SECTION 13: LABOUR CATEGORIES

13.1. **General**

13.1.1. This section outlines minimum educational and experience qualifications for Contractor key personnel assigned to this Contract.

[SOW-886] *All Contractor's IEG-C project key personnel SHALL demonstrate spoken and written fluency in English language, at a minimum of 4343 as defined in [STANAG 6001, 2014].*

[SOW-887] *All Contractor's IEG-C project key personnel SHALL have a current NS security clearance and maintain it throughout the lifecycle of the Contract. Contractor personnel who need System Administrator or Operator privileges when working on NATO SECRET systems SHALL be required to hold NATO CTS (Cosmic Top Secret) clearances.*

[SOW-888] *All Contractor's IEG-C project key personnel SHALL present references of successful project delivery and description of roles, responsibilities, activities executed, and SHALL include reachable points of contact for above.*

13.1.2. Substitution of experience or education is allowed as outlined in Table 19-1 below.

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

Table 25: Experience / Education substitution

13.2. **Management**

13.2.1. Project Manager

13.2.1.1. Responsible for project management, performance and completion of tasks and deliveries. Establishes and monitors project plans and schedules and has full authority to allocate resources to insure that the established and agreed upon plans and schedules are met. Manages costs, technical work, project risks, quality, and corporate performance. Manages the development of designs and prototypes, test and acceptance criteria, and implementation plans. Establishes and maintains contact with Purchaser, subcontractors, and project team members. Provides administrative oversight, handles Contractual matters and serves as a liaison between the Purchaser and corporate management. Ensures that all activities conform to the terms and conditions of the Contract.

13.2.1.2. Education: University Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master’s, supported by relevant certificates/ diplomas. Current Project Management certification (Prince2 Practitioner and/or Project Management Institute (PMI) Project Management Professional (PMP)). Current Information Technology Infrastructure Library (ITIL) Foundation Certificate.

13.2.1.3. Experience: At least ten (10) years of experience as an Information and Communications Technology (ICT) project manager. At least five (5) years of experience as the project manager for an effort of similar scope to the IEG-C project, preferably including the application of a formal project management methodology such as PRINCE2, supported by project references and description of role/responsibilities/activities executed.

13.3. Project Management Support

13.3.1. Project Control Analyst

13.3.1.1. Establishes and maintains project schedule and cost baseline and analyses risks and potential impacts. Prepares project highlight reports.

13.3.1.2. Education: Bachelor’s degree.

13.3.1.3. Experience: At least three (3) years of experience in project scheduling, project control, or project monitoring and reporting.

13.3.2. Webmaster

13.3.2.1. Provides website construction and administration, develops connections between databases and web-based front ends. Generates technical reports and related documentation as required. Provides expertise in the development and maintenance of web sites. Provides training on the uploading of documents, creating pages, links and other web functions. Maintains access rights to pages on web. Maintains reports and statistics on utilisation of the Project Website.

13.3.2.2. Education: Associates degree or two years of technical training.

13.3.2.3. Experience: At least one (1) year of experience in website support and at least one year in website construction.

13.3.3. Contract Security Specialist

13.3.3.1. Provides support in areas directly pertinent to administration, supervision, and control of facility security in an industrial and/or government environment. Possesses a working knowledge of government and industrial security regulations.

13.3.3.2. Education: Bachelor’s degree.

13.3.3.3. Experience: At least three (3) years of experience in Contract security administration.

13.4. Engineering and Technical

13.4.1. Senior Engineer

13.4.1.1. Performs complex engineering tasks and multiple tasks simultaneously. Assists with or plans major research and engineering tasks or programs of high complexity. Directs and co-ordinates all activities necessary to complete a major, complex engineering program or multiple smaller tasks or programs. Performs advanced engineering research, hardware or software development.

13.4.1.2. Education: Master's degree in engineering. ITIL Foundation and Service Transition certificates

13.4.1.3. Experience: At least seven (7) years in engineering positions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use. Member of recognised professional body.

13.4.2. Intermediate Engineer

13.4.2.1. Performs engineering tasks and additional duties as assigned. Assists higher level engineers with larger tasks. Manages or directs multiple engineering tasks, directing research and development activities as required. Performs advanced engineering applications programming and analysis for systems/equipment assigned.

13.4.2.2. Education: Bachelor's degree in engineering.

13.4.2.3. Experience: At least three (3) years of experience in engineering functions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use.

13.4.3. Junior Engineer

13.4.3.1. Performs engineering tasks under the direction of higher level engineers. Performs independent research, conducts studies and analysis, and participates in the design and development of complex systems.

13.4.3.2. Education: Bachelor's degree in engineering.

13.4.3.3. Experience: At least one (1) year of experience in engineering functions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use.

13.4.4. Senior Systems Engineer

13.4.4.1. Plans and co-ordinates engineering activities to meet SRS requirements. Provides comprehensive definition of all aspects of system development from analysis of mission needs to verification of system performance. Competent in technical disciplines as applied to government and commercial information and communications systems. Prepares trade-off studies and evaluations for vendor equipment. Recommends design changes/enhancements for improved system performance. Supervises the work of a design, integration, test, and implementation team. Analyses architectural options for performance and manageability.

13.4.4.2. Education: University Degree in Electronic Engineering, Computer Science, Telecommunications, or related discipline, preferably equivalent to a Master's, supported by relevant certificates/ diplomas. Current ITIL Foundation and Service Design certificates.

13.4.4.3. Experience: At least seven (7) years of experience in system design and integration. At least five (5) years in the design, integration, or implementation information systems, defence systems and large scale systems.

13.4.5. Intermediate Systems Engineer

13.4.5.1. Performs system engineering assignments in support of the analysis of complex system design, formulating requirements, developing alternative approaches, conduct of studies, and application of standards. May function as a member of an engineering team assigned responsibilities for specific task areas.

13.4.5.2. Education: Bachelor's degree in engineering or computer science.

13.4.5.3. Experience: At least three years of experience in system design and integration.

13.4.6. Junior Systems Engineer

13.4.6.1. Conducts research and application of system design principles for the design, development, implementation, or support as a member of assigned task staffing. Develops alternative solutions, concepts, or processes through research into assigned systems and components.

13.4.6.2. Education: Bachelor's degree in engineering or computer science.

13.4.6.3. Experience: At least one (1) year of experience in system design and integration.

13.4.7. Senior Communications Engineer

13.4.7.1. Performs communications system transition planning, engineering design for integration with processing systems, specification development, standards, interface design, testing, and the conduct of transmission and traffic studies.

13.4.7.2. Education: Master's degree in engineering.

13.4.7.3. Experience: At least seven (7) years of experience in the engineering of communications systems via all transmission media.

13.4.8. Intermediate Communications Engineer

13.4.8.1. Prepares communications systems designs and technical documentation, and other design criteria. Implements COTS and emerging communications systems and develops technical plans, documentation, and support.

13.4.8.2. Education: Bachelor's degree in engineering.

13.4.8.3. Experience: At least three (3) years of experience in the engineering of communications systems via all transmission media.

13.4.9. Junior Communications Engineer

13.4.9.1. Conducts engineering analysis, develops technical documentation, investigate communications requirements, formulates network interfaces, and assists in project/program execution.

13.4.9.2. Education: Bachelor’s degree in engineering.

13.4.9.3. Experience: At least one (1) year of experience in the engineering of complex communications systems via all transmission media.

19.4.9bis Systems Integration Analyst

19.4.9bis.1 Develops and implements solutions using the optimal technology, capability, and interfaces Researches available tools and technologies to determine alternate technology solutions. Researches, implements, and supports multiple computing platforms, operating systems, processing environments, and telecommunications technologies. May conduct cost/benefit or feasibility analyses; perform capacity analyses and planning.

19.4.9bis.2 Education: Bachelor’s degree in engineering or computer science.

19.4.9bis.3 Experience: At least seven (7) years of experience in the integration and implementation of information systems, defence systems, C2 systems, preferably in maritime domain.

13.4.10. Senior Software Programmer

13.4.10.1. Performs complex program development using standard and specialised languages to create special purpose software, modify existing programs, and enhance system efficiency and integrity. Translates detailed designs into software, tests, debugs, and refines software packages. Manages software development teams in modular development of complex applications. Provides technical direction to assigned programmers.

13.4.10.2. Education: Bachelor’s degree in engineering or computer science.

13.4.10.3. Experience: At least seven (7) years of experience in the design, programming, and testing of applications software.

13.4.11. Intermediate Software Programmer

13.4.11.1. Analyses systems requirements and design specifications to develop block diagrams and logic flow charts. Translates detailed designs into computer software for specific applications. Prepares documentation, including program and user documentation.

13.4.11.2. Education: Bachelor’s degree in engineering or computer science.

13.4.11.3. Experience: At least three (3) years of experience in the design, programming, and testing of applications software.

13.4.12. Junior Software Programmer

13.4.12.1. Performs programming tasks based upon specifications and flow diagrams. Translates concepts into program modules for testing, debugging, refinement, and integration with other modules. Prepares draft documentation including program and user documentation. Functions as a member of a software development team under the guidance of more experienced programmers.

13.4.12.2. Education: Bachelor’s degree in engineering or computer science.

13.4.12.3. Experience: At least one (1) year of experience in the design, programming, and testing of applications software.

