.

[SOW-503] The CQAR(s) shall participate in the early planning and development stages to ensure that all quality related requirements are specified in plans, standards, specifications and documentation.

[SOW-504] After establishment of attributes, controls and procedures, the CQAR(s) shall ensure that all elements of the QA Process are properly executed, including inspections, tests, analysis, reviews and audits.

[SOW-505] The Contractor, through its CQAR(s), shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services which conform to contractual requirements only.

[SOW-506] The Contractor shall maintain and, when required, deliver objective evidence of this conformance.

[SOW-507] The Contractor shall give written notice to the NQAR(s) at least four weeks in advance that the services and/or products are being presented for review, testing, verification, validation and acceptance.

[SOW-508] Testing shall only be permitted by using test procedures and plans approved by the Purchaser.

8.11.3 Quality Management System

[SOW-509] The Contractor shall establish, document and maintain a Quality Management System (QMS) in accordance with the requirements of [ISO-9001:2015].

[SOW-510] The Contractor’s and Sub-Contractor’s QMS relevant to performance under the Contract shall be subject to continuous review and surveillance by the cognizant NQAR(s).

[SOW-511] The Contractor shall include in orders placed with its Sub-Contractor(s) and Supplier(s), the QMS requirements necessary to ensure the supplies and services covered by the Sub-Contract(s) and/or Purchase Orders conform to the requirements of the prime Contract.

[SOW-512] The Contractor shall specify in each order placed with its Sub-Contractor(s) and Supplier(s), the Purchaser’s and its NQAR(s) rights of access to all premises where contractual work is performed, in order to carry out audits, inspections, tests and other functions as may be required by the NQAR(s).

[SOW-513] If sub-contracted quality resources are used, the Contractor's Quality Management process shall describe the controls and processes in place for monitoring the Sub-Contractor's work against agreed timelines and levels of quality.

8.11.4 Quality Assurance process

[SOW-514] The Contractor's QA process shall ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.

[SOW-515] The requirements for these processes shall be derived from the Contract, the QMS, the applicable AQAPs and referenced best practices, in that sequence of priority.

[SOW-516] The Contractor shall perform verification and validation of the Contractual deliverables before proposing them for the Purchaser review and approval.

[SOW-517] The Contractor's QA process shall be described in the QA Plan as outlined below. The process is subject to approval by the Purchaser.

[SOW-518] The Contractor shall demonstrate, with the QA process, that the processes set up for design, develop, test, produce and maintain the product will assure the product will meet all the requirements.

[SOW-519] The Contractor shall assure that all the test and procedures used to demonstrate the requirements will be monitored and controlled under the QA process.

[SOW-520] On request, the Contractor shall provide the Purchaser with a copy of any Sub-Contracts or orders for products related to the Contract.

[SOW-521] The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser NQAR(s).

[SOW-522] The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

8.11.5 The Quality Assurance Plan

[SOW-523] The Contractor shall provide a QAP for review to the Purchaser in accordance with the requirements identified in the [AQAP-2105] (Reference to the [STANAG-4107]) and the SOW requirements.

[SOW-524] The Contractor's QAP shall be compatible and consistent with all other plans, specifications, documents and schedules, which are utilised under the Contract.

[SOW-525] All Contractor procedures referenced in the QAP shall either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.

[SOW-526] The QAP and all related QA procedures, and all their versions/revisions, shall be subject to NQAR(s) approval based on an agreed checklist.

[206] The acceptance of the QAP by the Purchaser only means that the Purchaser agrees to the Contractor’s approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

[SOW-527] The Contractor shall review his QA programme periodically and audit it for adequacy, compliance and effectiveness.

[SOW-528] The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

[SOW-529] 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-530] The Contractor shall include a risk management section within the QAP including the risks connected to the sub-Contractors of the Contractor.

[SOW-531] The Contractor shall make its quality records, and those of its Sub-Contractors, available for evaluation by the NQAR(s) throughout the duration of the Contract.

[SOW-532] The Contractor shall update the document, as required, from the delivery date of the initial QAP through Final Operating Capability (FOC), under Configuration control. The Contractor shall provide a copy of each new version of the QAP to the Purchaser for review and approval.

8.11.6 Quality for Project Documents

[SOW-533] A formal change management process shall be applied to all project documents, including documents naming conventions as defined by the Purchaser and coordinated with the Contractor.

[SOW-534] Project documents shall be configuration controlled. Each version of a project document is subject to Purchaser approval (unless otherwise specified).

[SOW-535] The Contractor shall ensure that any change related to the project documents are controlled, with the identity, approval status, version and date of issue are clearly identified.

[SOW-536] Project documents file names shall not contain any variable part, like version number, reviewer initials or maturity status. Version numbers and maturity status shall be marked in the document content and/or attributes.

8.11.7 Risks

[SOW-537] The Contractor and Sub-Contractor shall provide objective evidence, that risks are considered during planning, including but not limited to Risk Identification, Risk analysis, Risk Control and Risk Mitigation.

[SOW-538] The Contractor shall start planning with risk identification during Contract review and updated thereafter in a timely manner. The Purchaser reserve the right to reject Risk Plans and their revisions.

8.11.8 Defects

[SOW-539] The Contractor shall establish and implement a quality/product assurance Issue Tracking System (ITS) to ensure prompt tracking, documentation and correction of problems and deficiencies, during the lifecycle of the Contract.

[SOW-540] The ITS shall implement a lifecycle (status, responsibilities, relationship to affected Contract requirements, if applicable, and due dates) for each recorded defect.

[SOW-541] If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any supplies, the Contractor shall log it in the ITS, coordinate with the Purchaser and promptly correct it.

[SOW-542] The Contractor shall demonstrate that all deficiencies are solved / closed before product acceptance.

[SOW-543] When the Contractor establishes that a Sub-Contractor or a Purchaser Furnished Equipment (PFE) product is unsuitable for its intended use, it shall immediately report to and coordinate with the Purchaser the remedial actions to be taken.

[SOW-544] The Contractor shall ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.

8.11.9 Support Tools

[SOW-545] All tools used by the Contractor in the context of project execution shall be available for demonstration to the Purchaser, upon Purchaser request.

[SOW-546] 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.

8.11.10 Certificates of Conformity

[207] A Certificate of Conformity (CoC) is a document, signed by the Supplier / Vendor of a product, stating that the product conforms to contractual requirements and regulations. A CoC template is available in [AQAP-2070] (Reference to the [STANAG-4107]).

[208] The CoC, provides evidence that the items produced or shipped comply with test procedures and quality specifications prescribed by the customer.

[209] The Contractor is accountable for the conformance to requirements, of products provided to the Purchaser.

[SOW-547] The Contractor shall deliver all the CoC's for COTS products (software, including firmware and hardware) released by the COTS Vendors.

[SOW-548] The CoCs delivered by the Contractor shall be part of the acceptance data package of the product.

[SOW-549] The Contractor shall provide a CoC at release of product to the Purchaser unless otherwise instructed.

8.12 Integrated Product Support Plan

[SOW-550] The integrated product support plan (IPSP) shall specify how integrated product support will be designed, managed, procured and delivered, and how it intends to meet the integrated product support requirements of the Contract.

[SOW-551] The IPSP shall in general comply with the requirements and the format defined within [AI-16.31.03].

[SOW-552] The IPSP shall to meet the following requirements. Any requirements deemed by the Contractor to be not applicable for the Contract shall be marked not applicable (N/A) followed by a short justification why the requirement is deemed not applicable.

(1) **Introduction -** The IPSP shall provide general information on the purpose and scope of the IPSP and top-level supportability issues such as software description, management organization, milestone schedule, and indicate any applicable documents.
(2) **Supportability -** The IPSP shall describe the strategies for attaining IPS objectives within the context of the Contract. A description of the operational requirements and supportability objectives will provide essential information to ensure that supportability is thoroughly planned.
(3) **Operational and supportability requirements -** The IPSP shall briefly describe the mission scenarios and requirements, operational environment, security requirements, transportability requirements and employment.
(4) **Acquisition strategy -** The IPSP shall describe the anticipated third-party software and components (COTS and FOSS) acquisition approach.
(5) **Personnel requirements -** The IPSP shall describe actions to limit the requirements for a high degree of skill to support and maintain the software.
(6) **IPS element plans -** Provide details on plans for the IPS element (i.e. DEMETER with its documentation and training materiel).
    (a) Maintenance planning

(i) Describe the maintenance concept for the software including all levels of maintenance. Identify trade-offs to be performed and maintenance considerations peculiar to the software.
(ii) Identify maintenance tasks required to sustain the end item at a defined level of readiness, include all critical and high driver tasks.
(iii) Describe maintenance environment.
- Describe the maintenance environment, limitations, constraints, and requirements projected for the deployment timeframes.
- State the nature and extent of maintenance to be performed by each level of maintenance.
- Identify the organizational and logistic support structure that will be responsible for providing direct and general supply support and maintenance support.

(b) Personnel
(i) Describe the operation and maintenance personnel requirements.
(ii) Describe skill requirements for personnel necessary to operate, maintain, and support the end item. Consider the following:
- Present skills that may be used with little or no retraining.
- New skills required (skill evaluation and justification).
- Assigned duties.
- Task, skill, behaviour, and user interface analyses.

(iii) Identify safety and human factors constraints to help minimize problems with the user interface during operation, maintenance, and transport.
(c) Training
(i) Describe how training requirements will be met and who is responsible for meeting those requirements in reference to the Training Plan (Section 4.3.2.1).
(ii) Describe training requirements and plans unique to operation and maintenance of software.
(d) Packaging, handling, storage, and transportation (PHS&T)
(i) Describe requirements, management responsibilities, and procedures used to ensure that PHS&T requirements are identified and met in a timely manner.
(ii) Describe anticipated PHS&T modes and constraints.
(iii) Describe PHS&T assets required and those expected to be available/in-place.
(e) Supportability in fielding and operational life
(i) Initial fielding - Briefly describe planning for initial fielding and achieving initial operational capability. Summarize the procedure and schedule for preparation of all materiel fielding documentation. Provide information on how fielding will be implemented.
(ii) Transition - If applicable, provide a description of how and when the Integrated product support will be transferred from the Contractor to the Purchaser. Show how components usage, skills, training, procedures, technical data, and so forth will be obtained and used. Provide sufficient detail to assure that all

necessary data is provided in time to adequately provision, train, and maintain the software after transition.

8.12.1 In-Service Support Plan

[SOW-553] The In-Service Support Plan (ISSP) is an annex to the IPSP and shall cover the following as a minimum:

(1) The Contractor's support organization, roles, responsibilities, processes and procedures (from the first baseline release till FSA, during warranty and during the optional maintenance and support post the warranty period);
(2) Description of the capability of interest in scope of integrated support;
(3) Description of the integrated support concept, including the maintenance concept, warranty concept, support concept, service management & control concept, including but not limited to the incident, problem management, release and deployment management;
(4) Description of the parties involved, their responsibilities for the various levels of support (with indication of start and end dates), interfaces, response times and points of contact;
(5) Description and allocation of operation, service management & control and corrective, preventive, adaptive and perfective maintenance tasks required to operate and maintain the capability; and
(6) Procedures to follow in case of failures; Contractor response times for analyses and resolution.

8.13 Deliverable Requirements Traceability Matrix

[SOW-554] The DRTM shall be established to track the status of deliverables and contractual requirements throughout the contract lifecycle and prove that requirements have been fulfilled, verified and validated.

[SOW-555] The DRTM shall allow tracing of contractual requirements, to sprints, to design artefacts, to product backlog items, to test cases, to deliverables, and back.

[SOW-556] The DRTM shall for each contractual requirement include the agreed WP allocation.

[SOW-557] The DRTM shall include a Verification Cross Reference Matrix (VCRM) identifying the method(s) for verifying the requirements and trace requirement with test cases. The verification methods are defined in Table 8.1 - Verification Methods.

[SOW-558] The DRTM shall track the verification and validation status (e.g. Verified, Not Verified…) of all requirements.

[SOW-559] The DRTM shall track the verification and validation results of all requirements against test cases and test/verification/validation execution, with identification of the deliverable and baseline release, and include references to objective evidence supporting the assessment of each entry.

[SOW-560] The DRTM shall for each requirement that has been invoiced by the Contractor, record the Contractor's invoice number and the invoice date.

[SOW-561] The DRTM shall be delivered as an Excel spreadsheet where the information is organized and can be pivoted, filtered and sorted by column values as well as in the tooling provided by the Purchaser such that it is updated immediately as soon as changes are made.

[SOW-562] The DRTM Excel spreadsheet shall include a view that is importable into the DOORS application.

Table 8.1 - Verification Methods

Method	Description
Analysis	The processing of accumulated data obtained from other qualification methods. Examples are reduction, interpretation, or extrapolation of test results; analysing the performance of design by running simulations. This method can be used if a test scenario cannot be created at the test environment.
Test	The operation of the software element or component, using instrumentation or other special test equipment to collect data for later analysis. Controlled condition, configurations, and inputs are used in order to observe the response. Results are quantified and analysed. This method can be used where user interaction is involved and when computations with input data are necessary.
Demonstration	The operation of the software element or component, that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis. This method is used to prove a capability meets a requirement.
Inspection	The visual examination of software code, documentation, etc. This method can be used where testing is not possible (e.g. the maximum number of items used as a limitation inside the code).
Special Case	Any special qualification methods for the software element, such as special tools, techniques, procedures, facilities, and acceptance limits.

8.14 Interface Control Document

[SOW-563] The ICD shall document the service interfaces provisioned by the baseline (existing, updated or new), as well as the external service interfaces that the capabilities interact with. Service interfaces also include file-based exchange services.

[SOW-564] The ICD includes machine-readable interface files, in a standardized format/representation, i.e. OpenAPI for describing RESTful services, etc.

[SOW-565] The ICD shall include service specifications to document the services so that software developers implementing functionality that consumes the service will have sufficient information to build functionality that can successfully interact with the service.

[SOW-566] The service specifications shall, when applicable, include documentation of, or reference to, a conceptual information model.

[SOW-567] The service specifications shall include documentation of the business logic and business rules implemented by the service.

[SOW-568] The service specification shall include documentation on the service non-functional/ performance characteristics (e.g. response times).

8.15 Installation and Configuration Manual

[SOW-569] The installation and configuration manual shall describe the procedures to install, configure and activate the applications and shall cover the following topics at minimum:

(1) General introduction and description of the capabilities and of functional components and interfaces, with appropriate drawings;
(2) Prerequisites:
  (a) Platform requirements, including storage space;
  (b) Access rights to perform the installation;
  (c) Required interfaces to external services; and
  (d) Accounts and settings, i.e. ports, to operate and to maintain.
(3) Configuration of the platform and third-party software and components required to operate the capabilities;
(4) Configuration file information (location, content, available settings and purpose);
(5) Recovery procedures;
(6) Migration and update procedures as far as these are not covered by the automatic installation routines;
(7) Installation and configuration tasks, detailed step by step with screenshots of the feedback, displayed after each action;
(8) Backup, restore and maintenance procedures to be enabled;
(9) Activation checklist to verify correct installation and configuration; and
(10) Troubleshoot information and techniques to solve installation and configuration problems.

[SOW-570] For third-party products, maximum advantage shall be taken of the vendor-supplied third-party software and component documentation artefacts, however specific settings and procedures pertaining to the baseline delivered shall be covered by this manual, and in case there is no vendor-supplied documentation, this manual shall include all possible information needed to configure, manage and maintain the third-party product.

8.16 Maintenance and Administration Manual

[SOW-571] The maintenance and administration manual shall describe the procedures to perform the maintenance tasks as defined in the maintenance concept, and shall cover the following topics as a minimum:

(1) General introduction and description of the capabilities and of functional components and interfaces, with appropriate drawings;
(2) A full product breakdown of configuration items, including third-party software and components;
(3) Scheduled (preventive, adaptive and perfective) and unscheduled (corrective) maintenance procedures defining step-by-step how to perform the first, second and third level maintenance tasks and service management and control (SM&C) tasks for the configuration items;
(4) Usage of third-party applications or tools (if any) needed to configure, manage and maintain the capabilities;
(5) Configuration, use and the locations of the log files;
(6) Disaster recovery procedures, including backup and restore procedures;
(7) Database maintenance plan, including executable scripts; and
(8) Troubleshoot information and techniques to check for and solve a full range of (potential) problems or to enable workarounds.

[SOW-572] Each procedure described within the maintenance and administration manual shall incorporate the results of the operations and maintenance task analysis (OMTA) and include the following topics as a minimum:
(1) The support level to be assigned;
(2) Location/facility involved (if the operation is performed remotely, it has to be specified);
(3) Task duration and frequency, reusing Mean-Time Between Failure (MTBF) and Mean-Time to Repair (MTTR) data available (if applicable);
(4) Personnel skills required;
(5) Labour required;
(6) Tools required (if any); and
(7) The steps to perform the procedure.

[SOW-573] The task described within the maintenance and administration manual shall make reference to the different Purchaser operations and maintenance roles and identify where the interfacing between Contractor and Purchaser takes place.

[SOW-574] For third-party products, maximum advantage shall be taken of the vendor-supplied third-party software and component documentation artefacts, however specific settings and procedures pertaining to the baseline delivered shall be covered by this manual, and in case there is no vendor-supplied documentation, this manual shall include all possible information needed to configure, manage and maintain the third-party product.

8.17 Release Notes

[SOW-575] The release notes shall summarise the changes and the new features provided with the release and shall cover the following at minimum:
(1) Identification of the release, its media, and its associated artefacts;
(2) Overview;
(3) Intended audience;
(4) What's changed in this release:
  (a) List of new features (with reference work item);
  (b) List of enhancements (with reference work item);
  (c) List of fixes (with reference to work item);
  (d) List of updates to used third-party components which impact functionality; and
  (e) List of other changes (with reference work item).
(5) Installation:
  (a) Summary of new installation procedures; and
  (b) Summary of upgrade installation procedures.
(6) Security caveats; and
(7) Known issues and workarounds.

9 References

[210] These reference documents are providing contextual information that is relevant to this project. They shall be used by the Contractor to support his activity.

