Annex II to the Invitation to Participate – Descriptive Document for the Procurement of the GRC Infrastructure Evolution, Nominal Operations Support, and Maintenance

Reference:

EUSPA/CD/14/21/Annex II

Issue/Version: 1.0

Date: 08/02/2022

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Acronyms, Abbreviations, and Definition of Terms

Table 1: Acronyms, Abbreviations, and Definition of Terms

Acronym, Abbreviation, or Term	Definition
AIVP	Assembly, Integration and Verification Platform
AR	Acceptance Review
CADM	Configuration and Documentation Management
CAS	Commercial Authentication Service
CCB	Configuration Control Board
CDR	Critical Design Review
CIP	Contribution to Ionospheric Prediction
Data Products	Raw and processed GNSS data
DEV	Development platform
DMS	Document Management System
EC	European Commission
ECAS	European Commission Authentication Service
EEAS	European External Action Service
E-GSC	European GNSS Service Centre
EU	European Union
EUCI	EU Classified Information
EUSPA	EU Space Programmes Agency
EWS	Emergency Warning Service
FOC	Full Operational Capability
GACF	Ground Asset Control Facility

Acronym, Abbreviation, or Term	Definition
GCC	Galileo Control Centres
GCS	Galileo Control Segment
GDDN	Galileo Data Dissemination Network
GGTO	Galileo to GPS Time Offset
GMS	Galileo Mission Segment
GNSS	Global Navigation Satellite System (e.g. GPS, Galileo, GLONASS etc.)
GPS	Global Positioning System
GRC	Galileo Reference Centre
GRC products	GRC raw data and processed data
GRSP	Geodetic Reference Service Provider
GRUE	GSA RESTREINT UE (network)
GSA	European GNSS Agency (Precursor to the EUSPA)
GSF	Galileo Security Facilities
GSS	Galileo Sensor Station
GST	Galileo System Time
GTRF	Galileo Terrestrial Reference Frame
HAS	High Accuracy Service
IFQ	In-Factory Qualification
IONO	Ionosphere
IOV	In-Orbit Validation
ITRF	International Terrestrial Reference Frame

Acronym, Abbreviation, or Term	Definition
KMF	Key Management Facility
LRU	Line Replacement Unit
MCS	Monitoring, Control and Support
MDDN	Mission Data Dissemination Network
MGF	Message Generation Facility
MS	Member States
MS products	MS raw data and processed data
MSF	Mission Support Facility
MTCF	MEOLUT Coordination Facility
MUCF	Mission and Uplink Control Facility
NCR	Non-Conformance Report
NSS	Network & Security System
NRB	Non-Conformance Review Board
NRT	Non Real Time
ODTS	Orbit Determination and Time Synchronisation
OPE	Operational Platform
OPU	Operations Procedure Update
OR	Observation Report
OS	Open Service
OSNMA	Open Service Navigation Message Authentication
OSPF	Orbit and Synchronisation Processing Facility
OSQ	On-site Qualification

Acronym, Abbreviation, or Term	Definition
PDR	Preliminary Design Review
PRS	Public Regulated Service
PTF	Precise Time Facility
PVT	Position-Velocity-Time
Reference Data	Processed GNSS data to create GRC data products used in further processing
RFE	Request for Enhancement
RLSP	Return Link Service Provider
RT	Real Time
SAR	Search and Rescue
SGS	SAR Ground Segment
SIS	Signal-in-Space
SISA	Signal-in-Space Accuracy
SPF	Service Products Facility
SPR	Software Problem Report
SSEG	Space Segment
TMS	Training Management System
TPS	Time Prediction Service
TRA	Training Platform
TS	Timing Service
TSP	Time Service Provider
ULS	Up-Link Station
VAL	Validation Platform

2 Objectives of the Procurement

The scope of the GRC Infrastructure Evolution, Nominal Operations Support, and Maintenance Framework Contract (FWC) is to provide a turn key service for GRC infrastructure releases (including performing of the operational validation activities for the pending release), support the nominal operations for the version in operation, and follow up with the maintenance of the release in operation.

The EUSPA’s needs and requirements are identified in the Tender Specifications, including its annexes, and the present Descriptive Document. This said, the procurement of GRC is particularly complex in a number of technical aspects, especially in area of development where the Contractor will be asked to adapt the currently available solutions (GRC V1) and design and implement an innovative solution for the GRC V2. This will include:

- evolving the GRC V1 in-line with the required updates to existing functionality while simultaneously developing and integrating functionalities for the monitoring of new services,
- implementing a real-time solution into the GRC that will be capable of providing real-time monitoring of all services available at the time of the GRC V2 entry into operation (some of them are still to be developed, see section 4.5.2.1), and
- Elaborate a solution on how best to incorporate the GRC precise reference time and PRS monitoring functionalities into the real-time solution.

Due to the described complexity, the Agency is not able to define the most appropriate technical and management solutions to fulfil its needs. For this reason, the Agency has opted for a competitive dialogue procurement procedure where the Candidates/Tenderers will be asked to propose possible solutions to deliver the needs of the Agency. Additionally, due to the complexity and high technical nature of the contract subject, dialogue on risk allocations and liabilities are foreseen.

Finally, despite not being overly complex in itself, the solutions for nominal operations support and infrastructure maintenance rely, and are highly dependent, on the final requirements related to the new version of the infrastructure and for this reason they are planned to be discussed during the dialogue. Accordingly, the dialogue is expected to take place in the following indicative areas:

1. Real-Time Monitoring functionality and reporting, including:
    a. Carrier phase-based processing,
    b. Monitoring and Reporting KPIs.
2. The GRC core infrastructure Operational Validation and Operational Migration,
3. PRS Navigation Monitoring Evolutions,
4. Interface with the GSMC,
5. Precise Reference Time at the GRC,
6. SBAS/EGNOS Monitoring functionality,
7. Repurpose of the GRC V0 to create a robust tool for incident investigation support,
8. Development of Functionalities to Support the GRC Secondary Mission (see Section 4.1.2):
    a. Including GRC archive quality of data management and data accessibility.

9. GRC V2 Nominal Operations Support and GRC V2 Maintenance:
    b. the solution will be dependent on the dialogue and solutions for the above mentioned points;
10. Handover from the current incumbent,
11. Risk allocation and Liability.

The Agency reserves the right to complement / modify the foreseen areas of dialogue as a result of candidates' proposals and its development.

Through one or more rounds of dialogue with Candidates/Tenderers, the Contracting Authority aims to achieve the following overarching procurement objectives:

i. Select a Contractor ensuring genuine competition according to the principles of the Financial Regulation and GNSS regulation;

ii. Entrust the Contractor with clear responsibilities for the delivery of the complex tasks as described in this document and in particular:

    a. Ensure the continuous evolution of the design, qualification, and acceptance of the existing GRC core infrastructure to enable the independent monitoring and operations in a timely and secure manner that meets the needs of the Programme;

    b. Ensure the correct deployment, installation, integration, and migration of the new GRC operational infrastructures;

    c. Ensure the commissioning of the new GRC infrastructure releases procured under this framework contract, covering both, previously existing capabilities (see 4.2) and the new associated ones to the new GRC infrastructure releases, which is required in order to test and validate the infrastructure performances and accept it according to the terms and conditions which will be specified in the draft contract. During the commissioning, the infrastructure will have to undergo initial operations prior to acceptance review.

    d. Provide technical support and expertise to the Contracting Authority for all matters relating to the GRC.

    e. Provide support to the accreditation process of the GRC.

    f. Provide operations support for the GRC release in operation.

    g. Perform the maintenance services on the GRC release in operation.

3 Background Information on Galileo and EGNOS

3.1 Overview of the Main Stakeholders

3.1.1 Role of the European Union (EU)

The Galileo and EGNOS programmes are funded by the EU. The infrastructures are owned by the EU.

3.1.2 Role of the European Commission (EC)

The European Commission has overall responsibility for the programme, managing and overseeing the implementation of all activities on behalf of the EU.

EC is responsible of the formal interface with the Security Accreditation Board (SAB), which is the sole Security Accreditation Authority of the European GNSS systems and acts independently of the authorities in charge of the programmes.

With the Financial Framework Partnership Agreement (FFPA) signed between the Commission, EUSPA, and ESA and the ensuing Contribution agreement on 22/06/2021, the Commission entrusted EUSPA with the management, operation, maintenance, continuous improvement, evolitoon and protection of the infrastructure, including GRC.

.

3.1.3 European Union Agency for Space Programmes (EUSPA)

According to Regulation (EU) 2021/696 (Space Regulation), EUSPA is the Agency in charge of managing the exploitation of Galileo and EGNOS. In this frame, EUSPA has been entrusted with the GRC tasks under Section 3.1.2.

3.1.4 Role of the Galileo Service Operator (GSOp)

The GSOp is the Galileo service operator and, as such, plays a central supporting role to the EUSPA in the provision of all Galileo Services. GSOp is supposed to take over the L2/L3 maintenance duties for all the Galileo infrastructures, however, in order to safeguard the independence of the performance monitoring of Galileo and EGNOS, the responsibilities of the GRC maintenance will reside with the provider of the infrastructure of the GRC.

3.1.5 Role of the EGNOS Service Provider (ESP)

The ESP is the EGNOS service provider, certified to deliver the Safety of Life (SoL) services, and, as such, plays a central supporting role to the EUSPA in the provision of EGNOS services.

3.2 The Galileo Programme

This section providers the reader with a very high-level overview of the Galileo system and services. Further information can be found on the Agency's website: https://www.euspa.europa.eu/european-space/galileo/What-Galileo.

Galileo is an autonomous European satellite radio navigation system which is interoperable with other existing GNSS systems, in particular the Global Positioning System (GPS). Galileo provides a number of services through a combination of capabilities of the core system components (GCS/GMS/SSEG) and interfacing entities: Support Facilities, Service Facilities, and External Entities.

The Galileo Programme is structured in the following main phases:

- In-Orbit Validation (IOV) phase to develop the Galileo System and validate its in-orbit performance. This phase started in 2004, covering the design, development, deployment and in-orbit validation of the first 4 Galileo satellites together with the associated ground segment and initial operations activities. The IOV Phase was completed in December 2013 with the In-Orbit Validation Review (IOVR) and concluded formally in May 2014 with the successful closure of this milestone;
- Full Operational Capability (FOC) phase to deploy in full the ground and space infrastructure as required for achieving full operational capability. The FOC phase effectively started in 2010 with its FOC#1 and is on-going. It is composed of Deployment activities related to infrastructure completion, development of additional system functionalities and Exploitation activities related to the service operations in the full operational capability scheme. The FOC#2 technical requirement baseline represents the targeted final infrastructure configuration for this Phase. In particular, the first steps toward the implementation of the **Full Operational Capability (FOC)** was the progressive provision of "Early" and an "Enhanced" phases. These phases have followed a common logic based on a validation period followed by the corresponding service provision declaration. The validation period started in 2015 with a minimum number of satellites transmitting nominal, continuous, and stable Signal in Space (SiS) and having the scope to demonstrate the capability of the Galileo System to provide the Galileo Services to the Users with a committed level of performance (even if reduced with respect to the target FOC system). It was concluded by 2016 with a service review milestone and a service declaration. These milestones represented for the EUSPA and the Galileo Service Operator (GSOp) the first steps toward the nominal "service provision".

3.2.1 Overview of the Galileo Services and Functions

The Galileo system provides high quality navigation services with associated performance guarantees. The main services that are planned to be provided by Galileo are the following:

- **Open Service (OS):** implemented through two navigation signals separated in frequency (E1, E5). The Open Service provides position and timing information, free of charge for Users. Performance is competitive with, but complementary to, GPS allowing for dual constellation usage;
- **Open Service Navigation Message Authentication (OS-NMA):** the OS-NMA SiS provides the authentication data for OS geolocation information contained within the navigation signals;
- **High Accuracy Service (HAS):** the Galileo HAS design is currently mainly based on the SiS broadcast of specific signals on E6 band, in addition to the open service signals, as well as the provision of the same corrections made via a terrestrial data dissemination server. Without precluding the provision of other services in the future, the main services foreseen to be part of the HAS are high accuracy corrections to the OS;
- **Commercial Authentication Service (CAS):** the Galileo CAS design is currently mainly based on specific code encrypted signals on E6 band, in addition to the open service signals. Without precluding the provision of other services in the future, the main services foreseen to be part of the CAS are commercial high accuracy authentication;
- **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, it is 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;

- **Support to Search And Rescue (SAR):** Galileo will provide support to the international SAR satellite services by relaying distress signals from SAR beacons operating to COSPAS-SARSAT standards and relaying responses to those beacons equipped with Galileo receivers through the Galileo specific Return-Link service.
- other Galileo services or functions are currently undergoing definition. These include, but are not limited to: Timing Service, Emergency Warning Service, and Ionospheric Prediction Capability, (which are outlined below).
  - **Emergency Warning Service (EWS)**: Galileo shall be able to broadcast emergency warning messages to users worldwide to warn population about life-threatening situations (tsunami, volcanoes, forest fires, terrorist attacks, and all types of exceptional weather conditions). This service shall allow broad reception by mass market type receivers so as to directly alert the population at risk.
  - **Timing Service (TS):** Time parameters shall be provided in the Galileo Navigation messages to relate the time information derived by user receivers to UTC. The performance objectives for the TS shall allow the usage of the information in high-demanding applications as well as in regulated environments. In addition to the requirements with respect to UTC, the TS will also provide Service commitments with respect to the Galileo System Time (GST) itself. These commitments will be useful to users only interested in synchronisation, for which the specific time is not relevant. For those users, the synchronisation with respect to Galileo System time represents a significant advantage since they can benefit from a higher accuracy (the uncertainty inherent to the translation between GST and UTC is avoided).
  - **Ionospheric Prediction Capability (IPC)**: Ionospheric effects are well-known sources of disturbance on GNSS. In some cases, the impact is so penalising on man-made systems that it is better to anticipate upcoming disturbances. By being informed in advance, users are able to mitigate (e.g. postponement) the executions of potentially costly operations. The IPC shall serve the purpose of informing GNSS users, via means of notifications, of upcoming ionosphere-induced degradation of performance.

The attention of the Candidates is drawn to Article 44 of the Space Regulation which provides for a list of the services provided by Galileo.

3.2.2 Overview of the Galileo Infrastructure

The Galileo Infrastructure is composed of two main elements:

- The Galileo Space Segment, and
- The Galileo Ground Segment.

3.2.2.1 Overview of the Galileo Space Segment

The final **Galileo Space Segment** consists of a constellation (defined by the Walker parameters 24/3/1) of 24 operational satellites plus 3/6 active spare satellites in Medium-Earth Orbit (MEO), providing adequate coverage for the provision of the Galileo services on a worldwide basis:

- 3 orbital planes with ascending nodes distributed at intervals of 120 degrees,
- 8 slots per orbital plane, distributed at intervals of 45 degrees,
- 1 spare (and up to 2 possible) satellite per orbital plane.

This Galileo constellation provides the capability of broadcasting globally a set of navigation signals in L-band. The constellation also supports Search and Rescue international mission, by relaying distress messages to the COSPAS-SARSAT ground mission segment and providing a return link channel to the users.

3.2.2.2 Overview of the Galileo Ground Segment

The **Galileo Ground Segment** consists of two Galileo Control Centres (GCC):

- GCC-I in Fucino (Italy),
- GCC-D in Oberpfaffenhofen (Germany).

Each of these centres host a Ground Control Segment (GCS) to command and monitor the constellation and a Ground Mission Segment (GMS) to compute and uplink the navigation data to the satellites and monitor the SiS performance:

- GMS-I and GCS-I,
- GMS-D and GCS-D.

The GMS and GCS interface the Satellites though a worldwide network of Remotes Sites, hosting Telemetry, Telecommand & Control stations (TTC), C-band data Uplink Stations (ULS) and L-band data receiving Sensor Stations (GSS).

In order to interconnect the elements of the Galileo Ground Segment, the system implements the **Galileo Data Dissemination Network (GDDN)** interconnects the Galileo Control Centres (GCCs) with the remote sites, the Galileo Support Facilities and the Galileo Service Facilities. The network is composed of a combination of VSAT links (especially for the Remote Sites) and terrestrial links (mainly for facilities in Europe).

Within the Ground Mission Segment, the GCC is connected to the relevant Ground Stations (Ground Sensor Stations GSS, Uplink Stations ULS) through Mission Network Elements (MNE), and is connected to the TTC stations using the Satellite Network Element (SNE) within the Ground Control Segment. The two GCCs are interconnected via the inter-GCC link interfacing with (Common Network Equipment) CNE Network Elements at both GCC sites. In order to satisfy the Galileo system performance requirements, the GDDN service has to meet specific performance requirements in terms of availability, latency and continuity of data dissemination.

3.2.2.2.1 Galileo Ground Control Segment

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 their payload, planning, and automation functions that allow safe and correct operations to take place, and the support of payload related operations such as uplink of navigation data. The GCS is responsible for ensuring the safety of the satellites and their payloads, this includes performing monitoring and manoeuvring activities related to collision avoidance.

The GCS consists in the following facilities:

- **Satellite & Constellation Control Facility (SCCF):** the entity that performs the on-line monitoring and control of the satellites, both for routine and critical operations;
- **GCS Key Management Facility (GCS KMF):** element that supports security aspects and data protection (generation of encryption keys, encryption/decryption process, etc.);
- **Central Monitoring and Control Facility (CMCF):** providing the monitoring and control of all GCS ground assets, including the TT&C stations, GCC resident facilities and networks;
- **Flight Dynamics Facility (FDF):** that supports non-nominal orbit determination (GMS provides nominal) and manoeuvre planning;
- **Operations Preparation Facility (OPF):** that supports the preparation and configuration control of all operational databases and procedures, including those that are destined for automated execution;
- **Satellite Constellation Planning Facility (SCPF):** which supports the scheduling of regular contact (once per orbit) with all satellites in the constellation to support routine operations and special extended contacts to support critical operations;
- **Constellation Simulator (CSIM):** that is used for validation of operational processes and procedures, training and anomaly investigations;
- **Satellite Data Distribution Network (SDDN):** that connects the remote TTCF sites with the GCS elements at the GCC;
- **External Data Distribution Network (EDDN):** infrastructure for spacecraft data secure access permitting the exchange of non-real-time products between GCCs and external entities (satellite payload & platform manufacturers, external satellite control centres, test centres).

In addition, the GCS includes facilities at remote sites:

- **Telemetry Tracking and Control Facilities (TTCF) (TT&C Stations):** for satellite tracking, TC reception from the SCCF, up-linking to the satellites, telemetry reception from satellite and forwarding to the SCCF. The TTCF also performs satellite ranging and provides related data to the FDF.

3.2.2.2.2 Galileo Ground Mission Segment

The **Galileo Ground Mission Segment (GMS)** determines the navigation and timing data part of the navigation messages and transmits this information to the Satellite via C-Band ground stations. The GMS consists of the following 3 chains:

1. Processing Chain
2. Dissemination Chain
3. Operational Chain

The **Processing Chain** contains the following facilities:

- **Orbit and Synchronisation Processing Facility (OSPF):** for the determination of satellite navigation parameters, i.e., ephemeris computation, satellite clock prediction, and determination of the Signal-in-Space accuracy (SISA);
- **Message Generation Facility (MGF):** for the multiplexing of all the messages, generated either within the GCC or received by external entities, into a single data stream to be sent to each ULS in order to be uploaded to satellites;
- **Precise Time Facility (PTF):** for the generation of a physical realisation of Galileo System Time (GST) that is provided to all elements for time synchronisation purposes. This facility also computes parameters to be disseminated to the users, i.e.:
  - UTC-GST conversion models;
  - Galileo to GPS Time Offset (GGTO).

  In addition, the PTF includes a GSS station synchronised directly to the physical realisation of GST that collects the measurements needed to calibrate the OSPF

The **Dissemination Chain** contains the following facilities:

- **Mission Data Dissemination Network (MDDN):** supports the transport of data between GMS-GCC and ULS, and between the GSS and GMS-GCC. The MDDN includes both Realtime and Non-Realtime networks depending on the type of data to be disseminated. In addition, the MDDN includes the GNMF which is used for GMS and GCS network monitoring and control (and GNMF-S for secure network M&C);
- **Service Products Facility (SPF):** that is dedicated to the implementation of the exchange gateway between the GCC and the external world;
- **GMS Key Management Facility (GMS KMF):** that supports security aspects and data protection (generation of encryption keys, encryption/decryption process, etc.).

The **Operational Chain** contains the following facilities:

- **Mission and Uplink Control Facility (MUCF):** that supports the on-line and off-line mission monitoring and control including the Galileo overall long-, mid- and short-term mission planning and uplink scheduling;
- **Ground Asset Control Facility (GACF):** for the monitoring and controlling all the elements of the GMS in real time;
- **Mission Support Facility (MSF):** that provides off-line support functions including the computation of configuration and calibration data for the real-time elements;

In addition, the GMS includes facilities at remote sites, i.e.:

- **Up-Link Station (ULS):** that formats and up-links messages to the satellites in C-Band;
- **Galileo Sensor Station (GSS):** for tracking Galileo satellites, acquiring Galileo SiS, collecting and providing the SIS observables for Navigation and Integrity processing chains. One GSS is collocated together with each PTF, and takes the time input directly from the PTF, so that it becomes the GST reference.

3.2.2.3 Galileo Service Facilities

Facilities that support the provision of services and which, due to their criticality and strategic nature for the Galileo service provision are developed as part of the FOC System:

- **Time Service Provider (TSP):** monitors and steers the Galileo system time (GST) aligned to the Universal Time Coordinated (UTC);
- **Geodetic Reference Service Provider (GRSP):** the facility responsible for maintaining the Galileo Terrestrial Reference Frame (GTRF) close to the International Terrestrial Reference Frame (ITRF);
- **Galileo Security Facilities (GSF):** consisting of the GSMC-FR and GSMC-ES for system security monitoring and exploitation of PRS access and the Point of Contact Platforms (POC-P) that perform the interface between the GSMC and the Competent PRS Authorities;
- **European GNSS Service Centre (E-GSC):** The European GNSS Service Centre, E-GSC, is the element of the Galileo infrastructure acting as the single interface between the system established under the Galileo programme, on the one side, and the users of the open service, of the former commercial service and the users of safety of life applications based on the integrity monitoring service of that system on the other side. As per GSC Hosting Agreement, any future Safety of Life service interface will be hosted and operated in the GSC. GSC will play a key role in the provision on the OS-NMA, HAS, and CAS.
- **SAR Ground Segment (SGS):** receives and processes the SAR downlink data. The SAR GS includes three MEOLUT (SAR ground tracking stations) with 4 antennas each in Larnaca (CY), Maspalomas (ES) and Spitzberg (NO), and one facility in Toulouse (F) comprising a MEOLUT coordination facility (MTCF);
- **Return Link Service Provider (RLSP):** sends distress messages back to the distress beacons and to rescue personnel. The Return Link Service Provider facility is located in Toulouse and provides messages through a real-time interface to the GMS for uplink to the Galileo satellites;
- **Galileo Reference Centre (GRC):** Located in Noordwijk, the Netherlands, the GRC performs independent service performance monitoring and reporting, service performance investigation and support, and campaign based monitoring and experimentation, through cooperation with EU Member States, Norway and Switzerland (MS).