13.4.13. System Support Engineer

13.4.13.1. Designs and integrates system support applications and protocols to meet system requirements. Analyses architectural options for performance and manageability. Analyses and designs implementations to meet specialised message formats or interfaces.

13.4.13.2. Education: Bachelor’s degree in engineering.

13.4.13.3. Experience: At least seven (7) years of experience in the design, integration, and implementation of information systems. At least three years of experience with Simple Network Management Protocol (SNMP) and system support applications.

13.4.14. Information Systems Security Engineer

13.4.14.1. Analyses and develops network systems and information security practices to include: operating systems, applications, Transmission Control Protocol (TCP)/Internet Protocol (IP), security architecture, multi-level security, intrusion detection, virus detection and control, PKI, vulnerability assessment. Documents findings and recommend changes in procedures, configuration, or design.

13.4.14.2. Education: Bachelor’s degree.

13.4.14.3. Experience: At least three (3) years of experience in information systems security. At least five years in information systems integration, implementation, or operation.

13.4.15. Information Systems Security Specialist

13.4.15.1. Provides support in implementing procedures and practices prescribed for safeguarding and control of an automated information system and the processing of classified information.

13.4.15.2. Education: Associates degree or two years of technical training.

13.4.15.3. Experience: At least two (2) years of experience as an Information Systems Security Officer for an operational system.

13.4.16. Field Engineer

13.4.16.1. Conducts site surveys, prepares implementation plans, prepares implementation procedures, supervises installation and activation, reports on installation status, manages repair and modifications to systems/equipment, performs field maintenance, and performs system configuration changes based upon approved specifications. Supervises provision of support to installed systems.

13.4.16.2. Education: Bachelor’s degree. ITIL Foundation and Service Operations certificates

13.4.16.3. Experience: At least five (5) years in the installation and support of information systems.

13.4.17. Senior Technician

13.4.17.1. Supervises technicians in the troubleshooting, repair, installation, training, integration, and upgrade of systems and equipment. Works closely with assigned engineers and systems personnel to support implementation and activation efforts.

13.4.17.2. Education: Associates degree.

13.4.17.3. Experience: At least seven (7) years of experience in the installation and maintenance of network and information systems.

13.4.18. Intermediate Technician

13.4.18.1. Performs troubleshooting, repair, refurbishment, and installation of systems and equipment. Performs factory or field testing of systems, development of maintenance or repair procedures, and supports installation teams in specific areas of expertise.

13.4.18.2. Education: Associates degree.

13.4.18.3. Experience: At least three (3) years of experience in the installation and maintenance of network and information systems.

13.4.19. Junior Technician

13.4.19.1. Performs troubleshooting, repair, and installation functions as assigned. May be assigned as technical support technician for specific systems or hardware. Performs factory or field testing and supports installation teams as assigned.

13.4.19.2. Education: Secondary school graduate with one year of technical training.

13.4.19.3. Experience: At least two (2) years of experience installing and maintaining network and information systems.

13.4.20. System Management Specialist

13.4.20.1. Analyses, develops, and maintains operational system configuration parameters. Establishes and implements system policy, procedures and standards, and ensures their conformance with system requirements. Ensures that security procedures are established and implemented. Provides technical assistance to operational, logistics, and system engineering staff.

13.4.20.2. Education: Bachelor’s degree and completion of a formal system administration or network management certification course.

13.4.20.3. Experience: At least three (3) years of experience in the administration of distributed information systems.

13.5. **Testing**

13.5.1. Senior Test Engineer

13.5.1.1. Directs test planning, design and tools selection. Establishes guidelines for test procedures and reports. Co-ordinates with Purchaser on test support requirements and manages Contractor test resources.

13.5.1.2. Education: Bachelor's degree in engineering.

13.5.1.3. Experience: Integration and testing engineering skills with five (5) years' experience as part of technical projects, supported by project reference and description of role / responsibilities / activities. Demonstration of practical experience in planning, conducting and assessing integration and testing activities in support of projects for at least equivalent to IEG-C for at least two (2) years, supported by project references and description of role/responsibilities/activities

13.5.2. (Deleted)

13.5.3. Intermediate Test Engineer

13.5.3.1. Designs and documents unit and application test plans. Transforms test plans into test cases and executes those cases. Supervises individual tests and prepares test reports.

13.5.3.2. Education: Bachelor's degree in engineering.

13.5.3.3. Experience: At least three (3) years of experience in the design and execution of information systems tests.

13.5.4. Junior Test Engineer

13.5.4.1. Performs testing activities under supervision of more experienced test personnel. Executes defined test cases and procedures. Collects and analyses test data; prepares test reports.

13.5.4.2. Education: Bachelor's degree in engineering.

13.5.4.3. Experience: At least one (1) year in the design and execution of information systems tests.

13.5.5. Test Technician

13.5.5.1. Provides installation and administration support to information system testing. Constructs and tests prototype equipment for electrical systems and components, consistent with engineering and other specifications. Executes tests and collects test data. Assists in preparing test reports.

13.5.5.2. Education: Associates degree or two years of technical training.

13.5.5.3. Experience: At least two (2) years of experience in the configuration and administration of information systems or test and measurement systems.

13.6. **Implementation Support**

13.6.1. Logistics Management Specialist

13.6.1.1. Provides support in the development of support documentation to include as a minimum, elements such as support equipment, technical orders, supply support and computer resources support, process of evolving and establishing maintenance/support concepts.

13.6.1.2. Education: Bachelor’s degree.

13.6.1.3. Experience: At least seven years of experience in supply and support of information systems. At least three (3) years in support of distributed systems in more than one NATO nation.

13.6.2. Logistics Analyst

13.6.2.1. Creates and helps execute plans for the ILS of complex systems. Analyses adequacy and effectiveness of current and proposed logistics support provisions. Supervises the efforts of other logistics personnel in the execution of assigned tasks.

13.6.2.2. Education: Bachelor’s degree.

13.6.2.3. Experience: At least three (3) years of experience in ILS planning and analysis.

13.6.3. Inventory Specialist

13.6.3.1. Creates and maintains an inventory control system. Tracks materials, coordinates shipping and receiving, and supervises packing operations.

13.6.3.2. Education: Associates degree.

13.6.3.3. Experience: At least three (3) years of experience in shipping, receiving, and inventory control.

13.6.4. Shipping and Receiving Clerk

13.6.4.1. Coordinates the shipping and receiving of materials. Tracks property using automated equipment. Performs and records materials inventory checks.

13.6.4.2. Education: Secondary school graduate.

13.6.4.3. Experience: At least three (3) years of experience in shipping and receiving.

13.6.5. Technical Writer

13.6.5.1. Develops, writes, and edits materials, briefs, proposals, instruction books, and related technical and administrative publications concerned with work methods and procedures for installation, operations and enhancement of equipment. Organises material and compiles writing assignments for clarity, conciseness, style, and terminology. Prepares and edits documentation incorporating information provided by users, and technical and operations staff. Possesses a substantial knowledge of the capabilities of computer systems. Capable of writing, editing, and generating graphic presentations.

13.6.5.2. Education: Bachelor's degree.

13.6.5.3. Experience: At least three (3) years as a technical writer.

13.6.6. Senior Configuration Manager

13.6.6.1. Establishes and maintains a process for tracking the life cycle development of system design, integration, test, training, and support efforts. Maintains continuity of products while ensuring conformity to Purchaser requirements and commercial standards. Establishes configuration control forms and database.

13.6.6.2. Education: Bachelor's degree.

13.6.6.3. Experience: At least five (5) years of experience in specifying Configuration Management requirements, standards, and evaluation criteria in acquisition documents, and in performing configuration identification, control, status accounting, and audits. At least three years in computer and communication systems development, including physical and functional audits and software evaluation, testing and integration. At least two years of experience with application of Configuration Management tools.

13.6.7. Intermediate Configuration Manager

13.6.7.1. Maintains a process for tracking the life cycle development of system design, integration, test, training, and support efforts. Maintains continuity of products while ensuring conformity to Purchaser requirements and commercial standards. Maintains configuration control records and databases.

13.6.7.2. Education: Associates degree or two years of technical training.

13.6.7.3. Experience: At least three (3) years of experience in technical system Configuration Management. At least two years in communication and information systems development, including physical and functional audits and software evaluation, testing and integration.

13.6.8. Junior Configuration Manager

13.6.8.1. Prepares and coordinates change requests, configuration items, and configuration baselines. Maintains configuration control records and databases.

13.6.8.2. Education: Associates degree or one year of technical training.

13.6.8.3. Experience: At least one (1) year of experience in technical system configuration or document management.

13.6.9. Data Control Specialist

13.6.9.1. Performs assigned portions of managing the data input into complex information systems. Analyses and administers data for both the developing team and the customer. Handles daily administrative tasks, produces and edits technical reports based on data system processing, monitors use of data and performs updates as required. Participates in all phases of system development with emphasis on the data collection, input, documentation, and acceptance phases. Designs and prepares technical reports and related documentation, and makes charts and graphs to record results.

13.6.9.2. Education: Associates degree.

13.6.9.3. Experience: At least three (3) years of experience in administration of Configuration Management or technical documentation.

13.6.10. Quality Assurance Manager (QAM)

13.6.10.1. Establishes and maintains process for evaluating software, hardware, and associated documentation. Determines the resources required for QC. Maintains the level of quality throughout the system life cycle. Develops project QA plan. Conducts formal and informal reviews at predetermined points throughout the system life cycle. Audit subcontractors, suppliers and outsource companies to ensure that appropriate standard practices are applied.

