EUSPA/OP/12/23 ERAS Framework Contract – Statement of Work – after corrigendum n. 4

Reference:

EUSPA-GAL-SE-SOW-A24016

Issue/Version: 1.1

Date: 20/06/2024

Change Log:			
Issue/ Version	Changes & Pages Affected	Author	Date
1.0	Version for ITT publication	EUSPA	30-04-202430/04/2024
1.1	Updated as per Corrigendum 04	EUSPA	20-06-2024

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

1 Introduction

The purpose of this Framework Statement of Work (FWC SOW) is to define the common set of requirements applicable to all activities under the Framework Contract for the provision of the activities to be performed by the Contractor that are necessary to design, develop, deploy, maintain and evolve the Emergency Alerting System (ERAS) related to Galileo infrastructure throughout the duration of the Framework Contract.

The tasks defined herein will be selectively called up by dedicated Specific Contract Statements of Work that will have a unique time frame and context within the Framework Contract period.

This document is structured in the following subsections:

1. Introduction, including scope of work,

2. Statement of Work Documents,

3. Galileo Context,

4. ERAS Milestones and Schedule Logic,

5. Tasks of the Contractor,

6. Contractor Deliverables,

1.1 Overarching Objective

The overarching objective of the ERAS Contractor activities is to deliver new functionalities onto the European Union Galileo operational infrastructure for EUSPA to provide new services, namely the Emergency Warning Satellite, SAR/Remote Beacon Activation service and SAR/Two-Way Communications.

Furthermore, this overarching objective must be achieved in a safe, secure and reliable manner that preserves the current Galileo services (e.g. Open Service) and that protects the Galileo operational infrastructure.

1.2 Scope of Work

1.2.1 Overall Scope

The Contractor's responsibilities shall include, inter alia, the following main activities:

▪ The engineering design, development, deployment, verification, integration, qualification and acceptance review of the infrastructure fulfilling the technical specifications in the Contractual Index Status List [AD-1] and to be deployed at the SAR/Galileo Service Centre (SGSC) within the Return Link data Service Provider (RLSP) and operated by the SAR/Galileo Data Service Provider (SGDSP),

▪ The overall management including project control and product assurance activities,

▪ The overall security activities, including cyber security, supporting activities leading to accreditation of the infrastructure and any necessary security measures for protection of products, documentation, infrastructures and personnel,

- A maintenance period, for the Solution delivered in execution of the Contract,

- The production, update and delivery of documents, hardware, software, tools and all other items delivered under the Contract,

- The potential replications of the Solution in another Galileo operational centre (GSC) and a virtual environment,

- The management and technical interfacing with the Contracting Authority, including regular reporting, progress meetings, reviews, etc.

1.2.2 Additional Documentation

This SoW is complemented by the CISL [AD-1] which includes a number of programmatic, engineering, operational, security and quality requirements that shall be applicable to the Contractor for the purpose of the execution of the tasks described herein.

2   Statement of Work Documents

2.1 Applicable Documents

The Applicable documents listed below are to be considered as an integral part of the present document. They are labelled with a code "AD-n" within the present document, as depicted in the table below. The applicable version of the document is specified in the CISL.

Applicable Documents:		
Type	Title	Reference
AD-1	EUSPA/OP/12/23 Contractual Index Status List (CISL)	EUSPA-GAL-SE-CISL-A24679

Table 1 - Applicable Documents

For the list of Acronyms and Abbreviations, please refer to the FWC Annex I.F

2.2 Requirement Convention

Each requirement in the present document is numbered with a unique code. Each requirement is written using the following terminology:

"Shall"   Indicate a mandatory requirement

"Should"   Indicate a preferred alternative but is not mandatory

"May"   Indicate an option

"Will"   Indicate a statement of intention or fact

3 Galileo Context

3.1 The Galileo Programme

The Galileo programme is Europe's initiative for a state-of-the-art Global Satellite Navigation System (GNSS) completely independent of other existing or potential systems. Galileo is the largest industrial project ever organised on an EU scale, and the first public infrastructure owned by an EU institution.

The Galileo programme consists of a definition phase, a development, a validation phase and an exploitation phase. The deployment phase established all the space and ground-based infrastructures as well as related operations, preparing for the exploitation phase that formally began December 2016 with the provision of Galileo Initial Services.

Galileo provides a number of Services (par. 3.2) through a combination of capabilities of the Core Infrastructure (Galileo Control Segment (GCS), Galileo Mission Segment (GMS) and Space Segment (SSEG)) and a number of interfacing entities: Support Facilities, Service Facilities and External Entities (Figure 1).

3.2 Overview of the Galileo Services

The Galileo system provides high quality satellite services with associated performance guarantees. The main services provided (and planned to be) by Galileo are the following:

- **Open Service (OS):** implemented through two navigation signals separated in frequency. The Open Service provides position and timing performances, free of user charge. Performance will be competitive with, but complementary to, GPS to enable dual constellation usage;

- **Open Service Navigation Message Authentication (OSNMA):** the OSNMA SiS provides the authentication data for OS geolocation information contained within the navigation signals;

- **High Accuracy Service (HAS**): The Galileo High Accuracy Service (HAS), unless augmented by certified or otherwise legally approved dedicated systems designed to this effect, has been designed and can only be used for non-safety critical purposes, i.e. purposes that have no impact on the safety of human life and where an underperformance in availability, continuity, accuracy and/or integrity of the Galileo Signal-in-Space (SIS) could not cause any kind of direct or indirect personal damage, including bodily injuries or death.;

- **Public Regulated Services (PRS):** implemented through two navigation signals separated in frequency, with encrypted ranging codes and data. The Public Regulated Service is restricted to government authorised users, for sensitive applications which require a high level of service continuity, free of charge for the Member States, the Council, the Commission, EEAS and, where appropriate, duly authorised Union agencies. This service uses strong, encrypted signals;

- **Search And Rescue (SAR):** The SAR Services are Galileo's support to the international Search and Rescue satellite system Cospas-Sarsat (C/S). Galileo contributes by detecting (through the satellite constellation) and locating (through a dedicated ground segment) radio beacons activated by persons, aircraft or vessels in distress, and forwarding the alert information to relevant authorities (SAR responders) and also by relaying response messages to those beacons users equipped with Galileo receivers through the Return Link service.

- **Emergency Warning Service (EWS)**:
  The Galileo Emergency Warning Service (EWS) allows for on-demand broadcast of alert messages and associated guidance to affected population in minutes. The service – introduced by the EU Space Programme Regulation – will be free of charge with global coverage and provided in cooperation with Member States National Civil Protection Authorities. It complements existing warning systems and its implementation via Galileo satellites makes it resilient to ground destruction, independent of terrestrial mobile networks.

- **Remote Beacon Activation (RBA)**:
  The SAR/Galileo Remote Beacon Activation Service is an enrichment of the current Return Link Service allowing on-demand Authorised Users to send predefined commands to compatible SAR beacons to perform specific actions namely to start transmitting (i.e. activate). The Service will be free of charge with global coverage thanks to the Galileo Open Service (E1). Once activated, the beacon starts transmitting distress alert messages which are detected by Galileo SAR payloads and its estimated position is provided to the Authorised User allowing the tracking of the beacon.

- **Two-Way Communications (TWC)**:

  The SAR/Galileo Two-Way Communications Service (TWC) represents an enhancement of the Return Link Service, allowing for the exchange of information between Rescue Control Centres and individuals in distress. This capability aims to enhance the situational awareness of TWC beacon' owners in distress and is beneficial in effectively managing rescue operations. The operator of the Rescue Control Centres (Authorized Users) will have the capability to send questions to the activated beacon to gather information about the ongoing distress situation or to provide instructions to facilitate the rescue process.

3.3 Overview of the Galileo System

The Galileo System is composed of the Core Infrastructure, the Support Facilities and the Service Facilities.

- The Galileo **Ground Control Segment** (GCS) provides a large range of functions to support the management and control of the satellite constellation. The scope of this functionality includes control and monitoring of the satellites and payload, planning and automation functions that allow safe and correct operations to take place, and the support of payload related operations by means of TT&C links.

- The Galileo **Ground Mission Segment** (GMS) determines the navigation and timing data part of the navigation messages and transmits it to the satellite via its C-Band ground stations. The GMS architecture consists of facilities deployed in the 2 Galileo Control Centres (GCCs) plus ULS and GSS Stations deployed at remote sites located around the world. The Ground Mission Segment is the Galileo segment allowing the provision of the RLS Service.

- The **Galileo Space Segment** (SSEG) is part of the Core Infrastructure and once fully deployed, will consist of a 24/3/1 Walker constellation of 24 medium Earth orbit satellites that are fitted with SAR Repeater instruments allowing the reception of Cospas-Sarsat compliant 406MHz distress signals and retransmit them in the L-band at 1544.1MHz without on-board processing.

- The **Galileo Service Facilities** are elements located outside the perimeter of the Galileo Core Infrastructure that support the provision of Galileo services, among others the **SAR Galileo Service**

Centre **(SGSC)** and the **European GNSS Service Centre (E-GSC)** are key players for the provision of the Emergency Warning Service.
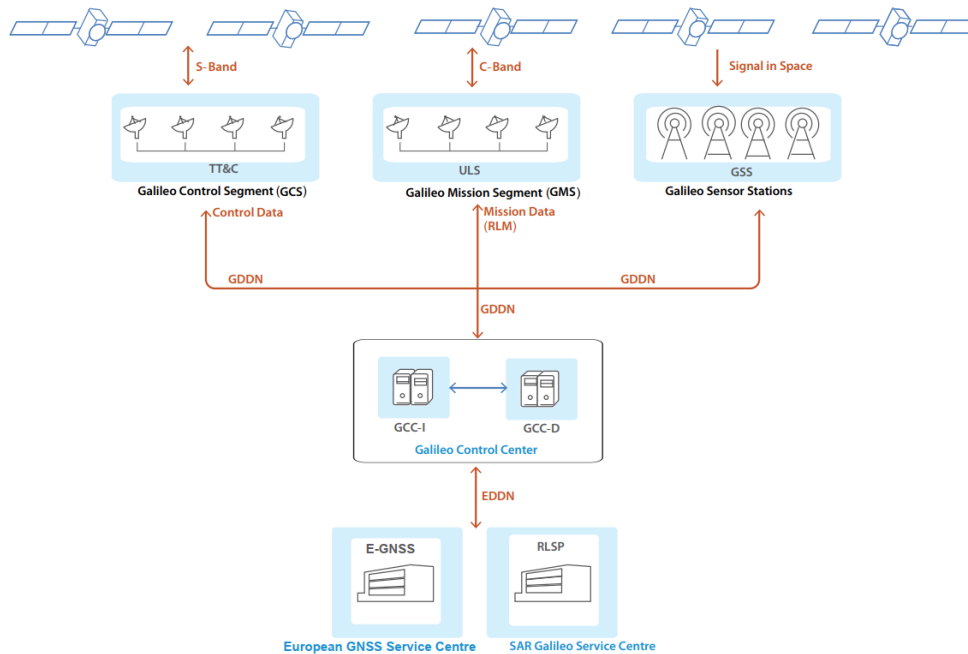
Figure 1 – Galileo Service Facilities and System Architecture Overview

3.4 The SAR/Galileo Service Centre

The SAR/Galileo Service Centre (SGSC) is the designated centre for the SAR/Galileo Service monitoring located in Toulouse, France within the CNES premises.

The SAR/Galileo Service Centre hosts a number of critical infrastructures for the provision of the SAR/Galileo Services, in particular the prime Return Link Service Provider and the hosting site for the SGDSP the RLSP and SAR/Galileo operator.