3.2.2.4 Galileo Support Facilities

In addition, certain Support Facilities have to be available during the FOC phase as they are critical for the Deployment, Validation and Maintenance of the Galileo system. The In-Orbit Test (IOT) station is one example of support facilities that is currently deployed and in used:

- **In-Orbit Test (IOT) station:** located in Redu (Belgium) which provides high gain antenna measurement system in L-band for navigation payload signal in space characterisation during commissioning and routine operations, as well as C-band and UHF transmit antennas for mission uplink and SAR transponder in-orbit testing respectively.

3.2.3 Galileo 2nd Generation

There are ongoing activities for the development of the 2nd Generation of Galileo (G2G). The aim is to keep Galileo ahead of the technological curve compared to global competition and maintaining it as one of the best performing satellite positioning infrastructures in the world while strengthening it as a key asset for Europe's strategic autonomy.

G2G developments are planned to take place during the timeframe of the Galileo Reference Centre (GRC) Infrastructure Evolution, Maintenance, and Nominal Operations Support Framework Contract (FWC), therefore the GRC will require undergo evolutions triggered by G2G developments.

3.3 The EGNOS Programme

This section providers the reader with a very high-level overview of the EGNOS system and services. Further information can be found on the Agency's website: https://www.euspa.europa.eu/european-space/egnos/what-egnos.

3.3.1 Overview of the EGNOS Services

EGNOS is the European Satellite Based Augmentation System (SBAS). The purpose of EGNOS V2 is to address a range of user services requirements by means of an overlay augmentation to GPS based on the broadcasting through GEO satellites of signals in the L1 (1575.42 MHz) frequency. The EGNOS signals contain integrity and differential corrections information applicable to the navigation signals of the GPS satellites. EGNOS can provide integrity positioning with Safety-of-Life (SoL) quality that allows it to address needs of all modes of transport, including civil-aviation. EGNOS V3 augmentation to Galileo satellites will also be provided in the L5 (1176.45 MHz) frequency.

EGNOS Services are provided free of charge to users. Based on the dissemination means (SIS broadcasted from the GEO satellites or data via Internet) and the safety implications of the applications (either safety critical application or non-safety critical applications), they can be classified in three main categories:

- **The EGNOS Safety of Life (SoL) Services**: aimed at users for whom safety is essential, typically for transport applications in different domains, and accessible via the EGNOS Signal-in-Space (SiS). The EGNOS product has been designed so that the EGNOS SiS is compliant to the ICAO SARPS for SBAS and at this stage, a detailed performance characterisation has been conducted only against the requirements expressed by civil aviation (for this reason it is usually understood that there exists one EGNOS SoL Service which is in fact an EGNOS Aviation SoL Service). Nevertheless, the EGNOS SoL service might also be used in a wide range of other application domains (e.g. maritime, rail, road…) in the future.

  A so-called NOTAM proposals service is also provided to support Air Navigation Service Providers using EGNOS to comply with SES Regulations.

  Currently, only single-frequency services are available. Dual-frequency SoL services will be provided with EGNOS V3.

- **The EGNOS Open Service (OS)**: it is aimed at users of non-safety critical applications in any domain that require improved positioning with respect to the GPS stand-alone performance. It is accessible also through the EGNOS SiS to any user equipped with a GPS/SBAS compatible receiver for which no specific receiver certification is required.

The applications of the EGNOS Open Service cover a wide range of domains: agriculture for high precision spraying of fertilisers and pesticides; geodesy for property boundary mapping, land parcel identification and geo-traceability; road transport for “pay-per-use” insurance, automatic road tolling and fleet tracking; etc.

EGNOS OS SiS also offers a precise and stable atomic time reference which allows users to have a highly accurate time reference to be used for synchronisation and timing applications.

Currently, only single-frequency services are available with EGNOS V2. Dual-frequency OS services will be provided with EGNOS V3 to any user equipped with a dual-frequency receiver.

EGNOS V3.1 will provide single frequency GPS augmentation services (SBAS L1) equivalent to the one provided by EGNOS V2, while EGNOS V3.2 will provide dual frequency multi constellation GPS and Galileo augmentation services (SBAS L1 & L5).

EGNOS V3 is fully independent from EGNOS V2. However, the GEO space services are shared resources between V2 and V3 (e.g. GEO-2 and GEO-3 can be used either by EGNOS V2 or by EGNOS V3, see Sections 3.3.2) but are not allocated to both EGNOS Products at the same time.

- **The EGNOS Data Access Service (EDAS)**: it is the EGNOS terrestrial data service which offers ground-based access to EGNOS data in real time and also in a historical FTP archive to authorised users (e.g. added-value application providers). EDAS is the single point of access for the data collected and generated by the EGNOS ground infrastructure mainly distributed over Europe and North Africa. EDAS also offers DGPS and RTK products in different formats and protocols to users. In addition, application providers are able to connect to the EGNOS Data Server, and exploit the EGNOS data, offering high-precision services to final customers.

3.3.2 Overview of the EGNOS Infrastructures

EGNOS V2 and V3 share the same architectural concept even though they are two different systems:

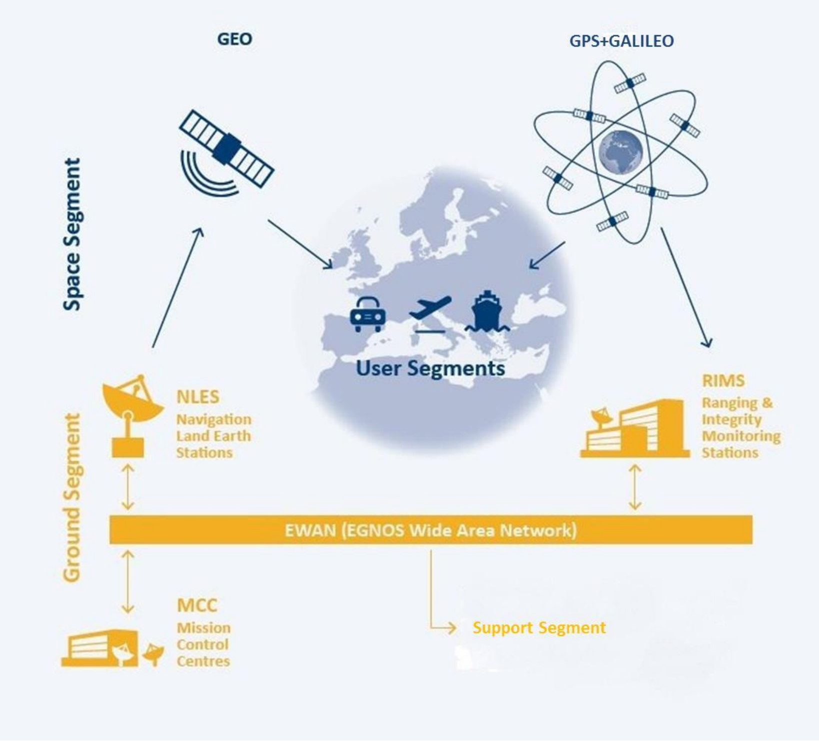


Figure 1: EGNOS V2/V3 High level architecture

The EGNOS space segment, composed of EGNOS geostationary (GEO) satellites, broadcast corrections, and integrity information to be applied to the GPS constellation in EGNOS V2 and to the GPS and Galileo constellations in the future EGNOS V3. The coverage area is primarily the EU-Member States, Norway and Switzerland Flight Instrument Regions (FIRs).

The EGNOS ground segment is in charge for the computation of the integrity measurements and wide area differential corrections. To this purpose a set of Ranging and Integrity Monitoring Stations (RIMS) are deployed and operated within and beyond the European Union territories. The RIMS collect the GPS, Galileo (for V3) and EGNOS GEO raw pseudo-range measurements. The network of RIMS is connected to two Mission Control Centres (MCCs) (of which one is master) where the integrity, differential corrections, ionospheric delays are computed by the Central Processing Facility (CPF). This information is sent in a message to the Navigation Land Earth Stations (NLES) to be uplinked in a GPS-like signal to the two GEO satellites. The ground segment is operated from the Central Control Facility (CCF) located in the MCCs. All EGNOS sites are connected through an EGNOS Wide Area Network (EWAN).

EGNOS service provision and operations are supported by specific tools hosted in the EGNOS support facilities sites.

EGNOS V2 and V3 Infrastructures, based on the architectural concept presented above, is composed of the main building blocks as shown in Figure 2.

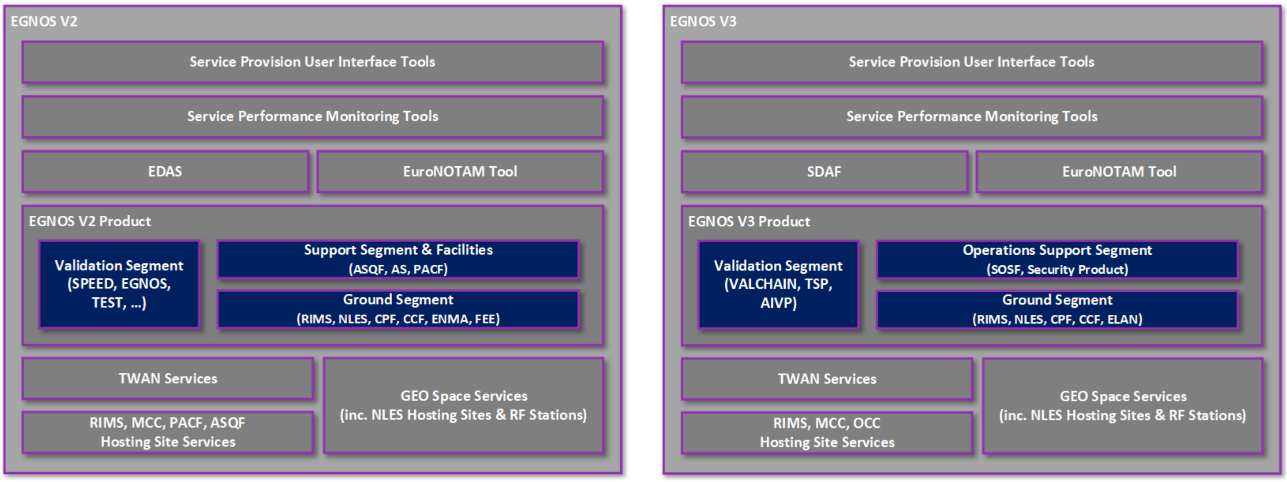

EGNOS V2
Service Provision User Interface Tools
Service Performance Monitoring Tools
EDAS
EuroNOTAM Tool
EGNOS V2 Product
Validation Segment (SPEED, EGNOS, TEST, ...)
Support Segment & Facilities (ASQF, AS, PACF)
Ground Segment (RIMS, NLES, CPF, CCF, ENMA, FEE)
TWAN Services
RIMS, MCC, PACF, ASQF Hosting Site Services
GEO Space Services (inc. NLES Hosting Sites & RF Stations)
EGNOS V3
Service Provision User Interface Tools
Service Performance Monitoring Tools
SDAF
EuroNOTAM Tool
EGNOS V3 Product
Validation Segment (VALCHAIN, TSP, AIVP)
Operations Support Segment (SOSF, Security Product)
Ground Segment (RIMS, NLES, CPF, CCF, ELAN)
TWAN Services
RIMS, MCC, OCC Hosting Site Services
GEO Space Services (inc. NLES Hosting Sites & RF Stations)

Figure 2: Comparison of EGNOS V2 and V3 - Main Infrastructure Blocks

3.3.3 Context of GRC Monitoring of EGNOS

The European GNSS operational status monitoring is based on the information provided by[1]:

(a) GRC for the core constellations of the GNSS;

(b) the ESP for the EGNOS system;

In addition, EUSPA has

- established a stable and structured partnership between the Agency and the national agencies, institutions, independent experts and bodies from the EU Member States and third countries participating in the GNSS Programme which commit themselves to establish, maintain and implement an EGNOS performance monitoring network. This partnership is set up through the signature of a Framework Partnership Agreements (FPA);
- a need for internal purposes to monitor certain parameters (see Section 4.5.1.3.1) which are part of this procurement based on data provided from the GRC network (GRC receivers, GESS, MS contribution though Framework Partnership Agreements, etc.)

[1] European GNSS monitoring strategy presented at the NAVIGATION SYSTEMS PANEL (NSP) JOINT WORKING GROUPS – 7th MEETING, 26 April – 6 May 2021

4 The Galileo Reference Centre (GRC)

For the purposes of understanding the structure of this section:

- Section 4.1 details the Mission of the GRC;
- Sections 4.2 to 4.3.4 detail what is currently in place at the GRC through GRC V1;
- Section 4.4 provides an overview of the current contractual situation and what will be done to ensure the establishment of fair competition conditions; and,
- Section 4.5 offers an indicative roadmap and expected new functionalities anticipated during the execution of the GRC V2 contract.

4.1 Mission

The GRC, located in Noordwijk (NL), has a current primary mission and envisaged secondary mission which are detailed in the following sub-sections.

4.1.1 Primary Mission

The GRC current primary mission (as agreed with the European Commission (EC) and Member States (MS) through the GRC Working Group (WG) and documented in the Galileo Mission Requirements Document (MRD)) is to:

- provide an independent means of evaluating the performance of the Galileo Service Operator (GSOp) and the quality of the signals in space. It is technically independent of the system infrastructure (as far as possible) and fully independent of the operations of the rest of the system performed by GSOp.
- Perform independent monitoring and assessment of Galileo service provision;
- Perform independent monitoring and assessment of Galileo data dissemination;
- Integrate raw data and processed data products from EU Member States, Norway and Switzerland with GRC products (both raw and processed data) and utilises the relevant expertise of the data providers;
- Report service performance to the Programme;
- Provide service performance expertise to the Programme, including (but not limited to) supporting the GSC on performance-related user requests;
- Support investigations of service performance and service degradations;
- Archive all relevant service performance data;
- Assess compatibility and interoperability between Galileo and other GNSS (GPS, GLONASS, BeiDou) and regional systems (EGNOS, QZSS, IRNSS).

In addition, following successful accreditation, the GRC will allow EUSPA to perform navigation analyses in support of incident investigations, validation of service improvements, etc.

Section 4.3.2 provides a more detailed view of the functionality of the GRC.

4.1.2 Secondary Mission

The GRC has a variety of tools developed within the core and secondary infrastructures as well as a strong operational team with a broad professional knowledge of GNSS systems.

For these reasons, the following secondary functions are currently identified to be developed within the GRC V2 by the successful tenderer:

- Provision of GNSS monitoring data (raw and processed),
- Campaign based GNSS performance investigations,
- GNSS receiver and service certification technical support,
- GNSS receiver and service development support,
- GNSS support to (European) R&D programs.

4.2 Independence of the GRC

The GRC is organised in order to guarantee on one side operational and organisational independence and on the other side technical independence.

4.2.1 Operational and Organisational Independence

With regard to its operations tasks, taking into consideration that both the GRC contractor and the Galileo Service Operator (GSOp) have to report independently to the EUSPA on the performance of the Galileo services, the GRC is organised in a way which ensures an absence of conflict of interest between the GRC contractor and the organisation operating the GSOp and the one providing system and service engineering support services to EUSPA.

4.2.2 Technical Independence and Robustness

For the GRC Infrastructure, the technical solution of the GRC V1 has been designed to be as different, as far as possible, from the overall Galileo system in terms of:

- GMS performance monitoring infrastructures (including processing software),
- Systems used to generate reference data (including the input data and configuration), such as GRSP and TSP, GMS navigation message generation system (OSPF); and,
- Galileo Support Facilities.

The technical independence of the GRC V2 is planned to follow this logic, please see Section 5.1.

4.3 GRC Infrastructures, Operations, and Maintenance

In order to establish a level playing field and allow for fair and equal competition, the following section provides a thorough description of the existing GRC infrastructure and its evolutions. Further measures to the purpose are described under Section 2.2.10 of Annex I of the Invitation to Participate (Tender Specifications).

4.3.1 GRC V0

The GRC V0, to be provided to the successful tenderer in the frame of this procurement for redevelopment (see Section 7 and Section 8), represents a tailored replica of the Time and Geodesy Validation Facility (TGVF) Core Infrastructure (CI) and was provided as a CFI under the first GRC FWC for the purposes of initial operations and preparations for the entry into operation of the GRC V1.

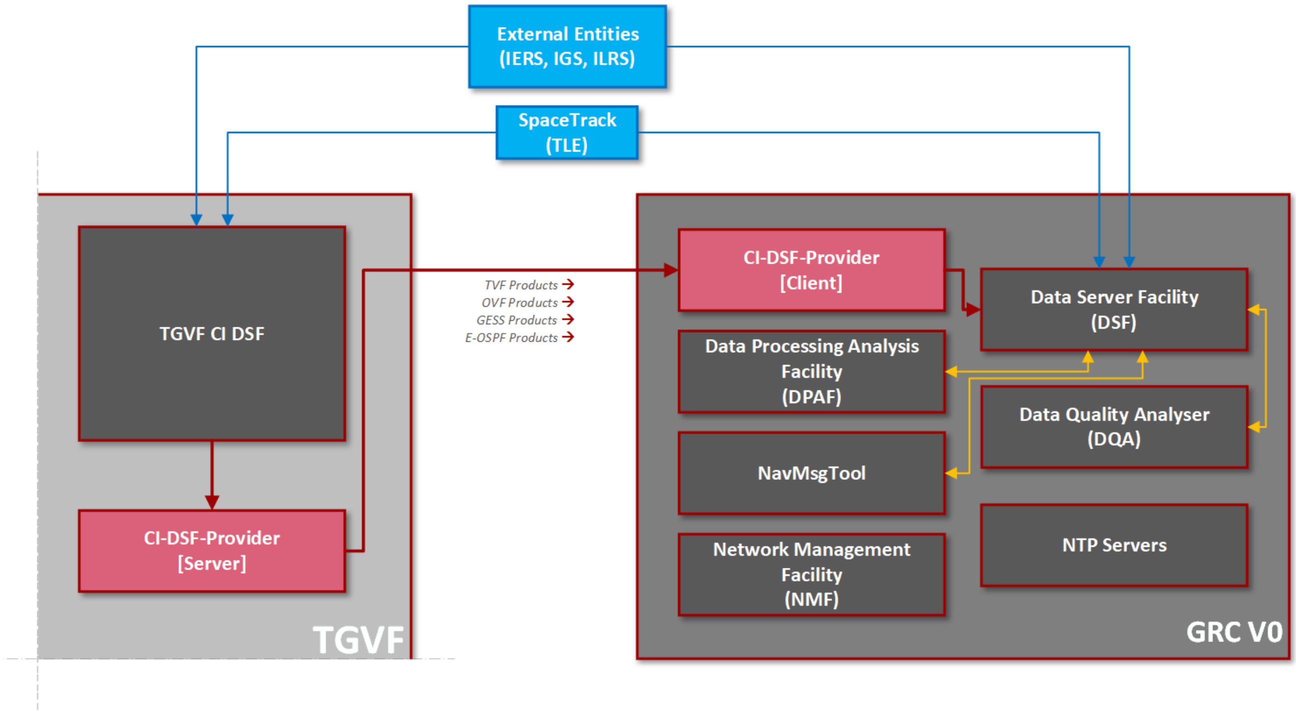


Figure 3: GRC Infrastructure - V0 High-Level Functional Components and Data-Flows

Figure 3 provides a high-level overview of the main functional components and data-flows of the GRC V0. As can be seen, a large number of raw and processed data are provided directly from the TGVF, through a client-server interface, to the Data Server Facility of the GRC V0. A brief over view of the main tasks of each component of the GRC V0 functional block is provided for understanding:

The ***Core Infrastructure Data Server Facility Provider (CI-DSF-Provider) [Client]*** is located on-site at the GRC and is the client-side of the client-server interface with the main TGVF core infrastructure for the reception of TVF, OVF, GESS, and E-OSPF data to the GRC V0.

The ***Data Server Facility (DSF)*** is the component inside the GRC V0 that is in charge of the data centralisation, formatting, and archiving. Data is collected from the CI-DSF Provider see above), External Entities (IERS, IGS, ILRS), and SpaceTrack (TLE). It is responsible for the provision of data to the processing functions of the GRC V0.

The ***Data Quality Analyser (DQA)*** is in charge of the over data quality analysis of the GRC V0 data stored within the GRC V0 DSF.

The ***Data Processing Analysis Facility (DPAF)*** routinely assesses a number of Key Performance Indicators (KPI) automatically or on-demand, through the ability to perform assessment on already available raw and processed data. The types of KPIs assessed include; SiS Ranging Accuracy (SISE), Dual-Frequency Availability, Position Accuracy of the GESS PVT, Timing KPIs, End-User Performance UERE, and End-User PVT Accuracy Validation.

The ***NavMsgTool*** is responsible for the parsing and decoding of the raw data and outputs in a readable format that can be used by other functions of the GRC V0.

The ***Network Management Facility (NMF)*** is responsible for the overall Monitoring and Control (M&C) of the GRC V0 by routinely analysing connectivity, services, and dataflows. It provides alerts to the operators if abnormal or sub-par behaviour is detected.

The ***NTP Servers*** are responsible for maintaining the overall network time of the GRC V0.

The GRC V0 entered into operation during Q2 2017 from a temporary location at ESTEC. From Q2 2018 it was moved to its permanent location at the GRC building.

4.3.1.1 Transition from GRC V0 to GRC V1

Following the entry into operations of the GRC V1, the GRC V0 operational outputs, along with the raw and processed data, have been integrated into the nominal operations of the GRC V1 to improve the overall robustness of the solution. The handover between GRC V0 and GRC V1 took place in Q2 2019.

4.3.2 GRC V1

For the purposes of performance of activities, the GRC V1 core infrastructure is divided into two operational platforms, as seen in Figure 4 (for the purposes of this document, only the UNCLA infrastructure will be discussed in greater detail).