13.6.10.2. Education: Bachelor’s degree.

13.6.10.3. Experience: At least seven (7) years working with QC methods and tools. At least four (4) years supporting system development and test projects.

13.6.11. Quality Assurance (QA) Specialist

13.6.11.1. Develops and implements quality standards. Reviews hardware, software, and documentation. Participates in formal and informal reviews to determine quality. Participates in the development of system QAPs. Examines and evaluates design, integration, and test processes and recommends enhancements and modifications.

13.6.11.2. Education: Bachelor’s degree.

13.6.11.3. Experience: At least four (4) years of working with QC methods and tools.

13.7. **Training Support**

13.7.1. Instructional Systems Designer

13.7.1.1. Conducts the research, necessary to identify training needs based on performance objectives and existing skill sets; prepares training strategies and delivery methodology analyses; and prepares cost/benefit analyses for training facilities and deliverables. Develops training delivery plan, instructional guidelines, and performance standards and assessment mechanisms. Plans and directs the work of training material developers and coordinates activities with system development staff. Supervises the implementation and adaptation of training products to customer requirements.

13.7.1.2. Education: Bachelor’s Degree.

13.7.1.3. Experience: At least three (3) years of experience in the design and development of training for information systems and defence systems using an Instructional Systems Design approach such as the Systems Approach to Training, Performance-Based Training, Analysis, Design, Development, Implementation, and Evaluation (ADDIE), or Criterion Referenced Instruction.

13.7.2. Senior Training Materials Developer

13.7.2.1. Conducts the research necessary to develop and revise training courses and prepares training plans. Develops instructor (course outline, background material, and training aids) and student materials (course manuals, workbooks, hand-outs, completion certificates, and course feedback forms). Trains personnel by conducting formal classroom courses, workshops, seminars, and/or computer based/computer-aided training. Provides daily supervision and direction to staff.

13.7.2.2. Education: Bachelor’s Degree.

13.7.2.3. Experience: At least five (5) years in the preparation of technical training, including CBT materials.

13.7.3. Training Materials Developer

13.7.3.1. Conducts the research necessary to develop and revise training. Develops training materials (course outline, manuals, workbooks, hand-outs, completion certificates, and course feedback forms).

13.7.3.2. Education: Associates degree.

13.7.3.3. Experience: At least three (3) years of experience in the preparation of technical training materials.

13.7.4. CBT Developer

13.7.4.1. Uses CBT tool to design and implement course flowchart, text, animation, voice, and graphic displays.

13.7.4.2. Education: Bachelor’s degree.

13.7.4.3. Experience: At least three (3) years of experience in the preparation of CBT courses.

13.7.5. Senior Instructor

13.7.5.1. Supervises trainers who conduct technical training classes. Conducts training classes. Works closely with Purchaser personnel to determine training and scheduling requirements. Develops and maintains training materials. Reviews and provides inputs for technical documentation.

13.7.5.2. Education: Bachelor Degree.

13.7.5.3. Experience: At least four (4) years of experience in systems administration or operation and at least four (4) years as technical training instructor in defence systems and maritime C2 systems.

13.7.6. Junior Instructor

13.7.6.1. Conducts technical training classes. Prepares and updates training documentation.

13.7.6.2. Education: Bachelor's Degree.

13.7.6.3. Experience: At least four (4) years of experience in systems administration or operation and at least two (2) years as technical training instructor.

13.8. Operational Support

13.8.1. System Administrator

13.8.1.1. Administers systems operations and configuration. Maintains user accounts and profiles. Performs system backup and restoration procedures. Troubleshoots operational problems. Coordinates system configuration and performance issues with central network support staff and Purchaser site personnel.

13.8.1.2. Education: Associates degree or two years of technical training.

13.8.1.3. Experience: At least one (1) year in systems administration of Windows Server 2012 systems. At least one (1) year in the administration and operation of an integration capability. At least one (1) year in the administration and operation of a virtualized environment.

13.8.2. Network Manager

13.8.2.1. Oversees administration and operation of network and service management applications. Develops and implements operating procedures. Administers upgrades to system support and network management components. Collects operational performance data and performs performance analysis.

13.8.2.2. Education: Associates degree.

13.8.2.3. Experience: At least two (2) years in administration and implementation of SNMP or other system support systems.

13.8.3. Database Administrator

13.8.3.1. Manages network-wide configuration databases. Develops and implements data synchronisation procedures and resolves database discrepancies. Maintains and publishes network configuration tables and indices. Designs and implements queries and other utilities. Ensures that Back-ups are scheduled and that the directory / database is restorable from them. Ensuring BC and DR preparedness is maintained.

13.8.3.2. Education: Associates degree.

13.8.3.3. Experience: At least two (2) years in database administration.

13.8.4. Operational Support Manager

13.8.4.1. Organises, directs and manages operational support activities. Analyses system performance data and prepares reports and assessments. Meets with Purchaser personnel to coordinate support issues and coordinates with system deployment personnel on activation and cut-over. Ensures conformance with all requirements.

13.8.4.2. Education: Bachelor’s degree.

13.8.4.3. Experience: At least five (5) years of experience in the administration and operation of a distributed information system.

SECTION 14: INTERFACES WITH OTHER PROJECTS / SYSTEMS

14.1. NS Domain (ITM)

14.1.1. The ITM project, which is the amalgamation of the three CP 9C0150 Projects: 0IS03091; 0IS03092, and 0IS03101, will transform the way IT services are provided to Users across the NATO enterprise, including the NATO Command Structure (NCS), the NATO Headquarters (NHQ) and NATO agencies.

14.1.2. The project will provide modern effective and cost-efficient Infrastructure as a Service (IaaS) supporting IT services at NS level on the ON domain. The project is, in effect, a hardware replacement and service consolidation project as it will maintain the existing NS AIS domain (or future ON – Operational Network at NS classification) at NATO military command structure HQs.

14.1.3. The architecture is based on various different types of implementation: Data Centres, Enhanced Nodes, and Standard Nodes. As for the Client Connectivity, ITM will support Thick Clients (Desktop/Laptop) and Thin Clients (Virtual Desktop Infrastructure).

14.2. MS Domain (x-FOR)

14.2.1. NATO implements 'mission' Secret domains in current operations and exercises in order to provide CIS access to non-NATO mission partners. Examples are the KFOR Secret domain supporting NATO-led operations in Kosovo, the EUFOR Secret domain supporting operations in Bosnia & Herzegovina and the Resolute Support domain supporting operations in Afghanistan. 'Mission' Secret domains are also established to support Exercises and are a central feature of NATO's 'Future Mission Network' concept.

14.3. Management Domain

14.3.1. The IEG-C system components will need to be managed from the Management domain already existing in Purchaser operations in addition to the Management tools which the Contractor will add. These components will include Servers, Switches, Firewalls Toolsets and any other appliance needed for the final IEG-C capability. The Management Consoles/Equipment that will host these toolsets will be provided as PFE to this contract.

[SOW-889] *The Contractor SHALL assist the Purchaser to configure existing Management Suites in Purchaser's toolset to integrate and manage IEG-C components, in consistence with the IEG-C system design and management.*

14.4. NCIA Cyber Monitoring Capability (former NCIRC)

14.4.1. The NATO Cyber Security Monitoring Capability involves capturing network traffic at key points in the global CIS infrastructure, and the collection of system logs, which can then be used to support cyber security incident analyses. In order to monitor the IEG-C and the traffic it mediates, probes will capture network packets at appropriate network interfaces connecting to the IEG-C, or within the IEG-C by software system agents installed at the components comprising the IEG-C. This traffic capture is transparent to the IEG-C.

14.4.2. The Contractor will assist the Purchaser or any other sub-contracted entity by the Purchaser to enact necessary changes and additions to the IEG-C Contractor's design and system, so that the aforementioned monitoring capability will integrate the IEG-C system like all other CIS equipment and systems operated by the Purchaser.

[SOW-890] *The Contractor SHALL assist the Purchaser to integrate the IEG-C system in the Purchaser's NATO Cyber Security Monitoring Capability.*

14.5. **Mission Information Room**

14.5.1. The 'Mission Information Room' (MIR) at SHAPE and JFC Naples allows HQ Staff access to a local extension of a 'mission' network and to the 'at risk' NATO Secret domain established for operations and exercise support. The MIR places this NATO Secret domain in the IEG-C DMZ.

SECTION 15: DELIVERABLES OUTLINES

15.1. General

15.1.1. This section describes the outline content of a subset of all deliverables (management products and specialist products) to be provided by the Contractor under this Contract.