The RLSP is in Galileo infrastructure in charge of securely providing the ground segment interface between the external parties and the Galileo Core Infrastructure for the provision of data to be injected into the SAR bits of the Galileo Signal in Space.

3.4.1 The SAR/Galileo Data Service Provider

The SAR/Galileo Data Service Provider (SGDSP) is the Entity entrusted to perform the tasks required for an uninterrupted SAR/Galileo Service provision as defined in the Service Definition Document (SAR-SDD)[1] . SGDSP's activities are executed from the SAR/Galileo Service Centre and include suitable operations, maintenance, hosting and SAR/Galileo Service performance monitoring and reporting.

The following list SGDSP's key tasks:

---

[1] https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-SAR-SDD.pdf

1. Management and coordination of the SGS operations (including L1);

2. Management and coordination of SGS hosting and maintenance tasks (L3)

3. Provision of System maintenance (L2);

4. Continuous monitoring and reporting of the SAR/Galileo Service performance;

5. Overall reporting and notification of SAR/Galileo Service matters to the Agency (and C/S for operational matters);

6. Provide expertise to the Agency in engineering and technical matters related to Cospas-Sarsat and SAR/Galileo;

7. Support the Agency in SAR/Galileo Service evolutions.

4 ERAS Milestones and Schedule Logic

The following figure depicts at high-level the activities and milestones of the roll-out logic and key milestones towards the delivery of the Contractor's Solution, to be delivered as part of each specific contract. The Contractor is not responsible for all the phases included in this figure (see 4.1.2), e.g. the Service Provision phase.
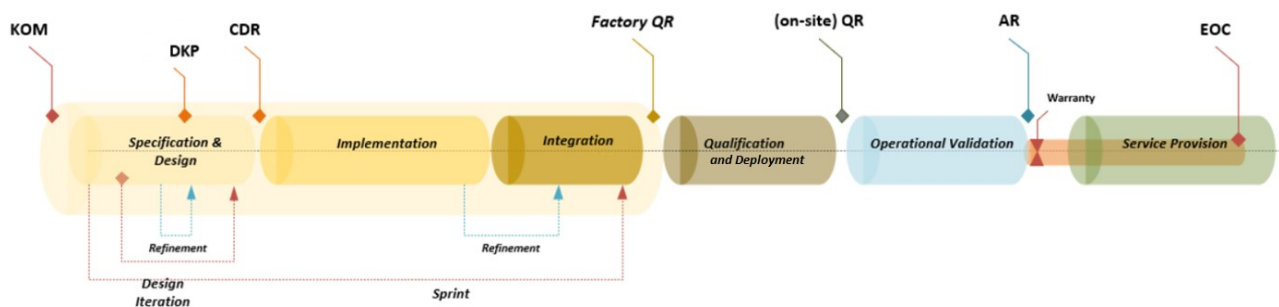
Figure 2 – High-level Roll-out Logic merging Agile development in relation with ECSS

4.1.1 FWC-SOW-01: Development Lifecycle Methodology

The Contractor shall apply a development methodology highly adaptable (i.e. Agile processes):

a) allowing a value-driven approach including provisions for an iterative and evolutionary implementation (see 5.4 for additional requirements), without prejudice to the Project reviews (provided in Figure 2)

b) enabling the Contracting Authority to follow the progress of the project with respect to cost, schedule and technical objectives.

4.1.2 FWC-SOW-02: Key Milestones

For the activities identified in the overall roll-out logic (Figure 2), the mandatory Key Milestones are:

1. **Kick Off (KOM):** Refer to section **4.1.3**

2. **Design Key Point (DKP):** Refer to section **4.1.4**

3. **Critical Design Review (CDR):** Refer to section **4.1.5**

4. **Qualification Review (QR)** To be performed both in Factory and on-site, refer to section **4.1.6** to **4.1.7** [2]

5. **Acceptance Review (AR):** Refer to section **4.1.8**

6. **Maintenance Period until End of Contract (EoC):** Refer to section **4.1.9**

Duly justified changes to the list above might be proposed by the Contractor (e.g. for efficiency purposes).

---

[2] NB: Between the on-site QR and the final Acceptance Review, the Solution Operator will perform an operational Qualification Campaign aiming at confirming the suitability of the Solution prior entering operations.

The Contractor shall perform the activities to achieve each of the Key Milestones. A milestone will be considered achieved at the date of the corresponding board (including close-out) that declares it successful as per [AD-1].

4.1.3 FWC-SOW-03: Kick-Off Meeting (KOM)

The prerequisites for the KOM shall be the following:

- Contract signature,
- Delivery of KOM Data pack under review (covering at least the items in DRL [**Table 6**]).

The Contactor shall organise a KOM which shall confirm and approve (by the CA) the following:

- the Contractor project team,
- the contract major milestones and objectives,
- the preliminary design and identification of dataflows,
- the confirmation of the compliance matrices to CISL as per the Contractor proposal,
- Approval of the deliverables as specified in the DRL (6.1).

The KOM shall be considered successful if the above elements are fulfilled.

Note: Following a successful KOM, the Contractor shall prepare a detailed approach to the system design, security and accreditation of the Solution (as detailed in section 5.4, section 5.10 and 5.11) to be reviewed and approved by the CA at the Design Key Point as defined .

4.1.4 FWC-SOW-04: Design Key Point (DKP)

The prerequisites for the DKP shall be the following:

- Successful achievement of previous milestone.
- Delivery of the Data pack under review (covering at least the items in DRL [**Table 6**]).

The Contactor shall organise a DKP which shall confirm and approve (by the CA) the following:

- the detailed system specifications proposed,
- the general security approach including the authentication for the Solution,
- the proposed accreditation needs,
- the management approach to any Crypto material provided to the Contractor for the implementation of the authentication function.

The DKP shall be considered successful if the above elements are fulfilled, including approval (by the Contracting Authority) of the deliverables pertaining to the milestone. The successful achievement shall grant authorisation to the Contractor for the next phase.

4.1.5   FWC-SOW-05: Critical Design Review (CDR)

Note: the Contractor shall run the engineering processes (detailed in section 5.4.1) to define the interface specifications, detailed design for hardware and software sub-systems and components, and detailed plans for the development and factory AIV processes. Such process shall be performed in an iterative manner implementing AGILE methodology.

The prerequisites for the CDR shall be the following:

- Successful achievement of previous milestone.

- Delivery of the Data pack under review (covering at least the items in DRL [**Table 6**]).

The Contactor shall organise a CDR which shall confirm and approve (by the CA) the following:

- the Solution design definition and justification files (including a trade-off between new development and adoption of COTS), the final internal ICDs, DDVP and factory AIV Plan, as well as those of sub-systems, including security related aspects.

- the verification files, including RVMs, plus all qualification evidence already collected towards technical requirements even if they could be verified at lower level (subsystem and/or equipment).

- the RAMS analysis is up-to-date and correctly reflected in the design documentation.

- any Solution critical issues have been correctly monitored and resolved (e.g. algorithms and performance, operational and safety aspects).

- Preliminary Solution operator's documentation files (e.g. Installation, Operations and Maintenance Manual (IOM)), including the approval of the inputs to the operations and maintenance (e.g. concept of operations, training plan…).

- the Iterative Development Plan (IDP) including but not limited to the number of planned iterations, assessment of the product features and testing. The IDP shall maximise the qualification in-factory.

- the qualification test plan and related test case and procedure documentation, including test cases for demonstration of the capability of the infrastructure to execute the procedures identified in the Solution operator's documentation files (IOM).

- completeness of the detailed definition, qualification process, manufacturing and verification documentation and planning.

- the approach to the obsolescence strategy and planning.

- the expected Solution performance by using adequate engineering methods and tools.

- the proposed inputs to the threat scenarios.

- the Solution security aspects (including cybersecurity) as per applicable security requirements in the [AD-1].

- the required PA/QA processes.

- Review and close out of all pending actions from previous reviews.

The CDR shall be considered successful if the above elements are fulfilled, including approval (by the Contracting Authority) of the deliverables pertaining to the milestone. The successful achievement shall grant the Contractor authorisation for the next phase.

Note: The approval of one of design iteration by the Contracting Authority does not discharge the Contractor from liability related to design flaws detected at later design iterations (e.g. artefact, missing information, side-effects).

4.1.6   FWC-SOW-06: In-factory Qualification Review (Factory QR)

Note:–The Contractor shall collect the testing results from every sprint iteration during the contract development phase and shall run a complete verification phase at the Contractor's premises. The testing to be performed shall implement the Qualification Test Plan, the Test Cases and Test Procedures previously approved by the Contracting Authority (at CDR).

The purpose of this milestone is to demonstrate the qualification status of the Solution and all its interfaces, including the external ones. The Factory QR, shall be conducted in accordance to the deployment approach described in section 5.12.

The prerequisites for the Factory QR shall be the following:

- Successful achievement of previous milestone.

- Delivery of the Data pack under review (covering at least the items in DRL [**Table 6**]) ;

The Contactor shall organise a Factory QR which shall confirm and approve (by the CA) the following:

- the configuration baseline, including lower-level components.

- the qualification of the final architecture based on the different iteration qualification reports, the complete design justification files and the finalised user's documentation.

- the results of the lower-level Qualification Reviews, if applicable.

- the level of compliance of the deployed infrastructure to applicable requirements and interface requirements, including performance.

- Final version of the Solution operator's documentation files (e.g. Installation, Operations and Maintenance Manual (IOM)), allowing the operator readiness the perform the Operational Validation phase after the on-site QR (4.1.7).

The Factory QR shall be considered successful if the above elements are fulfilled, including approval (by the Contracting Authority) of the deliverables pertaining to the milestone. The successful achievement shall grant the Contractor authorisation to procced with the system deployment and integration on-site activities (see 5.12).

4.1.7   FWC-SOW-07: On-site Qualification Review (QR)

The on-site Qualification Review (QR) main purpose is to confirm that the technical specifications and the requirements baseline functions (and its performance) are met by the Solution on the final deployed configuration. The Contractor shall implement the Qualification Test Plan, the Test Cases and Test Procedures previously approved by the Contracting Authority (at previous milestones).

The purpose of this milestone is to confirm the qualification status of the Solution and all its interfaces, including the external ones on the final deployed configuration. The Factory QR, shall be conducted in accordance to the deployment approach described in section 5.12.

The prerequisites for the on-site QR shall be the following:

- Successful achievement of previous milestone.
- Delivery of the Data pack under review (covering at least the items in DRL [**Table 6**]).

The Contactor shall organise an on-site QR which shall confirm and approve (by the CA) the following:

- the configuration baseline, including lower-level components.
- the correct integration of the deployed Solution (including any sub-systems) as part of the rest of the Galileo infrastructure (i.e. RLSP).
- the absence of non-regression in the compliance of the deployed infrastructure to the applicable requirements (e.g. technical, interface, security).
- the qualification status of all interfaces including external ones.
- the successful completion of the test plan (including functional and performance) with corresponding evidence.
- the capability to execute the procedures identified in the Solution operator's Manual/User's Documentation files.
- any remaining deployment activities leading to the Acceptance Review.

The on-site QR shall be considered successful if the above elements are fulfilled, including approval (by the Contracting Authority) of the deliverables pertaining to the milestone. The successful achievement shall grant the Contractor authorisation to procced with the system deployment and integration on-site activities (see 5.12).

Note: After successful on-site qualification, the Contractor shall provide right of use to the Solution to the Operator to run the Operational Validation activities as described in section 5.12.

4.1.8   FWC-SOW-08: Acceptance Review (AR)

Note: The Contractor shall keep custody of the Solution until successful AR.