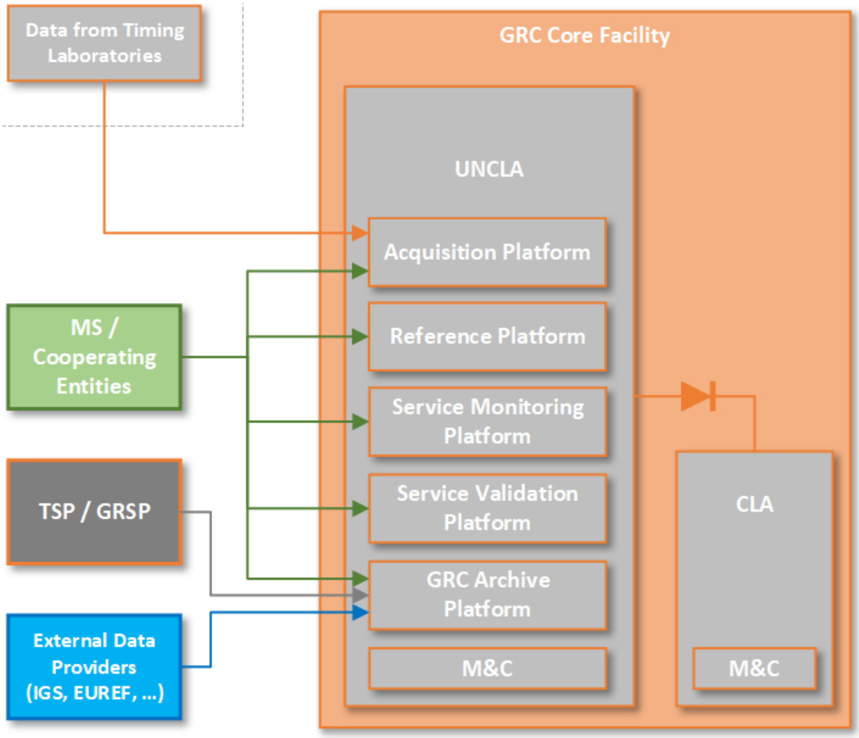

Data from Timing Laboratories
GRC Core Facility
UNCLA
Acquisition Platform
MS / Cooperating Entities
Reference Platform
Service Monitoring Platform
TSP / GRSP
Service Validation Platform
CLA
GRC Archive Platform
External Data Providers (IGS, EUREF, ...)
M&C
M&C

Figure 4: GRC Core Infrastructure - V1 High-Level Functional Components and Data-Flows

These operational platforms are further divided into a series of sub-components, with the UNCLA platform performing the data collection and product generation necessary for the operations of both the UNCLA and CLA domains.

Component	Sub-Component	Sub-Module
Acquisition Platform	GRC Local Sensor Stations GRC Remote Sensor Stations (data from Timing Laboratories) GRC PRS Sensor Station[2] GRC Ground Station (Medium Gain Antenna + Signal Analyser)	- - - -
Reference Platform	ODTS Reference IONO Reference	- -
Service Monitoring Platform	Satellite Monitoring	SiS Monitoring and Performance Analysis SiS ICD Monitoring Navigation Service Monitoring Health Status Monitoring
	Station and User Monitoring	PVT Monitoring Signal Quality Monitoring UER(R)E Monitoring
	Time Performance Monitoring	-

[2] Not included in current GRC version deployed, planned to be implemented in future version

Component	Sub-Component	Sub-Module
	Service Volume Simulator	-
Service Validation Platform	GSOp Validation NAGU Validation GSC Validation SDD/MRD Validation Service Validation Platform	- - - - -
GRC Archive Platform	Data Retriever GRC Archive Server External Data Server	- - -
Monitoring and Control	-	-

Table 2: GRC Core Infrastructure - V1 Component Overview

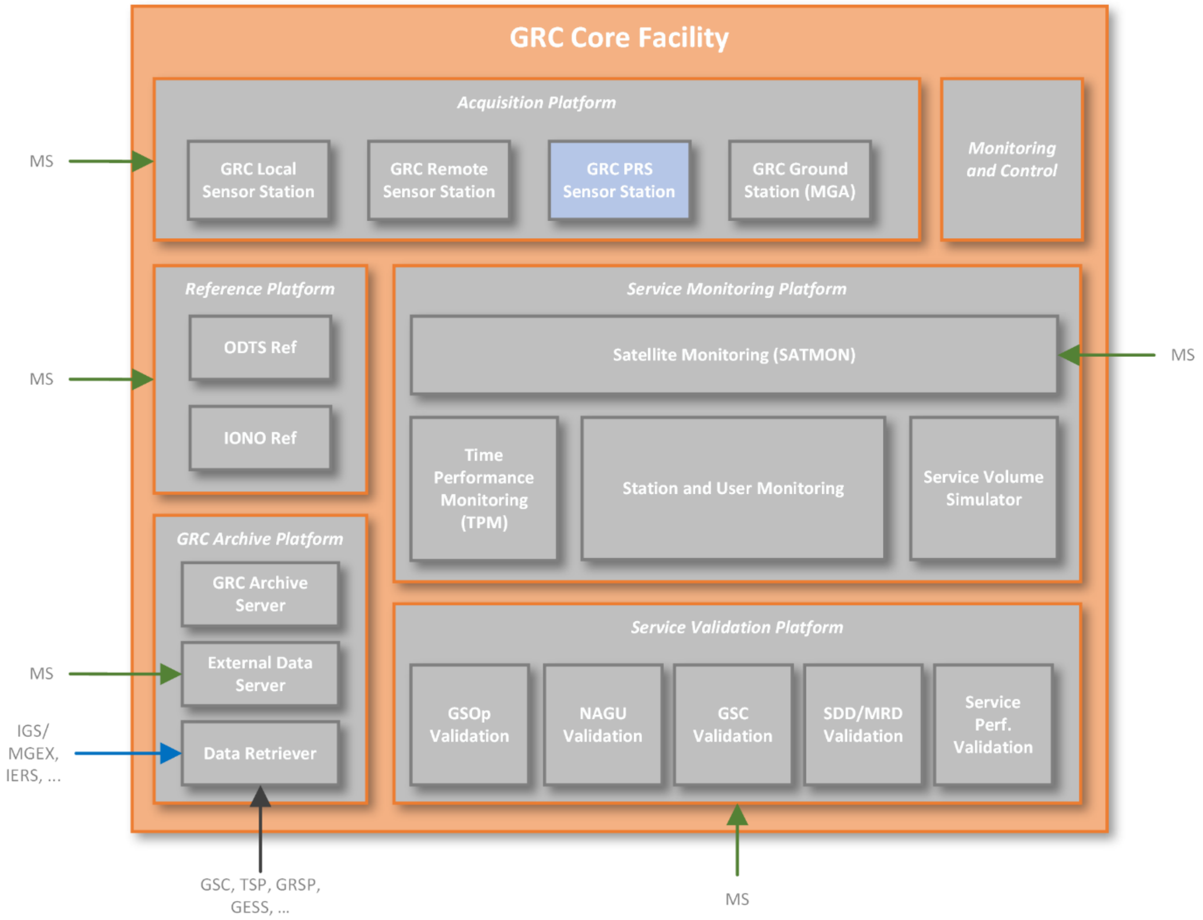


Figure 5: GRC Core Infrastructure - V1 Functional Component Overview

The GRC V1 UNCLA operational system, as seen in both Figure 4 and Figure 5 and summarised in Table 2, is composed of six main building blocks (five of which are further divided into a set of sub-components), more detail is provided in the following sub-sections.

4.3.2.1 Acquisition Platform

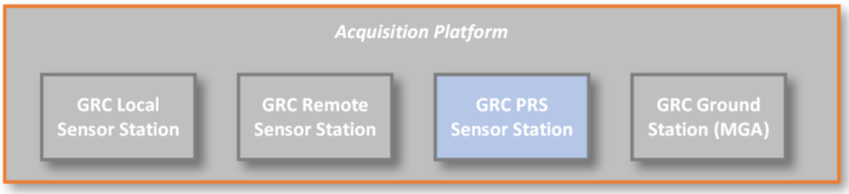


Figure 6: GRC Core Infrastructure - V1 Acquisition Platform Functional Components

The task of raw data acquisition is performed by the Acquisition Platform, which is formed of several sub-components:

The ***GRC Local Sensor Station*** is located on-site at the GRC and comprises multiple GNSS receivers connected to GNSS antennas on the roof of the GRC building.

The ***GRC Remote Sensor Station*** currently comprises two sensor stations, one based at the Royal Observatory of Belgium (ORB) and the other at the Physical Technical Institute of Germany (PTB)

The ***GRC PRS Sensor Station*** (shown in blue to highlight its planned implementation) will be installed locally and will be handled by the EUSPA for performing monitoring and data analysis on the PRS signals.

The ***GRC Ground Station*** utilises a steerable Medium Gain Antenna (MGA) installed on the roof of the facility and a signal analyser connected to the GRC core facility for the analysis and tracking of the SiS.

4.3.2.2 Reference Platform

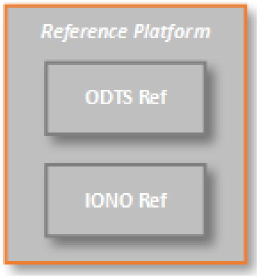


Figure 7: GRC Core Infrastructure - V1 Reference Platform Functional Components

Following from the acquisition of data, the GRC is required to generate its own set of reference data products for use in subsequent processing stages. This task is carried out by the Reference Platform, which is responsible for the generation of both ODTS and IONO reference data products:

The ***ODTS Ref*** component is in charge of generating the GRC orbits, clocks and troposphere reference data.

The ***IONO Ref*** is the component of the GRC in charge of generating the reference ionospheric data, including VTEC Global Ionospheric Maps (GIMs), Group Delays (GDs) and Inter-frequency Biases (IFBs).

4.3.2.3 Service Monitoring Platform

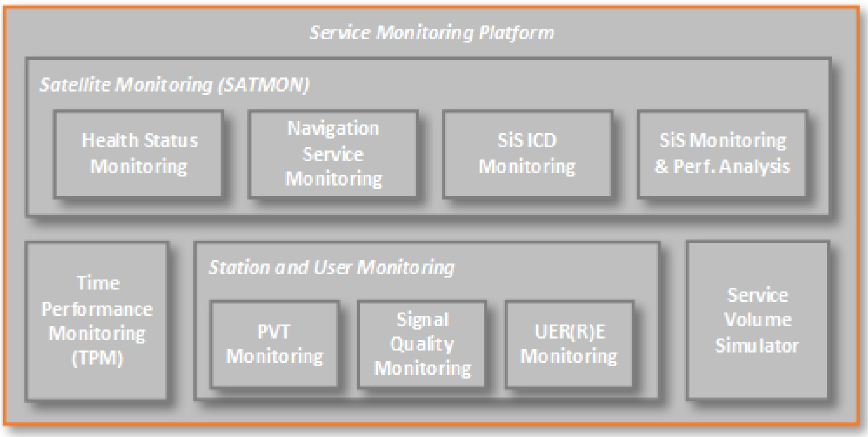

Service Monitoring Platform
Satellite Monitoring (SATMON)
Health Status Monitoring
Navigation Service Monitoring
SiS ICD Monitoring
SiS Monitoring & Perf. Analysis
Time Performance Monitoring (TPM)
Station and User Monitoring
PVT Monitoring
Signal Quality Monitoring
UER(R)E Monitoring
Service Volume Simulator

Figure 8: GRC Core Infrastructure - V1 Service Monitoring Platform Functional Components

After successful generation of the required reference data, the GRC Service Monitoring Platform function component is responsible for the overall performance monitoring of the provided service. This functional block is broken down into several sub-components:

The ***Satellite Monitoring (SATMON)*** is comprised of four main sub-components:

- The ***SiS Monitoring and Performance Analysis (SSM)*** is a tool for offline processing of recorded signals (exchanging data with the GRC Archive Platform through local input/output folders) using a set of processing functions for performing the different computations.
- The ***Navigation Service Monitoring (NSM)*** monitors the accuracy of the navigation message of the GNSS constellations (Galileo, GPS, GLONASS, and BeiDou). In addition, it allows for the configuration of the different satellites, services, signals, and outputs (as main configuration parameters). By exchanging data with the GRC Archive through the local input and output folders, a set of processing functions perform the different computations (whose outputs are sent to the GRC Archive Platform).
- The ***Health Status Monitoring (HSM)*** monitors the overall health status of all supported constellations (Galileo, GPS, GLONASS, BeiDou). Navigation data and Notice Advisories are used as input by the Processing functions, whose outputs are sent to the GRC Archive Platform.
- The ***SiS ICD Monitoring (SIM)*** monitors the Galileo SiS in respect to the SiS ICD. The actual content of the Navigation words is used as input by the processing functions which generate the processing outputs and the log files whose outputs are sent to the GRC Archive Platform.

The ***Station and User Monitoring*** is made from three sub-components:

- The ***Position, Velocity, Time (PVT) Monitoring (PVM)*** computes the position, velocity, and time solutions individually for each supported GNSS constellation (or combination of GNSS constellations) and is in charge of checking the accuracy and availability of the PVT solutions. The PVM operates as an independent module from the rest of the system.

- The ***Signal Quality Monitoring (SQM)*** analyses the GRC Sensor Station's receivers data quality by means of several indicators and statistics so as to generate a series of graphics and logs using the obtained information.
- The ***User Equivalent Range (Rate) Error (UER(R)E) Monitoring (UEM)*** is the module in charge of computing both the total and the individual UERE and UERRE. In order to perform this task, it computes several error contributions such as the satellite orbit determination error, ionospheric divergences, or the group delays.

The ***Timing Performance Monitoring (TPM)*** in charge of monitoring the timing performance of Galileo and other GNSS constellations. Such monitoring includes the estimation of GNSS System Time versus UTC, the estimation of the offsets between different GNSS System Times, the monitoring of timing parameters in the navigation message and the stability analysis of the satellite and station clocks. These functions are split in two separate groups. The first one is related to the monitoring of the SiS, including the dissemination of GNSS System Time, UTC, and GGTO. The second is related to the monitoring of the satellite and station clocks from ODTS. These two groups of functions are done by two separate elements inside the TPM.

The ***Service Volume Monitoring (SVM)*** is in charge of providing service volume analysis for Galileo and supported GNSS constellations based on post-processing of real data for selectable periods as well as other functionalities that require prediction of the Figures of Merit (FOM) or comparison with their predictions. The SVM allows navigation performance analysis to be performed for past or future time periods as well as over large geographical areas. It computes figures of merit that predicts the overall GNSS system performance and provides analyses of visibility and coverage, positioning accuracy and availability of service.

4.3.2.4 Service Validation Platform

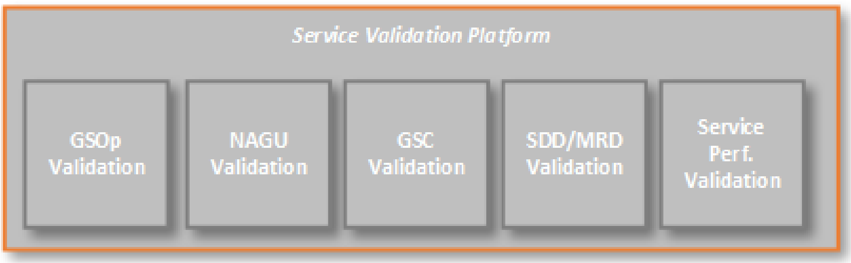


Figure 9: GRC Core Infrastructure - V1 Service Validation Platform Functional Components

As part of the GRC mission involves the cross-check of data and reports coming from other Galileo facilities via the GSOp, the Service Validation Platform carries out this task of KPI and metric comparison in relation to those reported by the operator. In order to do so, the functional block is composed of:

The ***GSOp Validation*** module is the component of the GRC in charge of both the KPI computation and the KPI comparison / cross-check. Electronic KPI reports (containing KPIs computed by the GSOp) are provided and compared to those that are computed at the GRC (using the GSOp Validation function) using the GRC Reference Products (raw and processed data).

The ***NAGU Validation*** module analyses the system performances during the time period notified by an unplanned NAGU, which is automatically downloaded and ingested by GRC archive platform. The consistency between the NAGU information and the satellite Health Status contained in the SiS will be checked along with the assessment (from a user point of view) of the impact of the NAGU. This involves performing checks related to the impact of the NAGU in the domains of PVT, UERE / UERRE, and service volume both with and without the NAGU information taken into account.

The **European GNSS Service Centre (*GSC) Validation*** cross-checks the navigation and Service Performance Predictions published by the GSC against those received through the Signal in Space.

The ***Service Definition Document (SDD) / Mission Requirements Document (MRD) Validation*** is responsible for assessing that the computed KPIs are within the thresholds defined by both of the Programme documents. In this case, the tool will compute the KPIs values and will assess the achievement of the KPI versus a target value. There exists a KPI database in the GRC where the target values and thresholds described in the SDD and MRD documents as well as the results of the comparison between the computed KPIs and the defined thresholds are stored.

The ***Service Performance Validation*** generates all the service performance reports to be provided daily, weekly, monthly, and yearly as well as generation of the validation reports (e.g. GSOp, SDD/MRD, NAGU, GSC, …).

4.3.2.5 GRC Archive Platform

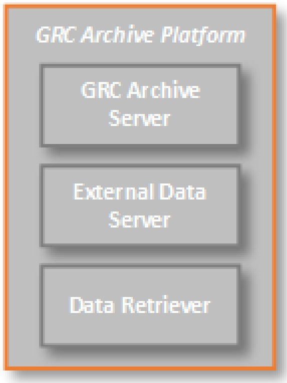


Figure 10: GRC Core Infrastructure - V1 Archive Platform Functional Components

The last component in the GRC data processing chain is that of the GRC Archive. The functional component is responsible for the archival of all data coming into and generated within the GRC for the complete lifetime of the facility. This component includes the following sub-components:

The ***Data Retriever*** has the overall responsibility for the collection of data from the entities external to the GRC as well as the collection of data from the GRC Acquisition Platform.

The ***External Data Server*** provides GRC data to external, trusted, users following completion of an authentication process.

The ***GRC Archive Server*** is responsible for the overall collection and archival of GRC data into the storage media of the medium and long term archives. It also responds to requests from the other modules of the GRC with the regards to the provision of data for processing.

4.3.2.6 Monitoring and Control (M&C)

The monitoring and Control function of the GRC has three main tasks:

Technical Monitoring of the hardware, software, and network architecture;

Mission Monitoring for the management of problems and incidents;

Control of the GRC core facility via the ability of scheduling and commanding.

A series of COTS and bespoke software solutions are utilised for these purposes.

4.3.2.7 GRC V1 UNCLA Platforms and Networks

Firstly, it is important to note, the use of the word platform here refers to a larger platform that includes the lower level platforms described in the previous sections.

The GRC core infrastructure procured under the first FWC includes the following:

- Operations Platform (OPE)
- Assembly, Integration, and Verification Platform (AIVP),
- Development Platform (DEV).

In general, the CLA environment is mirror of the UNCLA area with respect to the networks.

4.3.2.7.1Operational Platform (OPE)

The GRC V1 UNCLA ***Operational Platform*** is composed of five different networks:

- ***Operations*** (OPS) and ***Experimentation*** (EXP), which includes:
    - ***Acquisition Platform***:
        - ***GRC Local Sensor Stations***,
        - ***GRC Ground Station.***
    - ***Reference Platform***,
    - ***Service Monitoring Platform***,
    - ***Service Validation Platform***,
    - ***GRC Archive Platform***:
        - ***GRC Archive Server (Operational)***.
- ***Training***, ***Validation***, and ***Maintenance*** (TRA/VAL/MNT), which is a downscale version of the Operations and Experimentation network and includes:
    - ***Reference Platform***,
    - ***Service Monitoring Platform,***
    - ***GRC Archive Platform***:
        - ***GRC Archive Server (Training)***.

- ***DMZ Service***, which includes:
    - ***Data Retriever (Operational)*** (external connections),
    - ***External Data Server.***
- ***DMZ Service Training*** which includes:
    - ***GRC Archive Platform***:
        - ***Data Retriever (Training)***.
- ***DMZ Untrusted.***

4.3.2.7.2 Assembly, Integration, and Verification Platform (AIVP)

The ***Assembly, Integration and Verification Platform (AIVP)***, to be provided in the frame of this procurement (see Section 7), is a reduced replica of the Operational Platform (including some limitations as a smaller storage capacity and without some secure communications/redundancy), this platform provides a complete solution to perform (a) the AIV activities needed for the GRC development as well as (b) to develop, pre-develop and test new releases of the GRC infrastructure. This component is responsible for:

- Simulating the external interfaces to the GRC,
- Emulating the GRC components,
- Providing tools to execute tests, results assessment, control of scenarios, etc.,
- Assist in validation activities.

Currently the GRC AIVP is hosted at the premises of the GRC infrastructure contractor.

4.3.2.7.3 Development platform (DEV)

The ***Development Platform*** of the GRC, to be provided in the frame of this procurement (see Section 7), infrastructure is a development environment that is located at the GRC infrastructure contractor premises. It contains all the needed resources to perform development, building, and initial testing of the GRC software prior to installation on the GRC AIVP.

4.3.2.8 Interfaces Overview

In order to perform its duties, the GRC V1 interfaces with the Space Segment, via an acquisition platform (obtaining data from local and remote sensor stations and the GRC Ground Station (Section 4.3.2.1) and the Data Retriever (retrieving data (such as the GESS data) from cooperating external entities (Section 4.3.2.5)), to receive the Signal in Space (SiS) and a variety of external elements to collect or provide the data necessary for operations, as shown in Figure 11:

- Directly with cooperating entities from the EU Member States;
- Additionally, with relevant time and geodesy external entities (e.g. BIPM, IGS, EUREF, ILRS, etc);
- With the GSC, to retrieve offline data and to provide support to service performance-related user requests; and,

- With the Time Service Provider (TSP) and Geodetic Reference Service Provider (GRSP), to retrieve offline Timing and Geodetic raw and processed data;

The GRC also interfaces with the GSMC (Galileo Security Monitoring Centre) via an operational interface to provide navigation performance expertise.