15.2. Risk Log

[SOW-891] *The Contractor SHALL provide the Risk Log listing the risks, and indicating for each one the following information (but not limited to):*

- *Risk identifier: unique code to allow grouping of all information on this risk;*
- *Description: brief description of the risk;*
- *Risk category (e.g., management, technical, schedule, and cost risks);*
- *Impact: effect on the project if this risk were to occur;*
- *Probability: estimate of the likelihood of the risk occurring;*
- *Risk rating (High, Medium, Low);*
- *Proximity: how close in time is the risk likely to occur;*
- *Response strategy: avoidance, mitigation, acceptance, transference*
- *Response plan(s): what actions have been taken/will be taken to counter this risk;*
- *Owner: who has been appointed to keep an eye on this risk;*
- *Author: who submitted the risk;*
- *Date identified: when was the risk first identified;*
- *Date of last update: when was the status of this risk last checked;*
- *Status: e.g., closed, reducing, increasing, no change.*

15.3. Issue Log

[SOW-892] *The Contractor SHALL ensure that the Issue Log comprises the following information (but not limited to):*

- *Project Issue Number;*
- *Project Issue Type (ECP, Off-specification, general issue such as a question or a statement of concern);*
- *Author;*
- *Date identified;*
- *Date of last update;*
- *Description;*
- *Action item;*

- *Responsible person. (Individual in charge of the action item);*
- *Suspense date (Suspense date for the action item);*
- *Priority;*
- *Status.*

15.4. **Project Status Report (PSR)**

[SOW-893] *The Contractor SHALL ensure that the PSR summarises activities and progress, including (but not limited to):*

- *Changes in key Contractor personnel;*
- *Summary of Contract activities during the preceding month, including the status of current and pending activities;*
- *Progress of work and schedule status, highlighting any changes since the preceding report;*
- *EVM KPIs, including Planned Value, Earned Value, Actual Cost, Schedule Variance, Schedule Performance Index, Budget at Completion and Estimate at Completion.*
- *CSA report addressing all products in the Project Breakdown Structure;*
- *Issue Log;*
- *Change Requests status;*
- *Off-Specifications status;*
- *Risk Log;*
- *Test(s) conducted and results;*
- *Summary of any site surveys conducted;*
- *Plans for activities during the following reporting period;*
- *Provisional financial status and predicted expenditures.*

15.5. **Change Request**

[SOW-894] *The Contractor SHALL ensure that any Change Request will respect the requirements in SOW 12.7 Requests for Change (RFC).*

15.5.1. Change Request Document

[SOW-895] *The Contractor SHALL ensure that CR documentation includes:*

- *The list of all Change Requests processed since the start of the project, in a tabular form, indicating for each of them the date it was created and the current status;*
- *All Change Requests processed since the start of the project.*

15.6. **System Design Specification (SDS)**

[SOW-896] *The Contractor SHALL include, at a minimum, the following information in the SDS document:*

- *System Architecture*
- *The following Operational and Systems Views, as defined in the NATO Architecture Framework (NAF, [NAC AC/322-D(2007)0048, 2007]):*
- *NOV-1, High-Level Operational Concept Diagram;*
- *NSV-1 Systems Interface Description (Composition);*
- *NSV-1 System Interface Description (Intra System);*
- *NSV-1 System Interface Description (Inter System);*
- *NSV-2, Systems Communications Description;*
- *NSV-2a: System Port Specification;*
- *NSV-4 System Functionality;*

[SOW-897] *The (minimum) information in the NAF views the Contractor SHALL supply is defined in Table 21-1 below.*

[SOW-898] *The NAF views SHALL be produced using applications compliant with NAF 4 and Archimate 3. If not, the Contractor SHALL ensure the exchange format SHALL be approved by the Purchaser upfront.*

[SOW-899] *Physical layout and operation principles of the IEG-C in the deployment sites (including the site of the IEG-C Reference System): identification of where the components will be installed, of how users (NATO Staff Users) will make use of the provided functionality, of how support staff (IEG-C Administrators will operate the system. This SHALL cover in particular how the IEG-C components SHALL integrate into the storage and backup solutions existing at the implementation sites.*

- *Results of the network simulation, showing the integration with the underlying network infrastructure, the mitigation of potential impact of the available bandwidth and of any latency;*
- *Replication, synchronisation and browsing protocols and flows;*
- *Proposed topology for the system;*
- *Routing, Transport, and connectivity to IEG-C components;*
- *Administration model design (Administrative groups and permissions, administrative roles, trust relationships between separate domains).*
- *Schema*
- *Attributes to which the NATO Staff Users have read-access.*
- *System Functionalities.*
- *Functional breakdown of the IEG-C system.*
- *Application Programming Interfaces (API) and libraries.*
- *System internal interfaces: Description of the interworking of all components to meet the system requirements (e.g., physical interfaces between components, data flows.)*

- *Performance Requirements: Performance requirements are defined in the SRS.*
- *Equipment*
- *Physical breakdown of the operational IEG-C system, of the Reference Test Bed, into hardware/software CIs (including the number of licenses for each software CI), with traceability to the functional breakdown.*
- *Identification of all COTS included in the system.*
- *CSA reports addressing all system CIs.*
- *All configuration information (parameters, settings, etc.) for all of the IEG-C components.*
- *Security*
- *Description of how the system complies with all security requirements.*

NAF view (subview)	Purpose	NAF objects to be used	NAF relationships to be used
NSV-1 (composition)	To show the different components of the envisaged IEG-C system	System	ResourceComposition (System->System)
NSV-1 (intra-system)	To identify the interactions between the different components of the IEG-C system. For each interaction applicable standards/formats/protocols need to be identified	System, DataElement, Standard/Protocol	ResourceInteraction (System->System), ConveyedElement (ResourceInteraction->DataElement) ConformsTo (ResourceInteraction->Standard/Protocol)
NSV-1 (inter-system)	To identify the interaction of the IEG-C system with other systems. This also incl. dependencies on hosting platforms. For each interaction applicable standards/formats/protocols need to be identified	System, DataElement, Standard/Protocol	ResourceInteraction (System->System), ConveyedElement (ResourceInteraction->DataElement) ConformsTo (ResourceInteraction->Standard/Protocol) ConformsTo (DataElement ->Standard/Protocol)
NSV-1 (deployment)	To show the deployment of components to locations (site-level). Note: this is a NAF extension	System, Location	RequiredLocation (System->Location)
NSV-2a (System port description) aka Interface Specification	To identify and specify each internal (i.e., between system components) and external (i.e., between IEG-C and other systems) interface.	System, System Port (aka interface), Protocol	Association (System->SystemPort), ImplementsProtocol (SystemPort->Protocol)
NSV-4 (system functionality)	To identify the functionality that each component provides. Each functional requirement must be traceable to a system function	System, SystemFunction, Requirement	FunctionProvision (System->SystemFunction), Satisfy (SystemFunction->Requirement)

Table 26: NAF Information Requirements

15.7. System Version Definition Document (SVDD)

[SOW-900] *The SVDD SHALL include the following:*

- *List of differences between this and the previous System version;*
- *List of capabilities of this System version;*
- *Guidelines on how to install this System version;*
- *Breakdown of the system into CIs and provision of accurate identification information for every CI.*

15.8. System Implementation Plan (SIP)

[SOW-901] *The Contractor SHALL submit to the Purchaser the SIP with the following information:*

- *The Contractor's approach to all system implementation tasks (including the sequence of activation of the sites to be implemented);*
- *The Contractor organisation and key personnel involved in system implementation;*
- *The overall schedule for implementation activities including site survey, site preparation, site installation and activation. This schedule SHALL show all planned outages of any kind in the sites;*
- *The schedule of all planned outages of any kind in the sites;*

[SOW-902] *The detailed implementation sequence of Technical Services and User services. The sequence SHALL carefully consider and adapt to the ITM implementation sequence in order to minimize the impacts on both projects.*

[SOW-903] *The installation plan, which SHALL specifically address:*

- *A general installation plan showing how the gradual installation and activation of the IEG-C will be carried out by the Contractor;*
- *The installation procedures, showing that those procedures will cause no or minimal disruption to the sites and to the User desktop applications;*
- *A site-specific design for each site;*
- *A detailed installation plan for each site;*
- *Site and system installation checklist;*
- *Site activation checklist;*
- *An Allocation Matrix showing the allocation of each system CIs (nature and quantities) to each site, and the number of users and support staff for each site;*
- *Any specific tools the Contractor intends to furnish and use during the site installation.*

[SOW-904] *The activation plan, which SHALL specifically address:*

- *The site activation activities;*

- *Any post-activation tasks;*
- *The "back-out" procedures. The back-out section to the SIP SHALL enable deactivation and/or removal of all installed IEG-C components and restoration of existing services without disruption of those services.*
- *The potential disruption/outage that the implementation activities might generate ensuring potential outages will be kept short (less than 3 hours in duration), planned (approved by the Purchaser at 48 hours in advance based on a Contractor-provided plan to restore functionality within 30 minutes), localised (limited to areas agreed to by the Purchaser), and if possible carried out during week-ends.*
- *The migration plan from existing gateways to IEG-C:*

[SOW-905] *The migration plan SHALL detail the migration activities. Schedule. Engineering activities for the migration of the existing gateways to IEG-C.*

[SOW-906] *The Contractor SHALL structure the SIP so that general implementation information is maintained in the body of the plan and site-specific details are kept as annexes.*

15.9. **Project Management Plan (PMP)**

[SOW-907] *The Contractor SHALL ensure that the PMP comprises at minimum of the following sections:*

- *An 'Organisation' section describing the Contractor's organisation for this project according to the requirements. This section SHALL include an organisational chart showing the members of the Contractor's Project Team (including the members of the Contractor PMO) and showing their respective responsibilities and authority. This section should also include proposed Project Communication Plan.*
- *A 'Project Planning' section describing the Contractor's processes supporting the development and maintenance of the PBS, PFD and PMS according to the requirements.*
- *A 'Risk management' section describing the Contractor's processes supporting Risk Management by the Contractor.*
- *A 'System Engineering' section describing the Contractor approach to these activities according to the requirements in SECTION 10.*
- *A 'System Implementation' section describing the Contractor approach to these activities according to the requirements in SECTION 13.*
- *An 'Operation and Maintenance' section describing the Contractor approach to these activities according to the requirements in SECTION 12.*
- *An "Operation and Maintenance" section describing the Contractor approach to these activities according to the requirements in Annex F: Annex F Maintenance and Support Concept (After FSA);*
- *A 'Testing' section describing the Contractor approach to these activities according to the requirements in SECTION 14.*

- *An "Earned Value Management Section" describing how the Contractor will assure EVM tracking and reporting.*

15.10. User and Maintenance Manuals

[SOW-908] *The Contractor SHALL develop all Technical Manuals compliant with the requirements in SOW 11.6.*

15.11. IEG-C Procedures and Work Instructions

[SOW-909] *The Contractor SHALL develop Standard Operating Procedures which detail the supporting processes described in ANNEX F.*

SECTION 16: OPTIONS

16.1. General

16.1.1. This section describes the options to be provided by the Contractor under this Contract, if these options are to be exercised by the Purchaser.