The acceptance review shall be achieved at the latest 12 months after the entry into force of the contract.

The prerequisites for the Acceptance Review milestone are:

- Successful achievement of previous milestone.
- Achievement of the Operational Validation (under CA responsibility).
- Delivery of the Data pack under review (covering at least the items in DRL [**Table 6**]).
- Completion of the Agency vulnerability assessment.

The Contactor shall organise an Acceptance Review which shall confirm and approve (by the CA) the following:

- the correct implementation of all major anomalies and the agreed way forward for any outstanding issue (including action plans).

The AR shall be considered successful if the above elements are fulfilled, including approval (by the Contracting Authority) of the deliverables pertaining to the milestone. The successful achievement shall mark the start of the maintenance phase (see 5.12).

Following the successful AR, the Contractor shall provide an "End Item Data pack" with all the products developed.

"End Item Data pack" **[DRL: PRG-01]**

4.1.9 FWC-SOW-09: End of Contract

Note: The EoC is not a milestone but a represent the period between the AR and the end of the baseline and optional maintenance phase.

The prerequisites for the End of Contract are:

- Successful Acceptance Review,
- Delivery of the End Item Data pack.
- No outstanding actions from the maintenance tasks (described in 5.13)

The EoC shall be considered successful if the above elements are fulfilled.

5 Tasks of the Contractor

5.1 General Requirements

The design, development, deployment, verification, integration and qualification of the Solution shall be implemented under the responsibility of the Contractor. The Contractor shall support the Contracting Authority level activities as defined in the present SOW and further as needed in order to provide all the products and services described herein.

5.1.1 FWC-SOW-010: Deliverable Document List

The Contractor shall produce and maintain up-to-date the Deliverable Document List (DDL), based on DRL.

5.1.2 FWC-SOW-011: Applicability and Conflicting Requirements

Unless otherwise stated, Applicable Documents are applicable in their entirety. Any inconsistency identified by the Contractor, shall be brought immediately to the attention of the Contracting Authority for resolution.

5.1.3 FWC-SOW-012: Nested Applicable Documents

Applicable documents may call up further documents, or parts thereof, which are applicable to the extent defined within the reference documents. If the Contractor identifies any such nested applicable document as being required to implement any contractual tasks (in particular, but not limited to, technical requirements), it shall request it to the Contracting Authority (who will assess whether it needs to be provided to the Contractor or not).

5.1.4 FWC-SOW-013: Completeness of the Work

Lack of mention of activities within this SOW shall not relieve the Contractor from its responsibility to identify and perform all tasks necessary to meet the overarching objective (deliver a product including hardware, software, documentation, data and services) and fulfil its contractual obligations.

5.1.5 FWC-SOW-014: Protection of the Galileo Services

The Contractor shall ensure that all activities and tasks under their responsibility do not hinder the continuity of the Galileo Service provision.

5.1.6 FWC-SOW-015: Evidence of Compliance

The Contractor shall make sure that evidence can be provided, upon request from the Contracting Authority, that all the requirements for which compliance has been stated are effectively fulfilled, if not already part of the delivered Project documentation. Any non-compliances shall be handled in accordance with Galileo PA, QA and RAMS Generic Requirements in [AD-1].

5.2 Organisational Requirements

5.2.1 FWC-SOW-016: Management and Organisation Structure

The Contractor shall provide an adequate organisational structure that is commensurate with the safe, coordinated and efficient execution of all the activities described in this Statement of Work, and ensuring efficient management of interfaces:

- With the Contracting Authority, in particular for what concerns reporting lines, frequency of reporting and timely provision of feedback and relevant;
- Within the Contractor management organisation;
- Between the Contractor and all their subcontractors.

5.2.2 FWC-SOW-017: Ad Hoc Meetings

In addition to the regular meetings specified in the Annexes to this Framework Statement of Work, the Contractor shall organise ad hoc meetings at the request of the Contracting Authority to address any issues that may arise. The Contractor shall ensure the appropriate Contractor participation to such meetings to enable the efficient and timely resolution of issues.

5.2.3 FWC-SOW-018: Standardisation of Reporting Periods

The Contractor shall ensure that, unless agreed otherwise by the Contracting Authority, the reporting periods for all regular reports (i.e. daily, weekly, fortnightly, monthly, quarterly, biannual and annual) defined in the Annexes of this Statement of Work are standardised so that:

- The reporting periods are coincident for all reports with the same reporting period duration;
    - Higher frequency reporting is synchronised with lower frequency reporting (e.g. weekly reports span the same reporting period as 7 consecutive daily reports, quarterly reports span the same reporting period as 3 consecutive monthly reports, etc).

5.2.4 FWC-SOW-019: Latency of Reporting

The Contractor shall deliver (if required) all regular reports (i.e. daily, weekly, fortnightly, monthly, quarterly, biannual and annual) as specified below, except if otherwise specified.

Report Type	Maximum delay in delivery of the report to the Contracting Authority (measured with respect to the end of reporting period)
Daily	12 hours
Weekly	48 hours
Fortnightly	3 calendar days
Monthly	5 calendar days
Quarterly	12 calendar days
Bi-annual	20 calendar days
Annual	30 calendar days

Table 2 - Maximum Latency of Regular Reports

5.2.5 FWC-SOW-020: Synchronisation of Reporting with Meetings and Reviews

The Contractor shall ensure that all regular meetings and/or reviews defined in the Annexes of this Statement of Work, and which have regular report inputs, are scheduled so that the Contracting Authority has a minimum of 10 working days to review the related reports.

5.2.6 FWC-SOW-021: Contractor's Performance Assessment

The Contracting Authority will assess the Contractor's performance through the key milestones defined in 4.1.2 and its associated reviews.

5.3 Project, Reporting, Risks, Schedule, Cost and Quality Management

The requirements in this section define how the Contractor is expected to manage and report on the status and progress of the different tasks. These requirements are supplementary to normal project management activities that the Contractor shall perform during the execution of the contract.

5.3.1 FWC-SOW-022: Interfaces to the Contracting Authority

The Contractor shall define the managerial and technical interfaces to the Contracting Authority for each of the main activities, under the overall responsibility of the Contractor.

The Project Manager should be the single point of contact that has full responsibility. A list of Point of Contacts (PoCs) for key roles must be identified in the Project Management Plan. These contact points above shall be entrusted with technical and managerial authority within their domain of responsibility.

5.3.2 FWC-SOW-023: Project Management Plan

The Contractor shall establish, deliver, implement and continuously maintain throughout the contract, a Project Management Plan (PMP), subject to the approval by the Contracting Authority.

"Project Management Plan" **[DRL: PRG-02]**

5.3.3   FWC-SOW-024: PA/QA and RAMS Activities

The Contractor shall comply with the requirements laid down in the *Galileo PA, QA and RAMS Generic Requirements* in [AD-1] and produce the deliverables required in **Table 6**.

Note: the document [AD-19] *GAL-MGT-ESA-SYST-X/0001 Galileo FOC Management Requirements* referred therein shall not be considered applicable.

"PA/QA Documents" **[DRL: PRG-11 - 21]**

5.3.4   FWC-SOW-025: General Schedule Management

The Contractor shall ensure an overall schedule management with the following objective:

- ▪   The timely delivery of all commitments;

- ▪   A common schedule basis for all work across the project and its participants;

- ▪   The rapid evaluation of progress, assessment of deviations, and the prediction of potential deviations;

- ▪   The rapid development and evaluation of corrective actions to avoid schedule overruns;

- ▪   The identification and management of work critical to the completion of the project and risks to the schedule;

- ▪   Visibility of the up-to-date project status at any time;

- ▪   Consistency of external entity deployment and evolution schedules with the Contractors operations plans.

5.3.5   FWC-SOW-026: Schedule Process

The Contractor shall implement schedule management processes, develop schedules and perform their activities accordingly. The process will be documented in a deliverable.

"Schedule Management Plan" **[DRL: PRG-03]**

5.3.6   FWC-SOW-027: Coherent Schedule

The Contractor shall ensure that a coherent set of scheduling techniques is used by its lower tier Contractors.

5.3.7   FWC-SOW-028: Schedule Outputs

The Contractor shall maintain both a "Project Baseline Schedule" (that is part of the contract) and a "Project Working Schedule" (that reflects the current situation). It shall also include a milestone trend-charts in order to track the achievement of milestones. Both Schedules shall be provided in a format compatible with *Microsoft Project* files, used by the CA.

"Project Baseline Schedule" **[DRL: PRG-04]**

"Project Working Schedule" **[DRL: PRG-05]**

5.3.8   FWC-SOW-029: Schedule Changes Assessment

The Contractor shall continually assess the impact of any changes in the Project Baseline Schedule and the Project Working Schedule. Any delays that subsequently impact Contract milestones shall be reported to the Contracting Authority either by registered letter or e-mail, with the inclusion of the new schedule.

5.3.9   FWC-SOW-030: Schedule Report

The Contractor shall provide a High Level Schedule, as part of their Monthly Reporting, to immediately indicate the status of the main Contract milestones. It shall be an extract of the more detailed Working Schedule and shall make use of a colour code, summarising the status of the different milestones. An example is shown in Figure 1 - Example of High Level Schedule. The high level schedule shall present the list of the main milestones with the contractual date, the expected date, and in case of drift, a short explanation of the drift. An example is shown in Table 3 – Example of Milestones summary.

Figure 1 - Example of High Level Schedule

Milestone	Contractual date	Actual date	Reason for Drift
Milestone 1	15/06/2023	15/06/2023	NA
Milestone 2	30/08/2023	30/09/2023	Difficulties with….
Milestone 3	01/12/2023	01/03/2024	Delay due to …..

Table 3 – Example of Milestones summary

5.3.10 FWC-SOW-031: Risk Management

The Contractor shall manage the risks related to the contractual activities and shall ensure that appropriate mitigation actions are implemented and prompt reporting to the CA.

5.3.11 FWC-SOW-032: Risk Management Plan

The Contractor shall maintain a Risk Management Plan (RMP) as part of the Project Management Plan, which shall be subject to approval by the Contracting Authority and shall include a full description of all risk management processes, including the processes for the initial population and subsequent updates of the Risk Register.

Outputs:

"Risk Management Plan (RMP)" **[DRL: PRG-06]**

"Risk Register" **[DRL: PRG-07]**

5.3.12 FWC-SOW-033: Risk Evaluation

The Contractor shall continuously evaluate the risks during the execution of the contract and ensure the timely implementation of all risk mitigation actions. It is highlighted that risks affecting service delivery and the primary assets require diligence from the Contractor.

5.3.13 FWC-SOW-034: Risk Register Update

The Contractor shall maintain a "Risk Register" covering a detailed and up-to-date description of the technical, schedule and financial risks for all activities described (including the sub-contracted activities). Risks shall be presented in accordance with the template form, inter alia the risk score. Each risk definition in the Risk Register shall contain as a minimum:

- A risk identifier;

- A description of the risk;

- An evaluation of their potential impact on the Service provision;

- A risk mitigation plan with the implementation schedule for risk mitigation actions;

- A risk identification matrix (including occurrence probability and impact severity on a scale of 5 for each risk);

- A list of Work Package(s) affected.

"Risk Register" **[DRL: PRG-07]**

5.3.14 FWC-SOW-035: Risk Reporting

The Contractor shall report the "Risk Register" as an input to the quarterly progress meetings, together with the status of all risk mitigation actions.

5.3.15 FWC-SOW-036: Cost Modelling

The Contractor shall use a cost modelling, analysis and reporting system to maintain the baseline and current cost data, with:

- A consistent approach;

- Proven methods and sound techniques;

- ▪ Appropriate source data;
- ▪ Established procedures and accountancy principles.