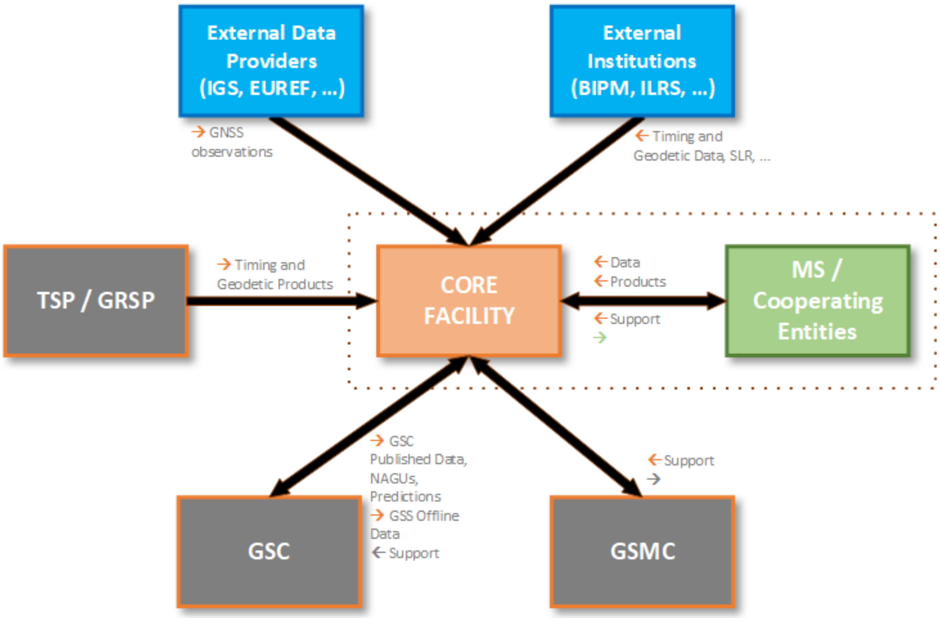

External Data Providers (IGS, EUREF, ...)
External Institutions (BIPM, ILRS, ...)
→ GNSS observations
← Timing and Geodetic Data, SLR, ...
TSP / GRSP
→ Timing and Geodetic Products
CORE FACILITY
← Data
← Products
← Support
→
MS / Cooperating Entities
→ GSC Published Data, NAGUs, Predictions
→ GSS Offline Data
← Support
← Support
→
GSC
GSMC

Figure 11: GRC Core Infrastructure - High-Level External Interfaces

These interfaces along with the GRC V1 core functionality provide the tools necessary for the performance of both the Unclassified (UNCLA) and Classified (CLA) operations of the GRC. More information will be made available later in the procurement process, only the most important interfaces are listed below.

4.3.2.8.1 External Interfaces

The following summarises the data flows of the GRC core infrastructure.

UNCLA Automated Data Flows:

- ***Real-Time (RT) Data Flows:***
    - There are no external real-time data flows in the GRC core infrastructure at present.
- ***Non-Real-Time (NRT) Data Flows:***
    - Download of External Data from External Data Providers:
        - IGS: Navigations and Observation Data;
        - NORAD: TLEs;
        - NASA/NSSDC: International Reference Ionosphere (IRI) Model Parameters;
        - NOAA: Solar Flus and Geomagnetic Pole Model;

- IERS:
  - Leap Seconds Announcement,
  - Earth Rotation Parameters,
  - Ocean Loading Information,
  - Terrestrial Reference Frame.
- PTB & ORB: UTC(k) Data:
  - GNSS Time Transfer Data: TW and CV,
  - Clock Measurements.
- BIPM: Circular T;
- Download of Data from TSP and GRSP:
  - Data provided to GMS as per applicable ICDs,
  - Additional monitoring data delivered to GMS for assessment of Timing and GTRF performance.
- Download of Data from GSC:
  - NAGUs,
  - Status and Performance Reports,
  - Performance Predications,
  - Galileo Ephemeris and Almanacs.
- Download of Data from Member States (MS);
- Data Retrieval from GNSS Stations:
  - GESS,
  - GRC own stations.

UNCLA NRT Non-Automated Data Flows

- Support to GSC Requests;
- Support to GSMC;
- Provision of data to MS cooperating entities;
- Manual download of external data by GRC operations engineer in case of:
  - Problem with the automated process (contingency action),
  - Problem with the external entity,
    - The GRC will have to provide the means to perform the ingestion of past data that was not retrieved due to a failure external to the GRC.
- Provision of the GSOp KPI Report and GSOp Data to EUSPA.

4.3.2.8.2 Internal Interfaces

UNCLA Automated Data Flows:

- ***Real-Time (RT) Data Flows:***
  - There are no internal real-time data flows in the GRC core infrastructure at present.
- ***Non-Real-Time (NRT) Data Flows:***
  - External raw and processed data from the DMZ network to the GRC operational network.
  - GRC monitoring data (raw and processed) from monitoring functions to the GRC Data Archive.
  - GRC reference products (raw and processed data) to the GRC Data Archive.

UNCLA NRT Non-Automated Data Flows

- Copying data to the experimentation platform.
- Manual recovery of monitoring data or processed reference data in case of problems. Provision of data to MS

4.3.2.9 Member State Contributions

The following provides an overview of the data made available to the GRC by cooperating member states:

- Daily RINEX with 3 hour latency,
- Hourly RINEX with 15 minute to 2 hour latency,
- Near real-time Binary with 15 minute latency,
- Real-time RTCM with a latency of a few seconds,
- Precise orbits and clocks:
  - Final with a 5 to 18 day latency,
  - Rapid with a 12 to 48 hour latency,
  - Ultra-rapid with a 3 hour latency (best effort),
  - Real-time with a 5 to 30 second latency.
- Code biases:
  - Final with a 5 to 18 day latency,
  - Rapid with a 12 to 48 hour latency,
  - Real-time with a 5 to 30 second latency.
- Ionosphere maps:
  - Final with a 5 to 18 day latency,
  - Rapid with a 12 to 48 hour latency.

The MS also provide campaign based data to the GRC, with data coming from:

- Automotive GNSS sensors,
- Airborne GNSS sensors,
- Marine GNSS sensors,
- Signal in Space sensors, and
- Satellite Laser Ranging.

4.3.3 GRC V1 Operations

The nominal operations are carried out in full from the GRC site in Noordwijk, the Netherlands, by a team of on-site operations engineers. The building is dimensioned such that there are rooms dedicated to both the unclassified (UNCLA) and classified (CLA) operations with space for seven UNCLA and three CLA operations positions.

Each of the Galileo services is monitored against Key Performance Indicators (KPI) and Figures of Merit (FoM) derived from the corresponding Service Definition Document. Additionally, the GRC evaluates the basic signal monitoring parameters for the Galileo signals against the values specified in the Galileo SiS ICD. Operational activities include the generation of processed data products and reports, using both data collected at the core facility and received from the cooperating entities from the Member States, as well as the integration of processed data products from Member States into the final GRC reference data. In addition, the operators may perform dedicated campaign-based analyses (taking advantage of data, facilities, and expertise contributed by the Member States) in support of service performance investigation and service validation campaigns, as well as the definition of upcoming service evolutions. The GRC makes use of automatic processes for continuous monitoring and processing of raw GNSS data. All operational processes are designed to be reliable, robust and cost effective, ensuring the quality of the final processed data products, but also supporting a standalone core functionality.

4.3.3.1 User Levels

From a user level point of view, there are three types of users that utilise the GRC core infrastructure or its resources:

The ***GRC Operations Engineers*** are users whose main responsibility is to keep the GRC core infrastructure equipment and processes up and running. They continuously monitor the system apply any necessary action to restore the nominal operation of a faulty GRC core element (considered as L1 maintenance, for L2/L3 maintenance see Section 4.3.4).

The ***Internal/Program Users*** are those utilising the GRC infrastructure internally and whose objective is to use the raw and processed data and services provided for specific analyses, tests, and experimentation. These users have access to all the internal services and data but with reduced permissions so as to preserve the integrity of the archive and its data.

The ***External Trusted Users*** (e.g. cooperating entities from Member State) are users with access to the GRC external data provision (no access to the internal services are granted) following a successful authentication process. The external access to the GRC data is granted if the following conditions are satisfied:

- Valid User Credentials,

- Origin Address is in the GRC Whitelist,
- Connection is secure (sFTP).

4.3.3.2 GRC V1 Nominal Operations

To provide an overview of how the infrastructure ties together with the operations of the GRC, Figure 12 provides and overview of the networks and the operational aspect.

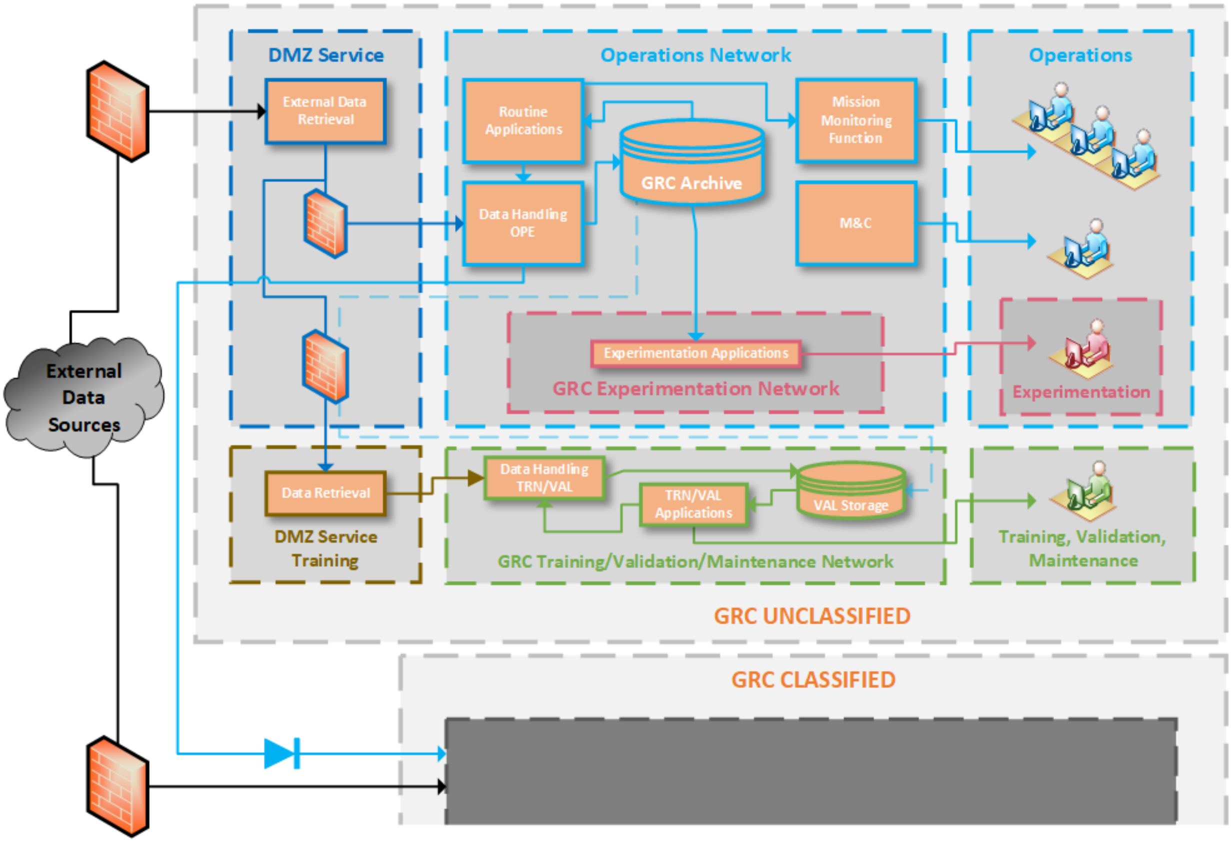


Figure 12: GRC Nominal Operations - Operational Correlation with Networks

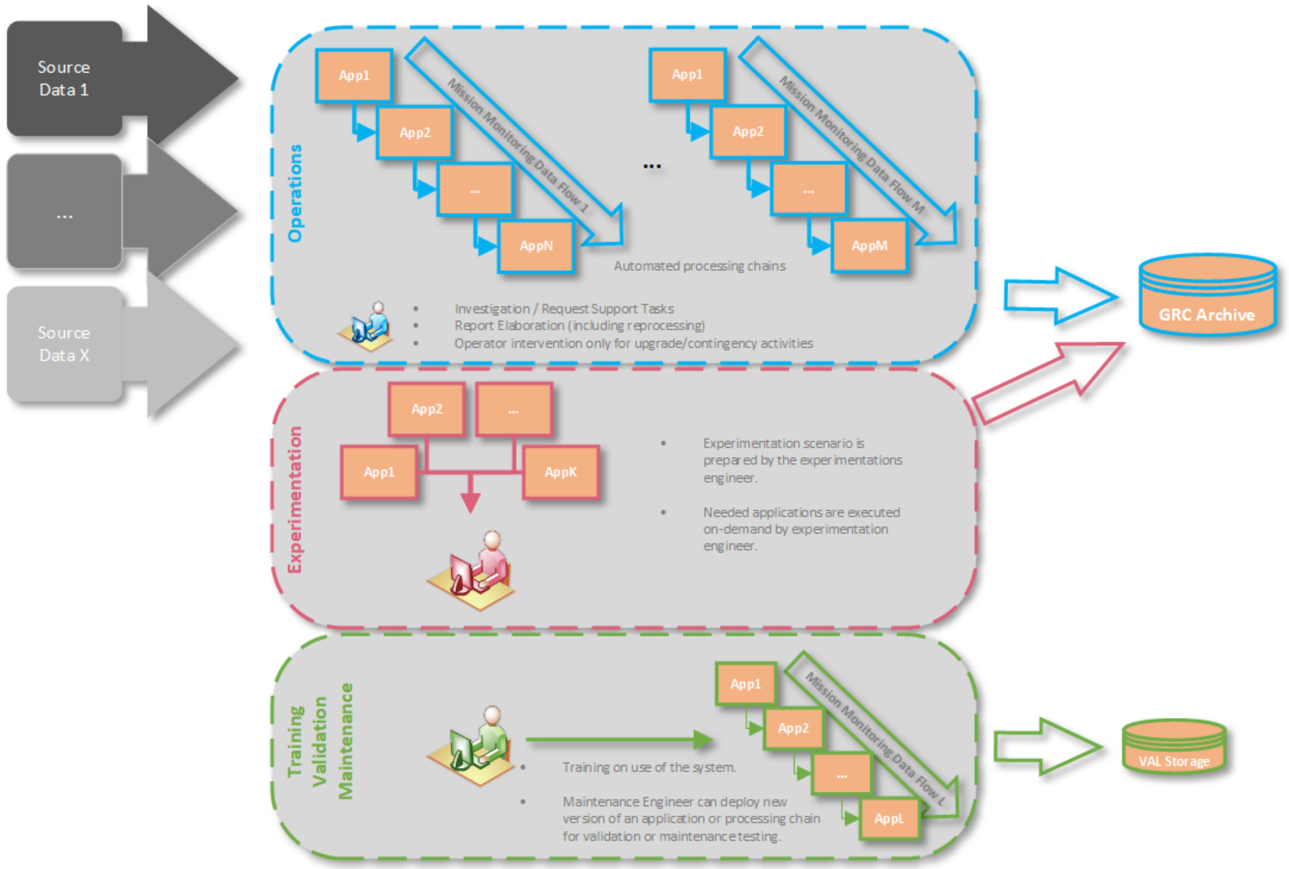
The nominal operations of the GRC V1 core infrastructure includes:

- Integration of the MS raw and processed data contributions along with all other external reference data provided, via the GRC V1 sFTP server, as input to the GRC V1.
- Routine operations based on operational procedures (see Section 4.3.3.5).
- Continuous update/improvement of the operational procedures from operational modification, including lessons learned during operations execution.
- Performing of independent monitoring of the Galileo services.

- Cross-check of the GSOp KPIs.
- Generation of the final service performance reports.
- Support to investigations of service performance degradations.
- Provision of service performance expertise to the Programme.

As such, three different processing modes are possible in the GRC (as shown in Figure 13):

- ***Routine Processing (Operations)***: the nominal mode in which the GRC V1 core infrastructure operates.
- ***Experimentation***: used for specific tests/investigations.
- ***Training, Validation, and Maintenance***: used for validation and training purposes.



- Investigation / Request Support Tasks
- Report Elaboration (including reprocessing)
- Operator intervention only for upgrade/contingency activities

- Experimentation scenario is prepared by the experimentations engineer.
- Needed applications are executed on-demand by experimentation engineer.

- Training on use of the system.
- Maintenance Engineer can deploy new version of an application or processing chain for validation or maintenance testing.

Figure 13: GRC Nominal Operations - Processing Modes Overview

In the operational processing, all data flows are completely automated and the mission analysis applications are pre-configured in routine mode. Within each processing dataflow, the applications are executed once the needed outputs of the previous application become available. All the results are then archived in the GRC Archive Server.

Conversely, in the experimentation mode, the operations engineer or experimenters are responsible for the configuration and execution of the applications. Furthermore, the availability of required inputs for a particular application must be obtained from the operational archive or generated as an output of an application execution on the experimentation network. Once the test or experiment has concluded, the results are then stored in the GRC archive as experimental results and are therefore available for future reference.

Finally, in the Training, Validation, and Maintenance network the applications are configured in routine mode but without write access to the GRC archive. The inputs and outputs of the maintenance processing chain are stored in a separate validation storage instead. In this mode, the operations engineer can deploy a particular version of an element or a complete processing chain for validation purposes or they can use the same configuration and version as that of the operational chain to train new operations engineers.

4.3.3.3 Operations Organisation

Figure 14 provides a high-level view of the current GRC Organisational Structure. For the purposes of operations, the right hand side of the diagram is relevant.

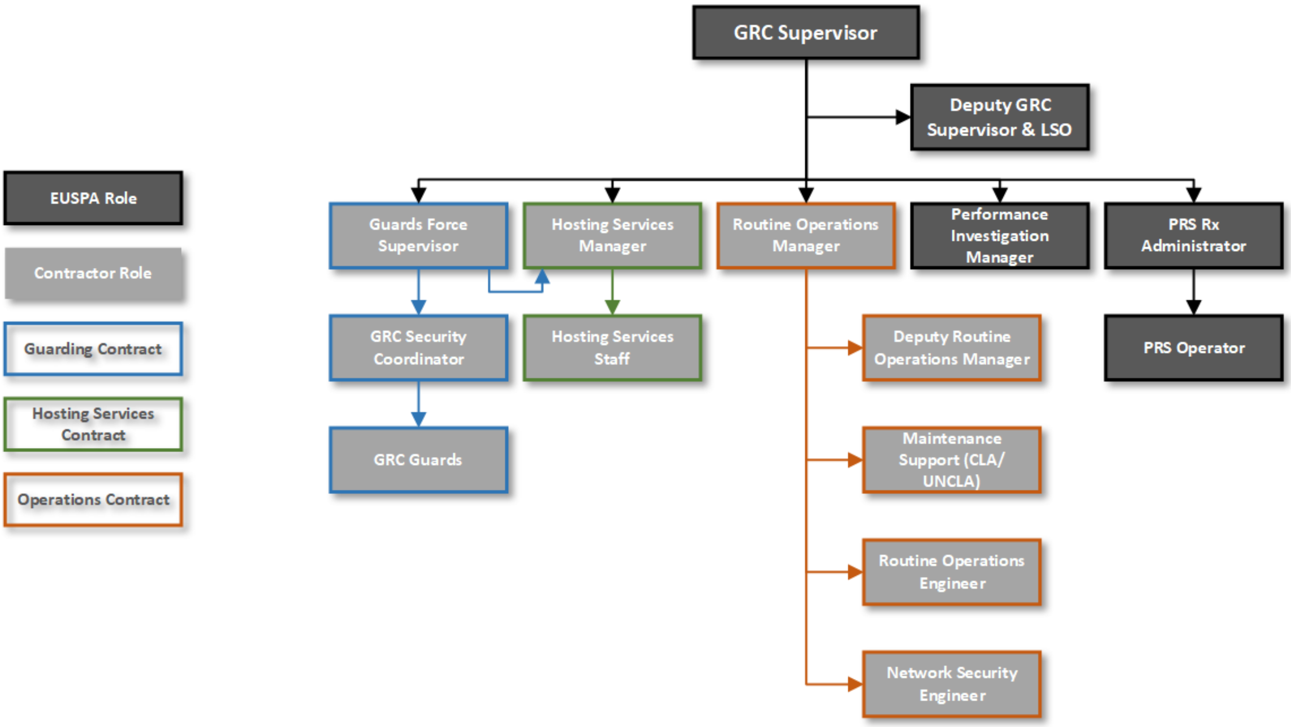

GRC Supervisor
Deputy GRC Supervisor & LSO
EUSPA Role
Contractor Role
Guarding Contract
Hosting Services Contract
Operations Contract
Guards Force Supervisor
Hosting Services Manager
Routine Operations Manager
Performance Investigation Manager
PRS Rx Administrator
GRC Security Coordinator
Hosting Services Staff
Deputy Routine Operations Manager
PRS Operator
GRC Guards
Maintenance Support (CLA/ UNCLA)
Routine Operations Engineer
Network Security Engineer

Figure 14: GRC Current Organisational Structure

The operational structure, from the nominal operations point of view, can be described by the following roles and their responsibilities:

The ***GRC Supervisor*** is responsible for the overall management of the general GRC activities and acts as the main interface between the EUSPA and Contractor as well as the contractual interface between the GRC and the external entities.

The ***Deputy GRC Supervisor and LSO*** is responsible for the operations of the GRC in the absence of the GRC Supervisor. In addition, while they may assume some delegated responsibilities of the operations, they are in charge of the overall site security operation of the GRC in their role as LSO.

The ***Performance Investigation Manager*** has the overall responsibility for performing performance investigation in the event of incidents or events that may arise in the Galileo service provision. These investigations can be instigated directly through detection by the GRC or from requests from within the other EUSPA teams.

The GRC UNCLA Routine Operations include the following roles:

> The ***Routine Operations Manager*** in the unclassified area is responsible for the coordination of all the activities executed by the nominal operations team in the unclassified area; i.e. they are responsible for the resources under their control and are responsible for the planning of the activities (subject to agreement with the EUSPA). The main objective being to ensure that the GRC UNCLA core infrastructure is successfully operated including the coordination of the performance investigation support.
>
> The ***Deputy Routine Operations Manager*** is responsible for assuming the responsibilities of the GRC Nominal Operations Manager during periods of their absence.
>
> The ***Routine Operations Engineers*** are responsible for the execution of their activities as defined in the agreed planning.

The ***Network Security Manager*** is responsible for ensuring the overall network security of the GRC core infrastructure.

The ***Maintenance Support (CLA/UNCLA)*** provides maintenance support to the GRC CLA and UNCLA operations environments in the event of anomalies or troubleshooting so as to ensure operability of the GRC core infrastructures.

The GRC CLA Operations are the responsibility of the EUSPA and include:

> The ***PRS Rx Administrator*** and the ***PRS Operator***.

The different nominal operational chain-engineering role correlation is provided in the high-level overview given by Figure 15. Eight main operational chains are utilised within the GRC UNCLA Operations and the responsibility of their operation is divided among the available GRC UNCLA Operations Engineers. In general, each assigned process / task has a primary and secondary operator to account for unavailability during certain periods.