Table 9.1 - References

[ACMP-2009-SRD-41]	Examples of Configuration Management Plan Requirements, Ed.A V1, Mar 2017
[ACMP-2100]	The Core Set of Configuration Management Contractual Requirements, Ed.A V.2, Mar 2017
[AD-070-001]	ACO Directive 070-001 Allied Command Operations Security Directive, Dec 2021
[AI-16.31.03]	NCIA - Agency Instruction 16.31.03, Requirements for the preparation of IPSP, Sep 2022
[ALP-10]	NATO Guidance on Integrated Logistics Support for Multinational Armament Programs, Ed.C V1, 2017
[AQAP-2070]	NATO Mutual Government Quality Assurance (GQA) Process
[AQAP-2105]	NATO Requirements for Quality Plans, Ed.C V1, Jan 2019
[AQAP-2110]	NATO Quality Assurance Requirements for Design, Development and Production, Ed.D V1, Jun 2016
[AQAP-2210]	NATO Supplementary SQA Requirements to AQAP-2110 or AQAP-2310, Ed.A V2, Sep 2015
[AQAP 4107]	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications, Edition A, Version 2, Nov 2018
[ASD-AIA-SX000i]	International Specification for Integrated Product Support (IPS), Issue No.3.0, Apr 2021
[ASD-S3000L]	International Procedure Specification for Logistic Support Analysis (LSA), Issue No.2.0, Apr 2021
[ASOP-07.01.25]	NCI Academy Standard Operating Procedure - Grading and Assessment, May 2020
[ISO-9000:2015]	Quality management systems – Fundamentals and vocabulary
[ISO/IEC/IEEE-29119]	International Standard for Software Testing, 2022
[ISO/IEC/IEEE-29148]	International Standard for Systems and software engineering – Life cycle processes – Requirements engineering, 2011
[NATO-Bi-SC-DIR-075-007]	NATO Bi-SC Education and Individual Training Directive (E&ITD) 075-007, Sep 2015
[NCIA-AD-06.00.16]	NCIA - Agency Directive 06.00.16, Configuration Management, Feb 2020
[NCIA-AI-23.02]	NCIA - Agency Instruction 23.02, Deployment Management Planning, Oct 2019
[NCIA-AI-TECH-06.03.01]	NCIA - Agency Instruction 06.03.01, Identification of Software Assets, Jun 2016
[NCIA-SOP-06.03.05]	NCIA – Agency Standard Operating Procedure 06.03.05, Software Patch Management, Oct 2020
[NCIA-SOP-23.01]	NCIA – Agency Standard Operating Procedure 23.01, Enterprise IT Change Management, Mar 2020
[R-ICD-NIRIS]	Track Store Open API interface – original version to be provided

[R-ICD-FasInterop]	TOPFAS/LOGFAS ADL-FPH ORBAT Scemas version 2022.7
[R-ICD-Intel-FS-DM]	CO-115718-I2BE, INTEL-FS Spiral 2 NAF 4.0 L7 Information Model Data Dictionary - All Entities, Nov 8, 2022 4:58 PM
[R-ICD-TOPFAS-DM]	TOPFAS Increment-2 Software Design Specification Annex 1: Database Model (Desktop), 8/5/2020
[R-ICD-TOPFAS-Excel]	Empty Plan Collecting Sheet Months All Collectors, Dec 2022
[R-ICD-TOPFAS-ICD]	TOPFAS Increment-2 Software Design Specification Annex 3: Interface Control Document (Desktop), 15/09/2020
[SOA-IdM]	SOA-IDM Service Oriented Architecture (SOA) and Identity Management (IdM) Platform - Wave 1 - Interface Control Document (ICD) V15.0, Jun 2021 - System Design Specification (SDS) V9.3, May 2021
[STANAG-4107]	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications
[STANAG-4427]	Edition 3 - Configuration Management in System Life Cycle Management
[XSD-LC2IS]	Interface Control Document (ICD) for LC2IS Inc 2 Contract no CO-14463-LC2IS F0057 62794795 558 Rev M - Annex E LC2IS Inc 2 XML Schema Definition

[211] All documents are unclassified or NATO Unclassified, unless indicated otherwise.

10 Abbreviations and Acronyms

Abbreviation	Description
ABL	Allocated Baseline
ACMP	Allied Configuration Management Plan
AD	Agency Directive
API	Application Programming Interface
AQAP	Allied Quality Assurance Publication
BM	Battlespace Management
CA	Contract Award
CBT	Computer Based Training
CCB	Configuration Control Board
CCD	Course Control Document
CIAV	Coalition Interoperability Assurance and Validation
CIS	Communication and Information System
CLIN	Contract Line Item Number
CMDB	Configuration Management Database
CMP	Configuration Management Plan
COA	Course of Action
CoC	Certificate of Conformity
CONOPS	Concept of operations
COP	Common Operational Picture
COTS	Commercial-Off-The-Shelf
CPM	Contractor Project Manager
CQAR	Contractor Quality Assurance Representative
CRQ	change request
CSA	Configuration Status Accounting
CWIX	Coalition Warrior Interoperability Exercise
DDP	Delivery Duty Paid
DIF	Difficulty, Importance and Frequency
DMT	Data migration testing
DRTM	Deliverable Requirements Traceability Matrix
E&T	Education and Training
ECP	engineering change proposals
EDC	Effective Date of Contract
ELO	Enabling/Learning Objectives
FAQ	Frequently Asked Questions
FBL	Functional Baseline
FCA	Functional Configuration Audit
FFT	Friendly Force Track
FLC2	Future Land Command and Control
FMN	Federated Mission Networking
FOC	Final Operating Capability
FOSS	Free and open-source software
FSA	Final System Acceptance
FTE	Full-time Equivalent
GQA	Government Quality Assurance

Abbreviation	Description
HQ	Headquarters
ICD	Interface Control Document
IDL	inventory and distribution list
ILS	Integrated Logistics Support
IPS	Integrated Product Support
IPSP	Integrated Product Support Plan
ISO	International Organization for Standardization
ISSP	in-service support plan
IT	Information Technology
ITA	Italy
ITB	integration testbed
ITIL	Information Technology Infrastructure Library
ITS	Issue Tracking System
ITSM	IT Service Management
IVVQ	Independent Verification Validation and Quality
JFC	Joint Force Command
LATO	limited authorization to operate
LMS	Learning Management System
LOE	Level-of-effort
LSA	Logistic Support Analysis
LTS	long-term support
MTBF	Mean-Time Between Failure
MTP	Master test plan
MTT	Mobile Training Team
MTTR	Mean-Time to Repair
NATO	North Atlantic Treaty Organisation
NCI Agency	NATO Communications and Information Agency
NCIA	NATO Communications and Information Agency
NCS	NATO Command Structure
NFS	NATO Force Structure
NLD	Netherlands
NOR	Norway
NQAR	NATO Quality Assurance Representative
NR	NATO RΞSTRICTED
NS	NATO SΞCRET
NSF	NATO Software Factory
NSIP	NATO Security Investment Programme
NU	NATO UNCLASSIFIED
NVG	NATO Vector Graphics
OCR	Object Character Recognition
OEM	Original Equipment Manufacturer
OMTA	operations and maintenance task analysis
OSS	Open-Source Stack
PBL	Product Baseline
PBS	Product breakdown structure
PCA	Physical Configuration Audit

Abbreviation	Description
PCR	Project Checkpoint Review
PFE	Purchaser Furnished Equipment
PHR	Project Highlight Report
PHS&T	Packaging, handling, storage, and transportation
PM	Project manager
PMP	Project Management Plan
PMS	Project Master Schedule
PO	Performance Objectives
POL	Poland
PRINCE2	PRojects IN Controlled Environments (2nd edition)
PSA	Provisional System Acceptance
PSA^{WP1}	PSA for WP1
PSA^{WP2}	PSA for WP2
PSA^{WP3}	PSA for WP3
QA	Quality Assurance
QAP	Quality Assurance Plan
QC	Quality Control
QMS	Quality Management System
RACI	responsible, accountable, consulted and informed
RAID	Risks, Assumptions, Issues, Decisions
RDP	Release and Deployment Plan
RFD	Request for Deviation
RFW	Request for Waiver
RGP	Recognized Ground Picture
SA	Situational Awareness
SiAT	Site Acceptance Test
SCORM	Sharable Content Object Reference Model
SIT	System integration test
SM&C	service management and control
SOA-IDM	Service Oriented Architecture (SOA) and Identity Management (IdM)
SOW	Statement of Work
SRS	Software Requirements Specification
SSS	Schedule of Supplies and Services
STANAG	Standard NATO Agreements
SW	Software
TAR	Training Analysis Review
TCER	Training Course Evaluation Report
TDR	Training Design Review
TMR	Training Material Review
TNA	Training Needs Analysis
TRA	Training Requirements Analysis
TRR	Test Readiness Review
TUR	Türkiye
TVVA	Testing, Verification, Validation and Assurance
UAT	User Acceptance Test

Abbreviation	Description
USA	United States of America
VCRM	Verification Cross Reference Matrix
WG	Working group
WP	Work Package

Annex A Software Requirements Specifications

[212] The software requirements specification (SRS) will be provided as a separate file.

Annex B Interfaces

[213] Table 10.1 lists the interfaces to and from DEMETER that are not based on common standards.

[214] ICD documents are included for reference in order for the Contractor to be able to assess the complexity and scope; ICD documents may be updated during contract execution.

Table 10.1 – DEMETER non-standard interfaces

Group	Information Product	System	DEMETER Role	Communication Means	Description	Reference	#
Common Operational Picture (COP)	Recognized Air Picture	NIRIS	Consumer	API	As-is API requires development	[R-ICD-NIRIS]	1
	Recognized Logistics Picture	LOGFAS	Consumer	File over HTTP	Interop.2022/07	[R-ICD-FasInterop]	2
	Recognized Intelligence Picture	INTEL-FS	Consumer	XML Web Service	Open Api Content	[R-ICD-Intel-FS-DM]	3
Plans	Order of Battle	TOPFAS/ LOGFAS	Consumer	Files over HTTP	Interop.2022/07	[R-ICD-FasInterop]	4
	CONOPS	TOPFAS				[R-ICD-TOPFAS-DM] [R-ICD-TOPFAS-ICD] [R-ICD-TOPFAS-Excel]	5
	OPLAN	TOPFAS	Consumer	XML Web Service	OData (till 2027), Open API (from 2024)	[R-ICD-TOPFAS-DM] [R-ICD-TOPFAS-ICD] [R-ICD-TOPFAS-Excel]	6
Course of Action (COA)	COA	NIP/ TOPFAS	Producer/ Consumer	Files over HTTP	LC2IS Data Over Odata or Open API	[R-ICD-TOPFAS-DM] [R-ICD-TOPFAS-ICD] [R-ICD-TOPFAS-Excel]	7
Infrastructure	Identity	IdM	Producer/ Consumer	XML Web Service	SOA-IDM	[SOA-IdM]	8
Cross Domain	Security Labelling	Mail Guard	Producer	SMTP/EMAIL PAYLOAD	Mail Guard	[R-ICD-IEGC]	9

		IEG	Producer	XML Web Service		[R-ICD-IEGC]	10
Service Management and Control	SMC	ITSM	Producer	XML Web Service	Interface to ITSM for incident development	[R-ICD-ITSM]	11
Situation and Problem	Red ORBAT	INTEL-FS	Producer/ Consumer	XML Web Service	Open API/Odata	[R-ICD-Intel-FS-DM]	12
	Red COA	INTEL-FS	Producer/ Consumer	XML Web Service	Open API/Odata	[R-ICD-Intel-FS-DM]	13
	ICP - RFI Process	INTEL-FS	Producer/ Consumer	XML Web Service	Open API/Odata	[R-ICD-Intel-FS-DM]	14

[215] Table 10.2 lists the interfaces to and from DEMETER that are expected to be part of the COTS as they are based on standards as specified.

Table 10.2 – DEMETER standard interfaces

Group	Information Product	System	DEMETER Role	Communication Means	Description
Situational Awareness (SA) / Recognized Ground Picture (RGP)	Recognized Ground Picture		Producer	XML Web Service	Part of NVG
				Files over HTTP	Part of NVG
				Informal Messaging	ADatP 3
Common Operational Picture (COP)	Recognized Maritime Picture	TRITON/ MCCIS	Consumer	XML Web Service	NVG, ADatP 3
				Informal Messaging	NVG, ADatP 3
	Recognized Air Picture	NIRIS	Consumer	TCP/IP - UDP	Link16
	Recognized Logistics Picture	LOGFAS	Consumer	XML Web Service	EVE Web Services - ESS NVG
	Battle Space Object		Producer	XML Web Service	ADatP 4733 NVG

Battlespace Management (BM)				Files over HTTP	ADatP 4733 NVG
				Military Messaging	ADatP 3
Friendly Force Track (FFT)	FFT	National Systems	Consumer	IP1 (TCP/IP Client/Server)	ADatP 34
Synch Matrix	Synchronisation Matrix	NIP	Producer	Files over HTTP	Document/Power Point
Plans	Order of Battle	National Systems	Producer/ Consumer	XML Web Service	WSMP, MIM 4 IES
	CONOPS	NIP	Consumer	Files over HTTP	Portal Link
	OPLAN	NIP	Consumer	Files over HTTP	Portal Link
	Assesment		Producer	NVG/APP-11 ? (al OWNSITREP)	Document/Power Point, ADatP 4733 NVG, ADatP 3
ORDERS	ORDERS	NIP	Producer/ Consumer	Files over HTTP	WSMP, MIM 4 IES , ADatP3
Simulation	Order of Battle	JTLS/NATO Simulations	Producer	Files over HTTP	ADatP3
	Tasking	JTLS/NATO Simulations	Producer	Files over HTTP	ADatP3
	Battle Space Object	JTLS/NATO Simulations	Consumer	Military Messaging	ADatP3
Infrastructure	Data	SQL Database Cluster	Consumer	TCP/IP	As-is
	Files/Lists	NIP	Producer/ Consumer	Files over HTTP	As-is
PKI	NPKI	E-PKI	Consumer	HTTP + files	NATO PKI Service

Service Management and Control	SMC	SCOM/ ZABBIX	Producer	XML Web Service	Interface to Service Monitoring

[216] The following figure illustrates this in a diagram. Note that the version numbers mentioned are for illustrative purposes only as these will evolve over time.

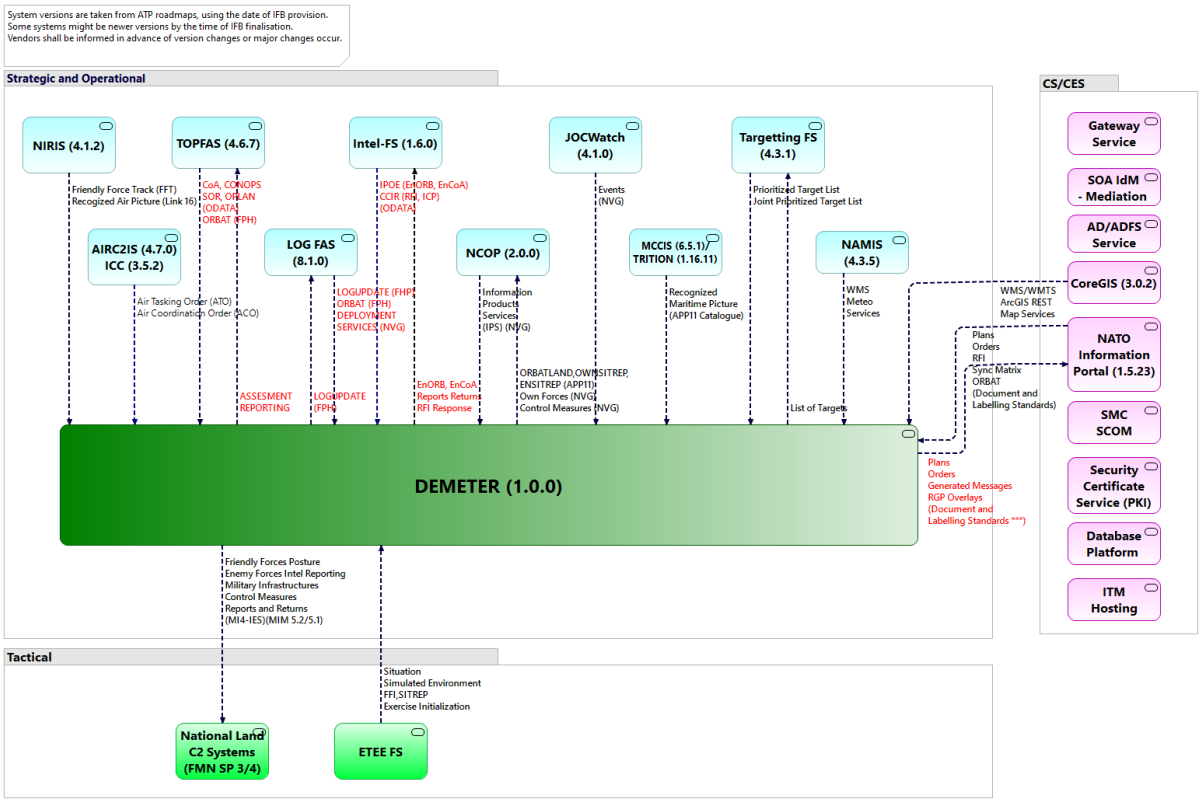

Figure 10.1 – DEMETER interfaces

Annex C Agency Approved Software (A2SL) – Required Documents

[217] The documents required to be submitted in order to obtain approval for the DEMETER application to be included on the A2SL is shown below.

		MAJOR / MINOR RELEASES	PATCH RELEASES
COMMON REQUIREMENTS	A&T Portfolio	✓	×
	Funding availability	✓	✓
	System Media	✓	✓
	Release information (Release Notes / Product Guide / Version Description document)	✓	✓
	Installation Instructions	✓	✓
	User Manual[1]	✓	×
	Administration Manual[2]	✓	×
	Security Settings[3]	✓	×
	Support Plan	✓	×
	Deployment Plan	✓	✓
	Design Description[4]	✓	×
ADDITIONAL REQUIREMENTS FOR NOTS	Requirement Traceability Matrix	✓	×
	Functional Test Report	✓	×
	User Acceptance Test Report[5]	✓	×
ADDITIONAL REQUIREMENTS FOR NEW SOFTWARE	CONOPS	✓	×

1 - User Manual is required for systems that have a human interface.
2 - 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.
5 - 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.