5.3.16 FWC-SOW-037: Cost Reporting

The Contractor shall provide every quarter an up-to-date "Cost to Completion Note" defining the state of the financial budget and the projection up to end of the contract.

"Cost to Completion Update" **[DRL: PRG-08]**

5.3.17 FWC-SOW-038: Certificate of Milestone Completion

The Contractor shall deliver a payment milestone achievement certificate for Contracting Authority approval, where the contents are derived from the approved Payment Milestone definitions.

"Acceptance Sheet" **[DRL: PRG-09]**

5.3.18 FWC-SOW-039: Reviews Organisation Note

If so requested by the Contracting Authority, the Contractor shall issue a specific "Review Organisation Note" based on the CA template, before each review describing, at least, the review objectives, participant roles and responsibilities, review process, schedule, success criteria, follow-up process, and the required documentation inputs to the review (including the mapping of all such documentation to the review objectives).

5.3.19 FWC-SOW-040: Meetings and Reviews Inputs

The Contractor shall make available to the Contracting Authority all documents to be reviewed no later than 15 working days in advance of the Review and no later than 5 days before the meetings (if needed) to allow the Contracting Authority sufficient time to review the delivered documents and to provide comments. As part of the Agile development process, the Contractor can propose different timelines for the technical documentation.

5.3.20 FWC-SOW-041: Meetings and Reviews Outputs

The Contractor shall deliver to the Contracting Authority the draft minutes of meeting, for review and approval by the Contracting Authority, no later than 2 working days after the meeting and including notification if any adverse results are identified.

5.3.21 FWC-SOW-042: Action List

The Contractor shall place actions taken by all parties into an Action Items Status List. This AISL shall be provided as an attachment to all minutes of meetings and shall be kept available and updated at each progress report.

"Action Item Status List" **[DRL: PRG-10]**

5.3.22 FWC-SOW-043: Face-to-Face Meetings

The Contractor shall participate in ad-hoc meetings, on request of the Contracting Authority, necessary to address any critical issues, to be held in any EC, ESA or Contracting Authority facility in Europe.

5.3.23 FWC-SOW-044: Subcontractors Reviews

The Contractor may invite the CA to Subcontractor reviews and specify every time for which reason.

5.4 Engineering Tasks

5.4.1 Requirements and Interfaces Consolidation

FWC-SOW-045: Requirements Management

The following activities shall be performed throughout the project:

- Generation and Maintenance of a Statement of Compliance to each of the Requirements Documents as defined in the CISL.
- Assurance of the correct flow down of the applicable infrastructure requirements down to sub-system and lower level.
- Traceability and coherence between the infrastructure requirements baseline and lower-level requirements (including Classified ones) as well as the design and their verification.

FWC-SOW-046: Requirements Consolidation Activities

The Contractor shall implement a requirement gathering process aiming to consolidate all the requirements from the different applicable and high-level CISL documents. Such process shall be done for all System and sub-system level requirements, ensuring consistent interpretation and traceability through to the lower-level design and verification documentation.

FWC-SOW-047: Interface Management Consolidation

The Contractor shall perform an interface consolidation process aiming at consolidating and/or defining all interfaces of the proposed implementation from the highest level down to sub-system level.

The exercise shall encompass the definition, contribution and control of the following interfaces:

- Connection with the RLSP and the rest of the premises
- Internal Interfaces
- Interfaces with the Security Functions
- Interfaces with the Authorised Users

FWC-SOW-048: Interface Workshops

The Contractor shall organise a technical workshop, with the Contracting Authority and SGDSP, as to exchange, discuss and design the interconnection needs (dataflows) between the proposed Solution and the RLSP.

Note: The main objective is to ensure the operability of the infrastructure within the current operations environment and considered as part of the "internal ICD".

"*Internal ICD*": **[DRL: ENG-06]**

FWC-SOW-049: Interface Maintenance Process

For the maintenance of the different interfaces, the Contractor shall perform the required updates following the Contracting Authority Change Management Process defined in SOPI-CCM [AD-1].

FWC-SOW-050: Management of Internal Interfaces

The Contractor shall identify, implement and control all the internal interfaces within the different sub-systems.

FWC-SOW-051: Use of DOORS

The requirement engineering, compliance (including RFDs and RFWs), flow-down to lower level, and verification (verification matrices, test cases, test procedures, test results and other qualification evidence) shall be performed using the DOORS requirements management tool.

FWC-SOW-052: DOORS Module Delivery to the Contracting Authority

The Contractor shall deliver all DOORS Modules / Databases to the Contracting Authority on a timely and regular basis. The Contractor shall propose a delivery mechanism and frequency of delivery that provides the Contracting Authority with up-to-date visibility of the AIV progress.

"DOORS Module" **[DRL: ENG-04]**

FWC-SOW-053: Software Development Standards

The Contractor shall develop software in accordance with space standards. Although the overarching standard is the European Cooperation for Space Standardisation (ECSS) in particular ECSS-E-ST-40C (Software) and ECSS-Q-ST-80C (Software Product Assurance), the Galileo Programme has developed its own software standard for space and ground systems development, i.e. the Galileo Software Standard for Ground (GSWS-G)[AD-1], which details about system and software engineering, software product assurance and software configuration management.

In this contract, ECSS and the GSWS-G are to be considered as benchmark. Thus the Contractor shall deliver a tailoring of the GSWS-G, with the objective to gain efficiency and flexibility in the development cycle.

That tailoring will be documented via a Statement of Compliance (SoC), where statements of non-applicability, non-compliance or partial compliance will be justified. Conversely, full compliance to the GSWS-G is not considered fit for purpose in that contract.

"SoC to GSWS-G" **[DRL: ENG-03]**

FWC-SOW-054: Agile Development Definition

The Contractor shall define and apply an agile software development lifecycle compatible with the tailored SoC to GSWS-G.

Note: The Agile Software Development Handbook [see AD-1] may be used as a reference guideline for definition of the agile software development lifecycle.

5.4.2 Design, Development and Verification Plan (DDVP)

FWC-SOW-055: Provision of a DDVP

The Contractor shall generate a Design, Development and Verification Plan (DDVP) for the Solution proposed in line with the CA process defined in SOPI EVO-DDV [AD-1]. That process is valid considering RLSP as service facility and the process map as per Figure 3 in SOPI EVO-DDV, without prejudice of not being listed in the scope of the document; EUSPA is the Design Authority of the RLSP. The DDVP shall be updated for every review, and whenever a significant change in planning occurs.

"DDVP" **[DRL: ENG-08]**

FWC-SOW-056: Scope of the DDVP

The DDVP shall contain a detailed flow of the Solution, its deployment and any necessary operations migration. The Contractor shall show an efficient logic including schedule and critical path, highlighting the objectives for each step, defining the role and responsibilities between all actors. The plan shall also contain references to the Contractor's approach to the release management planning and the foreseen iterations and retrospectives.

FWC-SOW-057: DDVP Structure

The Contractor shall maintain the DDVP according to the structure defined in the content guideline (see section 6.2). A related logic of milestones and reviews shall be developed in accordance with the applicable documentation and with the view of minimising schedule impacts and overhead in documentation. The organisation of the work shall consider the agile methodology and maturity and qualification status of the System and sub-systems to be deployed.

5.5 Design Activities

FWC-SOW-058: Consistency of the Design

As part of any requested evolution or change activities the Contractor shall ensure that the design remains consistent and cohesive across all sub-systems.

"Design Definition File" **[DRL: ENG-09]**

FWC-SOW-059: Design Justification

The Design Justification File shall contain information proving that the design meets all the applicable requirements and demonstrating how the requirements are fulfilled by the sub-systems.

"Design Justification File" **[DRL: ENG-10]**

FWC-SOW-060: Design Justification by Analysis and Simulation

The Contractor shall justify the design with analysis and simulations when needed. Analysis and Simulations tools procurement are under Contractor's responsibility.

FWC-SOW-061: Design Files

The Design Files shall reflect the actual status of the design and shall be maintained up-to-date, being updated at least for major design changes and according to recommendations from the any System or sub-system level reviews.

"Design Definition File" **[DRL: ENG-09]**

FWC-SOW-062: Incorporation of PA & RAMS Results into the Design

The Contractor shall incorporate the results of PA & RAMS activities into the design.

The Contractor shall pay particular attention to the impact of safety, failure tolerance and continuous service provision requirements from the CISL [AD-1].

FWC-SOW-063: Single Point Failure Avoidance

The Contractor shall avoid Single Points of Failures through the design of the solution. Whenever diversification and/or redundancies are needed, it shall be described in detail, duly justified and supported by all the necessary analyses. If the Single Points of Failures cannot be eliminated or the risk is justified and accepted it shall be duly recorded into the design documentation.

FWC-SOW-064: Single Point Failure/Critical Item List

For those Single point failures which cannot be eliminated from the design (or fault tolerance requirements which cannot be met) shall be summarised in a Single Point Failure/Critical Item List.

"SPF CIL" **[DRL: ENG-20]**

FWC-SOW-065: Operation & Maintenance Constraints ~~Design~~

The Contractor shall ensure the proper incorporation of Operation and Maintenance constraints in the design documentation.

FWC-SOW-066: Traceability of Design and Justification Results

Each analysis shall list the source documents, including their issue status, used in its preparation. The list shall include in particular the design definition documents (drawings, list, etc..) so that the relevance of the analysis to the actual hardware/software design and build status can be correlated and traced.

5.6 Development and Integration Activities

FWC-SOW-067: SW Testing Strategy

The contractor shall propose a detailed strategy for software validation and verification activities, in particular depicting the tools to be used, resources and methodologies (e.g. automation).

"DDVP" **[DRL: ENG-08]**

FWC-SOW-068: Concept of Operations Workshops

The Contractor shall organise an operations concept workshop, with the Contracting Authority and the operator, as to exchange and discuss how the design Solution fits the concept of operations (such workshop shall occur between CDR and QR milestones).

Note: The main objective is to ensure the right operability of the infrastructure within the SGDSP operations

FWC-SOW-069: Incorporation of Operational Inputs

The Contractor shall ensure incorporation of operational related inputs provided by the Contracting Authority in the design.

FWC-SOW-070: Incorporation of Design Evolutions

The Contractor shall allow Design inputs to be incorporated into the iterative design process. Such inputs would be mainly from the Contracting Authority Service Reviews for which the Contractor would be duly notified at KO.

The Contractor shall participate on technical workshops, with the Contracting Authority and other relevant stakeholders (ESA, EC), to exchange and discuss relevant information on the main areas of Design updates expected:

- Updates to the input format (CAP file) or Output format (EWM); [AD-1]
- Updates coming from the Programme as part of the iterative development process.
- Updates coming from the Design Key Point
- Operational inputs from the future EWS Operator (SGDSP).

FWC-SOW-071: Hardware Minimisation

The architecture proposed by the Contractor shall strive to minimise the hardware volume, heat generation and energy consumption of the operational asset with respect to the constraints of a Ground Segment Standard Rack described in [AD-1].

5.7 Performance

FWC-SOW-072: Performance Engineering

The Contractor shall perform all the necessary analyses to demonstrate the conformance of the proposed design to the performance requirements contained within the applicable documents of this contract (included in [AD-1]).

FWC-SOW-073: Performance Budget File

The Contractor shall provide and maintain a Performance Budget File (PBF) gathering all the inputs and essential information related to the performance of the Solution to present to the Contracting Authority a clear quantitative picture of the contractor commitment on performance requirements with associated justifications.