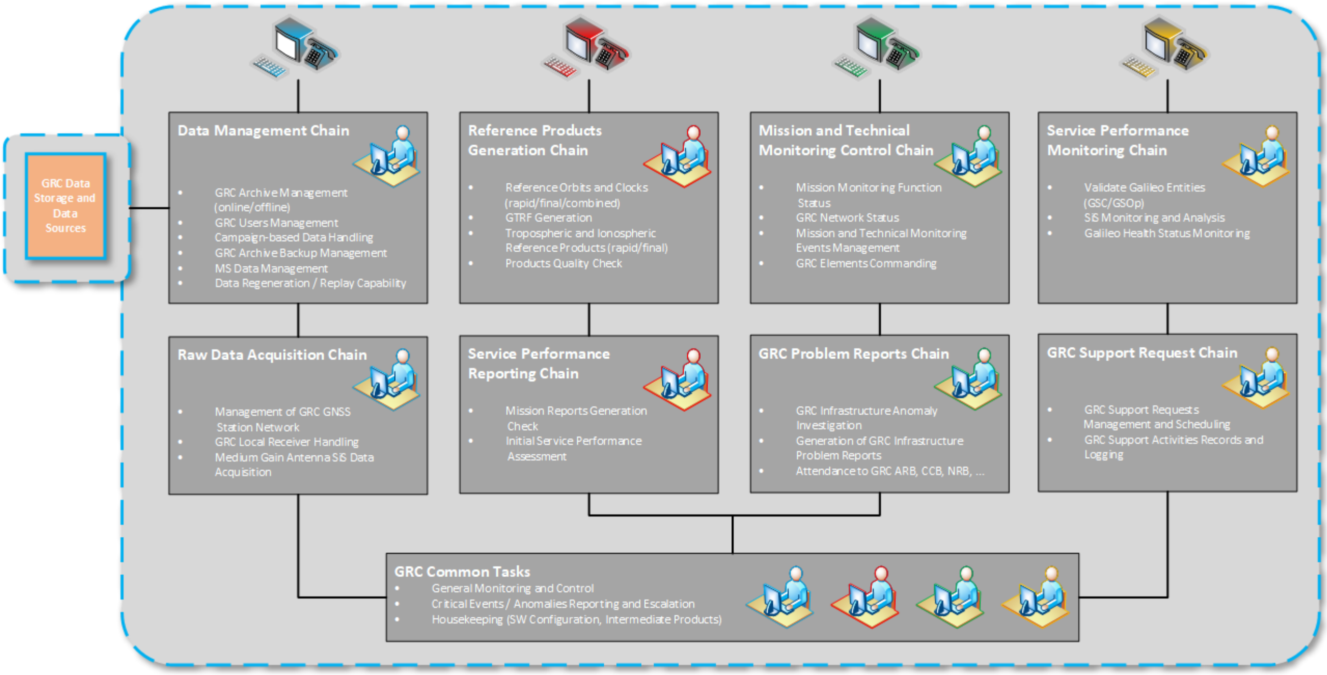

GRC Data Storage and Data Sources
Data Management Chain
GRC Archive Management (online/offline)
GRC Users Management
Campaign-based Data Handling
GRC Archive Backup Management
MS Data Management
Data Regeneration / Replay Capability
Reference Products Generation Chain
Reference Orbits and Clocks (rapid/final/combined)
GTRF Generation
Tropospheric and Ionospheric Reference Products (rapid/final)
Products Quality Check
Mission and Technical Monitoring Control Chain
Mission Monitoring Function Status
GRC Network Status
Mission and Technical Monitoring Events Management
GRC Elements Commanding
Service Performance Monitoring Chain
Validate Galileo Entities (GSC/GSOp)
SiS Monitoring and Analysis
Galileo Health Status Monitoring
Raw Data Acquisition Chain
Management of GRC GNSS Station Network
GRC Local Receiver Handling
Medium Gain Antenna SiS Data Acquisition
Service Performance Reporting Chain
Mission Reports Generation Check
Initial Service Performance Assessment
GRC Problem Reports Chain
GRC Infrastructure Anomaly Investigation
Generation of GRC Infrastructure Problem Reports
Attendance to GRC ARB, CCB, NRB, …
GRC Support Request Chain
GRC Support Requests Management and Scheduling
GRC Support Activities Records and Logging
GRC Common Tasks
General Monitoring and Control
Critical Events / Anomalies Reporting and Escalation
Housekeeping (SW Configuration, Intermediate Products)

Figure 15: GRC Nominal Operations - Routine Operations High-Level Breakdown

As an example, the high-level GSOp comparison and validation process is shown by Figure 16, which is the same approach for the Service Definition Document (SDD). In case of SDD, however, no external data source is available so the tool only computes the achievement of the KPI versus a target value. Electronic reports containing KPIs computed by the GSOp are stored in a KPI database that serves as the source for the comparison and validation. Any discrepancy found during the comparison is investigated and reported upon.

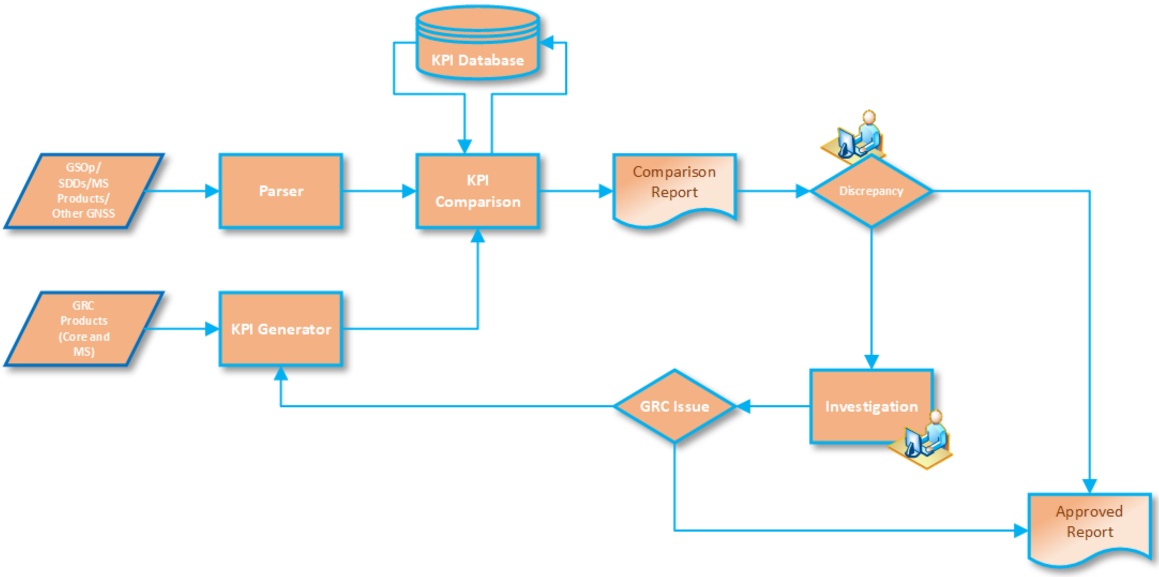


Figure 16: GRC Nominal Operations - GSOp/SDD Comparison High-Level Operational Approach

4.3.3.4 Operations Planning

In general, the operations planning is separated in three planning levels:

The ***Long-Term Plan (LTP)*** takes into account the Galileo Service roadmap and covers the operations for several months, typically updated on a monthly basis. The activities covered by this plan are the operations required to support the following Galileo System activities:

- Ground infrastructure and network deployments (e.g. GMS migration);
- In-flight spacecraft maintenance (e.g. SW patch uploads);
- Spacecraft launches and the In-Orbit Testing (IOT) schedule;
- Operation/experimentation/utilisation phases of the system requiring change of nominal system configurations;
- Events involving external entities for the coordination/deployment of the different services.

The ***Mid-Term Plan (MTP)*** is derived from the long term plan and covers operations during a sliding window of around one and a half months, typically being updated on a bi-weekly basis and comprises of tasks such as:

- Deployment of new GRC core infrastructure elements/releases;
- Galileo core infrastructure operations that requires specific monitoring by the GRC;
- Deployment of new/modified KPIs in the GRC.

The ***Short-Term Plan (STP)*** is subsequently derived from the mid-term plan and covers all tasks requiring execution until a new plan is generated following an update to the MTP, typically the STP is revisited on a weekly basis. This process takes into account the availability of the GRC operations team, the availability of the hardware and software resources, and availability of the GRC core infrastructure chains and networks. Usually the STP contains tasks such as:

- Routine operations to support the nominal functioning of the GRC;
- Tasks to support the activities of the mid-term plan;
- Any urgent task not scheduled in the mid-term plan.

A dedicated tool is available within the operational system to perform automated mission planning and it is used for the generation of the different levels of mission planning (LTP, MTP, STP). To assist in this process, the tool performs the following functions:

- Ticketing requests (from EUSPA);
- Automatic re-scheduling of the routine operations based on pre-agreed rules to face contingencies and urgent tickets;
- Manual task re-scheduling capability;
- Sequence of events generation considering the associated resources allocation.

4.3.3.5 Operations Procedures

The GRC V1 nominal operations are catalogued in a detailed set of procedures that act as the operations engineer's guideline for a proper operation of the GRC core infrastructure. All of the procedures start their life by undergoing an operational validation process prior to use on the GRC operational, the executions of which are documented in detail and reported on to the EUSPA. Following acceptance by the EUSPA, the procedure is authorised for activation in the GRC operational environment.

Software installed in the chains of the GRC core infrastructure is used for the writing and maintenance of the GRC Standard Operating Procedures (SOPs) and this also allows the GRC operations engineers to have access to the latest version of the procedures at any time. Both the UNCLA and CLA SOPs are managed in the GRC in the same manner, the UNCLA SOPs are accessible on the CLA platform but not vice-versa.

The general purpose of each Operating Procedure is:

- To document the way activities are to be performed so as to maintain the consistency with technical operations and to always perform operations in the same manner;
- To describe the analytical processes and processes for maintaining, calibrating and using the equipment;
- To maintain quality control and quality assurance;
- To be used as training tool as well as a guideline for performance evaluations;

Each SOP includes:

- A clear and concise statement on the purpose of the procedure;
- All necessary information to allow correct performance of the task described within the SOP, including any prerequisite and/or constraints;
- An accurate and detailed list of the equipment to be used;
- A section that provides its review and test status together with its current version;
- Detailed instructions and sequence of steps necessary to be executed by the operations engineer. For each step, the procedure provides any warning, caution, and notes to be taken into account by the operations engineer.
- Includes links and/or clear references to dependent procedures or task if it is not a standalone procedure;

4.3.4 Maintenance

In regards to the maintenance of the GRC V1, there are various aspects to be considered:

- Maintenance Classes,
- Maintenance Levels,
- Maintenance Environment,
- Problem Management,

- Operations Procedures Maintenance, and
- Obsolescence Management

4.3.4.1 Maintenance Classes

The GRC V1 maintenance concept is based on two maintenance classes:

Corrective Maintenance involves the reactive modification of a Hardware (HW) / Software SW product performed after delivery to solve discovered problems. It concerns the unscheduled maintenance actions, following failure recognition, to restore the product to a state in which it can perform its required function or a system to a specified condition. This maintenance class is focused on:

- HW Corrective Maintenance:
    - Replacement of faulty HW components,
    - Repair of faulty HW components.
- SW Emergency Corrective maintenance on-site;
- SW Corrective Maintenance from factory: fixing detected SW defects during the Software and during the Mission Operations:
    - Generate new SW versions,
    - Install new SW versions,
    - Integrate new SW versions.

Preventative Maintenance involves routine tasks to keep the GRC V1 systems functioning properly. Modification of a HW/SW product after delivery to solve latent faults before becoming effective faults. In particular, it concerns the scheduled maintenance actions performed to retain the product in an operational and serviceable condition. Typical preventative maintenance tasks include:

- Periodic inspections;
- Condition monitoring;
- Calibration;
- Trends calculation (Disk space, Memory usage);
- Non-destructive testing;
- Correcting deficiencies found through testing and inspections;
- Maintenance actions (back-ups, periodical purge of data, etc.).

4.3.4.2 Maintenance Levels

Maintenance levels are described for both HW and SW maintenance classes (corrective and preventative). All maintenance levels are provided by the GRC contractor determined by the nature of the maintenance required, considering task complexity, space requirement, skill level of assigned personnel, and scope of support responsibility. As a main rule and when possible, the maintenance of the GRC V1 is performed without stopping the mission monitoring functions and product generation, above all in the operational processing chain. The GRC V1 core infrastructure maintenance is divided into three maintenance levels:

The ***Level 1 (L1) Maintenance*** objective is to allow the product to remain operationally available, based on procedures not requesting any specific skills on the product. GRC V1 L1 Maintenance is performed on-site at the GRC by the Network and Operations Engineers and includes repairs and minor adjustments that do not require shop facilities nor removal and/or installation of components. As an example, the GRC V1 L1 Maintainer provides:

- Preventive/Corrective Maintenance within their capability,
- Non-conformance escalation,
- Redundancy activation,
- Replacement of units by spares,
    - Failed Line Replacement Units (LRUs) are then given to the L2/L3 Maintainer in order to follow the appropriate corrective actions.

The ***Level 2 (L2) Maintenance*** consists of in-depth fault analysis and troubleshooting requiring greater engineering support specific skills or tools and SW familiarity in order to determine the appropriate solution. The GRC V1 L2 maintenance is activated when actions are not within the capabilities of GRC V1 L1 Maintainer and normally the complexity of the tasks is higher. This implies a greater set of tools, test equipment, and personnel have undergone specific training (often with 2-5 years of experience in a service technician field) to perform the required maintenance tasks. Such activities can be performed either on-site at the GRC or in-factory at the Contractor premises, depending on the kind of problem and the necessary solution. As an example, the GRC V1 L2 Maintainer provides:

- Preventative/Corrective Maintenance beyond the capability of the L1 Maintainer;
- On-site or in-factory configuration or complex configuration;
- System repair by Shop Replaceable Unit (SRU) replacement:
    - Failed LRUs that cannot be repaired by the GRC V1 L2 Maintainer are then given to the GRC V1 L3 Maintainer in order to follow the appropriate corrective actions.
- Correction of non-conformances;
- Evolution maintenance;
- Replenishment of supplies/spares.

Concerning SW, support to the industrial manufacturer in charge of the production of the SW might be required in order to assess the origin of the SW problem, to help to the production of the corresponding problem, and later to request SW correction. In the case of Commercial off the Shelf (COTS) software it could imply re-installation of specific SW files corrupted or not working appropriately.

The ***Level 3 (L3) Maintenance*** consists of the performance of maintenance that cannot be effectively accomplished by either the GRC V1 L1 or L2 Maintainers. In general, it would be the result of requiring very specific knowledge of the product and the problems that could arise.

4.3.4.3 Maintenance Environment

The GRC V1 core infrastructure operational training, validation, and maintenance network provides the necessary support ability to aid in performing L1 and L2 on-site maintenance tasks. The maintenance environment is a mirror of the operational environment with the following particularities:

- Preventative/Corrective Maintenance beyond the capability of both the L1 and L2 Maintainers;
- The mission monitoring and analysis applications may either be limited to only those being tested or may be deployed in such a way that the number of deployed machines is optimised;
- Reduced monitoring display capabilities;
- The Storage is isolated from GRC data archive.

This provides an environment where the network GRC V1 L1 and L2 Maintainers test necessary fixes or perform diagnosis without any impact in the operational chain. The GRC V1 maintenance network assists with the following activities:

- Testing of new/repaired HW LRUs;
- Validation of new releases/patches;
- Investigations of anomalies and other problems in the GRC operational environment;
- Commissioning.

Once a new release has been installed and tested in the maintenance environment, a dedicated Operations Readiness Review meeting is held at the GRC to validate and agree its deployment in the operational environment.

4.3.4.4 Problem Management

In order to ensure the GRC V1 core infrastructure remains operational while managing the configuration, a problem management process is implemented at the GRC. Every issue detected during the operation of the GRC is reported by the operations team as an Observation Report (OR) and following a detailed analysis by the operations or support team, the issue is further categorised according to the following list:

- Anomaly Report (AR);
- Non-Conformance Report (NCR);
- Software Problem Report (SPR); or
- Operations Procedure Update (OPU).

Some issues are not direct software or hardware problems but may include, for example, some minor ‘nice-to-have’ elements or some reformatting of a reporting structure, in this instance they are raised as:

- Request for Enhancement (RFE) (improvements).

Starting from the raised Observation Reports and following the cycle through the categorisation via Internal Process, Configuration and Anomaly Review Board, Internal and External Change Control Boards and Non-Conformance Review Board; Figure 18 shows each of the various cycles of an Observation Report (OR). An on-site tool at the GRC is used for the reporting and tracking of all ORs detected during the operations of the system. All anomalies (taken to mean ARs, SPRs, and NCRs) are classified based on their impact, or potential impact, on system operations or service delivery in accordance with Table 3.

The classification of all anomalies is subject to review and ultimate approval by the EUSPA at the Configuration and Anomaly Review Board. Furthermore, the outputs of this process serve to act as inputs to the overall maintenance concept.

Anomaly Categorisation:	
Category	**Classification Criteria**
CAT-1	Anomalies having a severe, or persistent, detrimental impact on any of the following: • The provision of the GRC operations or reporting capabilities (e.g. substantive failure to fulfil GRC service and reporting requirements); • The availability of the key components of the operational infrastructure (e.g. GRC Infrastructure, Networks, etc.);
CAT-2	Anomalies having a detrimental impact on any of the following: • The provision of the GRC operations or reporting capabilities (e.g. marginal failure to fulfil GRC service and reporting requirements); • The redundancy levels within key components of the operational infrastructure (e.g. redundancy within the GRC Infrastructure, Networks, etc.); • Ability to operate and maintain the GRC Infrastructure.
CAT-3	Anomalies having a potential detrimental impact on any of the following: • The provision of the GRC operations or reporting capabilities (e.g. failure to fulfil GRC service requirements); • The redundancy of the operational GRC infrastructure; • The operations and maintenance of the GRC Infrastructure.
CAT-4	All other anomalies not falling within CAT-1 to CAT-3

Table 3: GRC Problem Management - Anomaly Categorisation

In order to better understand the details of Figure 18, Figure 17 is provided to act as a key and Table 4 provides a definition of terms.

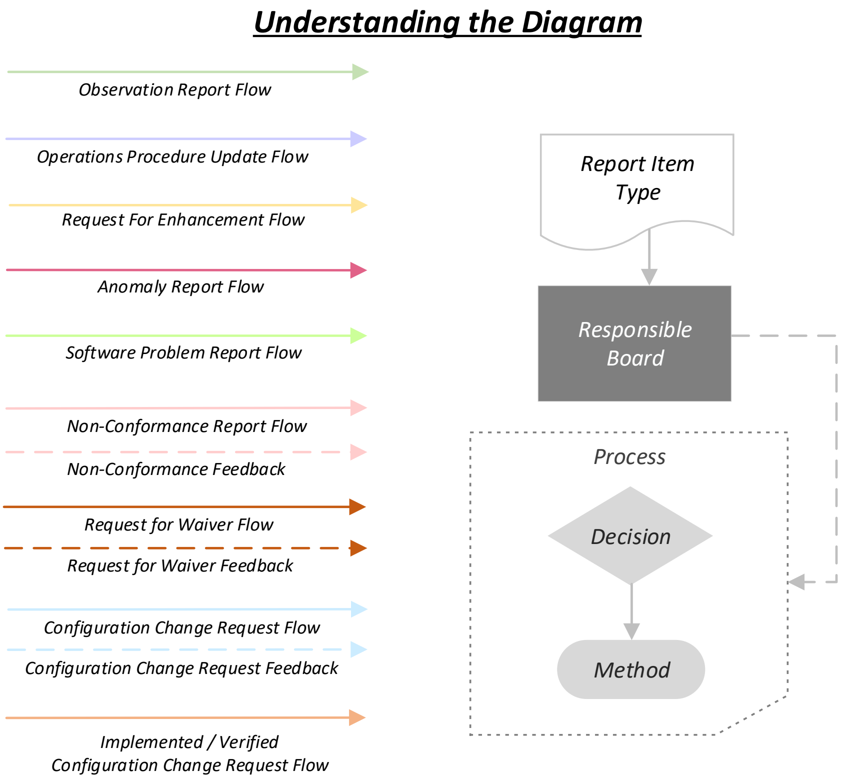

Understanding the Diagram
Observation Report Flow
Operations Procedure Update Flow
Request For Enhancement Flow
Anomaly Report Flow
Software Problem Report Flow
Non-Conformance Report Flow
Non-Conformance Feedback
Request for Waiver Flow
Request for Waiver Feedback
Configuration Change Request Flow
Configuration Change Request Feedback
Implemented / Verified Configuration Change Request Flow
Report Item Type
Responsible Board
Process
Decision
Method

Figure 17: GRC Problem Management - Key for Figure 18

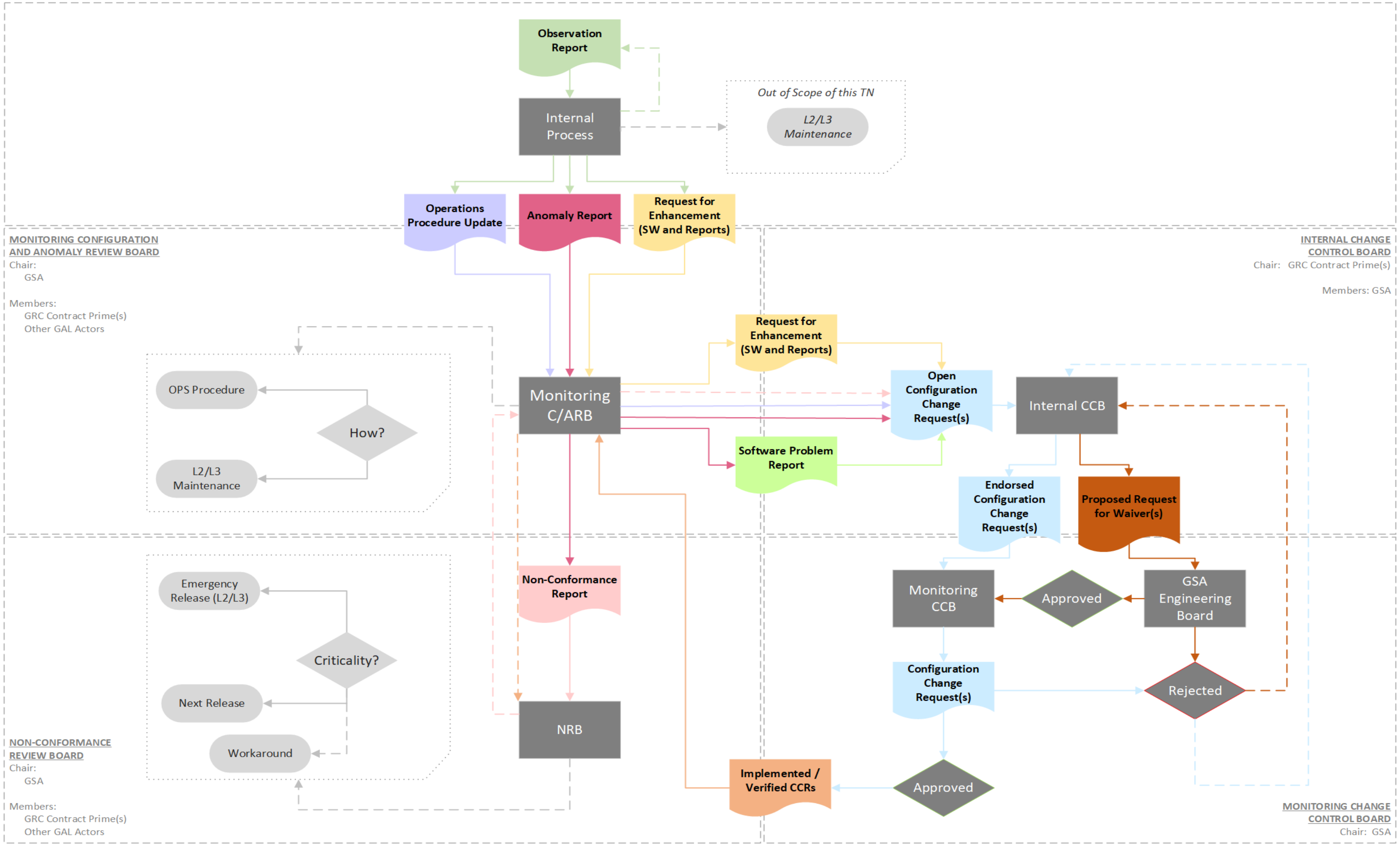

Observation Report
Internal Process
Out of Scope of this TN
L2/L3 Maintenance
Operations Procedure Update
Anomaly Report
Request for Enhancement (SW and Reports)
MONITORING CONFIGURATION AND ANOMALY REVIEW BOARD
Chair:
GSA
Members:
GRC Contract Prime(s)
Other GAL Actors
INTERNAL CHANGE CONTROL BOARD
Chair: GRC Contract Prime(s)
Members: GSA
OPS Procedure
How?
L2/L3 Maintenance
Monitoring C/ARB
Request for Enhancement (SW and Reports)
Open Configuration Change Request(s)
Internal CCB
Software Problem Report
Endorsed Configuration Change Request(s)
Proposed Request for Waiver(s)
Emergency Release (L2/L3)
Criticality?
Next Release
Workaround
Non-Conformance Report
NRB
Monitoring CCB
Approved
GSA Engineering Board
Configuration Change Request(s)
Rejected
Implemented / Verified CCRs
Approved
NON-CONFORMANCE REVIEW BOARD
Chair:
GSA
Members:
GRC Contract Prime(s)
Other GAL Actors
MONITORING CHANGE CONTROL BOARD
Chair: GSA