16.1.2. The optional gateways and respective locations are described in Annex B of this SOW.

16.2. WP 6 Hardware

16.2.1. All required equipment will be identified and selected by the bidders to conform to SRS, but part thereof may be provided by the customer as Purchaser Furnished Equipment (PFE). The main reason is to achieve homogeneity in the installed hardware base.

16.2.2. This equipment in general involves Infrastructure hardware (processing, storage, networking), firewall and guard products. To the extent that the Purchaser has other existing contracts, these equipment will be procured via these contracts. Lists will be finalized in the design phase, before the conclusion of the PDR at EDC+3.

16.2.3. The Contractor will in addition provide the costs for this same equipment. The Purchaser may decide to exercise this option, and the Contractor will then procure the aforementioned equipment.

[SOW-910] *The Contractor SHALL be prepared to procure all hardware required for the completion of this project, if the Purchaser exercises the corresponding option before the PDR (EDC+3MO).*

16.3. WP 7 Cyber Security Monitoring (former NCIRC)

16.3.1. As described in paragraph 14.4 in this SOW, the IEG-C infrastructure will need to accommodate and integrate to NCIA's Cyber Security Monitoring capability systems and services. This integration will normally be performed by the Purchaser or another sub-contracted entity.

16.3.2. The IEG-C contractor will be required to provide a costed, not evaluated, option for the delivery of the aforementioned activities and integration.

16.3.3. This integration will conform to the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017] and will comprise of the following activities:

16.3.3.1. Site Survey

16.3.3.2. Incorporation in IEG-C design

16.3.3.3. Installation

16.3.3.4. Integration and testing Mandatory Sites and Management Suite

16.3.3.5. Integration and testing Optional Sites

16.3.3.6. Initial Operational Support

16.3.4. The aforementioned activities are described in detail in Annex H and they will be concluded in parallel with the other relevant project activities

[SOW-911] *The Contractor SHALL be prepared to perform the activities of this Work Package, if the Purchaser exercises the corresponding option before the SRR (EDC+2MO). In particular:*

- ○ *Surveys will occur together with the main Site Surveys,*
- ○ *incorporation in the IEG-C design will occur before the PDR (EDC+3MO)*
- ○ *Installation will occur together the IEG-C equipment installations at various points in the project schedule (between the FAT at EDC+9MO and FSA at EDC+27MO).*
- ○ *Integration and testing will occur together with the other integration and testing activities as described in SECTION 7 : System Implementation and SECTION 8 : Test, Verification, Validation (TVV).*

16.4. **WP 11 Hardware additional gateways**

16.4.1. The same terms of paragraph 16.2 above will apply for the additional gateways referred to in paragraph 1.3.2 in this SOW.

16.5. **WP 12 Additional gateways**

16.5.1. This work package will contain all effort for the implementation of additional gateways referred to in paragraph 1.3.2 in this SOW. In general, all conditions in this SOW will also apply as for the mandatory gateways. The beginning date and duration of activities for this WP will be agreed together with the Purchaser and may be concurrent to WP3.

ANNEX A System Requirements Specification (SRS)

The SRS is a separate document that will be attached as Annex A

ANNEX B Implementation Scope

B.1. List of sites

Site ID	Geographic Location	Name of the Site	IEG-C ID	Operational use/network	Remarks
Mandatory Sites					
1	Mons, Belgium	SHAPE	IEG-C-01	Reference System & Management Facility	
			IEG-C-02	NATO Response Force (NRF)	
			IEG-C-03	Very high-readiness Joint Task Force (VJTF)	
			IEG-C-04	Exercise 1	
2	Stavanger, Norway	JWC	IEG-C-05	Exercise 2	
			IEG-C-06	Exercise 3	
3	Strasbourg, France	EUROCORPS	IEG-C-07	EUROCORPS	
4	Innsworth, UK	Allied Rapid Response Corps (ARRC)	IEG-C-08	ARRC	
5	Lago Patria, Italy	Joint Force Command (JFC), Naples	IEG-C-09	Active Endeavour	
			IEG-C-10	NRF Standby	
6	Bydgoszcz, Poland	Joint Force Training Centre (JFTC)	IEG-C-11	Exercise 4	
Optional Sites					
7	The Hague and/or NCIA Software Factory	NCIA Testbed	IEG-C-12	Integration Network Environment	
8	HQ Kabul, AFG		IEG-C-13	Resolute Support (option)	
9	Pristina, KSV	KFOR (option)	IEG-C-14	KFOR (option)	
10	Sarajevo, BiH	EUFOR (option)	IEG-C-15	EUFOR (option)	
-	Lago Patria, Italy	Joint Force Command (JFC), Naples	IEG-C-16	Ocean Shield (option)	
			IEG-C-17	Resolute Support (option)	
11	NATO flag ship	NATO flag ship	IEG-C-18	Afloat Command Platform (option)	

Table Annex B-15: Site Type and Location

B.2. Work Package Scope

B.2.1. Generalities

The purpose of this part of Annex B to the Statement of Work (SOW) is to describe the scope of work in terms of Contract Work Packages. This SOW is part of capability development activities under Project Serial 0IS03102 of Capability Package 9C0150 and for reference purposes it will follow the WP numbering of those activities. The sections below will give the relationships between these activities, their authorizations and the internal dependencies.

The list of Work Packages authorised under 0IS03102 is listed in Table Annex B-16. WP 1, 5 and 8-10 are not part of this SOW.

Number	Work Package
WP 2.1	Achieve FAT
WP 2.2	Installation of the Reference System
WP 2.3	Integration into NATO Enterprise
WP 3	Installation of Mandatory Gateways
WP 4	Decommissioning Legacy Gateways
WP 6	Hardware Purchase (PFE)
WP 7	Cyber Security Monitoring Capability (former NCIRC)
WP 11	Hardware Purchase Optional Gateways (PFE)
WP 12	Installation of Optional Gateways

Table Annex B-16: List of Work Packages

Each Work Package defined in this document has the following structure:

- General
- Work Package Dates
- Work Package Activities
- Milestones (indicated as Months after Contract – MAC)

Work Packages 2.2 and 3 will have in addition options that will be defined

B.2.2. Work Package 2

B.2.2.1. General

Work Package 2 has been split in three subpackages and those include the

a. WP 2.1 Initial desing and build of the first gateway on the Contractor's testbed to reach satisfactory Factory Acceptance Test (FAT at EDC+9MO)
b. WP 2.2 Provision of a Reference System to NCIA
c. WP 2.3 Integration in NATO Enterprise and Provision of a Central Management Solution

B.2.2.2. **Work Package Dates**

a. Work Package 2 will start at EDC.
b. Work Package 2 will end at EDC + 13 months

B.2.2.3. **Work Package Activities**

The contractor shall perform the following reviews:

a. System Requirements Review
b. Preliminary Design Review
c. Critical Design Review

The contractor shall have reached FAT by the end of this Work Package and the Acceptance of the IEG-C Security Accreditation Package shall be achieved.

B.2.2.4. **Milestones**

Milestone Description	MAC	Remark
System Requirements Review	2	
Preliminary Design Review	3	
Critical Design Review	6	
Factory Acceptance Test	9	
System Integration Testing	13	
Acceptance IEG-C Accreditation Package	13	

B.2.3. **Work Package 3**

B.2.3.1. **General**

Work Package 3 includes the installation of gateways at the authorised sites including Initial Support up to FSA

B.2.3.2. **Work Package Dates**

a. Work Package 3 will start at EDC + 13 months
b. Work Package 3 will end at EDC + 27 months

B.2.3.3. **Work Package Activities**

The contractor shall prepare, execute and monitor

a. The deployment Authorization
b. The Provisional System Acceptance
c. The Site(s) Acceptance Testing
d. The Operational Test and Evaluation

B.2.3.4. **Milestones**

Milestone Description	MAC	Remark
Deployment Authorization	17	
Provisional System Acceptance	20	
Site(s) Acceptance Accreditation	25	
Site(s) Acceptance Testing	25	
Operational Test and Evaluation	26	
FSA	27	

B.2.4. **Work Package 4**

B.2.4.1. **General**

Work Package 4 provides the additional decommissioning of legacy gateways on 3 sites that will not receive new ones from this project:

a. NDOG in SHAPE
b. F5 in Eggermond
c. F5 in Castlegate

B.2.4.2. **Work Package Dates**

a. Work Package 4 may start as soon as the first site has been accepted and the Purchaser has provided authorization
b. Work Package 4 will end at the same time as WP3

B.2.4.3. **Work Package Activities**

The contractor shall prepare, execute and monitor

a. The dismantling of the gateways at the sites mentioned in Par B.2.4.1 and this according to the policies and directives of the Purchaser.