The PBF shall clearly indicate the origin of all its data (simulations, measurements, assumptions, experimentation, etc.) and shall clearly show the margins considered. During the agile development cycle, the margins shall be managed in a consistent and visible manner.

"Performance Budget File" **[DRL: ENG-19]**

5.8 Hardware and Software Management

FWC-SOW-074: Compliance to Site Regulations

The Contractor shall comply with the designated site's regulations (e.g. health and safety).

FWC-SOW-075: Hardware and Software COTS Harmonisation

The Contractor shall maximise the harmonisation of hardware and software COTS products used throughout the proposed architecture.

5.9 Export Control

FWC-SOW-076: ITAR-Free

The deliverables under the contract shall be free from the International Traffic Arms Regulation (ITAR).

FWC-SOW-077: Compliance to Export Control Laws

Together with their tender, tenderers are required to provide a statement towards the relevant national export control laws and regulations along with a description of the export control procedures and structures when relevant.

Tenderers shall provide the same above-mentioned evidence for each of their sub-contractors (if applicable) having to deal with information, data and technology/ies subject of export control.

5.10 Security Activities

5.10.1 Security Management

FWC-SOW-078: Security Aspects Letter

The Contractor must comply with the security requirements detailed in the Security Aspects Letter (SAL), annex I.O of the Tender Specifications, and its applicable documents referred therein which are part of the CISL [AD-1].

FWC-SOW-079: Non-degradation of Security

The Contractor shall ensure no impact to security controls, operations, and accreditation before, during or after deploying, integrating, verifying, and qualifying any evolved, upgraded, or new infrastructures at the site.

FWC-SOW-080: Security Management Plan

The Contractor shall produce, deliver, and maintain a dedicated Security Management Plan (SMP), as per the DRL, based on ISO 27001, that specifies how the Contractor (and their sub-contractors) defines and/or implements:

- Security Policy and strategy;
- the security measures in term of organisation, procedures, roles, responsibilities (RACI matrix) and tasks;
- the European GNSS Program Security Instruction (PSI) (see SAL as per CISL [AD-1]);
- the Security Classification Guide (SCG) and COMSEC Security Instructions (see SAL as per CISL [AD-1]).

"Security Management Plan: SecMP" **[DRL: SEC-01]**

FWC-SOW-081: Cryptographic Management Plan

The Contractor shall ensure that symmetric and asymmetric key management systems, including but not limited to Public Key Infrastructure (PKI), are managed in accordance with a Cryptographic Management Plan. That plan will include relevant security controls, operations and deployment at the site during the full lifecycle of the COMSEC material (generation, distribution, renewal/revocation, destruction, decommissioning, etc…).

 "*Cryptographic Management Plan: CMP*" **[DRL: SEC-02]**

FWC-SOW-082: Implementation of Information Security Policy

An information security policy for any security related function shall be defined and implemented during the full life-cycle of the asset, addressing:

a) Planning of security activities for the deployment and management of equipment;

b) Handling procedures and operations for staff to perform operation of the equipment;

c) Validation and verification testing routines to ensure equipment is secure;

d) Maintenance and corrective actions that are required to ensure equipment is performing and lifetime requirements are met.

In addition, these items shall be used to provide input to the Business Continuity Plan (BCP), as per the DRL.

5.10.2 Security Engineering

FWC-SOW-083: Inputs to Business Continuity Plan

The Contractor shall provide inputs to the future Operator in the objective of maintaining the overall system Business Continuity Plan (BCP) where the Solution will be deployed, providing details on how the system would operate in the event of a disaster, ensuring appropriate system continuity and restoration. The BCP shall address appropriate contingency procedures (e.g. cybersecurity vulnerability, etc.), as well as including emergency destruction of EUCI equipment and material.

"*Input to Business Continuity Plan: BCP*" **[DRL: SEC-03]**

FWC-SOW-084: Inputs to Disaster Recovery Plan

The Contractor shall provide inputs to the future Operator in the objective of resuming the system back to operational state after disaster. The inputs to the DRP shall include the recovery time objective (RTO), which is the amount of time critical applications can be down, and the recovery point objective (RPO), for the files that must be recovered from data backup storage for normal operations to resume.

"*Input to Disaster Recovery Plan: DRP*" **[DRL: SEC-04]**

FWC-SOW-085: Compliance to the Security Baseline

The Contractor shall comply with the security baseline (including cyber security and accreditation requirements) and to the applicable security documentation, which are listed in the CISL [AD-1], and shall provide statements of compliance (as design and as built) at relevant milestones (CDR and QR). The Contractor shall demonstrate the 'As-Built' compliance status by providing a detailed VCM and VCD at the QR milestone and during the validation campaign.

"SoC to Security Documents" **[DRL: SEC-05]**

"VCM to Security Documents" **[DRL: SEC-06]**

"VCD to Security Documents" **[DRL: SEC-07]**

FWC-SOW-086: Identification and Security Classification of Assets

Any asset handling EUCI shall be identified and shall undergo a formal asset classification on the basis of the Security Classification Guide (SCG) (see CISL [AD-1]).

FWC-SOW-087: Interface Controls and Connections

The Contractor shall ensure interfaces are managed and controlled such that only authorised operators and systems can connect over secure networks, in accordance with interface control specifications, policies, and protocols.

FWC-SOW-088: Input to Local SECOPS

The Contractor shall provide a consolidated set of inputs allowing the Operator to fully develop the needed "Local Security Operational Procedures" according to the infrastructure functionalities developed and in line with the overall security requirements.

"Inputs to Local SECOPS " **[DRL: SEC-08]**

FWC-SOW-089: Input to Site Security Document

The Contractor shall provide a consolidated set of inputs allowing the Operator to fully evolve the "Site Security Document" according to the infrastructure functionalities developed and in line with the overall security requirements.

"Inputs to Site Security Description" [**DRL: SEC-09**]

FWC-SOW-090: Monitoring by GSMC (SECMON)

The ERAS functionalities shall be prepared to be monitored by the Galileo Security Monitoring Centre (GSMC) as specified in the *Monitored Entity Requirements* document in CISL [AD-1] through the collection and analysis of events, logs, and data.

"SoC to SECMON MER" [**DRL: SEC-14**]

5.10.3 Cybersecurity

FWC-SOW-091: Cybersecurity Technical Specifications

The Security Management Plan **[DRL: SEC-01]** shall describe how the applicable Cybersecurity Technical Specifications shall be implemented, identifying CSM (Cyber Security Manager) and CIA (Cyber Internal Auditor) for its organisation and for sub-Contractors.

The Security Management Plan for the infrastructure development and maintenance shall provide details at least on following aspects:

- Network map management;

- Vulnerability Management;

- Patch Management and installation;

- Obsolescence management;

- Infrastructure Acceptance Audit;

- Infrastructure Security Hardening;

- Infrastructure Security Lock Down;

- Support to cybersecurity incident response.

Output: *"Security Management Plan: SecMP"* **[DRL: SEC-01]**

FWC-SOW-092: Cybersecurity Compliance

For any non-compliance or partial compliance, a risk assessment shall be provided in the form of a Cyber Request for Waiver. Cyber Request for Waivers shall be provided as soon as possible.
Only waivers resulting from incremental deployment or exceptional circumstances (duly justified) can be submitted.

The Contractor shall implement the applicable Cyber Security requirements as per provided in CISL [AD-1].

"RFD/RFW Report" **[DRL: PRG-19]**

FWC-SOW-093: Content of Cybersecurity Request for Waiver

A cyber request for waiver shall include at least:

- The justification for the statement of partial or non-compliance;
- An assessment of the security risks resulting from the partial or non-compliance, in particular the potential exploitation of the partial or non-compliance;
- the description of the task(s), including impact in terms of schedule, budget and service provision, required to:
- recover the compliance to the concerned cyber requirement;
- mitigate operationally the assessed risk;
- A recommended way forward (e.g. operational mitigations) and justification;
- Expiry date for the waiver and a committed schedule for the complete recovery of the compliance to the concerned cyber requirement (action plan).

FWC-SOW-094: Cybersecurity Acceptance

Due to the criticality of ERAS, the Contracting Authority will exercise its right to perform an independent security assessment of the Solution (see CYB-INF-0380 from GSA-SEC-SREQ-SPE-232364). The Contractor shall already foresee such task in terms of support and schedule. The outcome of that assessment shall be an input for the Acceptance Review of the Solution.

5.11 Security Accreditation

FWC-SOW-095: Security Accreditation Tasks

The Contractor shall perform all the necessary security activities and deliver relevant information (as-design and as- built) as defined in the Galileo SACP document and of the Galileo Sites Local Security Accreditation Plan, found under Security Requirements in the CISL [AD-1].

FWC-SOW-096: Accreditation Plan

The Contractor shall produce an Accreditation Plan describing the plan to be followed in order to achieve the accreditation milestones.

"Accreditation Plan" **[DRL: SEC-14]**

FWC-SOW-097: Inputs to the Accreditation

The Contractor shall support the Contracting Authority providing relevant information in as-design and as-built information at CDR and QR/AR as per CISL [AD-1].

FWC-SOW-098: Threats Scenarios Coverage

The Contractor shall provide inputs to both Threats Scenario Coverage "As-Designed" and "As-Built", according to the Threats Scenarios prescribed by the Galileo SACP process, vol1B - Annex P, listed in the CISL [AD-1].

"input to the Threats Scenario Coverage" **[DRL: SEC-13]**

FWC-SOW-099: Accreditation Data Package

The Contractor shall support the preparation of the Accreditation Data Package by providing all the requested information as specified in the Galileo SACP and of the Galileo Sites Local Security Accreditation Plan, found under the Accreditation Requirements documents listed in the CISL [AD-1]. In particular the Contractor shall provide the following:

- Cryptographic Management Plan;

- Inputs to the Site Accreditation Milestone;

- Inputs to Security Risk Analysis, such as recommendations and countermeasures;

- Identification and Classification of Assets;

- Evidence of Approval of Cryptographic Products,

- Input to SECOPS;

Note: The Contractor should also be ready to provide other supporting information, when requested as per requirements in section 5.15, for the purposes of Accreditation. Such additional information may include, but should not be considered limited to: System Technical Documentation, Security related Testing Strategies (including any vulnerability testing that has been carried out), Security Incident Management Schemes / Policies, TEMPEST related documentation (if applicable), and Security related service/maintenance records. See for the subject

" Accreditation Files" **[DRL: SEC-13]**

5.12 Deployment Activities

FWC-SOW-0100: Deployment Approach

The activities leading up to the deployment of the Solution and or any sub-sequent releases are regulated by a number of reviews in order to ensure that an appropriate state of operational readiness is achieved and no risk to the System in Operations is identified.

Note: The duration times on the above figure are indicative. For the activities not under the responsibility of the Contractor (i.e. SIV, OVR) an average of three months shall be assumed.

The Contractor shall ensure that, as per applicable standards, checkpoints (e.g. TRR, TRB) are defined during qualification or acceptance tests.

The following activities (SIV, OVR) are led by the Contracting Authority however Contractor's input shall support (see section 5.15).

System Integration and Verification (SIV) Activities

The successful completion of the Factory Qualification Review is a prerequisite for the start of the System Integration and Verification (SIV) activities, which involve the integration of the release within the System on the validation chain (if available), and delta verification on the operational chains.

The scope of verification includes Non-regression Testing to demonstrate that the introduction of the release has not caused unintended adverse side effects, and that the integrated system still meets the system requirements (i.e. confirmation of "no regression").

Operational Validation Review (OVR)

The purpose of Operational Validation Review (OVR) is to confirm the Solution (including the integrated release) is suitable for its intended use (i.e. operational service provision). As such it is quite distinct from system verification (whose primary reference point is the system requirements).

