Cyber security requirements for service infrastructure maintenance

Reference:
GSA-SEC-SREQ-SPE-237266

Issue/Version: 1.2

Date: 31/05/2018

Prepared By		
	Signature	Date
GSA Cyber Security Team		5-6-2018

Reviewed By			
Name	Role	Signature	Date
Wieland Kuenzel	Quality Manager		12/06/2018
Andrea Scorzolini	PRS and Security Engineer		12/06/2018
Francisco Da Costa Cabral	GSMC Security Monitoring Supervisor		12/06/2018
Philippe Gaillard	Security Requirements and Standards Section Manager		12 VI 2018

Approved By			
Name	Role	Signature	Date
Stefano Iannitti	Head of Security		12/6/18

Change Log:				
WFID	Issue/ Version	Changes & Pages Affected	Author	Date
237266	1.0	First version approved at GSA EB 19.	F. Belli	16/01/2018
	1.1	Document updated after implementation of RIDs received during EnS Phase 2 consolidation review. Approved at GSA EB 26.	F. Belli	27/02/2018
	1.2	Document updated after EC review. Main differences from previous version: Added (according to current numbering): • CYB-MNT-0090 • CYB-MNT-0110 • CYB-MNT-0360 Removed (according to v1.1 numbering): • CYB-MNT-0180 Version approved at GSA EB#35.	F. Belli	31/05/2018

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This document defines the cyber security requirements for a generic maintenance contract for Galileo infrastructure, and applies to all GSA infrastructure maintenance contracts. It is a general requirement document, not tailored for a specific contract: depending on the specific security objectives, a statement of applicability will be prepared, defining the list of applicable requirements.

The successful implementation of all of these requirements ensures that appropriate measures are in place to keep the risk under control during system operations throughout infrastructure lifecycle.

The intended audience of these requirements are the contractors and their subcontractors in charge of the maintenance contract.

Compliance to these requirements shall be demonstrated to GSA during the different project phases. The requirement verification matrix and any associated RFD/RFW is provided to the appointed SAA in order to review the risk and enable the system accreditation process.

This document is complementary to the documents containing requirements for the service infrastructure itself [RD.08], and the requirements for the operations [RD.09], which will use the infrastructure. These requirement documents are replacing [RD.12].

Figure 1 shows applicable Mission Requirements documents, and also other security technical requirements documents applicable to infrastructure procurement. It shall be noted that the document tree reported, is not fully representative of the documents derived from these Mission Requirements.

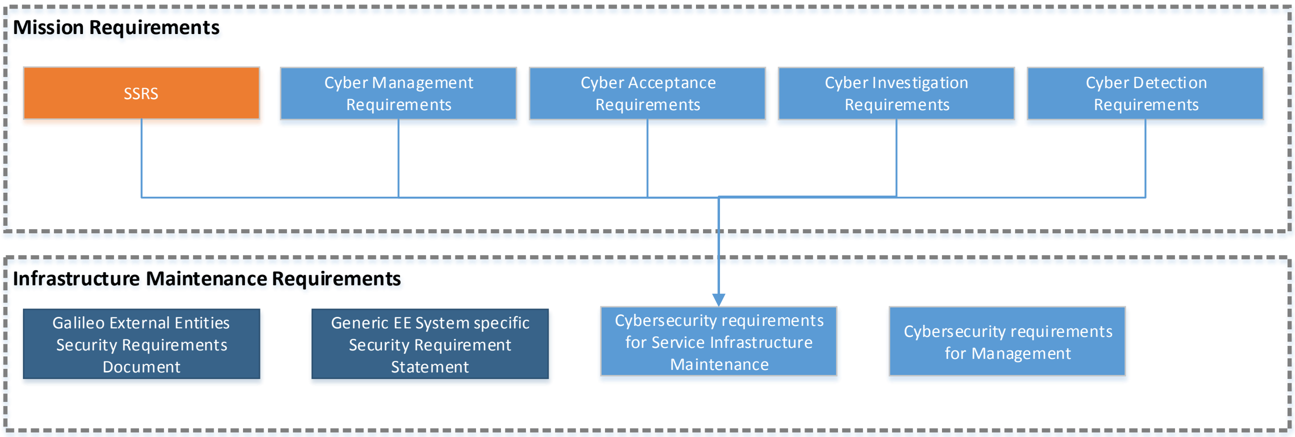
Mission Requirements
SSRS
Cyber Management Requirements
Cyber Acceptance Requirements
Cyber Investigation Requirements
Cyber Detection Requirements
Infrastructure Maintenance Requirements
Galileo External Entities Security Requirements Document
Generic EE System specific Security Requirement Statement
Cybersecurity requirements for Service Infrastructure Maintenance
Cybersecurity requirements for Management