B.2.4.4. **Milestones**

No specific milestones are defined, but WP4 will be concluded by FSA.

Annex C Purchaser Furnished Equipment (PFE) and services

C.1. Hardware

The contractor will determine what equipment will be required to conform to SRS and in general to fulfil the goal of this project. The customer has provided in Appendix D “Purchaser Furnished Equipment Detailed Specifications” of the SRS, equipment lists that can be provided as PFE to the winning bidder. If some equipment or appliances required for the IEG-C are not available in these lists, the bidders will include those in their design and cost them accordingly.

The aforementioned equipment lists in general include End User equipment, Servers, Storage, Firewalls, Guards, Racks and Switches and will be in principle provided to bidders to a location of their choosing (contractor premises or final installation location)

The bidders are requested nevertheless to include in their bids as costed options (options that will not be evaluated) all the hardware that will be required for the IEG-C, and make provision for that procurement in their project plans. The Customer reserves the right to exercise these options to the winning bidder, instead of providing this hardware as PFE. If PFE is physically transferred to the Contractor, a hand-over process will be put in place including the inspection and custody forms between parties. Lists will be finalized in the design phase before PDR+3.

C.2. Virtualized Environment

In regard to the optional NCIA Test Bed system requested in Annex B1 above, it is the customer’s intention to utilize a Virtualized Software Development environment based on Azure. When and if this option is exercised, this platform will be provided to the Contractor as PFE. This Test Bed will be used to provide IEG-C services to other developing projects of the customer.

If it is not possible to use such an environment to host an IEG-C, the contractor will notify the customer before the PDR (EDC+3MO) and an alternative solution will be commonly sought.

The Contractor can however request to create a development environment for their own use during the development phase, instead of creating and using their own environment in their premises, so as to facilitate transition to test. This service however is not part of this contract and if requested will be mutually agreed during pre-contract discussions.

C.3. Software Licenses

The purchaser's Enterprise License Agreement (ELA) shall be used by the contractor for the following products:

- All Microsoft products, including OS Server, Workstations, SCOM, RDP etc.
- McAfee
- VMWare
- Adobe
- Oracle

Annex D Abbreviations

Acronym	Description
A	
ABL	Allocated Baseline
ACMP	Allied Communication Management Plan
ACO	Allied Command Operations
ACP	Allied Communication Publication
ACT	Allied Command Transformation
ADDIE	Analysis, Design, Development, Implementation, and Evaluation
ADDS	Active Directory Domain Services
AFPL	Approved Fielded Products List
AIA	Authority Information Access
AIFS	Allied Information Flow System
AIG	Address Indicator Group
AIMS	AIFS Integrated Message System
AirC2IS	Air Functional Services
AIS	Automated Information System
AL	Address List
AMSG	Allied Military Security Guideline
AOM	Alliance Operations and Missions
API	Application Programming Interface
ARH	Allied Replication Hub
ARO	Authorised Release Officer
ASM	Abbreviated Service Message
ATO	Approval to Operate
AV	Anti-Virus
AVC	Advanced Video Coding
B	
Bi-SC	Bi-Strategic Commands
BLAT	Baseline Acceptance Test
BPD	Boundary Protection Device
BPS	Boundary Protection Service
C	
C2	Command and Control
C3	Consultation, Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAB	Change Advisory Board
CAD	Collective Address Directory
CAW	Contract Award

Acronym	Description
CBT	Computer Based Training
CC	Common Criteria
CCB	Configuration Control Board
CCEB	Combined Communications Electronics Board
CD-ROM	Compact Disc Read Only Memory
CDP	CRL Distribution Point
CDR	Critical Design Review
CES	Core Enterprise Services
CFI	Connected Forces Initiative
CIS	Communication and Information Systems
CI	Configuration Item
CIP	Content Inspection Policy
CIPE	Content Inspection Policy Enforcement
CLI	Command Line Interface
CLIN	Contract Line Item Number
CMP	Configuration Management Plan
CMS	Configuration Management System
CMS	Cryptographic Message Syntax
CN	Common Name
CoC	Certificate of Conformity
COI	Community of Interest
COMCEN	Communication Centre
CONOPS	Concept of Operations
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
CP	Capability Package
CPU	Central Processing Unit
CQAR	Contractor Quality Assurance Representative
CRL	Certificate Revocation List
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
CSR	Certificate Signing Request
CSV	Comma-Separated Values
D	
DA	Deployment Authorization
DAP	Directory Access Protocol
DBMS	Database Management System
DC	Domain Controller
DCIS	Deployable Communication Information Services
DDoS	Distributed Denial of Service

Acronym	Description
DI	Developmental Items
DIF	Difficulty, Importance and Frequency
DIT	Directory Information Tree
DL	Distribution List
DMZ	De-Militarized Zone
DN	Distinguished Name
DNS	Domain Name System
DoS	Denial of Service
DS	Directory Service
DSA	Directory Service Agent
DVD	Digital Versatile Disc
E	
EAL	Evaluation Assurance Level
EAPC	Euro-Atlantic Partnership Council
ECP	Engineering Change Proposal
EDC	Effective Date of Contract
EE	End Entity
EMS	Enterprise Management System
E-NPKI	Enterprise NATO Public Key Infrastructure
EOC	Essential Operational Capabilities
EPO	e-Policy Orchestrator
ERM	Event Review Meeting
ESS	Enhanced Security Services for S/MIME
ETP	Event Test Plan
EVM	Earned Value Management
F	
FAQ	Frequently Asked Question
FBL	Functional Baseline
FCA	Functional Configuration Audit
FFT	Friendly Force Tracking
FOC	Final Operational Capability
FQDN	Fully Qualified Domain Name
FSA	Final System Acceptance
FT	Factory Testing
FTE	Full Time Equivalent
FTP	File Transfer Protocol
G	
GbE	Gigabit Ethernet
GIF	Graphics Interchange Format
GIS	Geographic Information Systems

Acronym	Description
GFE	Government Furnished Equipment
GMT	Greenwich Mean Time
GA	Gateway Administrator
GO	Gateway Operator
GSSAPI	Generic Security Services Application Program Interface
GQAR	Government Quality Assurance Representative
GUI	Graphics Unit Interface
H	
HIDS	Host-based Intrusion Detection System
HL	High Low
HQ	Headquarters
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
I	
IAM	Identity and Access Management
ICD	Interface Control Document
ICT	Information and Communications Technology
IdM	Identity Management
IE	Internet Explorer
IEC	International Electrotechnical Commission
IEG	Information Exchange Gateway
IEG-C	Information Exchange Gateway – Scenario C
IEG-FS	Information Exchange Gateway Functional Services
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
IFB	Invitation for Bid
IFP	Information Flow Control Policy
IIS	Internet Information Services
ILS	Integrated Logistics Support
ILSP	Integrated Logistics Support Plan
INTEL	Intelligence
INTEL FS	Intelligence Functional Service
IOR	Interoperability Requirements
IOS	Initial Operational Support
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPMT	Integrated Project Management Team
IRC	Internal Release Candidate
ISA	Interim Security Accreditation
ISAF	International Security Assistance Force

Acronym	Description
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITM	IT Modernization
ITSM	IT Service Management
ITU-T	International Telecommunication Union
IV&V	Independent Verification and Validation
J	
JC2IS	Joint C2 Functional Services
JCOP	Joint Operational Picture
JFC	Joint Force Command
JFTC	Joint Force Training Centre
JPEG	Joint Photographic Experts Group
K	
KVM	Keyboard Video Mouse
JWC	Joint Warfare Centre
KPI	Key Performance Indicator
L	
LAC	Logical Access Control
LACS	Logical Access Control System
LAN	Local Area Network
LC2IS	Land Functional Services
LDAP	Lightweight Directory Access Protocol
LH	Low High
LOG FS	Logistics Functional Services
LOGA	Log Aggregator
LORA	Level of Repair Analysis
LSA	Logistics Support Analysis
M	
MARCOM	Allied Maritime Command
MaxTTR	Maximum Time To Repair
MCCIS	Maritime Functional Services
MCF	Main Computing Facilities
MDS	Material Datasheet
MDT	Mean Down Time
MG	Mail Guard
MHTML	MIME Encapsulated HTML
MIL-STD	Military Standard
MIME	Multi-Purpose Internet Mail Extensions
MM	Military Message