The OVR activities are the responsibility of the Operator, however the Contractor shall ensure support and shall provide the relevant inputs required to develop the operational products needed to provide the Galileo services in a safe, reliable and sustained manner.

Prior to the start of the OVR activities, the Operator will organise an Operational Validation Readiness Review (OVRR) with the participation of the Contractor to check that the appropriate preconditions are met, e.g. the availability of all resources, test plans, procedures, timelines, system status, etc.

FWC-SOW-0101: Coordination of Deployment

The Contractor shall co-ordinate with the Contracting Authority and the Operator for all for all aspects related to site availability and site support.

FWC-SOW-0102: Infrastructure Delivery

The Contractor shall ship all the Solution at the site(s) designated by the Contracting Authority.

FWC-SOW-0103: Configuration Control During Deployment

The Contractor shall maintain strict configuration control of the platform when deployed within the operational environment. The deployment process shall include as well hardening and lock-down of the platforms.

FWC-SOW-0104: Site Installation Procedures

The Contractor shall prepare the on-site installation procedures compliant with the technical requirements and the on-site installation constraints. The installation procedure shall describe the deployment activities,

their related schedule, the interface activities with the Operator, and the proposed installation schedule for all the deployed sub-systems.

FWC-SOW-0105: Deployment and Installation Time

The Contractor shall minimise the time needed for the deployment, installation and initial configuration of the Solution at the deployment site.

FWC-SOW-0106: Deployment Scheduling

The Contractor shall coordinate the scheduling of the deployment activities with the Contracting Authority and the Operator overall planning process.

FWC-SOW-0107: Reversion to Previous Version

The Contractor shall ensure that at any time that the infrastructure or any of its sub-systems can revert to a previously known and working version, without significantly impacting the continuity of operations.

FWC-SOW-0108: Deployment of evolutions

The Contractor shall be responsible for the safe shipping and installation of any new releases/patches of the infrastructure (e.g. corrective maintenance).

FWC-SOW-0109: Incorporation to the Operational Environment

Prior to the incorporation of the infrastructure within the Galileo operational environment, the Contractor shall prepare and submit all the inputs relevant (Change Control Request or CCR) to be evaluated by the Configuration Control Boards established by the Operator in accordance with the SOPI-CCM [AD-1].

FWC-SOW-0110: Configuration Management for Operations Needs

The Contractor shall provide support for the configuration of the infrastructure to the needs of the Operator implementing SOPI-CCM 2 [AD-1].

FWC-SOW-0111: No harm to the Operational Environment

The Contractor shall plan and conduct any deployment activities in a manner that ensure no-harm to the continuous and seamless provision of the Galileo Services during the integration and deployment activities under his responsibility. The Contractor shall also raise to the Contracting Authority and the Operator any potential risk prior the execution of the activity.

FWC-SOW-0112: Preparation for Validation

The Contractor shall provide the Operational System Validation plan containing:

• The scope and required content of the ground infrastructure release.

• The required changes to the operations and maintenance products (i.e. procedures, databases, documentation, etc.) and ILS process (i.e. supportability, training, obsolescence, etc.);

• The process, and associated procedures, to be used to validate the required changes to the operations and maintenance products;

• Any changes to the related to training and certification of the operations and maintenance following the new release.

• The coordination activities necessary to ensure the smooth implementation of the release;

• The proposed schedule for the operational preparation and validation activities.

" Design, Development, and Verification Plan (DDVP)" **[DRL: ENG-08]**

FWC-SOW-0113: Support to Operational System Validation

The Contractor shall provide support to the infrastructure operator in the execution of the Operational System Validation (OSV) phase. The purpose of OSV is to confirm that the integrated infrastructure is suitable for its intended use (i.e. service provision). The scope of the OSV activities will be tailored by the SGDSP. The Contractor shall support as needed during the preparation, execution and objective validation steps.

FWC-SOW-0114: Engineering Support for Procedure Preparation

The Contractor shall provide support and inputs in the procedure preparation for the Service Provision Phase.

FWC-SOW-0115: Review and Feedback on Operations Plan

The Contractor shall provide support and inputs to the Operations Plan issued by the Operator and shall incorporate the concept of operations to its design.

FWC-SOW-0116: Contribution to Galileo System Integration and Verification Process

The Contractor shall provide support for the System Integration and Verification with the rest of the elements of the Galileo infrastructure (SAR Ground Segment, RLSP, GMS).

Note: The successful completion of SIV activities shall be a pre-condition for the start of the operational validation.

5.13 ILS and Maintenance

FWC-SOW-0117: ILS Plan

The Contractor shall deliver, maintain and implement an ILS Plan describing the activities necessary to assure the development of the ILS and maintenance activities.

- Asset creation (collection of all data in the Asset Management System);
- Asset commissioning (follow-up of asset move, repair, storage, operations);
- Asset decommissioning (assessment: un-reparability, obsolescence, end of life, disposal risks);

- Asset disposal (request for Contracting Authority authorisation, production of disposal data package, Decommissioning Review process).

"ILS and Maintenance Plan" **[DRL: ILS-01]**

Note: The ILS Plan shall cover all the architecture as well as any additional asset needed for its operations and maintenance

FWC-SOW-0118: ILS Standards

The Contractor shall base its ILS program of activities on the relevant industry standards, such as the European Cooperation for Space Standardisation (ECSS), the International procedure specification for Logistics Support Analysis, or the Military Standards and should consider the best practices defined in the Information Technology Infrastructure Library (ITIL).

FWC-SOW-0119: Obsolescence Maintenance Analyses

The Contractor shall perform obsolescence maintenance analysis as input to the ILS plan.

"*Obsolescence Analysis*" **[DRL: ILS-02]**

FWC-SOW-0120: Obsolescence Impact Analyses

The Contractor shall perform on a yearly basis an obsolescence analysis to assess the level of obsolescence risk. This shall identify obsolescence impacts and issues affecting the day-to-day maintenance, stock of spares, and repairs. This analysis shall include, as a minimum:

- Assess whether any asset unit is at the end of its production cycle (but spares can still be procured), or at the end of availability of spares from the supplier

- Assess the level of obsolescence risk on software production chain components, operating systems and associated libraries, and software verification tools including the supplier cost for supporting obsolete software

- Assess the justifications for obsolescence dates of the elements of the system, including software / firmware and hardware analysis of units

- Provide recommendations for the introduction of alternatives or upgrades to new components.

"*Obsolescence Impact Analysis*" **[DRL: ILS-03]**

FWC-SOW-0121: Obsolescence Management Time Span

The Obsolescence analysis shall cover a time span of 5 years.

FWC-SOW-0122: Spare Parts Identification

The Contractor shall identify all the spare parts needed by the L1, L2 and L3 maintenance levels as part of the Solution ILS plan and shall aim at optimising the use of them.

"*Spare Part Analysis*" **[DRL: ILS-04]**

FWC-SOW-0123: Installation, Operations and Maintenance Manual (IOM)

The Contractor shall provide, update and maintain the Installation, Operations and Maintenance Manual containing all the actions needed to install, configure, operate and maintain the complete infrastructure. This document shall allow the future Operator (SGDSP) to derive L1 operations and maintenance procedures (refer to 5.15) for additional support on this topic.

Note: The IOM shall include preventive procedure for daily M&C activities (main parameters monitoring).

FWC-SOW-0124: Assets Custody

The Contractor shall be responsible of the custody of the Solution, procured and/or produced under this contract, which includes inter alia their storage and replacement, until it is accepted by the CA.

NB: this requirement is not applicable to the maintenance activities included as option(s) in the Specific Contract Statement of Work.

FWC-SOW-0125: Removal and Disposal of Obsolete items

The Contractor shall be responsible for the removal and disposal of obsolete items for the period under its custody (until acceptance by the CA).

"*Asset Disposal Record*" **[DRL: ILS-05]**

FWC-SOW-0126: Shipping, Removal and Disposal of items at the End of the Contract

The Contractor shall be responsible for shipping any assets procured within the Contract that remain in their premises at the end of the Contract (e.g. development or factory qualification platform) to an EU location upon request of the Contracting Authority, or for the disposal of any item not requested to be transferred without additional cost.

FWC-SOW-0127: COMSEC Assets

The inventory management of COMSEC assets shall be managed separately, in compliance with the European Legislation and compatible with EU GNSS COMSEC instructions [CISL].

FWC-SOW-0128: Assets Control Process

The Contractor shall implement and maintain an Assets Control Process (including associated set of procedures) as part of the "ILS and Maintenance Plan", addressing:

- Items to be controlled;
- Classification of property;
- Treatment of property;
- Recording of property;
- Marking of property;
- Disposal of property;
- Audit and physical inspection

FWC-SOW-0129: Assets Inventory

The Contractor shall maintain an up-to-date inventory, registered in an IT system in the form of a database allowing for the recording of all tangible and intangible Assets:

- Received as a CFI (if any);
- Developed, acquired or procured as part of the Contract;
- All other assets accepted and maintained.

The "Asset Inventory" shall follow the overall Galileo Inventory ICD structure and shall include, for each item, as a minimum the mandatory fields as described in [AD-1].

 "Asset Inventory" (UNCLA/UNCLA) **[DRL: ILS-07]**

FWC-SOW-0130: Assets Delivery

The Contractor shall deliver and hand over to the CA the tangible and intangible assets necessary to support the operations and maintenance of the solution; that is framed within the Acceptance Review. From that moment, the Contractor will be relieved from custody of the delivered assets (whilst CA will hand over to the Operations Contractor).

FWC-SOW-0131: Scope of Maintenance Services

The scope of the requested Maintenance Services any L3 corrective and preventive maintenance tasks related to HW and SW assets.

Note: L1&L2 corrective and preventive maintenance of the infrastructure will be provided by Operator following the AR.

		Maintenance Classes			
		Corrective	Preventive	Adaptive	Perfective
Maintenance levels	L1 & L2	Operator (procedure based)		Not applicable	
	L3	**Maintenance** (6 months baseline after AR) Maintenance Option (6 months)		Based on Ad-hoc Support (5.15)	

Table 3 - Scope of Maintenance Tasks

FWC-SOW-0132: Applicability of Maintenance

If the defect observed during the maintenance period is found to be due to a technical or design error of a systematic nature, the maintenance shall apply to all identical components even if these components are functioning correctly.

FWC-SOW-0133: Maintenance Period

The Contractor shall provide maintenance Services for the Solution from the time of successful Acceptance Review and for a period of 6 months.

FWC-SOW-0134: Maintenance Metrics

The Contractor shall measure monthly the following metrics related to the maintenance services provided including at least (non-exhaustive):

- Total number of outstanding ARs/NCRs

- Number of ARs/NCRs fixed during the reporting period

- AR/NCR fix rate

- AR/NCR fixed within the timescales specified in this SoW

- Average AR/NCR correction cost

- Spares status and number of units

FWC-SOW-0135: Maintenance Report

The Contractor shall deliver monthly to the CA Maintenance Reports in a standardised format, which shall allow processing of the data for identifying averages or trends. The contractor shall provide the Contracting Authority, on request, a snapshot of the raw data to provide visibility of the process.

The report shall include as a minimum:

- Summary of the activities carried out during the reported period

- Report on the activities performed by on-site support personnel

- The relevant maintenance performance indicators

"Maintenance Report" **[DRL: ILS-08]**

FWC-SOW-0136: Shipment of Defected/Repaired Items

The Contractor's shall cover the cost of repair by the Contractor, including the supply and updating of appropriate documentation, simulation and test equipment during the maintenance period. It shall also cover all travel expenses, packing and transport charges incurred in connection with the repair and all licence fees.