Annex D Templates

D.1 Engineering Change Proposal Template

[218] The ECP template will be provided separately.

D.2 Request for Deviation / Request for Waiver Template

[219] The RFD/RFW template will be provided separately.

DEMETER

IFB-CO-115791

BOOK II - PART IV SOW Annex A

SYSTEM REQUIREMENTS SPECIFICATION (SRS)

Document History

Edition	Date	Description
1.0	27/01/2023	SRS exported from NCIA Requirements Repository
2.0	23/02/2023	SRS exported from NCIA Requirements Repository after IFB feedback fixes. (Partial from CTO and full from security)

Table of Contents

Figures

No table of figures entries found.

Tables

No table of figures entries found.

1 Introduction

1.1 Document Purpose

This System Requirements Specification (SRS) contains the technical specifications for the system delivery of DEMETER. It describes the necessary functional, non-functional, interfaces and constraints to provide a comprehensive and complete description of the system.

1.2 Document Scope

The "Provide Land C2 System (DEMETER)" project is authorised as the NATO Security Investment Program (NSIP) project NSP017960, and shall provide the capability to the NATO Command Structure (NCS), support the planning, execution and assessment of land operations, to be interoperable with other CIS services in accordance with the Alliance requirements, and to integrate various inputs into an overall Recognised Ground Picture (RGP), which enhances the mission Common Operational Picture (COP), as Minimum Military Requirement (MMR).

This SRS contain Annex:

- Annex A.1. Glossary of Acronyms and Abbreviations: defines what acronyms and abbreviations used in the document stand for.

1.3 SRS Conventions

1.3.1 SRS structure

This SRS is structured to decompose the specified system into several functions and characteristics, each of them defined with a set of *Heading*, *Description* and *Requirement* elements.

1.3.1.1 Heading

Each system function or characteristic has its own *Heading*, together with a brief *Description*. Applicable *Requirements* are documented below *Headings* at the lowest hierarchy level.

1.3.1.2 Description

Each *Heading* is followed by a *Description* that might also include definitions, explanatory diagrams, figures and examples. All these elements provide context and relevant complementary information to *Requirement* statements, making them more unambiguous, complete and understandable.

1.3.1.3 Requirement

Each *Requirement* statement addresses only one system function or characteristic. Although *Description* text, context and definition of terms are not repeated inside a requirement statement, it shall be accepted that the *Requirement* is bound to them.

1.3.2 Requirements attributes

Requirements are formed by a structured set of elements (or attributes) that altogether compose a complete requirement. The requirement statement is the main element, as it formally expresses the need. However attributes are key to ensuring the requirement statement is understandable, as well as in supporting requirements management activities throughout the project lifecycle.

The whole attribute schema is defined and maintained in a formal SRS module located in the NCIA Requirements Repository (DOORS). Only a subset of these attributes are explicitly included in this SRS document, as exported from the NCIA Requirements Repository:

- **Requirement ID:** tag that uniquely identifies a requirement.
- **Verification Method:** chosen method to provide proof that the delivered system meets the requirement (possible values: Test, Demonstration, Analysis and Inspection).

1.3.3 Glossary of Terms Conventions

Terms used in requirements statements throughout this SRS document, for which there is an entry in the Glossary of Terms, will follow the following format:

- They will start with a capital letter.
- In case of a multiword term, words will be linked using the underscore "_" punctuation sign.

1.3.4 References Convention

References to external documents will be made to a short title following the format [[SHORT_REFERENCE_TITLE]]. The complete reference (full title, version, source, date, etc.) will be provided in section *2. References.*

Crossed-references to other sections in the SRS will be made to the section number and title following the format *[SECTION_NUMBER][SECTION TITLE].*

1.4 Verification methods

The requirements in this SRS will be verified using one of the methods described in the following subsections.

NOTE: In some cases, more than one verification method might be required in order to verify that a requirement has been fulfilled.

1.4.1 Inspection

Inspection is an examination of the item against applicable documentation to confirm compliance with requirements. It is the visual examination of a hardware item and associated descriptive documentation. Verification is based on the human senses or other means that use simple measurement and handling methods. No stimulus is necessary. Passive resources such as meter rule or gauge may be used. For software, traceable documentation and code inspection can be used.

For Non-Developmental Items (NDI), Modified NDI and Developmental Items, hardware inspection is used to determine if physical constraints are met, and hardware and/or software inspection is used to determine if physical quantity lists are met.

1.4.2 Analysis

Analysis is the review and processing of design products (documentation, drawings, presentations, etc.), or accumulated data obtained from other verification methods (such as manufacturer's tests of a product to be mass-produced), to verify that the system/component design meets the required design criteria. It may use analytical data or simulations under defined conditions to show theoretical compliance. Modelling and simulation may be used.

1.4.3 Testing

Testing is the operation of the system/service(s) (or a part of it), under controlled and specified either real or simulated conditions, generally using instrumentation, other special test equipment or specific test patterns to collect data for later analysis. This verification method usually requires recorded results to verify that the requirements have been satisfied. Input data and results are provided in the test procedures.

1.4.4 Demonstration

The operation of the system, or a part of the system/service(s), that relies on observable functional operation not requiring the use of instrumentation, special test equipment, or subsequent analysis. It is a qualitative exhibition of functional performance, usually accomplished with no or minimal instrumentation or test equipment.

2 References

The following list are referenced in the SRS using the abbreviated document titles given in square brackets […].

[R-RGP][AD 80-84 NATO Recognized Ground Picture]

[NREF-6][Allied Command Operations Comprehensive Operations Planning Directive COPD V2.0]

[NREF-7][ATP-3.2.2 Command and Control of Allied Land Forces]

[NREF-8][TIDE Transformational Baseline Version 4 NATO Vector Graphics Protocol 22 May 2015]

[R-4774-CMLS][STANAG 4774 Confidentiality Metadata Labelling Syntax - Edition A - Version 1]

[R-4778.2-BindProf][STANAG 4778.2 Profiles for Binding Metadata to a Data Object Edition A - Version 1 December 2020]

[NREF-11][AC/322-D(2019) 0038 (INV) CIS Security Technical and Implementation Directive for the Security of Web Applications.]

[AC_322-D_0048-REV3][Technical and Implementation Directive on CIS Security]

[R-NSIP][NATO Interoperability Standards and Profiles (NISP) Edition N, Version 1]

[R-ICD-AT-06.02.14-Map][Agency Technical Instruction AI Tech 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service 16 September 2016]

[R-ICD-Intel-FS-DM][CO-115718-I2BE, INTEL-FS Spiral 2 NAF 4.0 L7 Information Model Data Dictionary - All Entities Nov 8, 2022 4:58 PM]

[R-ICD-JOCWatch][JOCWatch 4.1 Interface Control Document Oct 2022]

[R-ICD-FasInterop][TOPFAS/LOGFAS ADL-FPH ORBAT Schemas version 2022.7]

[R-ICD-Namis][Interface Control Document NAMIS v3.4.16 version 1.0 date 21/11/2018]

[R-ICD-NCOP2][Interface Control Document NCOP2 ICD 7 June 2022]

[R-ICD-TOPFAS-DM][TOPFAS Increment-2 Software Design Specification Annex 1: Database Model (Desktop) 8/5/2020]

[R-ICD-TOPFAS-ICD][TOPFAS Increment-2 Software Design Specification Annex 3: Interface Control Document (Desktop) 15/09/2020]

[R-ICD-SOA_IdM][CO-14176-SOA-IDM Service Oriented Architecture (SOA) and Identity Management Platform (IdM) Wave I Interface Control Document (ICD) Doc. Version: 15.0 Date: 08/06/2021]

[R-ICD-TOPFAS-Excel][Empty Plan Collecting Sheet Months All Collectors Dated December 2022]

[R-SharePoint][Standard SharePoint message and content exchange protocols]

[R-ICD-LOGFAS][LOGFAS INTERFACE CONTROL DOCUMENT 30-Jan-23 Version 8.0.0]

[R-TD-NVG][TTB ANNEX N NATO Vector Graphics v2.0.2]

[C-M(2002)49][Security within the North Atlantic Treaty Organization]

[CM (2007)0118][NATO Information Management Policy (NMIP)]

[C-M (2011)0042][NATO Policy on Cyber Defence]

[AC/35-D/2004][Primary Directive on INFOSEC, NATO Security Policy supporting directive]

[C-M(2017)0062][NATO Enterprise Communications and Information (C&I) Vision]

[C-M(2015)0041][Alliance C3 Policy]

[C-(2008)0113(INV)][NATO Information Assurance Policy]

[C-M(2007)0118][NATO Information Management Policy (NMIP)]

[AC322-D(2019)0034 (INV)][C3B -Consultation Command & Control Board C3 TAXONOMY BASELINE 3.1]

[R_FMN][tide.act.nato.int/mediawiki/tidepedia/index.php/FMN_Spiral_Specification_Roadmap]

[R-ATP322][Command and Control of Allied Land Forces]

[R-TID-CISSec][NATO AC/322-D/0048 - Technical and Implementation Directive on CIS Security.]

[R-4774.2-MARKING][ADatP-4774.2 Guidance on the Digital labelling of NATO Information Edition A, Version 1 JUNE 2021]

[Ref-CCat][NATO Communications and Information Agency Costed Customer Services Catalogue v7.1 2023Service Definitions]

[Ref-DEFP][PO(2021)0360 Data Exploitation Framework Policy]

[R-ICD-IEGC][]

[R-STANAG-2211][STANAG 2211 - Geodetic Datum, Projections, Grids and Grid References (AGeoP-21) Edition A Version 1 February 2016]

3 System Requirements

3.1 General

Requirement ID: **SRS-001**

DEMETER is aligned with the NATO Vision detailed in [C-M (2017) 0062].

Verification Method: Inspection

Requirement ID: **SRS-002**

DEMETER is aligned with the NATO Alliance C3 policy detailed in [C-M (2015) 0041-REV2].

Verification Method: Inspection

3.2 Functions

3.2.1 Land Operations Planning Process Support

The Land Operations Planning activities are also performed in continues fashion, in different functional aspects and levels, supporting each other in a feedback loops, and traversing hierarchical levels of participating forces. They are usually triggered by specific events (rather expected or awaited) and/or decisions of commanders to respond to the situation. Planning has its own cycles on each level of operation. They start yet on strategic level and go down through joint operational level down to tactical one. In the context of this capability, Land domain planning is assumed between strategic command, joint headquarters and land component command so it covers operational and high-tactical levels. Preparation and visualization of Courses of Action is part of planning extent. The high level requirements addressed by this process support are; 1. Support to planning, assessment and execution of Land Operations 2. Maintain the Recognized Ground Picture 3. Enablement of Battle Space Management 4. Land information management 5. War gaming and simulation

3.2.1.1 Receive Process Planning Information

DEMETER uses the NATO Information Portal (NIP) for the purpose of sharing or collecting information products. DEMETER uses NIP as an Enterprise Information Management Tool (EIMT) storage or retrieval of files e.g. Information Products (IP).

Requirement ID: **SRS-003**

DEMETER allows the user read files (Information Products (IP)) from file system e.g. local/shared or NIP workspace.

Verification Method: Demonstration

Requirement ID: **SRS-004**

DEMETER allows the user to store NIP resources' (Documents, Images, Video) links (URL) within its entities (BSO's, Overlays, Other Objects (as appropriate)) for browsing purposes.

Verification Method: Demonstration

Requirement ID: **SRS-005**

DEMETER allows the user to open the hyperlinks that are linked to external NIP products.

Verification Method: Test

Requirement ID: **SRS-006**

DEMETER keeps the stored hyperlinks to the external entities e.g. NIP document in its information products, when the information product is exported or copied. Note that for various reasons (cross domain of user access rights) on target environment, hyperlinks cannot be reached.

Verification Method: Demonstration

Requirement ID: **SRS-007**

DEMETER may identify the changes, and notify the user, of the information products on NIP whose hyperlinks are stored in DEMETER.

Verification Method: Test

Requirement ID: **SRS-008**

DEMETER allows the user to write to file system e.g. local/shared or NIP) any Information Product (IP) produced in DEMETER such as overlays, documents, etc.

Verification Method: Test

3.2.1.2 Produce ORBAT

ORBAT, as an information product, is output from the Order of Battle Services and contains structural description of military organizational structures including all command relationships, rotation of forces, a transfer of authority, and changes to these factors over time. The Blue ORBAT is used to inform major commanders in peacetime and in periods of crisis and war of changes in the order of battle for coalition forces and thereby to assure that the most current information is available for operational planning. Federation with stakeholders mandates the dissemination, between units in the Land domain using Operational Command Information Systems (OPCIS), of battlespace geometry to represent planning and other battlefield entities and ORBAT/ TASKORG information using the Multinational Interoperability Programme (MIP) Information Exchange Specification.

Requirement ID: **SRS-009**

The user creates/updates/stores (maintains) ORBAT i.e. hierarchical organisation, command structure, type of relationship, strength, disposition of personnel and equipment and formations, between BSOs (BSO).

Verification Method: Demonstration

Requirement ID: **SRS-010**

DEMETER provides the user the capabilities to view and visually update the ORBAT hierarchy.

Verification Method: Demonstration

Requirement ID: **SRS-011**

DEMETER allows the operator to define multiple ORBATs e.g. base on multiple affiliation or hostility

Verification Method: Demonstration

Requirement ID: **SRS-012**

DEMETER allows the user to define reference ORBATs providing the units home hierarchical posture, or operational ORBAT/TASKORG, which provide hierarchies of units at missions/operations. Each phase or mission can have separate ORBAT/TASKORG.

Verification Method: Demonstration

Requirement ID: **SRS-013**

DEMETER allows the user to query BSOs (BSOs) based on one or more BSO attribute value, and within an information container e.g. overlay. Query results can be displayed, exported to file, and copied into clipboard for use by DEMETER or external MS Office application e.g. MS Excel.

Verification Method: Demonstration

Requirement ID: **SRS-014**

DEMETER allows the user to perform time boxed filtering of existing or historical BSO information, where user can select to display only those BSOs that have received updates between t (begin) and t (end).

Verification Method: Demonstration

Requirement ID: **SRS-015**

DEMETER allows user to access historical information of any BSO.

Verification Method: Demonstration

Requirement ID: **SRS-016**

DEMETER allows the user to filter BSOs based on any attribute value or multiple selection of BSOs, within a container e.g. overlay and produce a list of BSOs.

Verification Method: Demonstration

Requirement ID: **SRS-017**

DEMETER allows the user to define queries and filters to list a group of BSO/BSCM. DEMETER is able export this list in the same way it process overlays regarding conformance of standards, etc.

Verification Method: Demonstration

Requirement ID: **SRS-018**

DEMETER allows the user to export a list of BSOs obtained from query or filtering operation into a structured file for archiving, porting and future retrieval (capability to have mechanism to export/import DEMETER internal content to structure flat files).

Verification Method: Demonstration

3.2.1.3 Produce CONOPS

The CONOPS is mostly composed of textual content and is a "statement that directs the manner in which subordinate units cooperate to accomplish the mission and establishes the sequence of actions the force will use to achieve the end state." E.g. "Concept of the Operation: 1ABCT will accomplish this by conducting a penetration along multiple axes with TF 1-22 (DO) attacking to the south and TF 1-66 attacking to the north. Decisive to this operation is the seizure of OBJ LION. This is decisive because it will allow the division DO to attack east to BAYJI along an improved highway with a fixed crossing site over the wadi. Critical to this operation is the destruction of enemy reconnaissance forces west of the wadi and rapid improvement of crossing sites and passage operations. DEMETER takes part in planning process for short term land domain CONOPS development.

Requirement ID: **SRS-019**

DEMETER allows the user to create land CONOPS using the CONOPS templates provided by HQ.

Verification Method: Demonstration

Requirement ID: **SRS-020**

DEMETER allows the user to create CONOPS supporting products (possibly as an overlay).

Verification Method: Analysis

Requirement ID: **SRS-021**

DEMETER allows user groups to develop short term land CONOPS in a collaborative environment.

Verification Method: Analysis

Requirement ID: **SRS-022**

DEMETER allows user groups to develop short term land CONOPS documents using workflows (task assignments and process status).

Verification Method: Analysis

Requirement ID: **SRS-023**

DEMETER maintains configuration control and release of short term land CONOPS documents e.g. permits endorsement and sign-off process during the workflow process, versioning, etc.

Verification Method: Demonstration

Requirement ID: **SRS-024**

DEMETER allows the user to produce short term land CONOPS. The user is able to use information products from NATO Information Portal e.g. documents, copy relevant data from staff products (locations, textual content, etc.) and is able to paste into DEMETER CONOPS entities/overlays.

Verification Method: Demonstration

Requirement ID: **SRS-025**

DEMETER allows the user to disseminate short term land CONOPS, as a document that can be exchanged by email. Note: CONOPS is not a structured APP 11(D)(1) message.

Verification Method: Demonstration

Requirement ID: **SRS-026**

DEMETER allows the user to produce an initial short term land CONOPS by receiving HQ CONOPS relevant information from TOPFAS, to minimize manual entry or duplication of effort, for short term land CONOPS creation.

Verification Method: Demonstration

Requirement ID: **SRS-027**

DEMETER allows the user to maintain security classification labelling of short term land CONOPS created within DEMETER. Note: security labelling rules are stated in [NREF-JOEL]

Verification Method: Demonstration

3.2.1.4 Produce the Operation Plan (OPLAN)

This capability is a part of support for planning. OPLAN is specified in COPD, TOPFAS produce OPLAN in Operational and Strategic Level, and system may support OPLAN preparation process by providing planning artefacts that can be part of the main OPLAN.

Requirement ID: **SRS-028**

Those information elements (including BSO/BSCM overlays) georeferenced that are produced and maintained by TOPFAS as part of the OPLAN shall be made available to land planners for visualisation in DEMETER in the same format as the source (BSM/Overlays). The details, format and the protocols of the Information products are listed in [R-ICD-TOPFAS-ICD].