Acronym	Description
MMHS	Military Message Handling System
MN	Mission Network
MOD	Ministry of Defence
MPEG	Moving Picture Experts Group
MPIF	Metadata Policy Information File
MS	Mission Secret
MSO	Message Service Operator
MTBCF	Mean Time Between Critical Failures
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenance
MTP	Master Test Plan
MTTD	Mean Time To Diagnose
MTTR	Mean Time To Repair
MTTRSy	Mean Time to Restore (the System)
N	
NAF	NATO Architecture Framework
NAP	Network Access Protection
NAR	NATO Architecture Repository
NASIS	NATO Subject Indicator System
NAS	Network Attached Storage
NATO	North Atlantic Treaty Organisation
NCC	NCI Agency Control Centre
NCCIS	NATO Command, Control and Information System
NCIA	NATO Communication & Information Agency
NCIRC	NATO Computer Response Capability
NCIS	NATO Communications and Information Systems School
NCMS	NATO Core Metadata Specification
NCOP	NATO Common Operational Picture
NCI	NATO Communications Infrastructure
NCS	NATO Command Structure
NCSC	NATO Cyber Security Centre
NDI	Non-Developmental Items
NEDS	NATO Enterprise Directory Service
NEID	NATO Enterprise ID
NFR	Non-Functional Requirements
NGCS	NATO General Purposes Segment Communications System
NGO	Non-Governmental Organisation
NIAP	National Information Assurance Partnership
NIC	Network Interface Controller
NICE	(military-grade) NATO IP cryptographic equipment

Acronym	Description
NISP	NATO Interoperability Standards and Profiles
NNCS	NATO Network Control System
NNEC	NATO Network Enabled Capability
NNHQ	New NATO Headquarter
NOS	NATO Office of Security
NOV	NATO Operational View (ref. NAF V3)
NPKI	NATO Public Key Infrastructure
NQAR	National Quality Assurance Representative
NR	NATO RESTRICTED
NS	NATO SECRET
NU	NATO UNCLASSIFIED
NSA	National Security Authority
NSAB	NATO CIS Security Accreditation Board
NSON	NATO SECRET Operational Network
NSV	NATO System View (ref. NAF V3)
NSWAN	NATO SECRET WAN
NTP	Network Time Protocol
O	
O	Organization
O/R	Originator / Recipient
O&M	Operation and Maintenance
OAC	Operational Acceptance Criteria
OASIS	Organization for the Advancement of Structured Information Standards
OBL	Operational Baseline
OCSP	On-line Certificate Status Protocol
OCF	Online Computer Forensics
OEM	Original Equipment Manufacturer
OID	Object Identifier
OLA	Organizational Level Agreement
ON	Operational Network
OSA	Operational System Acceptance
OSATP	Operational System Acceptance Test Plan
OSS	Open-Source Software
ON	Operational Network
ORs	Off-specification Reports
OS	Operating System
OSP	Organizational Security Policies
OU	Organizational Unit
OVA	Online Vulnerability Assessment
P	

Acronym	Description
PAC	Physical Access Control
PACS	Physical Access Control System
PBL	Product Baseline
PBN	Protected Business Network
PBNE	Protected Business Network Environment
PBS	Product Breakdown Structure
PCA	Physical Configuration Audit
PDF	Portable Document Format
PDM	Product Delivery Meeting
PDR	Provisional Design Review
PFD	Product Flow Diagram
PFE	Purchaser Furnished Equipment
PfP	Partnership for Peace
PHST	Packaging, Handling, Storage, Transportation
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PLAD	Plain Language Address
PMIC	Programme Management and Integration Capability
PMO	Project Management Office
PMP	Project Management Plan
PMP	Project Management Professional (PMI Certification)
PMS	Project Master Schedule
PNG	Portable Network Graphics
POC	Point of Contact
PP	Protection Profile
PR	Pilot Release
PRM	Project Review Meeting
PSA	Provisional System Acceptance
PSC	Personnel Security Clearance
PSR	Project Status Report
PTP	Project Test Plan
PTS	Project Test Strategy
Q	
QA	Quality Assurance
QAM	Quality Assurance Manager
QAP	Quality Assurance Plan
QAR	Quality Assurance Representative
QOS	Quality of Service
R	

Acronym	Description
RA	Registration Authority
RACI	Responsible, Accountable, Consulted and Informed
RAM	Reliability, Availability, and Maintainability
RCCMD	Remote Console Command
RDP	Remote Desktop Protocol
RFC	Request for Change
RFC	Request for Comment
RFD	Request for Deviation
RFQ	Request For Quote
RFW	Request for Waiver
RI	Routing Indicator
RMP	Risk Management Plan
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RS	Resolute Support
RS	Release Server
RSA	Rivest, Shamir, and Adelman
RTF	Rich Text Format
RTM	Requirements Traceability Matrix
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTT	Round Trip Time
S	
S/MIME	Secure / Multi-Purpose Internet Mail Extensions
SA	IEG-C System Administrator
SAA	Security Accreditation Authority
SAN	Storage Area Network
SAP	Security Accreditation Plan
SAP	Site Activation Plan
SAT	Site Acceptance Testing
SBR	System Baseline Review
SBT	Service-based Testing
SCCM	System Centre Configuration Manager
SCOM	System Centre Operations Manager
SDS	System Design Specification
SDR	System Design Review
SecOPs	Security Operating Procedures
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SHAPE	Supreme Headquarters Allied Powers Europe

Acronym	Description
SI	Signal Instructions
SIC	Subject Indicator Code
SIP	System Implementation Plan
SIP	Service Interface Profile
SISRS	System Interconnection Security Requirements Statement
SIT	System Integration Test
SIVP	System Implementation Verification Procedures
SLA	Service Level Agreement
SLP	Standardised Language Proficiency
SMA	Signal Message Address
SMC	Service Management and Control
SME	Subject Matter Expert
SMP	System Management Plan
SMS	System Management Server
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service Operation Centre
SOM	System Operation Manual
SOW	Statement of Work
SPIF	Security Policy Information File
SQL	Structured Query Language
SRA	Security Risk Assessment
SRR	System Requirements Review
SRS	System Requirements Specification
SSCS	Site Security Compliance Statement
SSH	Secure SHell
SSL	Secure Sockets Layer
SSRS	System Security Requirements Statement
SSS	Schedule of Supplies and Services
SSWB	Site Survey Work Book
STANAG	Standards NATO Agreement
STR	System Test Review
STVP	Security Test and Verification Plan
STVR	Security Test and Verification Report
SUS	System Usability Scale
SVG	Scalable Vector Graphics
SWDL	Software Distribution List
SWID	Software Identifier

Acronym	Description
T	
TA	Target Architecture
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDL	Tactical Data Link
TEMPEST	TEMPorary Emanation ansd Spurious Transmission
TIFF	Tag Image File Format
TLS	Transport Layer Security
TNA	Training Needs Analysis
TOE	Target of Evaluation
TOPFAS	Planning Functional Services
TRR	Test Readiness Review
TSF	TOE Security Functionality
TTR	Time To Repair
U	
UA	User Agent
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time Coordinated
V	
VOE	Verifiable Objective Evidence
VLAN	Virtual LAN
W	
W3C	World Wide Web Consortium
WAN	Wide Area Network
WG	Web Guard
WSDL	Web Services Description Language
WSUS	Windows Server Update Services
X	
XML	Extensible Mark-up Language
XMPP	eXtensible Messaging and Presence Protocol
XSD	XML Schema Definition
XSL	eXtensible Stylesheet Language
XSLT	eXtensible Stylesheet Language Transformations
XSS	Cross-Site Scripting
xFOR	KFOR, SFOR or any other NATO operation
Y	

Acronym	Description
Z	
Z	ZULU
ZULU	Universal Time Coordinated (UTC)

Annex E Glossary

Term	Definition
C3 Taxonomy	It is an effort leading to: •Support delivery of coherent C3 capabilities to NATO •Provide a common taxonomy to improve communication across planning domains and organisations •Provide a framework for multinational capability development •Provide a framework to support interoperability •Facilitates the practical implementation of NNEC •Save money by encouraging re-use •Support deliverable, product, program & project management •Support C3 governance Through the definition of classes of CIS capabilities arranged in a hierarchical structure organised by supertype-subtype relationships.
Commercial Off-the-Shelf (COTS)	Any item that is priced and available for purchase and delivery from a commercial firm can be considered Commercial Off-the-Shelf (COTS). A COTS product is one that is used "as-is." COTS products are designed to be easily installed and to interoperate with existing system components. Almost all hardware and software bought by the average computer user fits into the COTS category: computers, monitors, printers, cables, operating systems, office product suites, word processing, and e-mail programs are among the myriad examples.
Configuration Item	A Configuration Item is a hardware, firmware, or software component, or combination thereof, that satisfies an end use function and is designated for separate configuration management.
Fire and forget	Fire and forget is an attribute of the Military Messaging service. It can be described as the ability of the system to monitor military messages from the moment they are sent, throughout their journey to the recipient. Moreover, fire and forget generates alerts to an operator if the message has not reached the recipient within the set pre-defined time period. At the moment, within AIFS, the fire and forget function is accomplished by Communication Centre (COMCEN) operators through both technology and procedures.
High Grade Messaging	A High Grade Messaging Service is the mechanism for exchanging critical information and official correspondence throughout Defence Organizations and with its partners, in a manner optimised to meet stringent requirements for assurance of delivery, survivability, reliability, ease of use, security, integrity, non-repudiation and archiving commensurate with a general purpose service.
ITM	The name of the project that is delivering the new core NATO architecture for platform hosted Virtualised capabilities, reusing core NATO network infrastructures.
Metadata	METADATA is "data about data". The term is ambiguous, as it is used for two fundamentally different concepts (types). Structural metadata is about the design and specification of data structures and is more properly called "data about the containers of data"; descriptive