Figure 18: GRC Problem Management - Process Overview

Problem Management Terminology Definitions:		
Acronym	**Definition**	**Description**
OR	Observation Report	All problems or observations are initially raised as Observation Reports (ORs) before being categorised during the contractor internal process. ORs can be raised by either the contractor or the contracting authority.
Internal Process	Internal Process	The internal process is managed by the contractor. All observation reports are first screened in the internal process. In case of doubts or any uncertainties, the contractor can request additional clarification on an issue. Once all necessary information is obtained, the internal process performs an initial categorisation on each observation report to decide if it is an anomaly report, request for enhancement, or operations procedure update. This information is then taken to the C/ARB for final categorisation and agreement.
AR	Anomaly Report	After categorisation of Observation Reports (ORs) during the internal process, some items are categorised as Anomaly Reports (ARs) to be discussed in the scope of the Configuration and Anomaly Review Board (C/ARB). ARs become either a NCR or SPR. Any ARs that have not been reclassified as a SPR or NCR are assumed to be hardware or hosting service related incidents affecting the service or infrastructure. These shall remain as ARs.
OPU	Operations Procedure Update	An Operations Procedure Update is: • a change to an operations procedure under configuration control; or, • the introductions or removal of a new or existing procedure, respectively. Each OPU has its own priority that will be defined at the C/ARB.
RFE	Request for Enhancement	After categorisation of Observation Reports (ORs) during the internal process, some items are categorised as Request for Enhancements (RFEs) to be discussed in the scope of the Configuration and Anomaly Review Board (ARB). In this context, RFEs mean the request to perform minor configuration changes or minor enhancements to the software, the GRC report templates or GRC technical documentation in case of misalignment with the operational software. Each RFE has its own priority that will be defined at the C/ARB
C/ARB	Configuration/Anomaly Review Board	The C/ARB is the Configuration and Anomaly Review Board.

Problem Management Terminology Definitions:		
Acronym	**Definition**	**Description**
NCR	Non-Conformance Report	During the process of categorisation of the Anomaly Reports (ARs) by the Configuration and Anomaly Review Board (C/ARB), anomalies affecting a customer requirement are further categorised as Non-Conformance Reports (NCRs) to be discussed in the scope of the Non-Conformance Review Board (NRB).
NRB	Non-Conformance Review Board	The Non-Conformance Review Board (NRB) is responsible for categorising the non-conformances in terms of criticality and assigning the timeline by which each must be fixed.
SPR	Software Problem Report	After categorisation of Anomaly Reports (ARs) during the Configuration and Anomaly Review Board (C/ARB), some items are categorised as Software Problem Reports (SPRs) which are then further discussed in the scope of the Configuration and Anomaly Review Board (C/ARB) before being forwarded for including in a change request to be managed by the contractor. A software problem report is an anomaly that is not directly impacting on a GRC customer requirement. The main scope of a SPR is a software issue that is impacting the functionality of the GRC without directly impeding on service provision, it may be impacting on a software requirement, feature, or function that is not linked to a customer requirement.
CCR	Configuration Change Request	A Configuration Change Request (CCR) is a collection of changes required to fix or implement relevant ARs, SPRs, NCRs, RFEs, or OPU under configuration. The collection may contain all the current pending issues or a reduced subset of these. Multiple CCRs can be raised, discussed, and ultimately endorsed simultaneously at the contractor Internal CCB. Once a change request is indorsed internally it is flown to the Contracting Authority for approval prior to implementation. Each CCR must detail: • the details of all items (ARs, NCRs, SPRs, RFEs, OPUs, and RFWs) it might contain. • The set of the tests to be executed in an appropriate validation environment for each item. • a set of regression tests to be performed on the operational system to ensure correct application of a fix. • a roll-back plan in event of detrimental impact to the operational system.

Problem Management Terminology Definitions:		
Acronym	**Definition**	**Description**
		• the security impact of each of the elements contained in the CCR.
CCB	Change Control Board	In the scope of this process there are two Change Control Boards (CCBs), each with different functions: 1. Internal CCB: In the case of the GRC, this Internal CCB is chaired by the Contractor. The contracting Authority shall be invited to participate if an item (AR, SPR, NCR, OPU, RFE) raised by them is under discussion or if inputs for any other topics of discussion is requested. The primary focus of this CCB is to analyse and endorse (or reject) CCRs. Any endorsed CCRs are then flown to the Contracting Authority for approval. 2. Monitoring CCB: This CCB is chaired by the Contracting Authority and has the primary purpose for approving or rejecting CCRs endorsed by the contractor at the contractor internal CCB. Any approved CCRs are provided the authorisation to implement and once implemented the verification results must be presented at the next C/ARB to close the items contained within that CCR. If a CCR is rejected for implementation, the Contracting Authority shall notify the contractor via the minutes of meeting distributed after the CCB that further work or evidence is required before the CCR can be approved for implementation.
RFW	Request for Waiver	Any problem affecting a Customer Requirement which has arisen and cannot be resolved is subject to a Request for Waiver (RFW). Each RFW should be presented with the problem, the requirement affected, the proposed way forward, duration, and other relevant information. A RFW can be permanent or temporary and all are subject to approval by the Contracting Authority.
-	Emergency Fix	An Emergency Fix (or Emergency Workaround) is fix (workaround) to an anomaly requiring immediate attention so as to prevent imminent operations or service degradation or failure. The workaround must be implemented in the time indicated within this document. The permanent correction may be handled by the nominal process described within this document, but exceptional circumstances force the need for an ad-hoc C/ARB.

Table 4: GRC Problem Management - Process Definitions

4.3.4.5 Operational Procedure Maintenance

Any issues detected within the GRC V1 operations procedures are managed by the process highlighted in Section 4.3.4.4 so as to ensure configuration control.

4.3.4.6 Obsolescence and Integrated Logistics Services

The GRC V1 core infrastructure implements an Obsolescence strategy and Integrated Logistics Services management process so as to support the maintenance concept and ensure the operability of the system. Outputs from the Obsolescence strategy act as inputs to the maintenance and outputs of the maintenance feed into the overall ILS approach for elements such as on-site spares and replacement of LRUs.

4.3.5 GRC V1

The first fully fledged version of the GRC, referred to below as the GRC V1, is currently in operation and it provides the contributions of the core infrastructure that have been procured under the first Framework Contract (FWC) for the GRC Development, Operations Support, and Hosting Services. Furthermore, it has undergone several evolutions throughout the execution of the FWC to include new functionality. Table 5 provides a summary of the GRC V1 updates over time.

Operational	Scope
Q4 2018	***GRC Core Infrastructure and Operations*** • OS Monitoring ○ Utilisation of TGVF GESS Stations and/or procedures with other GRC reference stations ○ Ranging Accuracy KPIs ○ Positioning Accuracy KPIs (at GRC/GESS) ○ Timing Accuracy (UTC/GGTO) ○ SiS Monitoring (SiS ICD compliance, etc) ○ Monitoring of GPS • Provision of Performance Expertise for EUSPA, EC, and MS • Establishment and Maintaining of Long term Archive of Service Performance Data • Integration and Steering of MS Assets • Secondary objectives: ○ Multi-GNSS benchmarking ○ GNSS intersystem interference, interoperability and compatibility monitoring ○ Support to Service Performance Investigations

Operational	Scope
	Secondary Infrastructure and Activities • Coordination of activities with ICG, IGS, EUROCONTROL, EASA.
Q2 2020	***GRC Core Infrastructure and Operations*** • Multi-GNSS Monitoring ○ Addition of BeiDou and GLONASS constellations
	Secondary Infrastructure and Activities • Prototype Quasi-Real-time monitoring at GRC
Q4 2020	***GRC Core Infrastructure and Operations*** • Interface to GRSP • Provide Performance Expertise for GSC
	Secondary Infrastructure and Activities • Coordination of activities with IGS, EUREF, etc. • Initial OS-NMA monitoring at GRC ○ Live test Q4 2020
Q2 2021	***GRC Core Infrastructure and Operations*** • HAS Initial Service Monitoring Infrastructure Capabilities (HAS Phase I) • HAS Validation and Operational Support • OS Representative Receivers (Phase I)
	Secondary Infrastructure and Activities • Support to OS FOC Preparation • Computing the ‘As-Design’ Metric • Initial Quasi-Real-Time Monitoring Implementation

Operational	Scope
Q2 2022 *(Target)*	***GRC Core Infrastructure and Operations*** • HAS Initial Service Monitoring Phase (HAS Phase I service declaration planned for Q2 2022) • Interface with TSP • PRS Navigation Monitoring • Provide Performance Expertise for GSMC • Standalone SiS Analysis Capability with Medium Gain Antenna
	Secondary Infrastructure and Activities • eMONITOR operations from GRC
Q4 2022 *(Target)*	***GRC Core Infrastructure and Operations*** • Enhanced OS Monitoring Capability • OS Representative Receivers (Phase II) • Monitoring of SoL and ARAIM • Monitoring of Initial set of Aviation KPIs ○ Based on EASA and EUROCONTROL inputs
	Secondary Infrastructure and Activities • EUSPA Downstream Platform • Prototyping of Precise Reference Time at the GRC

Table 5: GRC Infrastructure - V1 Release Overview

4.4 Current Contractual Situation and Establishment of Fair Competition Conditions

GRC core infrastructure releases covering the contributions to the GRC V1 releases have been contracted to GMV.

At the time of the GRC V2 kick off, it is expected to have completed the entry into operation of the elements identified in Table 5, Section 4.3.5.

Appropriate measures will be implemented throughout the procurement procedure in order to establish level playing field and fair competition conditions for all Candidates. For indicative purposes only such measures include, without limitation to:

a. a clear description of the GRC Infrastructure, Operation, and Maintenance and the stakeholders involved in all phases, Section 4.3;

b. information on the current contractual situation (i.e. scope of activities procured under the previous FWC), to be provided in Phase II (see Section 2.2.10 of Annex I of the Invitation to Participate (Tender Specifications);

c. information about the current Galileo Services provision (necessary to understand for monitoring);

d. due diligence organised across all phases of the procurement procedure, as further defined in the Tender Specifications.

4.5 EUSPA Needs and Objectives Related to the Present Procurement

It is to be noted that the European GNSS Programme management will evolve over the time, therefore this entire section shall be understood **as high level provisional information in the EUSPA needs and objectives concerning the evolutions of the GRC Infrastructure, Nominal Operations Support, and Maintenance**. To the extent and within the limits compatible with the applicable procurement rules, the Contracting Authority reserves the right to further specify and modify the elements contained in this section of the Descriptive Document, during the course and as a result of the competitive dialogue.

4.5.1 Elements of the GRC Roadmap

The evolutions of the GRC core infrastructure and its Operations will be mainly triggered by:

i. Evolutions of Existing Galileo Services and Implementation of New Galileo Services;

ii. Evolution of Existing Services from Other GNSS Constellations (GPS, GLONASS, BeiDou);

iii. Monitoring of and Compatibility with Regional Systems (EGNOS, IRNSS, QZSS, …);

iv. Enhanced Security Requirements and Improvements (cyber/accreditation);

v. GRC core infrastructure system improvements (e.g. real-time monitoring, integration of infrastructure from other procurements, enhanced receiver representativeness, GNSS RF simulation, …) ;

vi. Evolution of GRC Interfaces (internal and those to external entities);

vii. Support to User Domains (Aviation, Rail, Maritime, …).

4.5.1.1 Evolution of Existing / Implementation of New Galileo Services

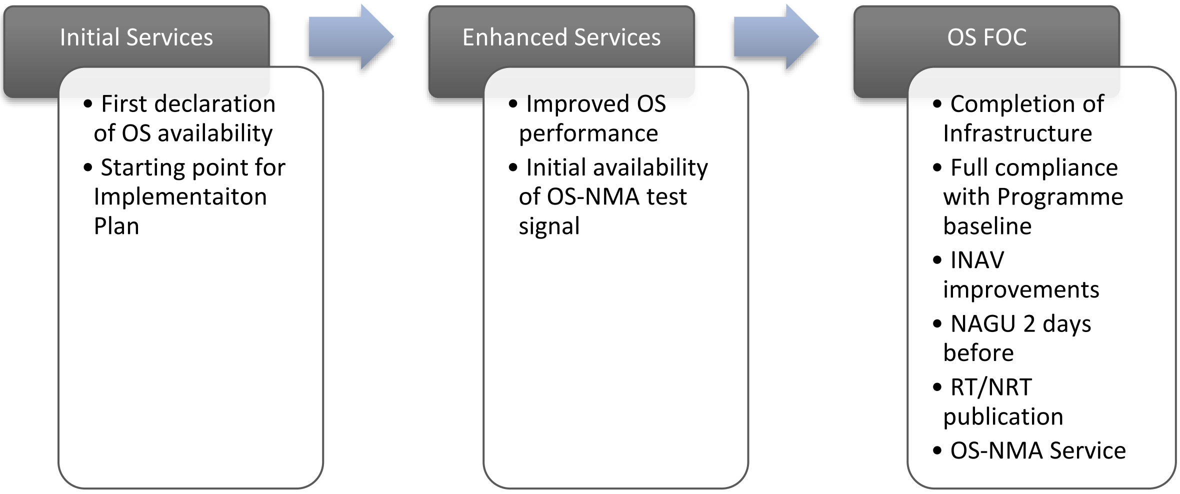
The independent monitoring of the Galileo Services by the GRC, will include the following Galileo service implementations among the main drivers for the forthcoming releases to be procured:

- ***Open Service (OS)*** Enhancements;
- ***Open Service Navigation Message Authentication (OS-NMA)*** Full Implementation and Enhancements;
- ***High Accuracy Service (HAS)*** Full Implementation and Enhancements;

- ***Commercial Authentication Service (CAS)*** Initial and Full Implementation;
- ***Public Regulated Service (PRS)*** Enhancements;
- ***Safety of Life (SoL)*** / ***Advanced Receiver Autonomous Integrity Monitoring (ARAIM)*** / ***Integrity Service Message (ISM)*** Full Implementation and Enhancements;
- ***Early Warning Service (EWS)*** Initial and Full Implementation;
- ***Search and Rescue Service (SAR)*** Initial and Full Implementation;
    - Including Remote Beacon Activation;
- ***Beacon Command Service (BCS)*** Initial and Full Implementation;
- ***Performance Prediction Service (PPS)***;
- ***Ionospheric Prediction Capability (IPC)*** Initial and Full Implementation,
    - Including provision of inputs to the IPC;
- ***Timing Service (TS)*** Implementation.

4.5.1.1.1 Galileo OS/OS-NMA

The following high-level Galileo OS/OS-NMA milestones cover the implementation of the OS/OS-NMA evolutions for which the GRC needs to fulfil specific requirements and functions to enable the independent monitoring capability:


Initial Services

- First declaration of OS availability
- Starting point for Implementaiton Plan

Enhanced Services

- Improved OS performance
- Initial availability of OS-NMA test signal

OS FOC

- Completion of Infrastructure
- Full compliance with Programme baseline
- INAV improvements
- NAGU 2 days before
- RT/NRT publication
- OS-NMA Service

Figure 19: Galileo OS/OS-NMA - High-Level Service Milestones

4.5.1.1.2 Galileo HAS

The following high-level Galileo HAS milestones cover the implementation of the HAS service for which the GRC needs to fulfil specific requirements and functions to enable the independent monitoring capability:

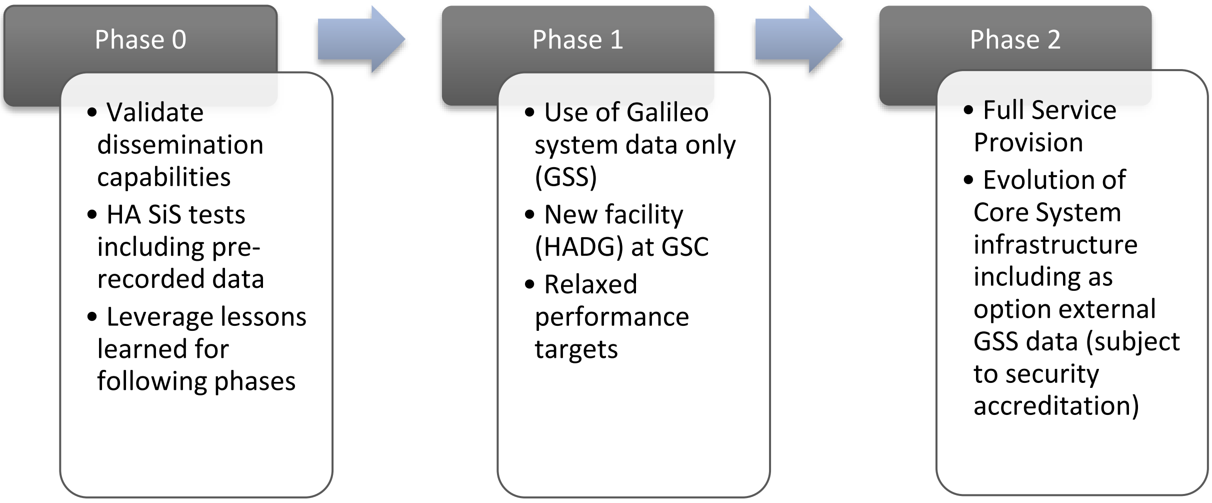

Phase 0
• Validate dissemination capabilities
• HA SiS tests including pre-recorded data
• Leverage lessons learned for following phases
Phase 1
• Use of Galileo system data only (GSS)
• New facility (HADG) at GSC
• Relaxed performance targets
Phase 2
• Full Service Provision
• Evolution of Core System infrastructure including as option external GSS data (subject to security accreditation)

Figure 20: Galileo HAS - High-Level Service Milestones

4.5.1.1.3 Galileo CAS

The following high-level Galileo CAS milestones cover the implementation of the CAS service for which the GRC needs to fulfil specific requirements and functions to enable the independent monitoring capability:

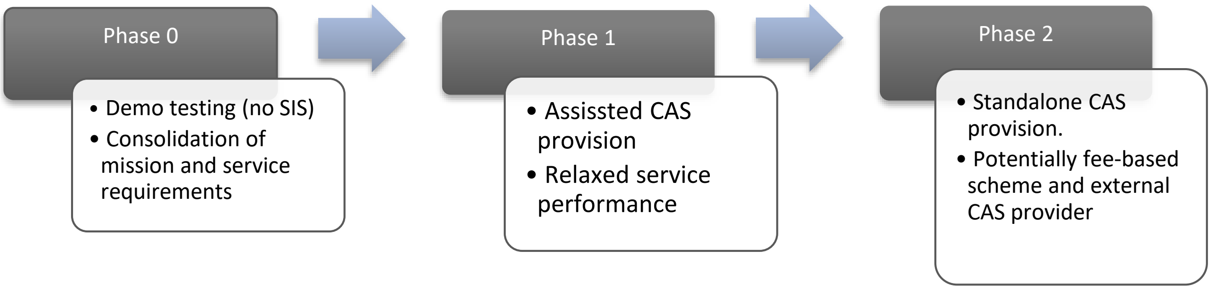

Phase 0
• Demo testing (no SIS)
• Consolidation of mission and service requirements
Phase 1
• Assissted CAS provision
• Relaxed service performance
Phase 2
• Standalone CAS provision.
• Potentially fee-based scheme and external CAS provider

Figure 21: Galileo CAS - High-Level Service Milestones

4.5.1.1.4 Galileo PRS

The following high-level Galileo PRS milestones cover the implementation of the PRS evolutions for which the GRC needs to fulfil specific requirements and functions to enable the independent monitoring capability of the PRS navigational and timing services:

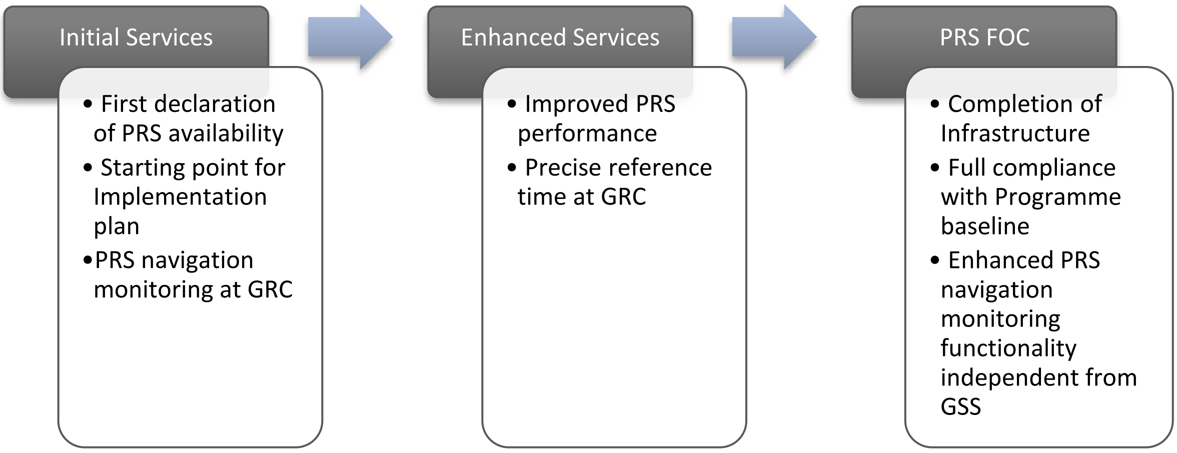

Initial Services
• First declaration of PRS availability
• Starting point for Implementation plan
•PRS navigation monitoring at GRC
Enhanced Services
• Improved PRS performance
• Precise reference time at GRC
PRS FOC
• Completion of Infrastructure
• Full compliance with Programme baseline
• Enhanced PRS navigation monitoring functionality independent from GSS

Figure 22: Galileo PRS - High-Level Service Milestones

4.5.1.1.5 Galileo SoL/ARAIM/ISM

There is an agreement at Galileo Programme level on the development of a Safety of Life Workplan (GOSOL) to support the use of Galileo Open Service in Safety of Life applications, such as EGNOS V3 or H-ARAIM. The main objective is that aviation stakeholders can safely use Galileo for navigation.