FWC-SOW-0137: Maintenance Fixes Deliveries Timescales

The Contractor shall deliver fixes as per decisions of the Operator Anomaly Review Board (ARB) or the Contracting Authority Non-Conformance Review Board (EUSPA NRB), in accordance with their terms of references (see AD-1).

FWC-SOW-0138: End of Maintenance Delivery

The Contractor shall provide an End of Maintenance delivery which shall reflect the latest status of the Solution both in terms of software and documentation.

"End of Maintenance Report" **[DRL: ILS-09]**

5.14 Support to Anomaly Report Management Process

Contracting Authority's staff, the Contractor development team and the Operator may raise anomaly reports (AR) whenever they encounter a problem or they require a possible correction. These ARs are classified and managed via operational processes, in particular they are submitted reviewed by an Anomaly Review Board (ARB)/Non Conformance Review Board (NRB), towards which the support of the Contractor is specified in this section. The process is described in Table 4 - Anomaly Classification and SOPI-ANM [AD-1].

AR Category	Classification Criteria
Major or CAT-1	Anomalies having a severe, or persistent, detrimental impact on any of the following: • The provision of the intended Solution services (e.g. substantive failure to fulfil service requirements); • The availability of the key components of the operational Solution • The safety of the Solution (including security).
CAT-2	Anomalies having a detrimental impact on any of the following: • The provision of the Solution services (e.g. marginal failure to fulfil service requirements); • The redundancy levels within key components of the operational Solution (e.g. subsystem redundancy, networks, etc.); • Ability to operate and or maintain the Solution (including the performance of time-critical operations or off-line).
CAT-3	Anomalies having a potential detrimental impact on any of the following: • The provision of the Solution services (e.g. failure to fulfil service requirements); • The redundancy of the operational Solution; • The operations and maintenance of the Solution
CAT-4	All others

Table 4 - Anomaly Classification

FWC-SOW-0139: Support to ARBs

The Contractor shall support the EUSPA ARBs and NRBs organised by the Contracting Authority, from the deployment phase up to the end of the EoC (e.g. periods covered by maintenance tasks)

FWC-SOW-0140: ARB Tool

The Contractor shall use the Operator's ticketing tool ("Jira") as the Anomaly Reporting and Tracking tool (single common system for generating, reporting, and distributing Anomaly Reports and system enhancements) for executing the anomaly report management process. The CA will grant access to the Contractor personnel (e.g. several accounts/credentials) proportioned to the need to perform the Tasks.

FWC-SOW-0141: Major Anomaly Analysis Time

The Contractor shall analyse all CAT-1 major Anomaly Reports (as described Table 4) assigned to its organisation with an initial analysis in maximum two working days.

FWC-SOW-0142: Minor Anomaly Analysis Time

The Contractor shall analyse all non-major Anomaly Reports (as described Table 4) assigned to its organisation with an initial analysis in maximum five working days.

FWC-SOW-0143: Major Anomaly Interim Fix / Work-around Time

The Contractor shall provide interim fixes or workarounds to all CAT-1 major Anomaly Reports (as described Table 4) in maximum five working days.

FWC-SOW-0144: Major Anomaly Permanent Fix Time

The Contractor shall provide permanent corrections to all CAT-1 major Anomaly Reports (as described Table 4) in maximum 20 working days.

FWC-SOW-0145: Non-Major Anomaly Permanent Fix Time

The Contractor shall provide permanent corrections to all non-major Anomaly Reports in maximum 40 working days.

FWC-SOW-0146: Fixes quality

All software fixes shall be subject to the same design and development controls, testing and documentation as the software component being repaired.

FWC-SOW-0147: Regression Testing

The Contractor shall perform appropriate regression testing on all changed software & hardware components.

FWC-SOW-0148: Regression Testing Records

The Contractor shall justify the choice of regression tests and record their results in the documentation accompanying the updated software.

The introduction of any updated software shall be only with the approval of the Contracting Authority. The Contracting Authority reserves the right to require additional testing of the change or regression testing before approving the release of an update.

FWC-SOW-0149: Patch Documentation

All deliverable approval documents shall be updated to reflect the software modifications and re-delivered for the ARB/NRB approval with the software update.

FWC-SOW-0150: Patch Deployment

The introduction of any updated software shall be only with the approval of the Contracting Authority. The Contracting Authority reserves the right to require additional testing of the change or regression testing before approving the release of an update.

5.15 Additional Engineering On-site and Off-site Support

The following requirements address additional engineering support that the Agency may request the Contractor to perform, either at the SGSC (so-called on-site), Contractor's premises or other (off-site), during the implementation of the Contract. The scope of such engineering support is laid out in the requirements below.

FWC-SOW-0151: Technical Assistance Description (TAD) Activation

Before starting engineering support activities, a Technical Assistance Description (TAD) shall be agreed between the Agency and the Contractor. The TADs will be of two types:

- Type 1: activities to be performed on a Cost Reimbursement basis;
- Type 2: activities to be performed on a Fixed Price basis.

A TAD shall include, as a minimum, the description of the activity, its duration (start date, end date), the documents to be delivered, the CFIs (if any), the required expertise and profiles, the effort level per profile, the TAD manager and the associated price (should be a ceiling price for type 1 TADs), supported by the relevant Cost Sheets.

Once approved by the Agency and signed by both parties, the related activity shall start.

FWC-SOW-0152: Technical Assistance Description Amendment

If agreed by both parties, a TAD may be amended with the addition, removal or modification of activities initially agreed.

In this case a new version of the TAD shall be defined and signed by both parties as per the process described in requirement FWC-SOW-0151: Technical Assistance Description (TAD) Activation.

FWC-SOW-0153: Technical Assistance Description Completion Report

Once the activities procured under a TAD are complete, the Contractor *shall* deliver a TAD report describing, as a minimum:
- the activities which were performed in the frame of the TAD;
- the list of deliverables;
- the actual schedule of the activities as compared to the TAD agreed schedule;
- the actual consumption of the budget including the detailed costs sustained as per applicable law in case of Cost Reimbursement TAD (type 1 TADs).

If the activity duration is more than 30 days, TAD progress report, describing the activities performed during the preceding month, shall be provided monthly.

FWC-SOW-0154: Engineering Support Areas

The Contractor shall provide support in the following areas as relevant for the performance of the activities under the Contract:

- Engineering & Design (e.g. interface with RLSP, evolutions)

- Integration & Verification (e.g. security audit support)

- Adaptative and/or perfective maintenance

FWC-SOW-0155: Cooperation with other Galileo stakeholders

The Contractor shall provide support related to co-operation and coordination with other relevant SAR/Galileo stakeholders such EC, ESA, SGDSP, GSOp (list not exhaustive) in order to address Programmatic or Service related matters, system integration, upgrades, maintenance or validation activities.

FWC-SOW-0156: Support to Galileo Programme Level Reviews

The Contractor shall participate in Programme level reviews, as planned and requested by the Contracting Authority.

FWC-SOW-0157: Support to Service Validation

The Contractor shall provide support to the Contracting Authority and the Operator in the execution of the Service Validation phase. The scope of Service Validation campaign is to validate the complete infrastructure and processes for the provision of Galileo Emergency Warning Service. For the Service Validation Campaign, the contractor shall, at least, provide inputs supporting:

- the preparation of the service validation readiness

- the execution of the service validation

- the assessment of the service validation outputs

5.16 Training

FWC-SOW-0158: Training Plan

The Contractor shall update and maintain the "Training Plan" document, specifying the training courses to be developed, and when they will be performed. The training plan shall define as a minimum per training:

- Training requirements, in terms of tasks and roles requiring training;
- Syllabus of the training, with objectives for each course;
- Training evaluation criteria;
- The operations & maintenance personnel who will receive the training;
- Duration of training for both initial and recurrent training;
- Frequency required for recurrent training.

"Training Plan" **[DRL: ILS-10]**

FWC-SOW-0159: Operations Team Training

The Contractor shall provide training session for trainers, maintainers, administrators and operations team members of the SGDSP team on-site. Such training shall enable the SGDSP trainers to provide subsequent training sessions to other team members and stakeholders.

FWC-SOW-0160: Training Plan Update

The Contractor shall update the course materials as required and maintain them within an overall "Training Plan".

FWC-SOW-0161: Support to the preparation of Training Need Analysis

The Contractor shall provide support to Operator in the preparation of the Training Needs Analysis and Training Plan regarding all related operational and maintenance tasks.

FWC-SOW-0162: Support to Certification Process

The Contractor shall provide support in defining the skill Certification and Certification criteria process applicable to the Operator trainees and trainers

6   Contractor Deliverables

The Contractor shall refer to Table 6 for the Deliverable Requirements List (DRL).

FWC-SOW-0163: Deliverable Hardware and Software

The hardware and software to be delivered together with delivery dates and delivery destination is reported in the DRL.

FWC-SOW-0164: Documentation Supplied by the Contractor

The Contractor shall deliver the documentation as defined in the DRL through the development of the Contract.

FWC-SOW-0165: Documentation Deliverables Format

Every document shall be delivered in two separate files: one PDF format and one compatible with Word format. Exceptions for some deliverables will be specified by the Contracting Authority.

FWC-SOW-0166: Documents with Tracked Comments

When documents are updated answering comments/RIDs, the updates shall be identified in the document change log and marked using track changes functionality (for word format documents).

FWC-SOW-0167: Deliverable Update Expectations

Despite the DRL, the Contractor shall update any document that contains obsolete or inaccurate information, and re-deliver at the earliest opportunity.

6.1   Deliverable Requirements List (DRL)

In the DRL, documents are to be categorised as follows:

Acronym	Description
UNCLA	Unclassified
CLA	EUCI

Table 5 – Document Security Classification Split

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
SEC-01	Security Management Plan (SecMP)	UNCLA CLA						X	X	-
SEC-02	Cryptographic Management Plan (CMP)	CLA						X	X	
SEC-03	Input to Business Continuity Plan (BCP)	CLA						X	X	
SEC-04	Input to Disaster Recovery Plan (DRP)	CLA						X	X	
SEC-05	SoC to Security Documents	CLA					X	X	X	
SEC-06	VCM to Security Documents	CLA						X	X	
SEC-07	VCD to Security Documents	CLA	X					X	X	
SEC-08	Inputs to Local SECOPS	CLA						X	X	
SEC-09	Inputs to Site Security Description	CLA						X	X	

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
SEC-10	Statement of Compliance to Cyber Requirements (SoC to Cyber)	UNCLA CLA					X	X	X	
SEC-11	Accreditation Plan	UNCLA	X							
SEC-12	Accreditation Files	UNCLA CLA					X	X	X	
SEC-13	Input to Threat Scenario Coverage	CLA							X	
SEC-14	SoC to SECMON MER	UNCLA CLA					X	X	X	
ENG-01	SoC for Emergency Warning Service – Processing Component (EWS-PC) Technical Requirements	UNCLA CLA	X (as contr.)				X (as des.)	X (as built)		
ENG-02	SoC for EWS-ADP to EWS-PC Interface Requirements Document	UNCLA CLA	X (as contr.)				X (as des.)	X (as built)		
ENG-03	SoC to GSWS-G	UNCLA	X							
ENG-04	Infrastructure Technical Specification DOORS Module(s)/Database(s)	UNCLA CLA	X				X	X	X	