Term	Definition
	metadata, on the other hand, is about individual instances of application data, the data content. Metadata is traditionally in the card catalogues of libraries. As information has become increasingly digital, metadata are also used to describe digital data using metadata standards specific to a particular discipline. By describing the contents and context of data files, the usefulness of the original data/files is greatly increased. For example, a webpage may include metadata specifying what language it is written in, what tools were used to create it, and where to go for more on the subject, allowing browsers to automatically improve the experience of users. Wikipedia encourages the use of metadata by asking editors to add category names to articles, and to include information with citations such as title, source and access date. The main purpose of metadata is to facilitate in the discovery of relevant information, more often classified as resource discovery. Metadata also helps organize electronic resources, provide digital identification, and helps support archiving and preservation of the resource. Metadata assists in resource discovery by "allowing resources to be found by relevant criteria, identifying resources, bringing similar resources together, distinguishing dissimilar resources, and giving location information.
Milestones	Major decision points that separate the phases of a project implementation.
Military Messaging Service	The Military Messaging Services provide a reliable, store and forward message transfer service for both users and applications in support of organizational messaging (messaging between organizations and organizational units). The service supports different qualities of service for different message priorities (e.g., expediting higher priority messages, timing out higher priority messages more quickly) to honour the precedence of the military messages. The Military Message Transfer Service supports a range of elements of service including access management, alternate recipients, conversion prohibition, deferred delivery, delivery notification, distribution list expansion, latest delivery, and message security labelling. [As defined by C3 Taxonomy]
Military Messaging Application	The Military Messaging Application provides users with the capability to create, receive, and manage military messages. The application allows the assignment of different qualities of service for different message priorities (e.g., expediting higher priority messages, timing out higher priority messages more quickly) to honour the precedence of the military messages. The Military Messaging Application allows the user to define a range of elements of service (EoS) including alternate recipients, conversion prohibition, deferred delivery, delivery notification, distribution list expansion, latest delivery, and message security labelling. [As defined by C3 Taxonomy]
Risk	A measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints. Risks have three components: a future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential

Term	Definition
	consequence from occurring; a probability (or likelihood) assessed at the present time of that future root cause occurring; and a consequence (or effect) of that future occurrence. Information system-related security risks are those that arise from the loss of confidentiality, integrity, or availability of information or information systems
Risk Analysis	The process of examining each identified program and process risk, isolating the cause, and determining the impact. Risk impact is defined in terms of its probability of occurrences, its consequences, and its relationship to other risk areas or processes. Consequences are typically identified and analysed in terms of performance, schedule, and cost.
System	Any organised assembly of resources and procedures united and regulated by interaction or interdependence to perform a set of specific functions.
Virtualised Technologies	Virtualisation describes a technology in which an application, guest operating system or data storage is abstracted away from the true underlying hardware or software. A key use of virtualization technology is server virtualization, which uses a software layer called a hypervisor to emulate the underlying hardware. Thus allowing for greater flexibility, control and isolation by removing the dependency on any specific hardware platform.

Annex F Maintenance and Support Concept (After FSA)

F.1. Introduction

The Maintenance Process shall ensure the maintainability of the configuration baselines. The Baseline Maintenance Process implements modifications to be made either proactively or reactively to the PBL to correct faults and/or deficiencies, to improve performance or other PBL attributes, or adapt the PBL/OBL to a modified environment. The maintenance concept is based on the incident management concept and each and any maintenance and support level could be managed by a different organization during the Life Cycle of the project. The responsibility of each level, in accordance to the life cycle of the project will be part of the Contract. The Baseline Maintenance process is decomposed into 1st, 2nd, 3rd and 4th Level Maintenance tasks.

The maintenance concept includes the following activities:

a. The Maintenance of all the CIs and all related items,

b. The execution of all the required preventive and corrective maintenance activities for all the system and its subsystems for each level,

c. The allocation of the Maintenance tasks to the respective maintenance levels and the related organisation.

F.2. Definition

Level of Support: Level of support indicates a specific extent of technical assistance in the total range of assistance that is provided by an information technology product to its customer. The Service management is divided in three different level of service, which interface each other, in order to activate the proper level of maintenance in accordance with the event (incident) happened on the system.

Level of Maintenance: are various echelons at which maintenance tasks are performed on systems and equipment. The levels are distinguished by the relative sophistication of skills, facilities and equipment available at them. Thus, although typically associated with specific organizations and/or geographic locations, in their purest form, the individual maintenance levels denote differences in inherent complexity of maintenance capability.

F.3. Support Concept

The Support concept is the set of activities and processes in charge of managing the various level of maintenance and to escalate the problem to the appropriate level in accordance with the defined responsibilities.

It uses a systematic approach, to minimize the logistic delay and assure the maximum level of Service and Operation availability.

It is based on the Incident management process defined in ISO/IEC 20000 and ITIL framework or equivalent.

The Service management is divided into three different levels of service that interface each other to activate the proper level of maintenance in accordance with a system event.

The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.

The process of Support/Maintenance and the escalation process between the various levels is shown in the following figure:

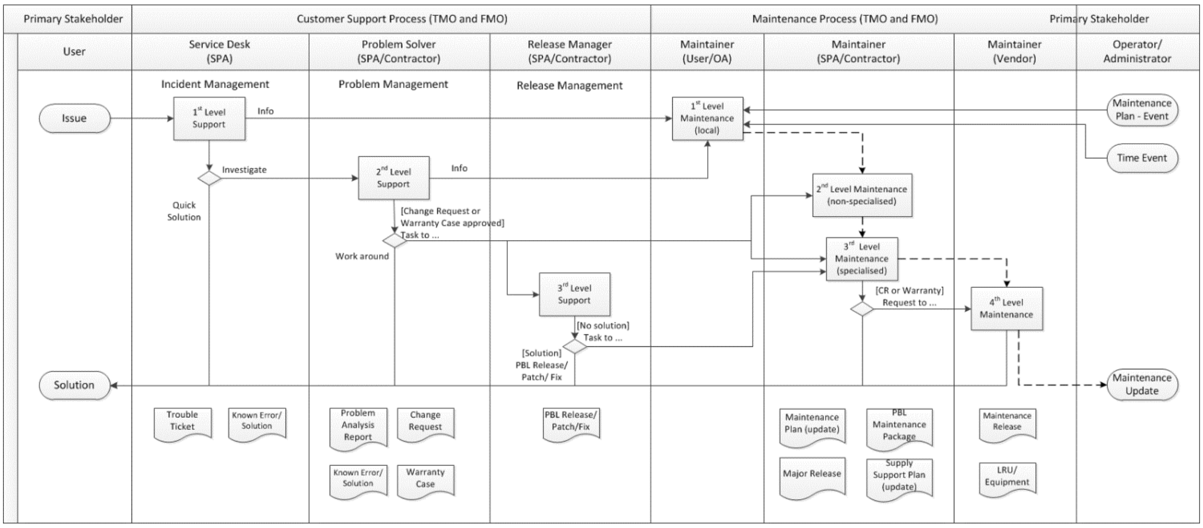

Figure 7: Support and Maintenance Concept Process

First Level Support Process

The 1st Level Support Process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket, TT), performs an initial assessment and distributes it to the predefined actors to solve it

Second Level Support Process

The 2nd Level Support Process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

The Problem Management process receives the TT from the Service Desk and performs the following tasks (not limited to):

a. (Re-)evaluation of TT category, criticality and priority,
b. Identification of the root cause of the issue (e.g., by issue replication testing),
c. Identification of workarounds,
d. Identification and initial planning of possible short, medium and long-term solutions (e.g., workarounds, patches, or new baseline or CI releases),
e. Create Problem Analysis Report and Change Request incl. schedule of implementation, and synchronization with the Baseline Maintenance process;
f. Presentation of the Problem Analysis Report and CR to the CCB for approval,
g. Monitor and Control the approved CR during implementation,
h. Trigger 3rd Level Support and/or 3rd Level Maintenance process to implement the CR, in case the incident cannot be solved at 2nd level;
i. Perform the post- CR implementation review.

Third Level Support Process

The 3rd Level Support Process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

The Deployment and Release Management process receives the approved Change Request from the 2nd Level Support and performs the following tasks (not limited to):

a. Release of the solution (release unit/record)

b. Development of the solution (e.g., new CI Fix, Repair, Replacement, Patch, or Release),

c. Testing of the solution (e.g., Regression testing, issue/deficiency replication testing),

d. Update of baseline content and status,

e. Delivery and deployment of the solution.

F.4. Maintenance Concept

The Maintenance Concept is the set of activities and processes in charge of restoring the system functionality in the shortest time possible.

The Maintenance shall be provided in a proactive and reactive manner by the Service Provider.

All proactive Maintenance tasks are defined in the Service/Capability and Site specific O&M Manuals (What) and corresponding Procedures (How) and scheduled in the Maintenance Plan.

Reactive Maintenance activities are triggered by Incident and Change Requests coming either from the Service Customer via the Customer Support Services or from the OEM/Vendor

First Level of Maintenance

It is responsible for the very basic maintenance activities. It is responsible to activate the second level of maintenance when it is needed.

It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding O&M Manual. All 1st Level Maintenance procedures do not require specialised tools and/or specialized personnel.

Second Level of Maintenance

It is responsible of isolation and resolution of system-level maintenance and management of deficiency reports and repair. It is responsible to activate the third level of maintenance when it is needed.

It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. All 2nd Level Maintenance procedures do not require specialised tools and/or specialized personnel.

Third Level of Maintenance