ARAIM concept has been developed under the current bilateral US – EU Agreement on GPS/Galileo Cooperation as an evolution of the current RAIM, which is based on GPS Single Frequency signals. Work is ongoing at ICAO for the standardisation of the concept. A key feature of ARAIM is the Integrity Support Message (ISM). The ISM includes information about GNSS constellations and satellites that the receiver requires in order to provide integrity to the user. The parameters are applied by the airborne GNSS Receiver to compute the ARAIM solution, ensuring the adequate level of safety.

According to the work developed in the frame of GOSOL, together with other EC related activities, Galileo ISM will be generated at the ground level based on the outcomes from Galileo SIS continuous monitoring. Galileo ISM message might be generated by an external entity out of Galileo System – this point is currently under investigation. Galileo ISM will be provided to the airborne fleet through the navigation information of Galileo OS signals. Such dissemination scheme enables a worldwide applicability of Galileo ISM information. The definition of Galileo ISM message will be part of Galileo OS ICD – ESA is currently working on a proposal for Galileo ISM ICD.

A technical solution shall be developed for full independent monitoring of this service by the GRC.

4.5.1.1.6 Galileo EWS

A new component, the Emergency Warning Processing Component (EWPC), dedicated to the provision of the Emergency Warning Service (EWS) shall be developed and implemented to allow authorised users to transmit Emergency Warning Messages (EWM) via the Galileo SiS to end-users within pre-defined authorised geographical areas.

The Emergency Warning Processing Component shall:

- provide an interface for accredited users, i.e. Emergency Warning Service Providers (EWSP), to launch specific service requests, to receive acknowledgements and feedback and to update user related information,
- host a database for user related information (including user contacts, EWSP IDs, country IDs and authorised geographical areas),
- validate service requests, and
- generate commands for distribution to other entities of the Galileo ground segment, including to the GMS.

A technical solution shall be developed for independent monitoring of this service by the GRC. As a minimum the GRC shall monitor not only the contribution due to Galileo (including the KPIs on Galileo SLA towards Galileo EWSP) but, if needed, the contribution due to a multi-GNSS system.

4.5.1.1.7 Galileo SAR/BCS

The ***Galileo SAR Service*** will in involve evolutions to make available to the SAR server community the orbital data received from the Galileo core infrastructure (computed at GCS and GMS) though the GMS-GSC ICD. The monitoring of the provision of SAR service will require implementation within the GRC core infrastructure.

Galileo SAR Beacon Command Service (BCS) Server: For the Galileo SAR Return Link Service it is foreseen to introduce a Beacon Command Service, in addition to the already implemented Acknowledgment Service. The Beacon Command Service is a function of the Return Link Service able to send commands via Return Link Messages (RLM) to Emergency Locator Transmitter (ELT) beacons to perform specific actions.

In a first step, these commands shall enable a Remote Activation (RCA)/Deactivation Service to remotely activate/deactivate beacon transmission of distress alert messages upon request as well as a Remote Triggering of Self-Test of the beacon. In the future, Enhanced Beacon Command Services such as Two-Way Communications (TWC) and Distress Position Sharing (DPS) shall be developed.

For the first step, the SAR Beacon Command Server shall:

- provide an interface for accredited users to launch specific service requests, to receive acknowledgements and feedback and to update user related information,
- host a database for user related information (including user contacts and beacon IDs),
- validate service requests, and
- generate commands for distribution to other entities of the Galileo ground segment (for example RLSP and potentially including the GMS).

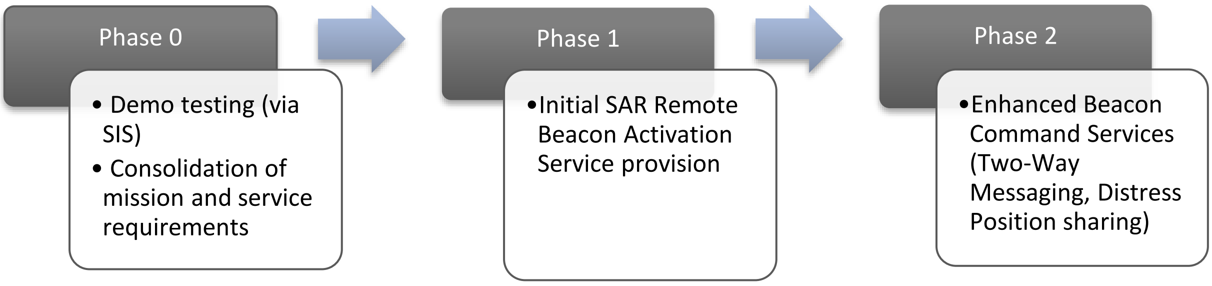

Phase 0
• Demo testing (via SIS)
• Consolidation of mission and service requirements
Phase 1
•Initial SAR Remote Beacon Activation Service provision
Phase 2
•Enhanced Beacon Command Services (Two-Way Messaging, Distress Position sharing)

Figure 23:Galileo SAR/BCS - High-Level Service Milestones

4.5.1.1.8 Galileo PPS

The Galileo PPS will generate performance predictions based on external sensor data. The predictions shall have with a minimum forecast horizon of 24 hours. A technical solution shall be developed for independent monitoring of this services by the GRC.

4.5.1.1.9 Galileo IPC

The IPC will provide ionospheric status and predictions based on external sensor data. The predictions shall have with a minimum forecast horizon of 24 hours. A technical solution shall be developed for independent monitoring of this services by the GRC.

4.5.1.1.10 Galileo TS

The GSC will act as the channel to offer ad-hoc timing data to users (beyond the information contained in the SiS). A technical solution shall be developed for independent monitoring of this services by the GRC.

4.5.1.2 Evolution of Existing Services from Other GNSS Constellations

The GRC currently monitors the open services of GPS, GLONASS, and BeiDou and it is important to maintain representativeness with the evolutions of these services from the other GNSS constellations throughout the evolution of the GRC core infrastructure.

4.5.1.3 Monitoring and Compatibility with Regional Systems

The GRC will implement a technical solution for the monitoring of EGNOS/SBAS service provision, as well as assess compatibility with and monitoring possibilities of other regional systems (i.e. QZSS and IRNSS), mainly those SBAS systems whose signal in space can be received and potentially used in EU airspace.

4.5.1.3.1 Independent Monitoring of EGNOS at the GRC

Using existing reference data available at the GRC, which includes:

- Raw and processed data for GNSS (e.g. ionospheric data and GPS/Galileo/SBAS GEOs constellation data);
- MS contributions, which will include EGNOS monitoring paramaters as part of a combined Galileo / EGNOS Framework Partnership Agreement (FPA) during the duration of this procurement;
- EGNOS system data delivered by EDAS service facilities (EDAS server, SDAF).

Along with existing infrastructure, such as the network of stations, the GRC, in-line with Section 3.3.3, shall perform the following activities:

- SBAS Navigation quasi-real-time performance monitoring,
- EGNOS OS and SoL services quasi-real-time performance monitoring (service coverage availability),
- EGNOS and SBAS long-term statistics on integrity and continuity safety margins,
- EGNOS RIMS Data Availability and Quality Monitoring,
- EDAS Service Availability and Quality Monitoring,
- GPS Flex Power analysis,

Any gaps in the required reference data or infrastructure, needed for this processing capability at the GRC, should be identified and proposed as part of this procurement.

Such independent monitoring shall be used for EUSPA internal purposes and made available on-line only to EUSPA authorised users (including for quasi-real-time performance monitoring).

4.5.1.4 Enhanced Security Requirements and Improvements

The GRC core infrastructure has to comply with the Galileo programme security baseline, which is updated on a regular basis. For the evolutions of the GRC, this implies:

Full implementation of the applicable ***EUSPA Cyber Requirements*** and their continued maintenance through the GRC evolutions procured in the frame of the present procedure, in line with the EUSPA Cyber implementation plan.

A new cyber ***Security Monitoring (SECMON)*** infrastructure is being established and includes dedicated enclaves at the Galileo Service Facilities. The GRC core infrastructure evolutions shall be compliant with the SECMON enclave needs, in line with the EUSPA Cyber implementation plan.

A tailored version of the new ***Programme Security Classification Guide (SCG)*** (v4.3.1) is planned to be made applicable from the GRC V2.0 onwards. At the same time the security capability of the GRC site is planned to be elevated to C-UE/EU-C.

4.5.1.5 GRC Core Infrastructure System Improvements

The following GRC improvements have been identified and it is the intention to procure these capabilities with the GRC V2 core infrastructure:

- ***Precise Reference Time at GRC***: the core infrastructure shall compute and include a precise GRC reference time.

- Implementation of ***Real-Time Interfaces*** to necessary external entities. This will also facilitate better dissemination of Timing and Reference Products (raw and processed data) to the user communities.
- Full ***Real-Time Monitoring*** will be implemented at the GRC so as to better execute the overall mission of the facility.
- With the inclusion of real-time interfaces and the ability to perform real-time operations, it is identified that utilising real-time data form the GRC archive in the ***Validation Platform*** would be required so as to perform operation validation of the new releases before deployment onto the GRC operational platform.
- ***Monitoring / reporting improvements*** at operations and infrastructure level.
- ***Archiving of PRS data at EUSPA and GSMC.***
- ***GRC Disaster Recovery*** will include the complete definition of the disaster recovery and its subsequent implementation to ensure the mission and business continuity of the GRC.

4.5.1.6 Evolution of GRC Interfaces

The GRC core infrastructure will be expected to implement any required new non-real-time interfaces as well as perform the maintenance and evolutions on these new interfaces as well as those that currently exist. Additionally, the GRC core infrastructure currently has no real-time interfaces with any external entity. During the execution of the present FWC, it is anticipated that the GRC core infrastructure will implement all necessary real-time interfaces with the following external entities:

- GSC,
- External data providers (e.g. data streams from MS),
- GSMC.

4.5.1.7 Support to User Domains

The GRC shall be able to monitor and report on the required KPIs/FoMs that the following user domains are most interested in:

- Aviation (EASA / EUROCONTROL);
- Maritime (EMSA);
- Rail (ERA).

In doing so, the GRC will provide expert support to these domains on the use of Galileo for their purposes.

In addition, the GRC will be in a position to provide receiver certification technical support capabilities that would be applicable to these domains.

4.5.2 GRC V2

The GRC V2 core infrastructure is envisaged to be the first major GRC evolution to be procured under the present FWC. Furthermore, it is expected that other major GRC core infrastructure contributions will be procured under this new framework contract (GRC V2.1, GRC, V2.2, …). The first high-level definition of the releases following GRC V2 (e.g. GRC V2.1, V2.2, …) are defined in the table below and will be defined further during execution of the FWC and in accordance with Programme needs.

4.5.2.1 GRC V2 Indicative Scope

Table 6 provides an indicative scope of the GRC V2 releases.

GRC Version	Operational	Scope
GRC V2.0	Q4 2023 *(Target)*	***GRC Core Infrastructure and Operations Evolutions*** • OS Monitoring Enhancements • OS-NMA Monitoring • HAS Phase II Monitoring • Initial CAS Monitoring • PRS Monitoring • Precise Reference Time at GRC • Enhanced Early Warning Service Monitoring • Initial SAR/BCS monitoring • Initial IPC Monitoring and Contribution • Initial GNSS Performance Prediction Service Monitoring • Initial EGNOS/SBAS Monitoring • Enhanced Support to Aviation ○ Including SoL and ARAIM • Implement Real-Time (RT) Interfaces at GRC • EUSPA Cyber Security Implementation and RT Connection with GSMC • Initial Real-Time Monitoring • Real-Time Interface Implementation ○ Including GSC, GSMC, …. • Full Implementation of EUSPA Cyber Requirements • SECMON • Dissemination of Time and Geodetic References Products (raw and processed data) to User Communities
		Possible Additions to the Scope • Support to Rail and Maritime • 24/7 Operations

GRC Version	Operational	Scope
GRC V2.x	Yearly Evolutions Targeted	***<u>GRC Core Infrastructure and Operations Evolutions</u>*** • Full OS-NMA Monitoring • Full CAS Monitoring • Integration of eMONITOR Data into IPC • Full RT monitoring • Support to Rail and Maritime (if not included in GRC V2.0) • 24/7 Operations (if not included in GRC V2.0) ***<u>Continuous Evolutions of Existing Monitoring Functionality</u>*** • OS, OS-NMA, HAS, CAS, PRS, External interfaces (TSP, GRSP, GSC, MS, …), EWS, IPC, GNSS Prediction, SAR/BCS, SoL/ARAIM, EGNOS/SBAS, MultiGNSS, Real-Time functionality.

Table 6: GRC Core Infrastructure - V2 Indicative Scope

Following the above indicative scope, the set of platforms to be accepted at the end of the GRC V2.0 core infrastructure release specific contract will be the following:

- Assembly, Integration, and Verification Platform (AIVP) in V2.0 core infrastructure configuration.
- Training Platform (TRA) in V2.0 core infrastructure configuration;
- Validation Platform (VAL) in V2.0 core infrastructure configuration;
- Operational Platform (OPE) in V2.0 core infrastructure configuration.

The same will be expected at the end of every GRC core infrastructure release, i.e. GRC V2.1, GRC V2.2, and so on.

4.5.2.2 GRC V2 Infrastructure Minor Releases

On top of the major GRC core infrastructure releases, it is envisaged to procure minor[3] releases.

[3] A minor release contains a limited evolution at GRC core infrastructure level, such as operability improvements, or changes which do not require a modification of the GRC Technical Requirement Baseline or any other design documentation at GRC system level. Its qualification requires the execution of a limited set of non-regression tests at GRC system (or lower) level which should be defined and agreed before their on the platforms of the GRC.

5 Scope of the Procurement

This section details what will be expected of the contractor responding to this procurement.

5.1 Procurement Perimeter

Ultimately, the procurement perimeter of the GRC framework contract is to provide turn key service for the GRC core infrastructure releases, the associated maintenance of each release, and the nominal operations support of the release in operation for the next seven years.

This procurement should follow the same independence logic as described in Section 4.2, while also ensuring technical independence from the solutions of OS-NMA and HAS that are currently under development in the frame of the Galileo service provision.

In addition, with the inclusion of independent monitoring of EGNOS by the GRC under this FWC, the independence criteria are expanded to include:

- Technical independence from the data and tools used by the EGNOS system;
- Operational independence from the EGNOS Service Provider (ESP) and the EGNOS System primes for both EGNOS v2 and EGNOS v3.

The following provisional tasks are foreseen, pertaining to all activities that may be procured under the present FWC:

- Management, PA/QA, and supporting tasks
    - management of lower level procurement and deployment activities to ensure the subcontracted sub-systems are delivered on time and within specification;
    - project control and product assurance activities;
    - interfacing with the Contracting Authority for the purposes of regular reporting, progress meetings, and reviews;
    - support to the Contracting Authority for technical matters relating to the GRC infrastructure, maintenance, and operations;
    - ensuring consistency of the schedule with respect to the major programme milestones, reviews, and delivery milestones;
- Infrastructure tasks:
    - Design and Development Engineering Tasks:
        - Engineering, design;
        - production, update, and delivery of necessary GRC infrastructure documentation for hardware, software, tools, and all other items;
        - preparation of the:

            - GRC core infrastructure user manuals and installation, operations, and maintenance procedures (L1/L2 and L3) for the platforms of the GRC infrastructure; and,
            - Training material and provision of courses for operations, maintenance, and system verification of the GRC core infrastructure platforms;
            - Operational data to execute the operational validation and the GRC service delivery.
    - Qualification Tasks:
        - upgrade of the GRC core infrastructure Assembly, Integration and Verification (AIV) facilities, tools and procedures to support the new functionalities of the GRC;
        - plan and execute qualification activities (in-factory with the GRC AIVP and on-site with the GRC VAL platform);
        - support to external (e.g. GRSP, TSP, GSC, GSMC, …) Integration & Verification activities;
    - Acceptance Tasks:
        - commissioning of the infrastructure releases:
            - Operational System Validation (OSV),
                - Including provision of inputs to the accreditation dossier to the GRC SAB to grant the authorisation to deploy to the operational (OPE) system;
            - Initial Operations;
        - Acceptance Review (AR).
- Operations Tasks:
    - Nominal Operations Support.
- Maintenance Tasks (as defined in Section 4.3.4):
    - Overall maintenance of the GRC core infrastructure;
    - Anomaly and Problem Management Handling processes;
    - Updating the obsolescence strategy in place for the GRC core infrastructure in order to have it compatible with the overall Galileo system and operations needs for the next 20 years;
    - Update, execution, and maintenance of the GRC Integrated Logistics Services (ILS) strategy and associated planning.
- Security Tasks:

  - security engineering activities related to the design, implementation verification, validation and acceptance of new GRC functionalities;
  - full compliance with the programme security requirements, including cyber security and accreditation requirements, and certification of the security equipment;
  - support the activities leading to accreditation of the GRC core infrastructure and operations, and any necessary security measures for protection of data, documentation, infrastructures and personnel, including the definition of security measures;
  - performance of internal penetration test and support an independent penetration test;
- Support Tasks;
  - Support to Hosting Services;
  - Support to Guarding, Security, and Safety Monitoring Services;
  - Support to Interface Management;
  - Support to the GRC Design Authority.
- Handover and Handback Tasks.

5.1.1 Management

The Contractor will have to setup and maintain all the necessary means and processes for the management of the project at highest standard. This includes, for instance, the definition and implementation of the following activities:

- Project Management,
- Project Breakdown Structures,
- Schedule Management,
- Cost and Financial Management,
- Configuration and Documentation Management,
- Inventory Control and Assets Management,
- Progress and Performance Evaluation (Regular Reporting),
- Project Reviews,
- Risk Management,
- Resources Management,
- Subcontractors’ Management, and;
- Documentation Management Processes.

5.1.2 PA/QA and RAMS Tasks

The Contractor is expected to perform at least the following tasks throughout the scope of the GRC contracts:

- Product Assurance (PA),
- Quality Assurance (QA) and Quality Management,
- Reliability, Availability, Maintainability, and Safety (RAMS),
- Dependability,
- Software Product Assurance,
- Configuration Management, and
- Audits.

This should include the setting up of the required processes and performing regular reporting on the activities of each.

5.1.3 Infrastructure

5.1.3.1 Design and Development Engineering Tasks

The Contractor is expected to perform the design and development engineering activities necessary to translate the needs and objectives, concerning the GRC core infrastructure, into a robust design. This activity includes a full system design, with low level specifications, to be derived and developed in all the necessary sub-systems as well as the definition of the ICDs between elements/components.

The design of the GRC core infrastructure releases shall allow a fast roll back to the previous existing GRC release should any major problem be encountered in the migration to the operational platform.

The scope of the activity includes, at least, the following elements:

- Requirements Management,
- Engineering Management,
- System Specification,
- System Design,
- External Interface Management,
- Component Specification,
- Internal Interface Specification, Design, Implementation, and Management,
- System Performance Engineering, and;
- Software Element Design, Development, and Verification.

The activities are separated into project milestones to be evaluated by the Contracting Authority at each phase. When applicable, the design should go through a Preliminary Design Review (PDR) and Critical Design Review (CDR) as well as lower level milestones that are internal to the contractor in the form of software reviews which are mandated by the Galileo Software Standards (GSWS).

Any non-compliance to the requirements identified during the engineering lifetime (from the point of contract kick-off, through the design phases, and to the qualification phase) shall be promptly formalised through a RFD/RFW and submitted to EUSPA for approval.

5.1.3.2 Qualification Tasks

The qualification shall take part in two steps:

- In-Factory Qualification (IFQ)
    - Performed on the GRC AIVP at the contractor premises; and,
- On-Site Qualification (OSQ)
    - Performed on the GRC VAL Platform.

Together, these reviews form the complete Qualification Phase of a GRC core infrastructure release.

5.1.3.2.1 In-Factory Qualification (IFQ)

The primary objective of the Assembly, Integration, and Verification (AIV) activities is to demonstrate that the GRC core infrastructure:

a) has achieved compliance with the GRC Statement of Work (including annexes) and the GRC Technical Requirements baseline, and

b) is technically robust and ready to perform operations.

The first set of activities to be performed under this area include:

- AIV Planning, Definition, and Management.
- Development of the Verification Test Cases and Procedures.
- Maintenance of the Verification Control Documentation (VCD).
- Assembly, Integration, and Verification Platform (AIVP) Assembly and Integration.
- In-Factory Qualification (IFQ) executed on the updated (to the release in question) AIVP.

5.1.3.2.2 On-Site Qualification (OSQ)

Following a successful In-Factory Qualification (IFQ) review, the GRC core infrastructure contractors will deploy/update the GRC VAL platform and conduct the On-Site Qualification Review (OSQ). This phase will involve:

- Performance of any necessary integration activities with external entities shall be part of the OSQ (firstly with internal tools/emulators and secondly, and when possible, through the connection with the real External Entities (GRSP, TSP, GSC, GSMC, ...) as part of the End to End System Integration Verification (SIV) Test);

- The GRC contractors will support third parties designated by the Contracting Authority to conduct independent penetration testing (PENTEST) of the GRC system.

Throughout the aforementioned steps, the Contractor shall document and maintain all verification evidences at each step so as to maintain an up to date and fully representative verification file.