Verification Method: Demonstration

Requirement ID: **SRS-029**

DEMETER user is capable of producing BSO/BSCM overlays with planning information that can contribute to the OPLAN, which is developed in TOPFAS. The type and protocol of the information provided to TOPFAS shall comply with [R-ICD-TOPFAS-ICD] and in the form of NATO standard NVG Protocol standards[R-TIDE]

Verification Method: Demonstration

Requirement ID: **SRS-030**

DEMETER maintains configuration control and release of short term land OPLAN documents e.g. version control, endorsement and sign-off with a workflow.

Verification Method: Demonstration

3.2.1.5 Produce ORDERS

ORDERs are part of planning process. A collaborative environment is needed which allow production/endorsement/publishing of ORDERS (a workflow), as well as change tracking of ORDERS.

Requirement ID: **SRS-031**

DEMETER has a workflow management and execution capability for the production of ORDERS.

Verification Method: Demonstration

Requirement ID: **SRS-032**

DEMETER allows the user with the assigned user role and permissions to set the 'approval' status for an ORDER, which shall include "DRAFT", "REVIEWED", "FINAL" or "OBSOLETE" for those ORDERS submitted inside the workflow process.

Verification Method: Demonstration

Requirement ID: **SRS-033**

During the production of ORDERS, DEMETER informs the workflow participants about the progress of the ORDERS status e.g. notification of "REVIEW" or "FINAL".

Verification Method: Demonstration

Requirement ID: **SRS-034**

DEMETER allows authoritative user (e.g. Commander) to sign-off ORDER to allow its execution.

Verification Method: Demonstration

Requirement ID: **SRS-035**

DEMETER allows document templates to be assigned to an originator - a DEMETER user - and for each section of the template to be assigned to other DEMETER users to be add/amend their associated entries. The originator will be able to accept or reject section submissions as appropriate

Verification Method: Demonstration

Requirement ID: **SRS-036**

DEMETER allows the user to export information products contained within the ORDERS template e.g. graphical overlays, as independent information products. DEMETER produces FRAGO, WNGORDER documents with templates provided in accordance with the APP-11(D)(1) message catalogue.[NSIP]

Verification Method: Demonstration

Requirement ID: **SRS-037**

DEMETER allows the user to be able to transfer e.g. via copy/paste information from DEMETER overlays and/or NIP Information Products e.g. document, into ORDER templates.

Verification Method: Demonstration

Requirement ID: **SRS-038**

In DEMETER, the authorized user accesses ORDERS for viewing, or opens ORDERS for updates based upon its workflow status e.g. rejected, and now needs update for submission.

Verification Method: Demonstration

Requirement ID: **SRS-039**

DEMETER allows user to set security classification and releasability information for each ORDER in accordance with [N-JOEL].

Verification Method: Demonstration

Requirement ID: **SRS-040**

DEMETER allows the user to view the ORDER version history, including the changes/alterations between versions of the ORDER as well as which DEMETER user made the changes/alterations in each version.

Verification Method: Demonstration

Requirement ID: **SRS-041**

DEMETER allows the user to set the approver(s) of the ORDER as a part of ORDER generation collaboration.

Verification Method: Demonstration

Requirement ID: **SRS-042**

DEMETER allows the user to disseminate ORDERS in the correct format APP 11 (D)(1) so that it can be transferred to the destination with NATO formal message communication platforms (AIMS, NMS) manually. DEMETER allows the users to disseminate ORDERS in other formats via subordinates as well (like MIP or email).

Verification Method: Demonstration

Requirement ID: **SRS-043**

DEMETER may require maintaining the status of the different organisations to which the ORDER was sent to confirm that all ORDER are received and understood.

Verification Method: Demonstration

3.2.1.6 Enablement of decision making cycle

Requirement ID: **SRS-044**

DEMETER allows the workflow process to be assigned to user groups and to user selected information products, including graphical overlays.

Verification Method: Demonstration

Requirement ID: **SRS-045**

DEMETER allows the users to perform war-gaming. Possible types of war-gaming are attrition centric, logistics, asymmetric warfare, perception centric (MOOTW type issues). Correlation to campaign/phase objectives is possible and includes include Air, Maritime, SOF actions (EW, PSYOPS, IO etc.).

Verification Method: Demonstration

Rehearsal is a session in which the commander and staff or unit practices expected actions to improve performance during execution. Commanders use rehearsals to ensure staffs and subordinates understand the concept of operations and commander's intent. Rehearsals also allow leaders to practice synchronizing operations at times and places critical to mission accomplishment. Effective rehearsals imprint a mental picture of the sequence of the operation's key actions and improve mutual understanding among subordinate and supporting units and leaders.

Requirement ID: **SRS-046**

DEMETER has tools to perform RoC for the HQ. The tools has capability to provide timed snapshots of enemy and own forces status (holding, operational level, etc.). Has capability to allow user to slide time and observe each snapshots for assessment, has capability to update any snapshot regarding addition/removal of units as well as updating of the units status (holding, operational level, etc.).

Verification Method: Demonstration

Requirement ID: **SRS-047**

DEMETER user manages results of RoC drills, exports the results as video, document or image, DEMETER support association of RoC drill results with the RoC drills and plan changes implemented (capable of configuration control)

Verification Method: Demonstration

Requirement ID: **SRS-048**

DEMETER supports the usage of artificial/synthetic environment (i.e. RoC or Simulation sand-box) in which artificial nations with codes (from standards) can be defined/used in BSOs and control measures (BSCM).

Verification Method: Demonstration

Requirement ID: **SRS-049**

DEMETER supports exercise-operating mode in order to work in artificial environments.

Verification Method: Demonstration

Requirement ID: **SRS-050**

DEMETER battle space object nationality code complies with ISO 3166-1 standards.

Verification Method: Demonstration

Requirement ID: **SRS-051**

Affiliation is membership or allegiance to an ethnic group, country, functional group, exercise group, or religion. Country typed affiliation complies with ISO-3166 country code standards. DEMETER allows the user to use other affiliations such as functional group or exercise group (NATO, SITFOR), and associate units/entities with these new affiliations. In addition DEMETER is able to publish entities with these new affiliation values, where standards allow e.g. MIM 4 IES or NVG compliant.

Verification Method: Demonstration

Requirement ID: **SRS-052**

DEMETER has capability to receive data from simulations which shall be marked with "exercise", those provide results for courses of actions.

Verification Method: Demonstration

Requirement ID: **SRS-053**

DEMETER has tools to permit user comparison of CoA results, including overlay comparison based on some defined criteria e.g. time, casualty, space (geographical related achievements, etc.

Verification Method: Demonstration

Requirement ID: **SRS-054**

DEMETER allows the user to produce staff products for decision-making to support G1 to G9 HQ functional areas. DEMETER has tools to serve for the purpose of production of Staff products in each functional area (i.e. G1 Personnel, G2 Intelligence, G3 Operation, G4 Logistics, G5 Planning, G6 CIS, G7 Exercise and Training, G8 Finance, G9 CIMIC).

Verification Method: Demonstration

3.2.1.7 Understanding Situation and Problem

Requirement ID: **SRS-055**

DEMETER has the capability to visualize and browse details of the contents of the IPOE (containing Enemy ORBAT and Courses of Action) that is received from NATO Intelligence systems.

Verification Method: Demonstration

Requirement ID: **SRS-056**

DEMETER allows the user to produce (edit/delete) Enemy ORBAT and Enemy Courses of Action (CoA) within its overlay editing capability, assuming IPOE is formed of basically Enemy ORBAT and Enemy Course of Action. Note: Authoritative Data Source for Enemy ORBAT and Enemy CoA in NATO is INTEL-FS.

Verification Method: Demonstration

Requirement ID: **SRS-057**

DEMETER can edit any ORBAT and CoA, such as Enemy ORBAT and Enemy CoA e.g. IPOE, and in some cases it might request that the IPOE can be provided to INTEL-FS for viewing and assessment, in which case DEMETER is able to export enemy ORBAT and enemy CoA overlays in the form that INTEL-FS might use for its IPOE maintenance. Note: Authoritative Data Source for Enemy ORBAT and Enemy CoA in NATO is INTEL-FS.

Verification Method: Demonstration

Requirement ID: **SRS-058**

DEMETER supports the RFI process initiated from NATO intelligence system in respect to Intelligence Collection Plan.

Verification Method: Demonstration

Requirement ID: **SRS-059**

DEMETER has capability to provide automated RFI updates to NATO Intelligence system. The format of the RFI Request and Response are provided in [R-ICD-Intel-FS-DM]

Verification Method: Demonstration

Requirement ID: **SRS-060**

DEMETER has workspaces to bring together internal or external products into one presentable content, providing users the capability to combine videos, images as hover objects, annotations, links to Portal documents and DEMETER overlays in this workspace content. This allows the user to prepare mission analysis briefings using DEMETER.

Verification Method: Demonstration

Requirement ID: **SRS-061**

DEMETER has a presentation mode capability (e.g. mission analysis briefing overlay or other such DEMETER information products).

Verification Method: Demonstration

Requirement ID: **SRS-062**

DEMETER allows the users to edit planning overlays associated with commander's guidance. In addition any change on time-space of BSOs are recorded and associated to guidance provided. This includes versioning of overlays and change history, including reasons for changes. The guidance emphasizes in broad terms when, where and how the commander intends to mass his combat power to accomplish the mission according to his higher commander’s intent. Planning guidance includes priorities for all combat, CS, and combat service support (CSS) elements and the commander’s vision of the elements’ support of his concept [R-ATP322].

Verification Method: Demonstration

Requirement ID: **SRS-063**

DEMETER allows storage of textual additional information e.g. commander's intent, that can be associated to overlays. The commander's intent serves as a driver of planning, not as a product. Later in the operations process, the commander’s intent focuses subordinates’ initiative [REF CCIR][R-ATP322].

Verification Method: Demonstration

Requirement ID: **SRS-064**

DEMETER provides a briefing capability in which the presenter can provide DEMETER commanders initial intent clearly and use pointing and marking tools to support the presentation.

Verification Method: Demonstration

Requirement ID: **SRS-065**

DEMETER provides the capability to deliver snapshots from overlays that can be used in briefing documents e.g. MS PowerPoint or MS Word.

Verification Method: Demonstration

Requirement ID: **SRS-066**

DEMETER allows the user to store and update commanders planning guidance information as a version-controlled entity. Note that each version of commanders planning guidance can be associated different overlays.

Verification Method: Demonstration

Requirement ID: **SRS-067**

DEMETER allows the user to utilize an information product template repository e.g. repository containing products templates such as WNGO, and allows the user to populate the products generated from the template using elements within DEMETER e.g. overlays, BSO/BSCM content.

Verification Method: Demonstration

Requirement ID: **SRS-068**

DEMETER has a presentation mode capability e.g. back briefing overlay or other such DEMETER information products. Presented information can be preserved and versioned in case presentation needs to be recalled. The backbrief is normally performed throughout planning. It is a briefing by subordinates to the commander to review how subordinates intend to accomplish their mission. This briefing allows the commander to clarify his intent early in the subordinates' tactical estimate procedure. It allows the higher echelon commander to a. Identify problems in his concept of operations, b. Identify problems in a subordinate unit commander's concept, c. Learn how subordinates intend to accomplish their missions. [R-ATP322].

Verification Method: Demonstration

Requirement ID: **SRS-069**

DEMETER allows the user to maintain a list of land related CCIRs, its associated definitions which are linked to the land RFI list (also managed within DEMETER), including showing the date and the functional area, submitted RFI and subsequent response and time of response. DEMETER also allows tracking of RFIs submitted to HQ (not just Int.) with a capability to track when received the individual who assigned as well as response date.

Verification Method: Demonstration

3.2.1.8 Develop COA

Requirement ID: **SRS-070**

DEMETER shall have many comparison capabilities that allow user to compare different CoAs and situations. These capabilities include being able to obtain a summary of attribute information e.g. number of person, equipment by type, logistics by

type, for BSOs within a user defined/drawn geographic area or provision of multiple map displays side by side with separate CoAs e.g. for comparison of CoAs, time or space specific searches for comparison.

Verification Method: Demonstration

Requirement ID: **SRS-071**

DEMETER's battle space management capability shall allow users to develop CoAs for own and adversary entities without limitations e.g. all BSO and BSCM types with their attributes.

Verification Method: Demonstration

Requirement ID: **SRS-072**

DEMETER allows validation of CoAs based on such aspects as time and space of participating entities or ensuring a CoA is associated a decision.

Verification Method: Demonstration

Requirement ID: **SRS-073**

DEMETER allows the user to analyse CoAs by providing summary information from the CoA, such as units' locations, capabilities, availabilities ranges of operation, etc.

Verification Method: Demonstration

Requirement ID: **SRS-074**

DEMETER allows user to support provision of briefing of CoA overlays by presenting the subject overlay in a briefing mode (most convenient to briefing provision, marking, pointing, etc.).

Verification Method: Demonstration

Requirement ID: **SRS-075**

DEMETER allows user to support provision of briefing of CoA overlays by disseminating the overlay information in a format which can be utilized by any briefing tool.

Verification Method: Demonstration

Requirement ID: **SRS-076**

DEMETER initializes short term land specific CoAs from TOPFAS's HQ CoAs, to minimize manual entry or duplication of effort. The format of the CoA is provided in the [R-ICD-TOPFAS-ICD] and [R-ICD-TOPFAS-DM].

Verification Method: Demonstration

3.2.2 Land Operations Execution Process Support

Directing Execution of Land Operations covers decision-making, monitoring and control functions. When decision is taken and action tasked the ongoing monitoring, synchronization and de-confliction are exercised. During mission execution various

unexpected events and manoeuvres may happen which can invalidate initial plans and require tight coordination to avoid fratricide or counter-effective outcomes. This demands for short-time decision making cycles, highly active monitoring and timely communication and tasking. It may engage other military domains (air, space, maritime and SOF) and therefore utilization of liaising elements. The high level requirements addressed by this process support are; 1. Support for Planning, Assessment and Execution of and Operations 2. Maintenance and provision of recognized ground picture 3. Enablement of Battle Space Management.

Requirement ID: **SRS-077**

DEMETER hosts XML Web Services that provide Recognised Ground Picture information products. The services comply with FMN spiral specific procedural instructions (PI) for Situational Awareness Annex A (Recognised Ground Picture (RGP)).

Verification Method: Demonstration

Requirement ID: **SRS-078**

DEMETER displays to the user a geographical view of AOR populated with maps, elevation data and vector graphics to be able to visually maintain and display recognized ground picture.

Verification Method: Demonstration

Requirement ID: **SRS-079**

DEMETER allows an administrative user to set default map services for each or group of users, which be displayed automatically when that user starts using the application.

Verification Method: Demonstration

Requirement ID: **SRS-080**

The standard user is able to select and store as a preference which default map layer they need to display upon login to the map related function, e.g. Battle space management application.

Verification Method: Test

Requirement ID: **SRS-081**

DEMETER provides working spaces for overlay management for individual and group users e.g. a single user can produce a draft product whilst a group of users can produce products collaboratively.

Verification Method: Demonstration

Requirement ID: **SRS-082**

DEMETER allows the user to create all of the APP 6D(1) symbols as BSO/BSCMs in map viewer.

Verification Method: Demonstration

Requirement ID: **SRS-083**

DEMETER user can edit overlays those are produced by the user, or overlays formed by copying BSOs from overlays those are reports from external systems. Original overlays created from Reports by automatic process cannot be edited.

Verification Method: Demonstration

Requirement ID: **SRS-084**

DEMETER allows the user to update location of BSOs, either through drag and drop or pasting the location information upon BSO selection.

Verification Method: Demonstration

Requirement ID: **SRS-085**

DEMETER allows the user to query/browse multiple overlays for identification of duplicated BSOs.

Verification Method: Test

Requirement ID: **SRS-086**

DEMETER allows the user to manage access of overlays, such that users can create, edit, save and delete authorized overlays e.g. owned by self or group of users, and only view (read-only) some of the authorized overlays e.g. generated by system using FFI or MIP feeds or overlays owned by other users. Copy from these read-only overlays is also possible.

Verification Method: Test

Requirement ID: **SRS-087**

DEMETER allows the user to export (copy/paste or image snapshots) from DEMETER overlays into document templates of OPLANs and WGNO. The export shall provide a tabular list of BSO/BSCMs and/or screenshots of overlays presented on a geographical view.

Verification Method: Demonstration

Requirement ID: **SRS-088**

DEMETER allows the user to generate and publish RGP by fusing information from different source/reports.

Verification Method: Test

Requirement ID: **SRS-089**

DEMETER has planning objective BSOs, containing attributes for who, what , where ,and when for each OPLAN objective, allowing entity BSOs to then be **associated** to one more OPLAN Objective BSO as well as the **associated** ORDER (ref to document), therefore enabling assessment of the progress of the entity to meet the ORDER and OPAN objectives.

Verification Method: Test

An effect is defined as, '[a] change in the state of a system (or system element), that results from one or more actions, or other causes.' NATO uses effects in the planning for, and conduct of, operations at the military-strategic and operational levels. Derived from objectives, effects bridge the gap between objectives and actions by describing what changes in a system are required, including changes in the capabilities, behaviour or opinions (perceptions) of actors within the operations environment and to the strategic environment. Effects play a crucial role because they provide a focus for actions and contribute to the achievement of objectives and the end state. Effects must be measurable and should be limited in number [NREF-6] Therefore subordinates needs to take actions to create effects, effects are derived from objectives.

Requirement ID: **SRS-090**

DEMETER provides the capability to produce a sync matrix based on the user selection of entities, time, tasks, effects, etc. based on the ORDERs maintained within the DEMETER information product repository.

Verification Method: Demonstration

Requirement ID: **SRS-091**

DEMETER provides the capability to refine a sync matrix based on the user selection of entities, time, tasks, effects, etc. based on the ORDERs maintained within the DEMETER information product repository.

Verification Method: Demonstration

Requirement ID: **SRS-092**

DEMETER allows the user to visualize within the geo map viewer geo-referenced reports and/or export them to MS Word or PDF (provided from external entities) using the APP-11(D) message catalogue messages e.g. Enemy Land Forces Situation Report, NBC Basic Wind Data Report, Own Land Forces Situation Report, etc.