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
ENG-05	Requirements Traceability & Verification Matrices (RTM and RVM)	UNCLA CLA					X			Incl. TRR
ENG-06	Internal Interface Control Document (IICD)	UNCLA CLA					X			
ENG-07	External Interface Control Document (EICD)	UNCLA CLA					X			
ENG-08	Design, Development and Verification Plan (DDVP)	UNCLA	X				X			
ENG-09	Design Definition File (DDF)	UNCLA CLA					X			
ENG-10	Design Justification File (DJF)	UNCLA CLA					X			
ENG-11	Integration and Verification Specification	UNCLA CLA					X			Incl. TRR
ENG-12	Integration and Verification Report	UNCLA						X		Incl. TRB

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
		CLA								
ENG-13	Verification Control Document (VCD)	UNCLA	X				X	X	X	Incl. TRB
ENG-14	Commercial Off-The-Shelf (COTS) List	UNCLA					X	X	X	
ENG-15	System User Manual and Operational Procedures	UNCLA					X	X	X	
ENG-16	Obsolescence Plan and Data	UNCLA					X	X	X	
ENG-17	Configuration and Installation Manual	UNCLA					X	X	X	Incl. TRR
ENG-18	Installation Report	UNCLA						X		Incl. TRB
ENG-19	Performance Budget File	UNCLA		X			X			
ENG-20	SPF and Critical Item list (CIL)	UNCLA	X	X			X	X		
ENG-21	Developed Software Source Code	UNCLA CLA						X	X	
ENG-22	Developed Software Binaries and Executables	UNCLA					X	X	X	

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
ENG-23	Development Software (including COTS)	UNCLA CLA						X	X	
ENG-24	Development Environment	UNCLA						X	X	
ENG-25	Automated Build and Test Scripts (including configuration files)	UNCLA CLA						X	X	Incl. TRR
ENG-26	Test and simulation tools	UNCLA						X	X	Incl. TRR
ENG-27	All test stubs	UNCLA						X	X	Incl. TRR
ENG-28	Developed AIV Software Source Code	UNCLA CLA						X	X	Incl. TRR
ENG-29	Developed AIV Software Binaries	UNCLA						X	X	Incl. TRR
ENG-30	AIV COTS (including databases)	UNCLA CLA						X	X	Incl. TRR
ENG-31	All Software Licences (including background Intellectual Property Rights (IPR)	UNCLA						X	X	Incl. TRR

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
ENG-32	Maintenance Equipment and/or Tools	UNCLA CLA						X	X	
ENG-33	Configuration Management Tools	UNCLA						X	X	Incl. TRR
ENG-34	Configuration Management Datasets (including configuration files)	UNCLA CLA						X	X	Incl. TRR
ILS-01	ILS and Maintenance Plan	UNCLA	X				X	X	X	
ILS-02	Obsolescence Analysis	UNCLA						X	X	Incl. OVR
ILS-03	Obsolescence Impact Analysis	UNCLA						X	X	
ILS-04	Spare Part Analysis	UNCLA		X						
ILS-05	Asset Disposal	UNCLA		X						
ILS-06	removed									
ILS-07	Asset Inventory	UNCLA CLA						X	X	
ILS-08	Maintenance Report	UNCLA		X						

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
ILS-09	End of Maintenance Report	UNCLA		X						
ILS-10	Training Plan	UNCLA					X	X	X	
PRG-01	End Item Datapack	UNCLA CLA							X	
PRG-02	Project Management Plan	UNCLA	x	x						
PRG-03	Schedule Management Plan	UNCLA	x	x						
PRG-04	Project Baseline Schedule	UNCLA								
PRG-05	Project Working Schedule	UNCLA		X	X					
PRG-06	Risk Management Plan	UNCLA	X	X						
PRG-07	Risk Register	UNCLA	x	X		X				
PRG-08	Cost Reporting	UNCLA		x		x				
PRG-09	Acceptance Sheet	UNCLA		x						
PRG-10	Action List	UNCLA		x						

ID	Document Title	Classification level	KO	Ad hoc	Monthly	Quarterly	DKP/CDR	QR	AR	Comments
PRG-11	PA, QA and RAMS Plan	UNCLA	x	x			x			
PRG-12	PA and QA Report	UNCLA	x			x	x	x	x	
PRG-13	RAMS Report	UNCLA	x				x	x	x	
PRG-14	Configuration Status and Accounting Report	UNCLA	x	X						As needed
PRG-15	Audit Report	UNCLA		x						
PRG-16	Non-conformance Reports Status List	UNCLA			x		x	x	x	
PRG-17	Non-conformance Report	UNCLA CLA			x		x	x	x	
PRG-18	RFD/RFW Status List	UNCLA	x	x			x	x	x	As needed
PRG-19	RFD/RFW Report	UNCLA CLA	x	x			x	x	x	As needed
PRG-20	Leasson learned Report	UNCLA					x	x	x	
PRG-21	Certificate of Conformity	UNCLA						x	x	

Table 6 - DRL Table

6.2   DRL Content Guidelines

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*
ENG-01	SoC for Emergency Warning Service – Processing Component (EWS-PC) Technical Requirements	SoC to each requirement in the Technical Specification	Different columns or sections may be used to distinguish as-contracted, as-designed and as-built SoCs. References to RFDs and RFWs shall be included.
ENG-02	SoC for EWS-ADP to EWS-PC Interface Requirements Document	SoC to each requirement from the IRD	Different columns or sections may be used to distinguish as-contracted, as-designed and as-built SoCs. References to RFDs and RFWs shall be included.
ENG-03	SoC to GSWS-G	SoC to each section or requirement, as relevant	See requirement FWC-SOW-0168 for the content required
ENG-04	Infrastructure Technical Specification DOORS Module(s)/Database(s)	Traceability to lower level requirements and link to tests	Extract from the DOORS database of all modules developed and maintained as part of this Contract.
ENG-05	Requirements Traceability & Verification Matrices (RTM and RVM)	Contractor's flow-down of requirements baseline	Refer to [ECSS-E-ST-10C Rev.1] annex N.\n\nIt shall include full traceability from contractual baseline to the lower levels (elements, components), including linked verification test case

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*
ENG-06	Internal Interface Control Document	The Internal Interface Control Document defines the interface between two lower level subsystems of the EWS-PC.	Refer to [ECSS-E-ST-10-24C] annex B, and to [ECSS-E-ST-40C] annex E The scope of the document includes internal interfaces, including in particular the interface of the EWS-PC F/E with the EEWS-PC core element/tool.
ENG-07	External Interface Control Document	The External Interface Control Document defines the interfaces between the EWS-PC and all external entities.	Refer to [ECSS-E-ST-10-24C] annex B, and to [ECSS-E-ST-40C] annex E The scope of the document includes external interfaces, e.g. between EWS-PC and EWS-ADP.

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*

ENG-08	Design, Development, and Verification Plan (DDVP)	The document shall outline the plan for the Design, Development, and Verification.	• Design:
			  o Strategy and methodology;
			  o Contribution from lower-level elements/components;
			  o Assumptions;
			  o Approach to security;
			• Development:
			  o Assumptions and constraints;
			  o Development methodology and lifecycles;
			  o Procurement plan (HW and SW);
			  o Security aspects of development;
			• Deployment:
			  o Installation plan;
			  o Usage of the different chains (HW and SW);
			  o Overall migration plan;
			• Verification plan:
			  o Detailed account of activities to be performed per platform;
			  o Acceptance test plan;
			• Interface management plan;
			• Operational preparation and validation plan;
			• Transversal to all the above:
			  o Schedule overview, including relations and dependencies between lower and higher lever milestones and tasks;
			  o Critical path analysis;
			  o Actors involved in each process and their responsibilities;
			  o Engineering tools;
			  o Configuration control;

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*
ENG-09	Design Definition File (DDF)	The objective of the design definition file (DDF) is to establish the technical definition of a system or product that complies with its requirements. It shall include the architecture definition and description, functional analysis and functional allocation to elements and components.	Refer to [ECSS-E-ST-10C Rev.1] annex G.
ENG-10	Design Justification File (DJF)	The objective of the design justification file (DJF) is to present the rationale for the selection of the design solution, and to demonstrate that the design meets the baseline requirements. The DJF is a collection of all documentation that traces the evolution of the designduring the development and maintenance of the product.	Refer to [ECSS-E-ST-10C Rev.1] annex K.

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*
ENG-11	Integration and Verification Specification	As required by the Statement of Work, this document provides detailed step-by-step instructions for conducting integration and verification activities (test, inspection, review of design…) in accordance with the relevant requirements.	Refer to [ECSS-E-ST-10-02C Rev.1] annex A. Refer to [ECSS-E-ST-40C] annexes I, J, K and L.
ENG-12	Integration and Verification Report	Report on the execution, result and conclusions (as per pass/fail criteria) of verification procedure, which may be test, inspection or review of design.	Refer to [ECSS-E-ST-10-02C Rev.1] annexes C, D, E and F. Refer to [ECSS-E-ST-40C] annex M.
ENG-13	Verification Control Document (VCD)	List of requirements with traceability to phase in which they are planned to be verified and status	Refer to [ECSS-E-ST-10-02C Rev.1] annex B.

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*
ENG-14	Commercial Off-The-Shelf (COTS) List	The purpose of this list is to provide the list of products (HW or SW) procured from third parties as COTS products, providing sufficient information to prove compliance to contractual conditions and justify their appropriateness for their intended use.	List of COTS, including at least: • traceability to design, • justification for selection, • proof of compliance to contractual conditions (IPRs, ITAR/EAR…), • information relevant for maintainer (spares policy, end of sale, cost, license management…).
ENG-15	System User Manual and Operational Procedures	The manual for all elements, equipment, tools and functionalities are to be provided related to operational topics.	Refer to [ECSS-E-ST-40C] annex H. The System User Manual shall include detailed information on all the functionalities available in EWS-PC, including at least: • Detailed information on the sections, content, functionalities and tools of the Front/End (F/E) interface; • F/E user procedures; Management of users personal data and compliance towards GDPR. • Helpdesk procedures (registration, ticket handling, etc.). • Other functionalities, e.g. email. • Data Distribution: description of interfaces, registration, access information, folder structures, contents.
ENG-16	Obsolescence Plan and Data	Monitoring	Refer to section 0

Engineering Documents			
ID	*Document title*	*Purpose*	*Content*
ENG-17	Configuration and Installation Manual	The manual for all elements, equipment, tools and functionalities are to be provided related to installation topics.	• The whole set of installation procedures • The whole set of start and re-start procedures • Environment controls and check-lists prior to installation • In process and after installation controls • Recovery procedures in case of control failure
ENG-18	Installation Report	The report shall compile the description of the actual works performed on site during the installation of the element and provide the summary conclusions of the status of the element 'as deployed'.	• Interactions with other elements/entities on site during installation period • Overall Site Description • Overall element description • Actors involved in the Site Installation • Installation tools checklist • Packing Inspection • Equipment Inspection • Installation detailed description • Installation schedule • Health and Safety procedures (General and Site specific) • Inputs to Site/Elements ICD • Local Rules and Regulations applicable to the installation activities on site • Recommendations for future installations
ENG-19	Performance Budget File	Report on the usage of all resources impacting the software system compared to available resources in the physical equipment running the software.	Refer to [GSWS-G] section A8.

Engineering Documents			
ID	Document title	Purpose	Content
ENG-20	SPF and Critical Item list (CIL)	To identify and to track all the items that are critical to dependability, safety, performance, procurement, manufacturing, and verification. The Contractor shall include any Long lead Items (LLI) here, in case there is any.	Refer to [ECSS-Q-ST-10-04C] annex A
ENG-21 to ENG-34	N/A	As per [GSWS-G].	Content as per [GSWS-G].

Table 7: Deliverables Requirement List Content Guidelines

End of Document