The GRC infrastructure contractor shall be responsible for ensuring the correct deployment of the GRC infrastructure and its sub-systems on-site at the GRC as well as ensuring the correct installation on the GRC VAL platforms.

Any deployment activity will be coordinated and approved in advance with the Contracting Authority and will be documented in the appropriate plans (including the necessary inputs from mandatory sub-contractors when required).

All procedures required for the migration to the Operational platform shall be validated first on the validation platform prior to approval for execution on the operational platform.

5.1.3.3 Acceptance Tasks

Prior to acceptance of the GRC core infrastructure release:

- the release installed on the GRC VAL platform must undergo Operational System Validation (OSV) by the GRC nominal operations team;
    - Including provision of inputs to the accreditation dossier to the GRC SAB to grant the authorisation to deploy to the operational (OPE) system, followed by,
- a period of initial operations, executed on the GRC operational platform, for a set period of time.

5.1.3.3.1Commissioning Tasks

The commissioning process is to provide confidence that the GRC core infrastructure combined with the relevant operational procedures and processes are designed, installed, tested, operated, and maintained according to the requirements of the Contracting Authority.

The commissioning tasks are divided in the following phases:

- Operational system validation (OSV);
- Initial operation of the GRC core infrastructure.

5.1.3.3.1.1 Operational System Validation (OSV)

The purpose of the OSV is to confirm that the new GRC core infrastructure release is suitable for its intended use (i.e. operations). As such, it is quite distinct from system verification (whose primary reference point is the system requirements).

The scope of OSV activities includes the demonstration that the GRC core infrastructure, in conjunction with the use of the associated operational data (plans, procedures, databases, timelines, etc.) and operated by trained and representative operational teams, is capable of performing the required GRC operations in a safe, reliable and sustained manner.

To achieve this objective, operational scenario testing is generally used (building upon the pre-validation activities of the various individual operational data) that starts with a restricted scope and progressively builds up to representative end-to-end testing that exercises the full operational functionality of the system using different operational scenarios.

The scope of the OSV activities will be tailored to reflect the assessment of the impact of the changes introduced by the particular GRC core infrastructure release.

Prior to the start of the OSV activities, the contractor may decide to organise an ***Operational Validation Readiness Review (OVRR)*** to check that the appropriate pre-conditions are met, e.g. the availability of all resources, test plans, procedures, timelines, system status, etc.

On completion of the OSV activities, an ***Operational Validation Review (OVR)*** is held with the Contracting Authority to check that the operational validation objectives have been satisfactorily achieved (including collection of operational credits to support the GRC core infrastructure release accreditation).

At OVR, explicit confirmation of the readiness (scope and quality) and acceptance of all service provision related documents (covering operations, maintenance, and security activities) shall be provided by the Contracting Authority.

As of the closure of the Qualification Review, Anomalies or Non-conformances can be raised by the Contracting Authority and the Contractor (including any involved sub-contractors) whenever a problem is encountered with a GRC release under deployment. These anomaly reports will be reviewed by an ***Anomaly Review Board (ARB) / Non Conformance Board (NRB)*** (to be organised, in this instance, by the Contractor). Any anomaly or non-conformance will have to be corrected by the Contractor (or relevant sub-contractor) prior to acceptance of the release. Any problems that present a blocking point will require to be fixed by the Contractor (or sub-contractor) prior to close out of the qualification.

5.1.3.3.1.2 Initial Operations

Upon successful accreditation and once the authorisation to deploy on the operational system is granted for the new GRC core infrastructure release, the migration activities on the operational platform shall commence.

During this phase, the Contractor shall be responsible for ensuring the correct deployment of the GRC core infrastructure and its sub-systems into the operational chain without impacting the nominal GRC operations. The design of the GRC core infrastructure releases and the migration procedures shall ensure that in case of need (major problems found during the migration of during the service monitoring phase), a roll back to previous operational release can be implemented without impacting the legacy service delivery.

Any deployment activity will be coordinated in advance with the Contracting Authority and will be documented in the appropriate plans (including the necessary inputs from the envisaged mandatory subcontractor when required) and CCRs.

The contractor is also responsible for ensuring the other platforms of the GRC (e.g. Training platform) are representative of the release entering into operation and that the installation is performed correctly.

5.1.3.3.2 Acceptance Review (AR)

Following successful OSV and initial operations phases, the Contract shall organise an acceptance review.

5.1.4 Nominal Operations Support

The Contractor is expected to perform the following operations activities:

- Delivery of the CONOPS;
- Delivery of the fully validated Installation, Operations and Maintenance Manual;
- Delivery of the fully validated operations procedures;
- Delivery of training on operations (including any security related training);
- Performing the nominal routine operations of the GRC.

5.1.4.1 Nominal Operations Support

The contractor is expected to support the nominal operations of the GRC core infrastructure release installed on the operational platform. This will involve the routine generation of all reference products (raw and processed data for orbits, clocks, atmosphere, etc) necessary for the elaboration of the reporting of the GRC. The Nominal Operations Support is expected to include the following:

- Generation of OS reference data outputs and provision of data to be used in the process of report elaboration for:
  - OS / OS-NMA,
  - HAS / CAS,
  - PRS,
  - Timing Services
- Generation of multiGNSS reference data outputs and provision of data to be used in the process of report elaboration.
- Generation of the above listed reference data at the following rates:
  - Real-time,
  - Ultra-rapid,
  - Rapid,
  - Final.

- Data management for RIMS stations, EDAS data, and SBAS networks.
- Generation and provision of core metrics and statistics.
- Collection and provision of metrics and data related to feared events.
- Retrieval of related data from relevant GNSS and regional systems for:
  - EWS,
  - SAR/BCS.
- Collection and provision of data in the scope of the IPC and GNSS Prediction.
- Provision of necessary data relevant for the user segments, certification support activities, and taskforces:
  - Aviation (EASA, EuroControl),
  - Maritime (EMSA),
  - Rail (ERA),
  - Receiver and Service Certification,
  - IGMA Taskforce.
  - GRC secondary functions
- Perform routine operations on an interim Quasi-Real-Time monitoring scale and latterly on a 24/7 basis for Real-Time Monitoring.
- Automation of routine data management and retrieval from MS.
- Provide support to investigations where required, namely:
  - Reprocessing of specific data corresponding to the period of investigation.

5.1.5 Maintenance

The Contractor is expected to perform the following Maintenance and ILS activities:

- Definition and delivery on Maintenance Training to L1 Maintainers;
- Implementation of a GRC Problem Management Process;
- Definition, planning, and execution of L1/L2/L3 maintenance activities for the GRC;
- Update and maintain the GRC Integrated Logistics Services (ILS) concept, ILS Plan, Logistic Support Analysis (LSA) Plan, Logistic Support Analysis Records (LSAR);
- Delivery of the Obsolescence Management Plan, Obsolesce Data, and execution of Obsolescence Tasks.

5.1.6 Security Tasks

Activities under this contract, including Galileo and EGNOS related operations monitoring will need to be conducted in accordance to the "European GNSS Program Security Instruction" (PSI), including its Annexes Security Classification Guide and the COMSEC Instructions. Any company at prime or subcontractor level involved, in any form, in the handling of EU classified information and COMSEC items have to comply with the above mentioned instruction. The European GNSS PSI provides notably instructions on the safeguarding of Classified Information that is provided or generated on behalf of any EU GNSS Program. Furthermore, the PSI informs the Contractors of their obligations as regards to the management of Classified Information. Finally, it provides instructions for the Participants on the classification of the information, security procedures, including the handling and transfer of Classified Information, and visit procedures for EU GNSS Programs.

The Security related activities are all the supporting, non-routine activities aimed at ensuring accreditation of the GRC, the security activities to be conducted from the beginning of contract to the successful acceptance review (aligned with the completion of the initial service phase). This includes, in particular, the following main areas:

- **Supporting activities for the security accreditation process:** The Contractor is expected to support the regular accreditation process required for the GRC. The contractor shall particularly produce and maintain a Security Risk Analysis and related security and cyber documentation. Based on the review of this analysis by the EUSPA, the requested security measure(s) to protect the GRC infrastructure releases. To this end, the Contractor shall establish a proactive reaction process to any potential threats to the GRC or any of the external entities that are connected to it by real-time means. The results of this process shall be reported to the EUSPA for analysis which could trigger a request to the Contractor for the implementation of additional security measure(s) in order to protect the GRC and, as such, External Entities. The Contractor will also contribute to the regular accreditation process in critical areas like production of Verification Control Documents (VCDs) and Request for Waivers (RFWs), implementation of and necessary Galileo and EGNOS System interconnection security requirement (SISRS), security operational requirements (SECOPS) and Local Security Operations.
- **General Security:** the Contractor will have to ensure that individuals only have access to classified information and equipment after their need-to-know has been established and, where appropriate, they have been security cleared to the relevant level by the relevant national authorities (NSA), to ensure that classified information and assets are protected against unauthorised access. In addition, the Contractor will need to ensure that users and processes are given the access, privileges or authorisations on information only if they require them to perform their tasks in order to limit any damage resulting from accidents, errors, or unauthorised use of it. To this end, the Contractor will need to ensure proper segregation of information for individuals (and processes) in terms of access to classified information on the basis of the need-to-know and, where appropriate, the relevant security clearance. All security operations will need to be performed by personnel with the adequate Security Clearance level recognised by the relevant national authorities (NSA).

- **Security monitoring & control:** the contractor will be expected to report on security events to EUSPA (usually GSMC), and the subsequent execution of EUSPA (usually GSMC) orders. To this end, the Contractor will need to ensure that a Security Assets Inventory is maintained in compliance with the Project Specific Security Classification guide (to be made available in Phase II of the procurement procedure, as explained in the Tender Specifications) to determine traceability on the security classification of the various elements of the contract, for the whole duration of the contract. Specific databases are required to manage classified and crypto items.

The security tasks expected to be performed throughout the duration of the GRC FWC are anticipated to cover at least the following:

- Implementation of the security requirements with analysis of the applicable National and European regulations;
- Protection and handling of European Union Classified Information;
- Security Management and associated planning activities;
- Demonstration of the compliance to the security baseline (including cyber and accreditation), and generation of Request for Waivers against requirements and against vulnerabilities when full compliance cannot be ensured;
- Security accreditation, threat, risk, and vulnerability and business impact assessment processes;
- Cryptographic controls including symmetric and asymmetric key management systems such as Public Key Infrastructure (PKI);
- Security archiving, configuration and change control processes and procedures that impact the operations and system;
- Non degradation of security accreditation, operations, systems, and controls without negative impact to the current operations and system;
- Business continuity and planning to minimise impact to Service confidentiality, integrity and availability compliance;
- Security Monitoring related to maintaining the compliance to the levels of confidentiality, integrity, and availability, through the collection and analysis of events, logs and data by the GSMC;
- Support the preparation and implementation of the security operations and maintenance;
- Cyber security activities, including:
    - Compliance reporting strategy;
    - Cybersecurity assurance for subcontractors;
    - Cybersecurity Training and awareness;
    - Cybersecurity audit strategy and plan;
    - Network map management;

- Vulnerability Management;
- Patch Management and installation;
- Obsolescence management;
- Infrastructure Acceptance Audit;
- Infrastructure Security Hardening;
- Infrastructure Security Lock Down.

5.1.7 Support Tasks

5.1.7.1 Support to the Hosting Services

Depending on the evolutions of the GRC core infrastructure to be procured under the present FWC, it is anticipated that there may be minor deficiencies with regards to the GRC hosting site's ability to host the fully evolved infrastructure. To this extent, the Contractor will be expected to conduct hosting site surveys to assess the current hosting provisions and assess their correctness in-line with the coming GRC core infrastructure evolution. In the event that this hosting site survey identifies shortcomings of the GRC Hosting Site, the Contractor shall ensure that these required changes are identified to the Contracting Authority at the earliest possible moment.

5.1.7.2 Support to Guarding, Security, and Safety Monitoring Services

Depending on the evolutions of the GRC core infrastructure to be procured under the present FWC, it is anticipated that assessment of Guarding, Security, and Safety Monitoring procedures would be required. Such assessment would be aimed at ensuring the procedures are accurate with respect to classification of the environments and infrastructure within the GRC. In the event that updates to the GRC infrastructure would necessitate a change in classification and hence a modification of a such a procedure, it should be alerted to the EUSPA as soon as possible via a dedicated report.

5.1.7.3 Support to Interface Management

During framework contract execution, the Contractor may be requested to support the process for the maintenance of the Interface Control Document (ICDs) between the GRC and other sites (e.g. GRSP, TSP, GSC, GSMC, …). If such a request is made, the Contractor may be asked to:

- produce Document Change Proposals (DCPs) to these ICDs,
- review DCP/DCNs proposed by other entities and
- as well as attend the necessary engineering boards to support the endorsement of the DCP/DCNs.

5.1.7.4 Support to the GRC Design Authority

The Contractor may be asked to support the Contracting Authority acting as the GRC Design Authority, during execution of the framework, by supporting Anomaly Review Boards, Change

Control Boards, Non-Conformance Review Boards, or other internal review processes or investigatory panels for matters related to the Galileo service monitoring.

5.1.8 Handover and Handback Tasks

The Contractor will be expected to perform handover and handback activities covering the demonstration of the readiness to start the activities of this FWC, the transfer of platforms between themselves and the current GRC incumbents, and the enabling of the successor contract (for the subsequent GRC infrastructure, operations, and maintenance FWC) to become fully responsible for the future (after the expiration of the FWC subject of this procurement) GRC required activities.

5.1.8.1 Handover

In addition to a complete End Item Data Package (EIDP) from the current GRC, containing all the final versions of the documentation and software source code, the handback plan of the current incumbent will be provided to the Contractor that details the steps to be completed during the handover period. The main goal of this plan is to complete the handover to the Contractor, which will involve:

- Transfer of the Operations Processes and Procedures;
- Training on the on the GRC Nominal Operations Support;
- Transfer of the Maintenance Processes and Procedures;
- Training on the GRC Infrastructure and Maintenance;
- Workshops, Shadowing, and Mentoring throughout the Handover, including managerial aspects.

In addition to the regular trainings and workshops, the Contractor shall organise a set of milestones to track the progress of the handover and to demonstrate their readiness, to the Contracting Authority, to perfom the nominal operations support and maintenance tasks. It is anticipated that the handover shall take no more than six months to complete. The handover milestones shall be as follows:

- Handover Kick-Off Meeting (HKOM):
    - The meeting shall be organised by the Contracting Authority between the current incumbent and the Contractor to finalise the handover schedule and agree on any potential outstanding issues.
- Nominal Operations Support Handover Key Point (OHKP):
    - The key point shall be arranged following the conclusion of the first round of training to assess the current status of the activities and to determine if any gap exists in that must be addressed before reaching the readiness review.
- Nominal Operations Support Handover Readiness Review (OHRR):
    - The readiness review will gather all evidence that the Contractor is ready to take over the operational tasks at the GRC.

- Maintenance Handover Key Point (MHKP):
    - The key point shall be arranged following the conclusion of the first round of training to assess the current status of the activities and to determine if any gap exists in that must be addressed before reaching the readiness review.
- Maintenance Handover Readiness Review (MHRR):
    - The readiness review will gather all evidence that the Contractor is ready to take over the maintenance tasks on the GRC infrastructure and software.

Following the successful conclusion of the handover, the specific contracts for maintenance and nominal operations support will enter into force.

5.1.8.2 Handback

The Contractor will be expected to prepare a handback plan that will include a schedule of activities to handover the contract (the GRC infrastructure development, nominal operations support, and maintenance) that cover the following activities:

- Transfer of a complete End Item Data Package (EIDP) at the end of the FWC, containing:
    - the final versions of all documentation produced, including:
        - operations procedures,
        - maintenance procedures and description of maintenance environments,
        - description of the development environment.
    - the latest software installation binary files;
    - the software source code;
    - the complete and up to date requirements verification status.
- Transfer of knowledge on the management of the contract;
- Nominal Operations Support training;
- Maintenance training;
- Training on the development environment;
- Shadowing and mentoring of the incoming economic operator.

In addition, the Contractor should accompany the plan with a staffing profile that clearly identifies a Handback Manager along with key points of contact for the nominal operations support, maintenance, and development activities.

5.2 Contractual, Logical, and Task Specific Interfaces

During the execution of the framework contracts and the specific contracts signed under it, the Contractor will need to interface with various stakeholders and entities. The following sub-sections provide an overview of what is envisaged at this point in regards to this.

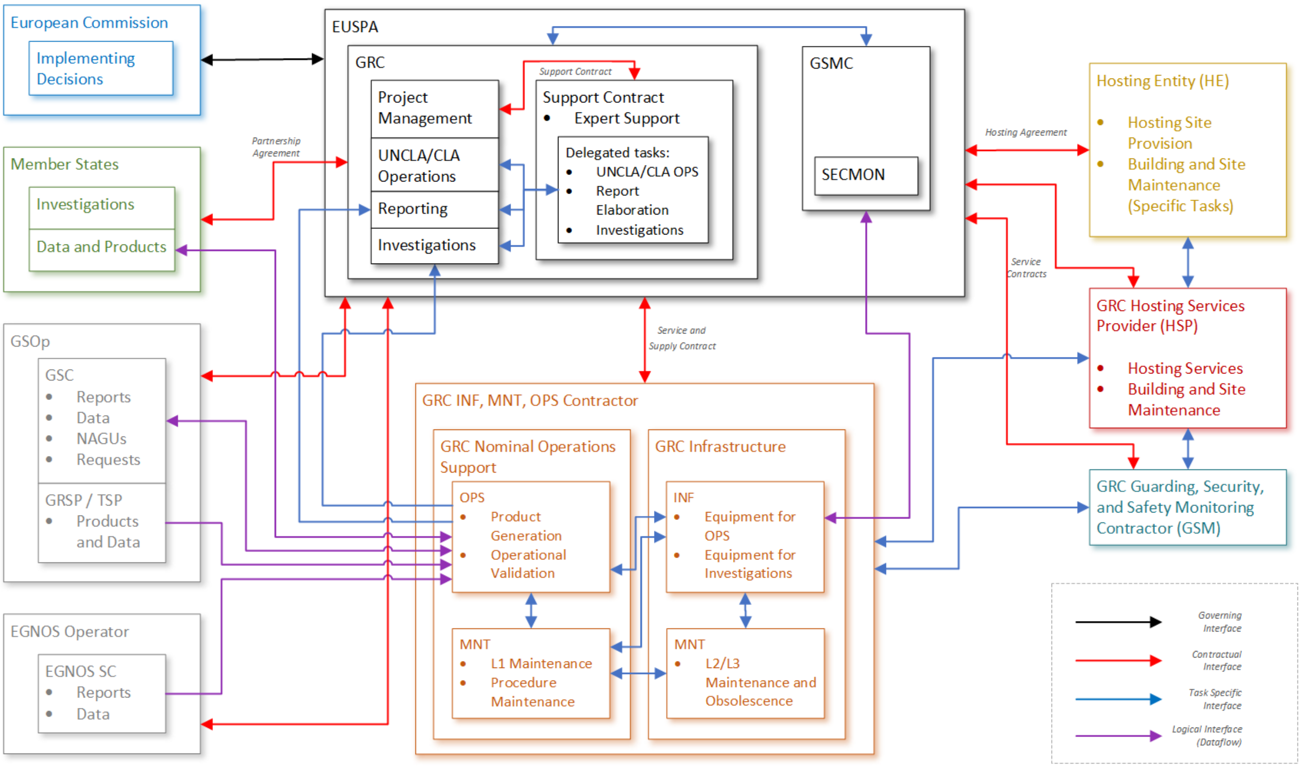


Figure 24: GRC Contractual, Logical, and Task Specific Interfaces

5.2.1 Interface with EUSPA

The Contractor will interface with the EUSPA for all matters concerning the execution of the contract.

5.2.2 Interface with External Entities / Data Providers

It may be possible, that in order to satisfy the implementation or operation of specific technical elements set out in the specific contracts, the Contractor may need interface with external data providers so as to obtain the data or support necessary to complete the implementation, qualification, and acceptance as well as to perform the operational activities for newly developed elements of the GRC core infrastructure.

5.2.3 Interface with GRC Hosting Service Provider (HSP)

Interface with the GRC HSP and their personnel will be required for deployment activities of the GRC infrastructure and general day to day working at the GRC premises (office cleaning, reporting of issues, etc).

5.2.4 Interface with GRC Guarding, Security, and Safety Monitoring Contractor (GSM)

Interface with the GRC GSM personnel will be required for deployment activities of the GRC infrastructure and general day to day working at the GRC premises (entry to the building, reporting of incidents, etc).

6 Contractual Performance Monitoring

The activities to be executed under this framework contract shall comply with the requirements defined in the relevant statements of work, both at framework level and at specific contract(s) level. The compliance to such requirements is envisaged to be measured against Key Performance Indicators (KPI) which are envisaged to address the following targets:

- timely and quality achievement of milestones (i.e. penalisation in case of late or not complete milestones);
- operations provision; and,
- maintenance provision.

These elements are envisaged to be discussed, in terms of general approach and structure, during the Dialogue phase and then refined and specifically applied in the context of the discussions leading to FWC conclusion.

The liquidated damages regime will be set out at FWC and SC level.

The Contractor may be requested to report regularly also on other metrics not directly subject to liquidated damages. The contractor will have to develop appropriate means to measure and monitor those metrics.

7 Assets

EUSPA is going to make available to the Contractor a set of assets which will be detailed in the course of the procurement procedure.

For the sake of exemplification and initial information the assets will comprise:

- GRC V0 Infrastructure,
- GRC V0 Documentation (latest versions),
- GRC V1 Core Infrastructure DEV platform,
- GRC V1 Core Infrastructure AIVP Platform,
- GRC V1 Acceptance Data Package (latest version).

Other assets maybe be provided during the course of the contract and these will be detailed when known during the execution of the contracts of the procurement.

8 Envisaged Areas of Dialogue

The following areas have been identified as main areas of dialogue:

12. Real-Time Monitoring functionality and reporting, including:
    a. Carrier phase-based processing,
    b. Monitoring and Reporting KPIs.

13. The GRC core infrastructure Operational Validation and Operational Migration,
14. PRS Navigation Monitoring Evolutions,
15. Interface with the GSMC,
16. Precise Reference Time at the GRC,
17. SBAS/EGNOS Monitoring functionality,
18. Repurpose of the GRC V0 to create a robust tool for incident investigation support,
19. Development of Functionalities to Support the GRC Secondary Mission (see Section 4.1.2):
    c. Including GRC archive quality of data management and data accessibility.
20. GRC V2 Nominal Operations Support and GRC V2 Maintenance:
    d. the solution will be dependent on the dialogue and solutions for the above mentioned points;
21. Handover from the current incumbent,
22. Risk allocation and Liability.

Candidates’ attention is drawn to the fact that this list is indicative and may be modified in the course of the dialogue phase and as a function of its development.

End of Document