Verification Method: Demonstration

It is required establishing capability to monitor, synchronize and control timely manoeuvres and lethal or non-lethal actions of subordinate Land forces in the designated AOR.BSO, as information element, is a discrete entity, thing or being that does exist at a particular time and place on the battlespace and has military or civilian significance. The objects of interest belong to the following categories: military units (different granularity), vehicles/aircrafts/ships, movement tracks (FFT), vital environmental features of terrain, facilities of important meaning, etc. BSOs are elementary pieces of information gathered within Recognized Pictures

Terrain management is the process of allocating terrain by establishing areas of operations, designating assembly areas, and specifying locations for units and activities to deconflict activities that might interfere with each other. Commanders assigned AOs are responsible for terrain management within the boundaries of those AOs. Throughout operations, commanders manage terrain within their boundaries by assigning subordinate units areas and positions. Their command posts track unit locations and movements and adjust control measures to deconflict space and control movements within their AOs

Requirement ID: **SRS-093**

DEMETER allows the user editing of BSO/BSCMs.

Verification Method: Demonstration

Requirement ID: **SRS-094**

DEMETER allows the user to produce overlays where there will be no restrictions on the BSO/BSCM types that can be placed within the individual overlay.

Verification Method: Demonstration

Requirement ID: **SRS-095**

DEMETER allows the user to create/update/delete BSO/BSCMs entities, including the following type of MIM IES objects; Actors, Features, Materials, and Facility, Actions (tasks and events), Staff products (Overlays, Plan/Orders, Task organisations and Order of Battles).

Verification Method: Demonstration

Requirement ID: **SRS-096**

DEMETER provides a geographical view to support the management of the BSO. The user may use this view to e.g. select a BSO, set the location of the BSO or BSCM vertices. The geographic properties can also be defined and managed using the manual entry.

Verification Method: Demonstration

Requirement ID: **SRS-097**

DEMETER supports the conversion of geographic coordinates in multiple map project systems e.g. UTM and LATLON, MGRS.

Verification Method: Demonstration

Requirement ID: **SRS-098**

DEMETER allows the user to select the preferred map project system in the system setting.

Verification Method: Demonstration

Requirement ID: **SRS-099**

DEMETER allows the administrator to fix the map project system to be used by all users.

Verification Method: Demonstration

Requirement ID: **SRS-100**

DEMETER allows the user to manage all attributes associated with 2D and 3D objects.

Verification Method: Demonstration

Requirement ID: **SRS-101**

The user is able to create overlays with battle space objects that serve for the operational staff work such as personnel, security, operations, logistics, plans, signals, education/training, finance and CIMIC.

Verification Method: Demonstration

Requirement ID: **SRS-102**

DEMETER allows the user to copy and paste BSOs and BSCMs and all associated attributes between overlays.

Verification Method: Demonstration

Requirement ID: **SRS-103**

DEMETER allows the user to customize the display/hide feature and select content of BSO labels from the BSO attribute data set.

Verification Method: Demonstration

Requirement ID: **SRS-104**

DEMETER allows the user to add a user defined attribute name and associated information e.g. new attribute called "assessment" and "text" can be entered as information to this new attribute.

Verification Method: Demonstration

Requirement ID: **SRS-105**

DEMETER allows the user to view the BSO attributes in a list view.

Verification Method: Demonstration

Requirement ID: **SRS-106**

DEMETER allows the user to filter the content of the list based on the list attributes e.g. echelon greater than BATTALION but less than CORPS.

Verification Method: Demonstration

Requirement ID: **SRS-107**

DEMETER allows the user to query the content of the list based on the list attributes.

Verification Method: Demonstration

Requirement ID: **SRS-108**

DEMETER allows the user to apply the results of the filter to the geographic view.

Verification Method: Demonstration

Reports and returns from subordinates are used to maintain up to date battle space situational awareness. For some events, user will have to release a FRAGO on short

notice. When the headquarters do not have enough time to run a complete decision making process (COPD), a crisis action team will take place in the JOC. Led by JOC DIRECTOR, this crisis action team will gather all necessary branches interested in the issue and will deliver orders to military subunits (MSU) as soon as possible. In such a case, FRAGO MANAGER will release WINGO and FRAGO to MSUs. A link with G35 must be established and maintained to ensure either that the reaction does not hamper current operations or that G35 is aware of the risks for operations. FRAGO MANAGER takes place in the crisis action team to gather as much information as possible in order to speed up the orders release. Subordinates' Initiative. Subordinates' initiative is the assumption of responsibility to decide and initiate independent actions within the commander's intent and when the commander's concept of operations no longer applies, the operation order no longer applies, or when an unanticipated opportunity leading to accomplishing the mission presents itself. Subordinates decide how to accomplish their missions within delegated freedom of action and exercise initiative during execution, but they have an absolute responsibility to fulfil the commander's intent. [NREF-7].

Requirement ID: **SRS-109**

DEMETER receives battle space events (incidents) JOCWATCH NVG services described in [R-ICD-JOCWatch] and displays as an overlay on the geographical view.

Verification Method: Test

Requirement ID: **SRS-110**

DEMETER receives information from authoritative data sources to enable timely situational analysis.

Verification Method: Test

Requirement ID: **SRS-111**

DEMETER allows user to create groups by authorizing users selected from the authenticated user list, to work collaboratively on production and releasing of information products (e.g. ad hoc planning for unpredicted occurrences).

Verification Method: Test

Requirement ID: **SRS-112**

DEMETER allows production of formal ORDER from templates.

Verification Method: Demonstration

Requirement ID: **SRS-113**

DEMETER allows usage of import graphical overlays, with BSO and BSCMs, as list into the ORDER document templates.

Verification Method: Demonstration

Requirement ID: **SRS-114**

DEMETER allows all information products to be produced in human readable form or as a file, as required.

Verification Method: Demonstration

3.2.3 Land Operations Assessment Process Support

Assessment is the determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. Assessment is a continuous activity of the operations process that supports decision making by ascertaining progress of the operation for the purpose of developing and refining plans and for making operations more effective. Assessment results enhance the commander's decision making and help the commander and the staff to keep pace with constantly changing situations. Assessment involves deliberately comparing intended outcomes with actual events to determine the overall effectiveness of force employment. More specifically, assessment helps the commander determine progress toward attaining the desired end state, achieving objectives, and performing tasks. DEMETER support the assessment activities during the different phases of the mission.

The Assessing activities are performed continuously from the initiation of operation, and cyclically adapted to the rhythm of operation and its actual effects. The cycles may put different emphasis on various aspects: situation assessment, risk analysis or fact-based performance evaluation. Assessment is supporting commanders and planners in understanding the conditions, context and environment from different perspectives, military and civilian, social and political, legal, logistical and physical within the AOR and beyond. It includes evaluation of an operation's progress based on the prepared Measures of Effectiveness and Measures of Performance (MOEs and MOPs). The high level requirements addressed by this process support are; support for planning, assessment and execution of Land Operations.

Logistics assessment based on operational thresholds are performed by LOGFAS in NATO Enterprise, An interoperability with LOGFAS to support logistics assessment, and in addition being able to use logistics assessment from battlefield is important. Note that Planning and Recommendations are done in TOPFAS, system will provide manoeuvre status information to TOPFAS for it to perform OPLAN to current status comparisons. Support TOPFAS to perform recommendations on the future phases of operations. The reuse of existing capabilities and services are the major driven the solution of meeting the assessment requirements.

Requirement ID: **SRS-115**

DEMETER allows the user to merge tracks and BSOs from various reporting data sources (FFT, MIP) or other authoritative data sources (JOCWATCH) into valid compiled single current update situation overlay visualisation and further assessment.

Verification Method: Demonstration

Requirement ID: **SRS-116**

DEMETER provides the capability to display, browse and query information from multiple operational overlays that might help comparing plans with current status of battle field entities.

Verification Method: Demonstration

Requirement ID: **SRS-117**

During the short term execution phases, where G33/G35 (J33/J35) providing assessment of the last executed phase, DEMETER provides Situation Update to TOPFAS for it to perform achievement analysis and provide recommendations.

Verification Method: Demonstration

Requirement ID: **SRS-118**

DEMETER provides RGP to the COP for it to be used in the Commander's assessment, other functional areas (J5, etc.), military domains (Air, CBRN, etc.), external stakeholders and partners.

Verification Method: Demonstration

Uncertainty and risk are inherent in all military operations. Recognizing and acting on opportunity means taking risks. Reasonably estimating and intentionally accepting risk is not gambling. Carefully determining the risks, analysing and minimizing as many hazards as possible, and executing a plan that accounts for those hazards contributes to successfully applying military force.

Requirement ID: **SRS-119**

DEMETER allows the user to identify, analyse and evaluate risks on operational activities.

Verification Method: Demonstration

Requirement ID: **SRS-120**

DEMETER allows the user to assess current on the ground achievements results with the activities stated in OPLAN e.g. comparison of overlays, current situational results overlay and OPLAN planning overlay. Attribute(s) based comparison and reporting is possible where entity attributes might be selected from ICP and aligned with MOE and MOP.

Verification Method: Demonstration

Requirement ID: **SRS-121**

DEMETER allows the user to compare attribute data values between entities in overlays, e.g. current location of a unit and the planned location of that unit.

Verification Method: Demonstration

3.3 Compliance with NATO security policies

Security is embedded in the life-cycle (design, development, deployment, maintenance) of bespoke software purposely developed to handle NATO information, by taking into account the security objectives defined for the CIS. Applications shall be subject to security testing, configuration management (e.g. baselines) and change control (e.g. patching), processes which shall be designed and managed by the CISP, in close coordination with the SAA or designated NATO authority for NATO CIS handling non-classified information, to ensure that the CIS Security objectives are properly taken into account.

Requirement ID: **SRS-122**

DEMETER provides correct authentication capabilities for user and/or administrator access to resources.

Verification Method: Demonstration

Requirement ID: **SRS-123**

DEMETER controls the functions that the user is authorized to perform, based on a role-based access control (RBAC) mechanism.

Verification Method: Demonstration

Requirement ID: **SRS-124**

DEMETER implements the applicable security measures defined in [R-TID-CISSec]

Verification Method: Demonstration

Requirement ID: **SRS-125**

DEMETER is able to manage the user and respective permissions

Verification Method: Demonstration

Requirement ID: **SRS-126**

DEMETER supports the authentication of the users

Verification Method: Demonstration

Requirement ID: **SRS-127**

DEMETER implements the necessary security measures to be used a System High Security mode specified in [AC/35-D/2004]

Verification Method: Inspection

Requirement ID: **SRS-128**

DEMETER shall not be dependent of obsolete third party products that are no longer supported with security patches or where a support entity is not known.

Verification Method: Inspection

Requirement ID: **SRS-129**

DEMETER is capable of operating different security environment (including servers, network, services and workstations) in the presence of the currently approved NATO security settings (e.g. for windows environment NATO NCIRC GPO settings). Any deviations from the approved security settings be identified by the Contractor prior to testing and be subject to approval of the Purchaser.

Verification Method: Inspection

Requirement ID: **SRS-130**

DEMETER utilizes NCI Agency **Security Certificate Services** provided certificate and revocation services [Ref-CCat] to comply NATO PKI architecture.

Verification Method: Demonstration

Requirement ID: **SRS-131**

DEMETER is compliant with the web security rules as described in NATO Web Security Directive [NREF-11].

Verification Method: Inspection

Requirement ID: **SRS-132**

DEMETER is compliant with security policy detailed in [C-M(2002)49].

Verification Method: Inspection

Requirement ID: **SRS-133**

DEMETER is compliant with confidentiality policies detailed in the [CM (2007)0118].

Verification Method: Inspection

Requirement ID: **SRS-134**

DEMETER allows the user to assign and maintain human readable information markings during creation and modification of information as per [R-4774.2-MARKING].

Verification Method: Demonstration

Requirement ID: **SRS-135**

DEMETER is compliant with cyber defence policy detailed in [C-M (2011)0042]

Verification Method: Inspection

Requirement ID: **SRS-136**

DEMETER is compliant with InfoSec policy detailed in [AC/35-D/2004-REV3].

Verification Method: Inspection

Requirement ID: **SRS-137**

DEMETER is compliant with information assurance policy detailed in [C-(2008)0113(INV)].

Verification Method: Inspection

Requirement ID: **SRS-138**

DEMETER meets the integrity expectations compliant with information management detailed in [C-M(2007)0118].

Verification Method: Inspection

Requirement ID: **SRS-359**

DEMETER is compliant with Data Protection, Identity and Access Management and Application Security policy detailed in [AC_322-D_0048-REV3]

Verification Method: Inspection

3.4 Availability Requirements

ISO 25010: Availability. Degree to which a system, product or component is operational and accessible when required for use.

Requirement ID: **SRS-139**

DEMETER system intrinsic availability is greater than 99.5%. **Intrinsic Availability (theoretical or planned)** - Based on MTBF and MTTR with the assumption that all the necessary support resources (spares, test equipment and human resources) are in place and available.

Verification Method: Analysis

Requirement ID: **SRS-140**

DEMETER makes use of micro environments (<10 person, liaison teams)

Verification Method: Demonstration

Requirement ID: **SRS-141**

DEMETER performs without error under the use of a maximum of 2 SATCOM links to reach home base (2x 2x300ms delay).

Verification Method: Demonstration

Requirement ID: **SRS-142**

While providing required services, DEMETER configures (limits/sets capacity and priority) client software bandwidth to server to effectively use provisions so that multiple clients can run over the same limited bandwidth networks channels e.g. SATCOM channel

Verification Method: Demonstration

Requirement ID: **SRS-143**

The applications and services are able to serve 373 [Ref-CPP-MJO+] concurrent users/connections for at least 99.5% of its Operational time.

Verification Method: Analysis

Requirement ID: **SRS-144**

DEMETER is available for an authorised user within 15 seconds assuming fully available DEMETER servers.

Verification Method: Test

Requirement ID: **SRS-145**

DEMETER is available for an authorized user within 5 minutes in the case when DEMETER resources e.g. server are recovered from shutdown.

Verification Method: Test

Requirement ID: **SRS-146**

DEMETER provides a Mean Time to Restore (MTTR) of 1 hour or less.

Verification Method: Analysis

3.4.1 Enterprise Deployment Targets

Requirement ID: **SRS-147**

DEMETER generated information comply with the XML Guard and other guards (Mail, HTTP Proxy) available in the IEG-C [R-ICD-IEGC](NS-MS scenario)

Verification Method: Demonstration

Requirement ID: **SRS-148**

DEMETER shall support the NATO preferred virtualisation platform (VMWare)

Verification Method: Demonstration

Requirement ID: **SRS-149**

DEMETER client application operates using Remote Desktop Session Host (RDSH).

Verification Method: Demonstration

Requirement ID: **SRS-150**

DEMETER, in case has a thick client application, supports App-Volumes packaging for deployments.

Verification Method: Demonstration

Requirement ID: **SRS-151**

DEMETER, in case has a thick client application, supports Microsoft Endpoint Configuration Manager (MECM) deployment.

Verification Method: Demonstration

Requirement ID: **SRS-152**

DEMETER infrastructure and platform requirements is compliant with NATO DCIS nodes infrastructure (current and planned).

Verification Method: Demonstration

Requirement ID: **SRS-153**

DEMETER is supportable in a deployed environment, supported by a limited staff and not depending on highly skilled specialised knowledge.

Verification Method: Inspection

Requirement ID: **SRS-154**

DEMETER is deployable to NATO's Mission Information Room (MIR) infrastructure used as the static Mission Anchor Function (MAF) for NATO Missions.

Verification Method: Demonstration

Requirement ID: **SRS-155**

DEMETER shall be able to automatically synchronise the information between different DEMETER instances

Verification Method: Demonstration

Requirement ID: **SRS-156**

DEMETER shall enable the system admin to select what information to be exchange between instances

Verification Method: Demonstration

Requirement ID: **SRS-157**

DEMETER shall enable the system admin to immediately stop (pause) the information exchange between instances e.g. in support of radio silence or emergency disconnection

Verification Method: Demonstration

Requirement ID: **SRS-158**

DEMETER shall enable the system admin to resume the information exchange between instances

Verification Method: Demonstration

Requirement ID: **SRS-159**

DEMETER shall synchronise the delta of information to be exchange without or with minor user intervention

Verification Method: Demonstration

Requirement ID: **SRS-160**

DEMETER is installable in multiple Deployable PoPs. The DPoPs are connected either with the Mission Anchor Function with a 4-8Mbps SATCOM link that has a latency of 700msec or between themselves also over SATCOM or other bearers of better characteristics. DEMETER is capable to support two way replicate data as a minimum over a single SATCOM Hop of as previous characteristics.

Verification Method: Demonstration

Requirement ID: **SRS-161**

DEMETER is able to resume the two way data replication after loss of communications.

Verification Method: Demonstration

Requirement ID: **SRS-162**

DEMETER architecture and system design ensures that it can support the seamless transition of user sessions between different service instances e.g. in existence of Network Load Balancers and Geo Load Balancers.

Verification Method: Demonstration

Requirement ID: **SRS-163**

DEMETER, in case has a thick client application, work on Windows Operating System (Windows 10+)

Verification Method: Demonstration

Requirement ID: **SRS-164**

DEMETER, in case has a thick client application can work on laptops with Intel Core i5, 8GB RAM and 600GB SSD Hard Disk Drive e.g. common specifications of laptops used with deployable kits.

Verification Method: Demonstration

Requirement ID: **SRS-165**

DEMETER application is able to operate in both IPv4 and IPv6 configured environments. Note: This is mostly abstracted by the infrastructure and platform services, mostly it impacts the system configurations of end points used in the information exchange (e.g. MIP)

Verification Method: Demonstration

3.5 Compliance NATO confidentiality policies

Requirement ID: **SRS-166**

Any information product that is exportable from DEMETER in any format e.g. file, xml, PDF, word, etc. is tagged with information products and its appropriate security classification.

Verification Method: Test

Requirement ID: **SRS-167**

The data that is exchanged through synchronization is wrapped in an electronic envelope with appropriate metadata. The envelop metadata attributes include the highest security classification and the most restrictive releasability constraint of the data within the data set.[R-4774-CMLS][[R-4778.2-BindProf]]

Verification Method: Inspection

Requirement ID: **SRS-168**

DEMETER is able to display the highest security classification of an information product that is on the current view in a coloured banner/header based. All security classifications have a unique colour. Colour setting is configurable per classification and initial/default setting of the colours shall be provided to vendor.

Verification Method: Test

Requirement ID: **SRS-169**

DEMETER complies with Common File Format labelling Profile of FMN Spiral 4 Web hosting Service Instructions [R-4774-CMLS] [R-4778.2-BindProf]

Verification Method: Demonstration

Requirement ID: **SRS-170**

DEMETER web services has metadata for confidentiality security labelling defined in accordance with [R-4774-CMLS] and the SOAP and REST based web services metadata binding comply to SOAP and REST profile bindings described in [R-4778.2-BindProf].

Verification Method: Inspection

Requirement ID: **SRS-171**

It is possible to transform the exported data resulting from structured formats into human readable document using separate/external and customizable transformations (e.g. XSLT-FO). The transformations use the exported XML file, icons, symbols, and thumbnails and produce a PDF file.

Verification Method: Inspection

3.6 Efficiency Requirements

Requirement ID: **SRS-172**

DEMETER has cost-effective adaptation capabilities for adapting NATO Enterprise Communication and Information. This will mean that it be able to adapt services provided by easy integration (like Active Directory, Mailing Services, ITM replication services) and easy interoperability adaptation e.g. presentation of achieving syntactic and semantic interoperability by easily implementable (possibly without code change) transformations to comply NATO Enterprise Communication and Information services TOPFAS, LOGFAS, metadata labelling, etc.

Verification Method: Demonstration

Requirement ID: **SRS-173**

DEMETER is deployed on NATO ITM cloud (ITM could profile be provided).

Verification Method: Demonstration

Requirement ID: **SRS-174**

DEMETER provides administration capabilities that can be remotely accessible from a network in order to perform centralized management and support of resources e.g. services/servers.

Verification Method: Demonstration

3.7 Integrity Requirements

The integrity is the property that information (including data) has not been altered or destroyed in an unauthorised manner.

Requirement ID: **SRS-175**

DEMETER implements a two-phase deletion process (i.e., a logical/soft delete with User-controlled permanent deletion/purging) for entities, including configuration data, logs, audit, etc. / information products the requirement applies.

Verification Method: Demonstration

Requirement ID: **SRS-176**

DEMETER clearly identifies all time values as Zulu and the date/time format is in accordance with ISO 8601.

Verification Method: Demonstration

Requirement ID: **SRS-177**

DEMETER represents the military relevant information dates and times using the military date times group format complying ISO 8601.

Verification Method: Demonstration

Requirement ID: **SRS-178**

DEMETER allows the user to define the default Military Time Code Letter Reference to be used for a mission

Verification Method: Demonstration

Requirement ID: **SRS-179**

DEMETER supports the user with the conversion of current date time to the military date time group representation complying ISO 8601.

Verification Method: Demonstration

Requirement ID: **SRS-180**

DEMETER displays non-military date and times group using the operating system settings.

Verification Method: Demonstration

Requirement ID: **SRS-181**

DEMETER logs front-end and back-end user activity in order that full audit traceability of client activities/actions can be carried out.

Verification Method: Inspection

Requirement ID: **SRS-182**

DEMTER reports all logs in files or databases using English (United Kingdom) as the default language.

Verification Method: Inspection

Requirement ID: **SRS-183**

DEMETER distance accuracy is lower than 0.11 meter for translation of values (UTM, Latitude/Longitude, others). Confidence interval should be shown within values.

Verification Method: Demonstration

Requirement ID: **SRS-184**

DEMETER ensures consistency and accuracy of all the data displayed on all open views and applications. DEMETER either ensure up to date information is pushed to all its open views (multi user or multi instance) or DEMETER indicate user current data is updated by clear notification for user to manually update the view to fetch latest information (Refresh not require page refresh in Web or client restart in thick client application)

Verification Method: Demonstration

Requirement ID: **SRS-185**

DEMETER has all functionality ready to use for an authorised user after invoking DEMETER function within 5 Seconds.

Verification Method: Demonstration

Requirement ID: **SRS-186**

DEMETER executes the authorisation (login) function within 5 seconds

Verification Method: Demonstration

Requirement ID: **SRS-187**

DEMETER, while performing peak load, completes the saving of dataset to file, database, by providing an evidence for saving (e.g. saved), within 5 seconds.

Verification Method: Demonstration

Requirement ID: **SRS-188**

DEMETER user interface responds to the user with an indication that the user action is accepted and in progress.

Verification Method: Demonstration

Requirement ID: **SRS-189**

DEMETER provide the internal or API that enable system observability monitoring, event management, problem management, availability for enterprise monitoring tools e.g. SCOM/Zabbix, to identify services health status any time.

Verification Method: Demonstration

Requirement ID: **SRS-190**

DEMETER processes and consumes external web services during a peak load environment with minimum delay so as not to introduce obsolescence to the content of the data e.g. BSO reporting time is too old if information flow is slow.

Verification Method: Demonstration

Fault tolerance is the degree to which a system, product or component operates as intended despite the presence of hardware or software faults.

Requirement ID: **SRS-191**

DEMETER server has a degraded mode of operation in the condition where any dependent services and components are not available and will notify the user of the limited functionality. Upon restoration of services, DEMETER will change operational state accordingly.

Verification Method: Demonstration

Requirement ID: **SRS-192**

DEMETER notifies the user for potential loss/deletion of information objects during modification of any information object e.g. by cascading deletion. When prompted by a notification about the data that might be lost/deleted, the user is able to choose the action that be taken by DEMETER e.g. cancel, continue, etc.

Verification Method: Demonstration

Requirement ID: **SRS-193**

DEMETER automatically reports errors and suggested corrective actions with respect to the creation, change, exchange and storage of data elements, objects and products.

Verification Method: Demonstration

Requirement ID: **SRS-194**

DEMETER shall be able to system administrator to configure the log information e.g. content and level in support of the specific security requirements.

Verification Method: Demonstration

Requirement ID: **SRS-195**

DEMETER logs shall be readable without the need for special tools e.g. plain text logs

Verification Method: Demonstration

Requirement ID: **SRS-196**

DEMETER logs can be configures to be exported for external consumption e.g. files or streams

Verification Method: Demonstration

Requirement ID: **SRS-197**

DEMETER log files shall be rotated in accordance with the configuration settings e.g. weekly, daily or hourly or limit size

Verification Method: Demonstration

Requirement ID: **SRS-198**

DEMETER does not in any case permit loss of user-entered data due to receipt of an error or other message. User input must never be lost, discarded or corrupted unless a user actually chooses to abandon entry.

Verification Method: Demonstration

Requirement ID: **SRS-199**

In case of network anomaly (High latency/timeout/loss of connect) DEMETER tries to get access to resources automatically as well as manually. High latency is defined as latency exceeding 1100 milliseconds.

Verification Method: Test

Requirement ID: **SRS-200**

DEMETER shall make efficient use of network bandwidth, so that multiple clients can run over the same limited bandwidth channels e.g. SATCOM.

Verification Method: Demonstration

Requirement ID: **SRS-201**

DEMETER operates in a comfortable way with low network quality (e.g. high latency for the data feeds)

Verification Method: Demonstration

3.8 Survivability Requirements

Requirement ID: **SRS-202**

DEMETER does not lose any loaded data once connectivity to the server is broken, as long as the client application remains open by the user. Once the connection with the server is restored, the most recent data will be loaded, to update the content.

Verification Method: Demonstration

Requirement ID: **SRS-203**

After any lost connection is restored, DEMETER client application automatically reconnects to the server, updates status, and restores the flow of information products to the client without user action.

Verification Method: Test

Requirement ID: **SRS-204**

DEMETER supports online-backup (hot backup) without the need to interrupt system functions.

Verification Method: Demonstration

Requirement ID: **SRS-205**

DEMETER, in the event of an interruption or a recoverable failure, recovers the data affected and re-establishes the desired state of DEMETER.

Verification Method: Demonstration

Requirement ID: **SRS-206**

DEMETER supports recovery facilities of the database(s) from backup and archive data to a stable/consistent state with minimal data loss.

Verification Method: Demonstration

Requirement ID: **SRS-360**

DEMETER shall allow the information to be archived and purged from the system when no longer required. Note: This is different from the product archiving defined in the Functional requirements and is associated with the need to safely remove any data or information that is no longer used (exercise finished). In this case the archive is a responsibility of the system (e.g. database or file backup/restore procedure)

Verification Method: Demonstration

Requirement ID: **SRS-207**

DEMETER provides maintenance procedures supporting recovery of its operation in limited time when failures occurs. The recovery procedures are applicable for all kinds of deployments of DEMETER e.g. redundancy available data centres, standalone deployments, etc.

Verification Method: Test

Requirement ID: **SRS-208**

When possible and available on the deployment environment, DEMETER utilizes NATO Database Platform Service as its storage facility to ensure highest availability is achieved

Verification Method: Demonstration

Requirement ID: **SRS-209**

When use of NATO Database Platform Service is not possible, DEMETER ensures industry standard database failover solution (e.g. Windows Server Failover Clustering with SQL Server in case of SQL use) to increase availability.

Verification Method: Demonstration

3.9 Usability Requirements

Requirement ID: **SRS-210**

DEMETER users are provided with standard procedures for similar, logically related transactions.

Verification Method: Demonstration

Requirement ID: **SRS-211**

The content and information within DEMETER is presented to the user in a consistent, standardized manner e.g. use of same units of measure, precision, for same entities in all views, providing filtering for all lists, providing all lists sorted by default on the major

natural key, every button press has a visible feedback, all errors are displayed in same format with error id to refer to, usage of same fonts and correct sizes on each view for labels, alignment of labels, provision of tooltips on each label.

Verification Method: Demonstration

Requirement ID: **SRS-212**

Every input by a DEMETER user consistently produces some perceptible response output from the computer.

Verification Method: Demonstration

Requirement ID: **SRS-213**

DEMETER presents connectivity status, last update time of view and mode of operation e.g. degraded or normal at all the times to the user.

Verification Method: Demonstration

Requirement ID: **SRS-214**

DEMETER minimizes memory load on the users by providing computer aids to aid process e.g. automatic insertion of standard information.

Verification Method: Demonstration

Requirement ID: **SRS-215**

DEMETER displays only data essential to the user's need.

Verification Method: Demonstration

Requirement ID: **SRS-216**

DEMETER is compliant to ISO 9241-13 for user guidance.

Verification Method: Demonstration

Requirement ID: **SRS-217**

DEMETER uses English (United Kingdom) as the default language. This apply to all applications and supporting components, including all user interfaces e.g. views, dialogs, help screens, tooltips, etc., error/notification/warning messages, training material and documentation.

Verification Method: Demonstration

Requirement ID: **SRS-353**

DEMETER allows user to configure the user interface (UI) language.

Verification Method: Demonstration

Requirement ID: **SRS-218**

DEMETER supports context menus i.e. right button mouse click, or equivalent menus. General and common functions should also be accessible through the function bar, ribbon, view or dialogue buttons.

Verification Method: Demonstration

Requirement ID: **SRS-219**

DEMETER offers undo/redo (not limited to formatting) support for all operations.

Verification Method: Demonstration

Requirement ID: **SRS-220**

DEMETER supports editing of information in a logical order. In the user interface, dialogues are navigable using the tab key in a logical order.

Verification Method: Demonstration

Requirement ID: **SRS-221**

Clickable (selectable) text e.g. links, is clearly distinguishable from non-clickable text.

Verification Method: Demonstration

Requirement ID: **SRS-222**

DEMETER notifies the user who has initiated a prolonged action that processing of the action has started with the software conveying the processing progress by means of a progress indicator.

Verification Method: Demonstration

Requirement ID: **SRS-223**

DEMETER provides information tooltips within views, dialogs and controls to provide further explanation about specific fields or options. However, it is not required to include these tooltips for every field or option; dialogs and views are self-descriptive.

Verification Method: Demonstration

Requirement ID: **SRS-224**

For hierarchical (tree) and grid views, DEMETER supports the full range of capabilities including sorting, filtering (Excel filter style), column selector, grouping, banded view, column ordering, column width selection, etc. The availability of those features may depend on the grid usage i.e. not all features are required for all grids based on the information content displayed.

Verification Method: Demonstration

Requirement ID: **SRS-225**

DEMETER allows the user to launch more than one instance of an application on the same workstation.

Verification Method: Demonstration

Requirement ID: **SRS-226**

The user interface of DEMETER supports a minimum resolution of 1280x1024 or wide-screen equivalent.

Verification Method: Demonstration

Requirement ID: **SRS-227**

DEMETER notifies the user for potential loss of information objects during change of any data element or information product. The user should be able to choose the action that has to be taken by the application, identified by a warning notification, which provides information about the data that might be lost.

Verification Method: Demonstration

Requirement ID: **SRS-228**

DEMETER highlights or marks empty required fields by means of error providers in dialogs and views after the user saves the information within the dialog or view. No information is lost when saving fails and the users must complete the remaining fields, before saving again.

Verification Method: Demonstration

Requirement ID: **SRS-229**

DEMETER might use the latest Microsoft Office theme look and feel e.g. Microsoft Office 2021.

Verification Method: Demonstration

Requirement ID: **SRS-230**

DEMETER user Interface is compatible with high DPI displays without blur or other artefacts. This includes the use of a common set of scalable vector icons for all user interface elements and replacement of bitmap icons by their scalable vector equivalent when applicable.

Verification Method: Demonstration

Requirement ID: **SRS-231**

DEMETER has a high degree of learnability, making it very easy to use even the first time. DEMETER score above 50% in user success rate without external support, for novice users.

Verification Method: Demonstration

Requirement ID: **SRS-232**

DEMETER scores above 95% in user success rate without external support, for experienced users.

Verification Method: Demonstration

Requirement ID: **SRS-233**

DEMETER is customizable at system level. When DEMETER is customized at user level, it overwrites system level customizations. Examples include colour, BSO sizes, BSO labels, default background maps, etc. Customisation of system parameters for users is stored, recalled and shared as files in between systems, installations and users as required.

Verification Method: Demonstration

Requirement ID: **SRS-234**

DEMETER allows the user to store and recall views, which contain customisation settings, map details and overlays that are being viewed. Each time a saved view is recalled DEMETER updates the view to present the recalled view.

Verification Method: Demonstration

Requirement ID: **SRS-235**

DEMETER allows users to quickly revisit recent functions and features and to save 'favourites' of features and functions that are often used.

Verification Method: Demonstration

Requirement ID: **SRS-236**

DEMETER allows the User to set up personal preferences for layout and content.

Verification Method: Demonstration

Requirement ID: **SRS-237**

DEMETER shall allow for changes of frequent changed parameters and reference data to be performed with the system online, not requiring a restart

Verification Method: Demonstration

Requirement ID: **SRS-238**

DEMETER provides a list of the 'last accessed objects' or recently used items/functions. This list is always selectable for display.

Verification Method: Demonstration

Requirement ID: **SRS-239**

DEMETER allows the user to save their personal customisation settings, which can be loaded or modified as required.

Verification Method: Demonstration

Requirement ID: **SRS-240**

DEMETER allows sharing of user settings between users and groups.

Verification Method: Demonstration

Requirement ID: **SRS-241**

DEMETER ensures all images in web applications include alternate (alt) text description (e.g. for actions)

Verification Method: Demonstration

Requirement ID: **SRS-242**

DEMETER installation and deployment is fully automated with a manual installation option. Automation is site configuration agnostic, whilst it is assumed no deep engineering knowledge is required.

Verification Method: Demonstration

Requirement ID: **SRS-243**

DEMETER DNS zone name reconfiguration or IP change does not require system reinstallation and can be achieved with Maintenance procedures provided and scripts that can be easily accessible.

Verification Method: Demonstration

Requirement ID: **SRS-244**

DEMETER can be scalable without system reinstallation.

Verification Method: Demonstration

Requirement ID: **SRS-245**

DEMETER does not need system reinstallation when changes to service accounts or password occur.

Verification Method: Demonstration

Requirement ID: **SRS-246**

In case DEMETER deployed on Windows environment, DEMETER is compliant to Managed Service Accounts mechanism.

Verification Method: Demonstration

Requirement ID: **SRS-247**

DEMETER provides format able usage statistics, for administrative purposes.

Verification Method: Demonstration

Requirement ID: **SRS-361**

DEMETER supports the monitoring of any required license limits and alerting. Note: Due to the critical and flexible usage of the system in support of critical tasks the system shall prevent from blocking the usage due to specific licensing limits on a single node. Instead it should log the potential exception to be reconciled as part of future needs

Verification Method: Demonstration

3.10 Operational Flexibility Requirements

System as a NATO Enterprise C&I service, comply the operational environments that NATO enterprise provides, in addition it integrates with the existing infrastructure and services provided by the NATO Enterprise to maximize reuse and efficiency.

Requirement ID: **SRS-248**

DEMETER operates at datacentre with specifications provided in [R-ITM]

Verification Method: Demonstration

Requirement ID: **SRS-249**

DEMETER operates at NSF Azure Public Cloud.

Verification Method: Demonstration

Requirement ID: **SRS-250**

DEMETER operates at NERS environment as an On Premise environment.

Verification Method: Demonstration

Requirement ID: **SRS-251**

DEMETER operates at Static/On Premise Server environment.

Verification Method: Demonstration

Requirement ID: **SRS-252**

DEMETER operates under an application farm which can support 373 users concurrently e.g. CPP - MJO+ requirement.

Verification Method: Demonstration

Requirement ID: **SRS-253**

DEMETER can be deployed and operated at environments where database cluster is used for storage.

Verification Method: Demonstration

Requirement ID: **SRS-254**

DEMETER provides services to NATO Enterprise users roles e.g. operational, administrative.

Verification Method: Demonstration

Requirement ID: **SRS-255**

DEMETER is designed with 4 types of configuration: -DS for NATO Data Centre, MR, for Mission Networks e.g. MIR), SC for scalable but not mission critical environments and SN for non-mission critical environments.

Verification Method: Demonstration

3.11 Maintainability Requirements

Maturity is the degree to which a system, product or component meets needs for reliability under normal operation. The concept of maturity can also be applied to other quality characteristics to indicate the degree to which they meet required needs under normal operation.

Requirement ID: **SRS-256**

DEMETER exhibits a mean-time-between-failure (MTBF) characteristic of less than 3.65 hours per month to ensure 99.5% intrinsic availability, and the total number of instances that are active during that period not affect that. The MTBF measurement not include failures resulting from factors determined to be external to application (e.g., loss of domain controller).

Verification Method: Analysis

Requirement ID: **SRS-257**

DEMETER provides its functions meeting the performance goals under normal operating conditions.

Verification Method: Demonstration

Requirement ID: **SRS-258**

DEMETER allows a user to report problems, bugs and change requests when they encounter a problem or an unexpected result. The feature provides a well formed structured output from the problem observed e.g. export of error to an XML file, or a PDF for to be used in issue tracking systems incident entry e.g. NATO formal ticketing system.

Verification Method: Demonstration

3.12 Modifiability Requirements

Degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality. Implementation includes coding, designing, documenting and verifying changes. Modularity and Analysability can influence Modifiability. Modifiability is a combination of changeability and stability.

Requirement ID: **SRS-259**

DEMETER has modular design and deployment capability; ensuring upgrade of part of the application does not stop the application from providing operational capabilities.

Verification Method: Demonstration

Requirement ID: **SRS-260**

DEMETER has partial upgrade/maintenance capability to minimize the required time of Agreed Service Interruption (ASI) that can contribute to the unavailability.

Verification Method: Demonstration

Requirement ID: **SRS-261**

DEMETER provides modular and partial installation types by which only a certain part of application is deployed to the operational environments (static, on premise, deployment, and external).

Verification Method: Demonstration

Requirement ID: **SRS-262**

DEMETER ensures operational data that is stored DEMETER is migrated without loss of data when any new version is installed.

Verification Method: Demonstration

Requirement ID: **SRS-263**

DEMETER does not lose its configuration information when DEMETER is upgraded.

Verification Method: Demonstration

Requirement ID: **SRS-264**

DEMETER ensures all provided services to external DEMETER continue functioning (provide the same capabilities stated in interface requirements) after any upgrade.

Verification Method: Demonstration

Requirement ID: **SRS-265**

DEMETER provides various APIs for to allow extensibility in user interface, data model and business logic-service layer. The API's provided by DEMETER is compliant to OpenAPI Specification v3.1.0 or newer.

Verification Method: Demonstration

Requirement ID: **SRS-356**

In accordance with NATO Policy [Ref-DEFP], DEMETER exposes maximum amount of information by the application interface e.g. Open API services. That allows external systems to set and get enough information from DEMETER. Here "enough" means, being able to fully initiate the DEMETER to operate with usage of provided APIs.

Verification Method: Demonstration

Requirement ID: **SRS-357**

In accordance with NATO Policy [Ref-DEFP], DEMETER exposed services comply security standards such as authentication and authorization.

Verification Method: Demonstration

Requirement ID: **SRS-266**

DEMETER architecture is based on web based technology

Verification Method: Demonstration

Requirement ID: **SRS-267**

DEMETER provides client UI using modern web technology and standards (HTML5/CSS3), older versions may also be supported

Verification Method: Demonstration

Requirement ID: **SRS-268**

DEMETER client UI is rendered in the browser without requiring any additional extensions or plugins

Verification Method: Demonstration

3.13 Scalability Requirements

Operational needs requires deployments to be scalable to minimal deployable environments where usage is limited as well as data centres those are utilized by huge number of users. This change also exists on connectivity resources and bandwidths. Modern applications cope up with this scale change with many convenient solutions. The system is ready for different scales of operation in terms of number of users accessing its server and number of servers replicating and synchronizing data between each other. It is envisaged that maximum number of users per one server will not exceed 373 (all users for an MJO+ activity) and that there can be up to 5 nodes connected and synchronizing together at one time.

Requirement ID: **SRS-269**

DEMETER has modules that can be installed separately to meet the operational requirements of an existing environment e.g. if no MIP communication no MIP installation, if no FFI communication no FFI services installation.

Verification Method: Demonstration

Requirement ID: **SRS-270**

DEMETER architecture shall allow the system increase the processing throughput by scaling (horizontal / vertically) in accordance with the infrastructure assigned to the system

Verification Method: Demonstration

Requirement ID: **SRS-271**

A full functioning DEMETER is installable to a single server to provide 1/2 user the full capability (experimental and demo nodes)

Verification Method: Inspection

Requirement ID: **SRS-272**

A full functioning DEMETER is installed to a minimum number of servers and requires minimum resources to provide service to 10 PAX. E.g. deployable nodes.

Verification Method: Inspection

Requirement ID: **SRS-273**

A full functioning DEMETER is scalable to be installed to various servers (by sharing processing requirements horizontally) to serve up to 373 concurrent users [Ref CPP - MJO+].

Verification Method: Inspection

Requirement ID: **SRS-274**

DEMETER is a Multi-Tenant system by which it can serve multiple missions/operation at the same time keeping all missions in isolation e.g. separate store, etc.

Verification Method: Test

Requirement ID: **SRS-275**

DEMETER shall be able to operate in different "modes of operation" e.g. training, demo and operational, each one associated with an independent data store.

Verification Method: Test

Requirement ID: **SRS-276**

DEMETER shall provide the user to change the "mode of operation"

Verification Method: Demonstration

Requirement ID: **SRS-277**

DEMETER operates on multiple security classification environments, in case of MS, NS DEMETER complies with IEG-C rules for exchanging data between these two security classification domains.[R-ICD-IEGC]

Verification Method: Test

4 Interface Requirements

DEMETER service shall function in static joint HQs via provision of service in redundant data centres. DEMETER service shall function in Mission Information Room (static data centres for NRF mission anchor point), DEMETER service shall function in Deployable kits for mission rehearsal and standby functions. These are the major service interoperability points at which DEMETER either interoperate with NATO C2 systems, or with National Systems that have the role of Land Component Command. DEMETER interoperability profile reuses the parts of FMN profile when communicating with National federation and some NATO C2 systems (e.g. NCOP situational picture service). In addition to that DEMETER needs to comply interface specifications of existing NATO C2 systems to exchange data with them. These are not comply with any standards but mostly proprietary (LOGFAS/TOPFAS). The information from non-standard sources are utilized to mitigate the non-existence of standard services that provide the same information (There is no ORBAT service so TOPFAS/LOGFAS ORBAT is utilized). This kind of interfaces are not the major part of the profile and needed based on functional requirements that DEMETER shall meet. DEMETER FFI interface comply with [Ref-ADatP-34].

Requirement ID: **SRS-278**

DEMETER is interoperable with the NATO C2 CIS and the Community of Interest (CoI) Services within the NATO C2 architecture, IAW [C-M(2002)49] and [AC322-D(2019)0034 (INV)].

Verification Method: Test

Requirement ID: **SRS-279**

DEMETER is compliant with the NATO C3, and the NATO Interoperability Standards and Profiles [R-NSIP].

Verification Method: Test

Requirement ID: **SRS-280**

In order to achieve federated interoperability, DEMETER is compliant with the Alliance interoperability requirements as documented in the current and emerging Federated Mission Networking (FMN) Spiral Specifications, details can be found in [R-FMN].

Verification Method: Test

Requirement ID: **SRS-281**

Current and Emerging FMN Spiral Specifications are identified as Spiral 3 and Spiral 4 at the time of the production of this document. The spiral compliance can be re-evaluated based on the time lines of delivery of DEMETER.

Verification Method: Demonstration

Requirement ID: **SRS-282**

DEMETER consumes reports from subordinates whose protocol and content is stated Service Instructions (SI) for Land C2 Information Exchange specified in Federated Mission Network (FMN)

Verification Method: Test

Requirement ID: **SRS-283**

DEMETER confidentiality labelling complies with the NATO Interoperability Standards Profile specified metadata bindings standards detailed in [[R-4778.2-BindProf]] and confidentiality metadata label syntax standards detailed in [R-4774-CMLS].

Verification Method: Test

Requirement ID: **SRS-284**

DEMETER authentication mechanism comply with standards and instructions specified in SI for Web Authentication of the applicable FMN Spiral.

Verification Method: Demonstration

Requirement ID: **SRS-285**

DEMETER comply with Service Instruction standards for Friendly Force Tracking of FMN Spiral

Verification Method: Demonstration

Requirement ID: **SRS-286**

DEMETER comply with existing FMN Spiral specific service instructions for information distribution e.g. Picture Distribution, and Overlay Distribution.

Verification Method: Demonstration

Requirement ID: **SRS-358**

DEMETER comply with the FMN Spiral Service Instructions for Geospatial Information for the presentation and exchange of georeferenced information.

Verification Method: Demonstration

Requirement ID: **SRS-287**

DEMETER meets the Information Exchange Requirements (IERs) [MC 593/1, MC 0640] through the transfer of data through network and bandwidth management.

Verification Method: Test

Requirement ID: **SRS-288**

DEMETER has capability to export BSO attributes, including order of battle (ORBAT) from Microsoft Excel and or Comma Separated (CSV) file. DEMETER define the format of the CSV file.

Verification Method: Test

Requirement ID: **SRS-289**

DEMETER has capability to import BSO attributes, including order of battle (ORBAT) from Microsoft Excel and or Comma Separated (CSV) file. DEMETER define the format of the CSV file.

Verification Method: Test

4.1 Service Reuse Requirements

Reuse of core NATO Enterprise capability is mandatory. This means that existing web hosting, database, communication, services utilisation. Some services roadmap may not align with system delivery so system can provide its own solution to mitigate e.g. SOA IdM. The list of services are provided in below table and detailed requirements for service is listed in subsection. Further details of services provisions can be provided upon request.

#	Name	Service ID
1	Managed Device Service	See [Ref-CCat]
2	Operations Centre Service	See [Ref-CCat]
3	Web Hosting Service	See [Ref-CCat]
4	Active Directory and Federation Service	See [Ref-CCat]
5	Database Platform Service	See [Ref-CCat]
6	DevSecOps	See [Ref-CCat]
7	Integration and Testing Platform Service	See [Ref-CCat]
8	Infrastructure Hosting Service	See [Ref-CCat]
9	DCIS – Deployable Nodes	See [Ref-CCat]
10	Service Management and Control Function Service	See [Ref-CCat]
11	Gateway Security Service	See [Ref-CCat]
12	Penetration testing and Continuous security posture assessment Services	See [Ref-CCat]

14	Security Certificate Service	See [Ref-CCat]
15	Education and Individual Training Delivery and Availability and Maintenance (EIT A&M)	See [Ref-CCat]
16	ITSM and CMDB Application Service	See [Ref-CCat]

4.1.1 NATO Managed Device Service

Requirement ID: **SRS-290**

DEMETER client UI shall be compatible with the generic modern browsers (NATO supports Microsoft Edge and Firefox ESR)

Verification Method: Demonstration

4.1.2 NATO Operations Centre Service

4.1.3 NATO Web Hosting Service

Requirement ID: **SRS-291**

DEMETER reuses where available resources provided by the NATO Web Hosting Platform Service or SOA IdM Service, such as MS IIS, Apache as web hosting.[Ref-CCat]

Verification Method: Demonstration

4.1.4 NATO Active Directory and Federation Service

Requirement ID: **SRS-292**

Authentication to DEMETER is possible through an authorized identity provider within the hosted infrastructure (standalone).

Verification Method: Demonstration

Requirement ID: **SRS-293**

DEMETER utilizes NATO Active Directory and Federation Service as an authorized authentication provider for NATO users[Ref-CCat]

Verification Method: Demonstration

Requirement ID: **SRS-294**

The method of authentication as well as authorisation is provided in the security requirements. DEMETER complies to NCI Agency provided SOA-IdM service Identity Management protocols as stated in [R-ICD-SOA_IdM]

Verification Method: Demonstration

Requirement ID: **SRS-295**

DEMETER servers join and operate within a NATO Active Directory Organisation Unit (OU), which ensures time synchronisation (reliable reference time (NATO uses different STRATUM time servers, for applications services the Windows Domain Controller provides STRATUM level 3 TS)) as well as automatic Domain Policy application

Verification Method: Demonstration

Requirement ID: **SRS-296**

DEMETER utilizes NATO Database Platform Service to provide RDBM server e.g. Oracle, MS SQL, MySQL, PostgreSQL, etc... Applicable only in case the platform service is available in the deployment location [Ref-ATP-A2SL].

Verification Method: Demonstration

Requirement ID: **SRS-297**

DEMETER storage, if based on RDBMS, complies with the NATO infrastructure RDBMS type in reference to [A2SL, ATP]

Verification Method: Demonstration

Requirement ID: **SRS-298**

DEMETER uses the Database Platform service while it is deployed in data centres for ITM project.

Verification Method: Demonstration

4.1.5 NATO DevSecOps Service

Requirement ID: **SRS-299**

DEMETER is deployable to NATO software system integration environments managed and operated by NCIA.

Verification Method: Demonstration

4.1.6 NATO Integration and testing Platform Service

Requirement ID: **SRS-300**

DEMETER ensures being tested by a detailed in a documented test plan for the interoperability of itself with other NATO systems, in NATO integration environments before any official release or introduction in operations.

Verification Method: Demonstration

4.1.7 NATO Infrastructure Hosting Service

Requirement ID: **SRS-301**

DEMETER operates only on the resources provided by NATO Infrastructure Hosting Service, all servers can be loaded with a Windows (Server 2016, 2019 or 2022) or Linux (Oracle 8.x and RedHat 8.x.7.x (excluding 7.4)) operating system; have pre-installed anti-virus and malware protections. As part of the provisioning, all servers are hardened based on the NATO security policies. [Service Catalogue, ATP, A2SL]

Verification Method: Demonstration

4.1.8 NATO SOA IdM Service

Requirement ID: **SRS-302**

DEMETER comply with NCI Agency provided NATO SOA-IdM services standards for the implementation of SOA related solutions and Identity Management (IdM) technical solutions. SOA-IdM service interface profiles are provided in [R-ICD-SOA_IdM]

Verification Method: Demonstration

4.2 Information Exchange Requirements

Requirement ID: **SRS-303**

DEMETER provides the user with the capability to export/import information to a file. [DEMETER ICD]

Verification Method: Demonstration

4.2.1 NATO Systems and Services

4.2.1.1 ETEE Functional Services

ETEE FS provides common architecture between C2/INTEL and LOG applications, the attempts to maintain those through events like CWIX and the need to verify and validate these custom applications before they can be operated on agency-managed networks. In addition ETEE FS comply with cyber security standards.

Requirement ID: **SRS-304**

DEMETER is able to initialize its database that be utilized in exercise using ETEE FS provided information using standardized message formats (e.g. APP 11 (C) ADatP 3 BL 15 Own SitREP and enemy SITREP stated in [R-NSIP])

Verification Method: Demonstration

Requirement ID: **SRS-305**

ETEE FS initialize DEMETER database, which contain exercise starting conditions including ORBAT, perceived situation of other forces or other parties involved in the operation as well as other relevant conditions such as mobility or infrastructure-related

items (e.g. APP 11 (C) ADatP 3 BL 15 Own SitREP and enemy SITREP stated in [R-NSIP])

Verification Method: Demonstration

Requirement ID: **SRS-306**

DEMETER initializes database using through a standardized and documented interfaces OWNSITREP, ENSITREP etc. with the format stated in [R-NSIP]

Verification Method: Demonstration

4.2.1.2 LOGFAS Service

Logistic services provide necessary information and services to Land C2 in order to allow proper planning and to maintain situation awareness. System might exchange some specific information products/elements Logistics system. These information products may be necessary to achieve complete SA in the Land domain. For assessment of logistics land C2 tools can provide secondary capability. Below are suggested logistics system interoperability cases. Recognized Picture (RP) from logistics system allows better land C2 assessment and complete the SA.

Requirement ID: **SRS-307**

DEMETER is able to produce Interop.2022 formatted LOGUPDATE message files, where the LOGUPDATE is defined as Force Profile Holdings (FPH) formatted file where schema provided in [R-ICD-FasInterop]

Verification Method: Test

Requirement ID: **SRS-308**

DEMETER imports files from LOGFAS with the format of ADL and/or FPH schema specified in detail [R-ICD-FasInterop]. The mapping of the DEMETER model into these schemas shall be defined in design time. The mapping shall ensure minimum information required to build an ORBAT in DEMETER shall be met such as command hierarchy, and equipment holdings.

Verification Method: Test

Requirement ID: **SRS-309**

DEMETER performs smart import, by which when importing ADL and FPH, if data already exists in DEMETER, the import is only updated (changed) information. The ADL and FPH schemas are provided in [R-ICD-FasInterop].

Verification Method: Test

Requirement ID: **SRS-310**

DEMETER allows the user to generate LOGUPDATE from DEMETER overlays, the LOGUPDATE file format complies with FPH schema stated in [R-ICD-FasInterop]. Mapping of entities from DEMETER model to FPH formatted LOGUPDATE shall be agreed during the design phase.

Verification Method: Demonstration

Requirement ID: **SRS-311**

DEMETER provides "LOGUPDATE" to LOGFAS for it to update posture/manoeuvre information of units, with the LOGUPDATE file format complying with FPH schema stated in [R-ICD-FasInterop]. Note: LOGUPDATE is not the message from the message catalogue APP 11 (D)(1).

Verification Method: Test

Requirement ID: **SRS-312**

DEMETER provides LOGUPDATE in the form of a file, with the format complying with FPH schema stated in [R-ICD-FasInterop].

Verification Method: Test

Requirement ID: **SRS-313**

DEMETER displays as overlay Airbase/Seaport using NVG services provided by Log FAS (EVE) C2 systems. [R-ICD-LOGFAS]

Verification Method: Demonstration

4.2.1.3 Map Services (CoreGIS)

As a core service, Core GIS provides services for presenting information on the terrain and geographical views. Core GIS service provide map resources in the format and protocol defined by OGC standards and implement a specific provide (SIP). Battle space management, terrain management and many other operationally relevant functionalities uses geographical views with the maps provided by Core GIS.

Requirement ID: **SRS-314**

DEMETER provides the UI for the user to manage the maps, display order, etc. of the individual maps displayed on the geographical view.

Verification Method: Demonstration

Requirement ID: **SRS-315**

DEMETER is able to consume geographic information from a GIS using the OGC WMS and WMTS map services.

Verification Method: Demonstration

Requirement ID: **SRS-316**

DEMETER should adopt the ICD CoreGIS [R-ICD-AT-06.02.14-Map] and applicable Agency profiles for WMS and WMTS services.

Verification Method: Demonstration

Requirement ID: **SRS-317**

DEMETER shall follow the current and emerging FMN spiral's Geographic Services specifications

Verification Method: Demonstration

Requirement ID: **SRS-318**

DEMETER uses TIME and ELEVATION dimensions provided as Map Web Service by CoreGIS or any OGC compliant server.

Verification Method: Demonstration

Requirement ID: **SRS-319**

DEMETER displays one or more legends of a geospatial Information Product or a map (based on WMS map service or Open ESRI Geo Services REST [R-ICD-AT-06.02.14-Map].

Verification Method: Demonstration

Requirement ID: **SRS-320**

DEMETER is capable of presenting geographical information e.g. map views in deployments where it is disconnected from infrastructure provided map services.

Verification Method: Test

Requirement ID: **SRS-321**

DEMETER georeferenced entities store and report geospatial information in the formats compliant with [R-STANAG-2211]. The preferred geodetic datum to be used in NATO operations is World Geodetic System 1984 (WGS-84).

Verification Method: Demonstration

Requirement ID: **SRS-355**

When for operational reasons different mission geodetic datum is to be used DEMETER is able to perform the geodetic transformation to the specific mission geodetic datum. Note: Preferable this transformation should be done by a GIS service (e.g. CoreGIS) if available

Verification Method: Demonstration

4.2.1.4 NATO Information Portal (NIP) service

NIP Increment 1 provides a Bi-SC Information Portal in the form of web-enabled technology incorporating dynamic data updates in a user-friendly interface in order to facilitate user data access. The Information Portal will become the user's single entry point into the Bi-SC/NATO AIS Knowledge Management System NIP Increment 2 enhances the role-based interface and delivers services that build and catalogue information sets; implements services to support automated knowledge acquisition; extends the NIP to the NR domain; establishes "portal-to-order" capability; addresses integration with Information Management, Identity Management and Collaboration

service; eliminates a need for individual FS portals When NATO Information Portal (NIP) is used for information management purposes, DEMETER will be able to send or receive Information Products to/from the NIP. DEMETER will support the interface standards for the NIP for sending or receiving Information Products.

It is assumed that EMDS (APP031) service is retired on sites and replaced with NIP (APP086) service

Requirement ID: **SRS-322**

DEMETER reads and processes metadata provided along with any information product provided in NATO Information Portal (NIP).

Verification Method: Demonstration

Requirement ID: **SRS-323**

DEMETER produces and stores metadata provided along with any information product developed within DEMETER when storing that information to NATO Information Portal (NIP).

Verification Method: Demonstration

Requirement ID: **SRS-324**

DEMETER produces files compliant to FMN Web Hosting mandatory File Format Profile standards i.e. Open Office XML (ISO/IEC 29500), Office Document Format (ISO/IEC 26300), PDF (ISO19005, ISO3200), etc.

Verification Method: Demonstration

Requirement ID: **SRS-325**

DEMETER receives notification data from NIP for the information products that are linked to the DEMETER information products. [R-SharePoint]

Verification Method: Demonstration

4.2.1.5 NATO Common Operational Picture (NCOP) Service

Requirement ID: **SRS-326**

DEMETER provides NVG Web Services that defines the set of filtering capabilities in accordance with the NVG specifications, allowing the consumer service to manage the NVG payload in accordance to the specific needs or constraints e.g. bandwidth, details contained in [R-TD-NVG].

Verification Method: Demonstration

Requirement ID: **SRS-327**

DEMETER provides one or more NVG services those are consumed as a source and presented as a COP layer from land domain. The interface specifications complies with [R-ICD-NCOP2].

Verification Method: Demonstration

Requirement ID: **SRS-328**

DEMETER provides Order of Battle (ORBAT), with the ORBAT including hierarchy, holding details, status, and unit attributes. The provided data is automated so that the receiving party does not need to manually import any data e.g. web services compliant to NCOP [R-ICD-NCOP2].

Verification Method: Test

Requirement ID: **SRS-329**

DEMETER consumes specific NATO COP information products from NCOP using its NCOP IPS interface defined in [R-ICD-NCOP2].

Verification Method: Demonstration

4.2.1.6 TOPFAS/LOGFAS Order Of Battle Service

Requirement ID: **SRS-330**

DEMETER imports TOPFAS/LOGFAS ADL files (format Interop.2022 or higher) automatically to initiate BSOs, Hierarchy and holdings for a mission.[R-ICD-FasInterop]

Verification Method: Test

Requirement ID: **SRS-331**

DEMETER imports TOPFAS/LOGFAS FPH files (format Interop.2022 or higher) automatically to initiate BSOs, Hierarchy and holdings for a mission nation.[R-ICD-FasInterop]

Verification Method: Test

Requirement ID: **SRS-332**

DEMETER maps equipment stated in the ADL/FPH file using NATO Reportable Item Code to its internal presentation in order to represent BSO holdings correctly.[R-ICD-FasInterop]

Verification Method: Test

Requirement ID: **SRS-333**

DEMETER ensures all mapping information is adaptable to new versions without changing the code or installing a new version of DEMETER e.g. mapping of entities via mapping files instead of hard coding). DEMETER does not hard code any of the mapping information such that all mapping can be adaptable without source code change. DEMETER provides all documentation necessary to support user/admin in extending/updating the mapping information e.g. map files [R-ICD-FasInterop].Preferentially, the RIC database should be kept externally maintained and linked to the equipment.

Verification Method: Test

Requirement ID: **SRS-334**

DEMETER allows user to import, fill and send the "Plan Collection Sheet" excel of planning tool (TOPFAS) to provide assessment.[R-ICD-TOPFAS-Excel]

Verification Method: Test

Requirement ID: **SRS-335**

DEMETER is able to read and ingest planning data from the TOPFAS OData interface, keeping the source links e.g. ingest a planning item, associate to a TOPFAS source URL. [R-ICD-TOPFAS-ICD]

Verification Method: Test

Requirement ID: **SRS-336**

DEMETER allows the user to export Reports and Results data to TOPFAS for Objective analysis and refinement.[R-ICD-TOPFAS-Excel]

Verification Method: Test

Requirement ID: **SRS-337**

To initialize a short term land CONOPS, DEMETER shall receive the planning entities defined in TOPFAS i.e. Action/Task/Effect/Centre of Gravity, End State, Objective, Resource, Organisation, Fix Event, Event, and Actor and for annotation, Text Items. These entities' types and information exchange principles are defined in [R-ICD-TOPFAS-ICD].

Verification Method: Demonstration

Requirement ID: **SRS-338**

DEMETER provide the means for the user (creator) to assign a security label to the OPLAN in accordance with [R-4774-CMLS][[R-4778.2-BindProf]]

Verification Method: Demonstration

4.2.1.7 JOCWATCH (APP021) Event Service

JOCWatch is web based electronic event log system developed by NCIA. It is designed to support Watch Keepers and Shift Directors in Combined Joint Operation Centres (CJOCs) to record and disseminate [Ref-ATP]

Requirement ID: **SRS-339**

DEMETER is able to consume the events of NVG Request/Response services provided by JOCWATCH in order to obtain the battle space events [R-ICD-JOCWatch].

Verification Method: Demonstration

Requirement ID: **SRS-340**

DEMETER displays the military operation events from NATO JOCWatch, by polling the web service with a predefined (stored) polling period with predefined (stored) polling filters.[R-ICD-JOCWatch]

Verification Method: Demonstration

4.2.1.8 INTEL FS (APP033) Service Interoperability

Requirement ID: **SRS-341**

DEMETER both automatically, or manually through user initiation, receives and maps entities from IPOE information product of INTEL-FS. [R-ICD-Intel-FS-DM]

Verification Method: Demonstration

Requirement ID: **SRS-342**

DEMETER permits the user to maintain the IPOE, which may be provided to INTEL-FS via the protocols defined in INTEL-FS Interface Control Document [R-ICD-Intel-FS-DM]

Verification Method: Demonstration

Requirement ID: **SRS-343**

The user provides information from DEMETER to support the RFI process. The information provision complies with the associated RFI response services standards provided by INTEL-FS Interface Control Document[R-ICD-Intel-FS-DM].

Verification Method: Demonstration

4.2.1.9 NAMIS (APP023) Service Interoperability

The NATO Automated Meteorological Information System (NAMIS) provides the only first-in and sustained NATO Meteorological and Oceanographic (METOC) data source for the NATO Command and Force Structure. NAMIS is used to provide direct weather support to NATO-led operations by providing coherent, comprehensive, and harmonized weather information and products throughout ACO activities. The weather data is provided in the form of a WMS geospatial information product and details of this can be found in [R-ICD-Namis].

4.2.1.10 LC2IS (APP017) Service Interoperability

The new Land C2 system needs to exchange information with the current operational Land C2 system for many reasons. Migration of existing operational data, parallel use of two systems during the transition period necessitates information exchange with old and new Land C2 system. The mechanism of information exchange shall be in both direction, and standard interoperability profiles such as MIP can be used in case that information exchange requirements are met.

Requirement ID: **SRS-354**

DEMETER shall provide a mechanism to integrate with LC2IS without significant loss of information.

Verification Method: Demonstration

4.2.2 National Systems and Services

Roadmap Versions	Spiral 1	Spiral 2	Spiral 3	Spiral 4	Spiral 5	Spiral 6	Spiral 7	Spiral 8
Proposed Specifications	---	May 2017	Apr 2018	Apr 2019	Nov 2021	Nov 2024	Nov 2026	Nov 2028
Final Specifications	Apr 2015	Nov 2017	Nov 2018	Nov 2020	Nov 2023	Nov 2025	Nov 2027	Nov 2029
Emerging operational use	2016	2018	2021	2024	2027	2029	2031	2033
Preferred operational use	2017-2018	2019-2021	2022-2024	2025-2027	2028-2029	2030-2031	2032-2033	2034-2035
FMN Spiral Specification Roadmap 2017	1	2	3	4				
FMN Spiral Specification Roadmap 2018	1	2	3	4	5			
FMN Spiral Specification Roadmap 2019		2	3	4	5			
FMN Spiral Specification Roadmap 2020		2	3	4	5	6		
FMN Spiral Specification Roadmap 2021		2	3	4	5	6		
FMN Spiral Specification Roadmap 2022			3	4	5	6	7	
FMN Spiral Specification Roadmap 2023			3	4	5	6	7	
FMN Spiral Specification Roadmap 2024			3	4	5	6	7	8

Interoperability (this includes standardisation efforts) is achieved through common initiatives between stakeholders. The most significant current one is the Federated Mission Networking (FMN). NATO contributes with the NATO Enterprise infrastructure and/or ICT services to fulfil its role as an FMN affiliate. This is facilitated by the NATO Command Structure (NCS).

4.2.2.1 Federation with NFS

To enable flexible and compliant interoperability with NATO Nations, Partners, Coalitions, and other organisations, including NATO as an Affiliate in the FMN Framework, DEMETER comply to current and emerging FMN Spiral standard that are related with the functionality. DEMETER might communicate between Operation to Tactical Operation level e.g. JFC to/from LCC or Tactical Operation to Tactical level e.g. LCC to lower echelon, although the former is the mandatory capability, latter has an added value.

Requirement ID: **SRS-344**

DEMETER processes and generates overlays from received FFI track information received from many sources from either one overlay per source or a single overlay presenting all sources.[R-NSIP]

Verification Method: Test

Requirement ID: **SRS-345**

DEMETER allows augmenting of BSOs generated from FFI tracks.

Verification Method: Demonstration

Requirement ID: **SRS-346**

DEMETER allows automatic update of augmented FFI track as BSOs with newly arrived FFI tracks.

Verification Method: Demonstration

Requirement ID: **SRS-347**

DEMETER receives or produces formatted messages compliant with APP 11(D) NATO Message Catalogue, ADatP-3 MTF and XML formats.[R-NSIP]

Verification Method: Test

Requirement ID: **SRS-348**

DEMETER is capable of processing Air Tasking Order, Airspace Control Order, Enemy Land Forces Situation Report, Fragmentary Order, Logistic Situation Report Land Forces, NBC Basic Wind Data Report, NBC Chemical Downwind Report, NBC1 Bio/Chem Report, Own Land Forces Situation Report, Personnel Report, Rules Of Engagement Implementation, messages from APP-11(D) message catalogue MTF formats in their associated ADatP-3 formats to ensure effective bandwidth usage. [R-NSIP]

Verification Method: Test

Requirement ID: **SRS-349**

DEMETER is capable of receiving APP11 (D) message catalogue messages that are relevant to the land domain. The whole list of messages shall comply with ADatP3 BL3 XML standards.

Verification Method: Demonstration

Requirement ID: **SRS-350**

DEMETER allows the production of similar products using other document templates defined by the HQs and addressing the specific mission or HQ needs.

Verification Method: Demonstration

Requirement ID: **SRS-351**

DEMETER displays as overlay, ICC/ACCS produced ADattP3 11(C)/(F) formatted messages respectively or NVG formats (Compliant to FMN).

Verification Method: Demonstration

Requirement ID: **SRS-352**

DEMETER displays as overlay, MCCIS/TRITON produced OTH-G (Contact/JUnit/Overlay 2/Overlay 3) messages or NVG content that is compliant with applicable FMN Spiral standards.

Verification Method: Demonstration

ANNEX A.1 Glossary of Acronyms and Abbreviations

[AD]:[Active Directory]

[ADatP]:[Allied Data Publication]

[ADFS]:[Active Directory Federated Services]

[ADL]:[Allied Disposition List]

[AIS]:[Automated Information System]

[API]:[Application Interface]

[APP]:[Allied Procedural Publication]

[ArcGIS]:[Family of client, server and online geographic information system (GIS) software developed and maintained by Esri]

[Bi-SC]:[Bilateral Strategic Command]

[BSCM]:[Battle Space Control Measures (e.g. Tactical Graphics)]

[BSO]:[Battle Space Objects (e.g. Units)]

[CAX]:[Computer Aided Exercises]

[CBRN]:[Chemical, biological, radiological and nuclear defence]

[CIMIC]:[Civil-Military Co-operation]

[CIS]:[Communication Information System]

[CISP]:[Communication Information System (CIS) Provider]

[CoA]:[Course of Action]

[COI]:[Community of Interest]

[CONOPS]:[Concept of Operations]

[COP]:[Common Operational Picture]

[COPD]:[Comprehensive Operations Planning Directive]

[CP]:[Capability Package]

[CPP]:[Capability Package Program]

[CSV]:[Comma Seperated File]

[DCIS]:[Deployable Communication Information System]

[DEMETER]:[Future Land C2]

[DNS]:[Domain Name Service]

[DOORS]:[Dynamic Object Oriented Requirements System]

[FFI]:[Friendly Force Information]

[FFT]:[Friendly Force Tracking]

[FMN]:[Federated Mission Network]

[FPH]:[Force Profile Holdings]

[FRAGO]:[Fragmanted Order]

[GIS]:[Geographical Informaation System]

[HQ]:[Headquarters]

[HTTP/HTTPS]:[Hyper Text Transfer Protocol (Secure)]

[ICD]:[Interface Control Document]

[IES]:[Information Exchange Specification]

[IP]:[Internet Protocol]

[IP]:[Information Product]

[IPOE]:[Intelligence preparation of the operational environment]

[ISM]:[Information Service Modules]

[ISO]:[International Standards Organisation]

[ITM]:[IT Modernisation]

[JCATS]:[Joint Conflict and Tactical Simulation]

[JFACC]:[Joint Force Air Component Command]

[JOC]:[Joint Operations Centre]

[JSON]:[Javascript Object Notation]

[JTF]:[Joint Task Force]

[JTLS]:[Joint Teather Level Simulation]

[LOGFAS]:[Logistics Functional Area System]

[MAF]:[Mission Anchor Function]

[MIM]:[MIP Information Model]

[MIP]:[Multinational Interoperability Program]

[MIR]:[Mission Information Room]

[MMR]:[Minimum Military Requirement]

[MOE]:[Measure of Effectiveness]

[MOP]:[Measure of Performance]

[MS]:[Mission Secret]

[MSU]:[Military Subunit]

[MTF]:[Message Text Format]

[MTTR]:[Mean Time To Recover]

[NATO]:[North Atlantic Treaty Organisation]

[NCS]:[NATO Command Structure]

[NDI]:[Non-Developmental Items]

[NERS]:[NATO Enterprise Reference System]

[NGO]:[Non Government Organisation]

[NIP]:[NATO Information Portal]

[NPKI]:[NATO Public Key Infrastructure]

[NS]:[NATO Secret]

[NISP]:[NATO Interoperability Standards and Profiles]

[NSIP]:[NATO Security Investment Program]

[NU]:[NATO Unclassified]

[NVG]:[NATO Vector Graphics]

[OPLAN]:[Operational Plan]

[ORBAT]:[Order Of Battle]

[PAX]:[Persons approximately]

[PDF]:[Portable Document Format]

[REST]:[Representational State Transfer]

[RFI]:[Request For Information]

[RGP]:[Recognized Ground Picture]

[SATCOM]:[Satellite Communication]

[SCOM]:[System Center Operations Management]

[SHAPE]:[Supreme Headquarters Allied Powers Europe]

[SI]:[Service Instructions]

[SIP]:[Service Interface Profile]

[SITFOR]:[Situational Forces]

[SLD]:[Styled Layer Descriptor]

[SOA IdM]:[Service Oriented Architecture - Identity Management]

[SOAP]:[Simple Object Access Protocol]

[SQL]:[Structured Query Language]

[SRS]:[Software Requirements Specifications]

[STANAG]:[NATO Standardization Agreement]

[TOPFAS]:[Tools for Planning Factional Area System]

[UN]:[United Nations]

[UTM]:[Universal Transverse Mercator]

[WMS]:[Web Map Services]

[WMTS]:[Web Map Tile Services]

[WNGO]:[Warning Order (APP-11)]

[WNGORDER]:[Warning Order (APP-11)]

[WSMP]:[Web Service Message Protocol]

[XML]:[eXtensible Markup Language]

[XSLT-FO]:[eXtensible Style Sheet Language - Formatting Object]

[System High]:["System High" - a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, but not all individuals with access to the CIS have a common need-to-know for the information handled within the CIS; approval to access information may be granted at an informal or individual level;]

[A2SL]:[Agency Authorized Software List]