Figure 1 - Requirements break down

1.1 Acronyms and Abbreviations

Table 1 - Abbreviations

Abbreviation	Definition
AD	Applicable Document
AR	Acceptance Review
CCR	Configuration Change Request
CERT	Computer Emergency Response Team
CDR	Critical Design Review
CEO	Chief Executive Officer
CIA	Cyber security Internal auditor
COTS	Commercial off the Shelf
CSC	Critical Security Controls
CSM	Cyber security Manager
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
EC	European Commission
EU	European Union
EUCI	EU classified information
GNU	GNU’s Not Unix
GPL	General Public License
GSA	European GNSS Agency
GSMC	In the document, the term refers to the GSA section responsible for Security Monitoring, and deployed at the Galileo Security Monitoring Centre

Abbreviation	Definition
LSAA	Local Security Accreditation Authority
NIST	(United States) National Institute of Standards and Technology
NtK	Need to Know
OPE	Operational Chain
OS	Operating System
PA	Product Assurance
PM	Project Manager
QR	Qualification Review
RD	Reference Document
RfD	Request for Deviation
RfW	Request for Waiver
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SACP	System Accreditation and Certification Plan
SIO	System INFOSEC Officer
SoC	Statement of Compliance
SSRS	System Security Requirements Specification
TBD	To be done
VAL	Validation Chain
WFID	Work Flow ID

1.2 Applicable and Reference Documents

The list of applicable documents contain the documentation as input for the generation of this requirements document.

Table 2 - Applicable Documents

Applicable Documents:			
Type	Title	Reference	Issue
[AD-01]	Galileo Cyber Security Policy	(Draft March 2017)	N/A
[AD-02]	Cyber Management Requirements	grow.ddg3.j.3(2017)600906_1.0	1.0
[AD-03]	Cyber Acceptance Requirements	grow.ddg3.j.3(2017)600632_1.0	1.0
[AD-04]	Cyber Investigation Requirements	grow.ddg3.j.3(2017)600828_1.0	1.0
[AD-05]	System Security Requirements Specification	Galileo SSRS Issue 3.9	3.9
[AD-06]	System Level Security Operating Procedures (secOps)	GAL-PRC-ALS-SYST-A-1000-x	6.4

Table 3 - Reference Documents

Reference Documents:			
Type	Title	Reference	Issue
[RD.01]	Concerning measures for a high common level of security of network and information systems across the Union	DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016	N/A
[RD.02]	Guide to Industrial Control Systems (ICS) Security	NIST 800-82 r2	R2
[RD.03]	Critical Security Controls	CSC-CIS version 6.1	6.1
[RD.04]	Generic EE System specific Security Requirement Statement	GAL-PL-CIMC-SEC-X/6240-x	1.2
[RD.05]	Galileo External Entities Security Requirements Document	GAL-REQ-ESA-SYST-X/1584	2.2

Reference Documents:			
Type	Title	Reference	Issue
[RD.06]	SACP Annex F - Security Vulnerability Management Requirements	GAL-PL-CIMC-SEC-X/7527	3.3
[RD.07]	Cyber security requirements for Management	GAL-SEC-SREQ-SPE-237329	1.2
[RD.08]	Cyber security requirements for service infrastructure	GAL-SEC-SREQ-SPE-232364	1.5
[RD.09]	Cyber security requirements for service operations	GSA-SEC-SREQ-SPE-232365	1.4
[RD.10]	Monitored Entity Requirements	GAL-REQ-ESA-SEC-X-1079-X	1.0
[RD.11]	Common Vulnerability Scoring System	https://www.first.org/cvss/calculator/3.0	N/A
[RD.12]	Security policy for system deployment and management	GAL-TN-GSA-SEC-215268-v01-0	1.0
[RD.13]	Network Map Template	GAL-GSA-GSMC-TMP-238093	1.0
[RD.14]	Cyber security Report Template	GAL-GSA-GSMC-TMP-238092	1.0
[RD.15]	Security Operations Scenarios	GSA-SEC-SREQ-TN-237908	1.0

2 Definitions

In the document the term contractor is used to identify the entity appointed by GSA for the procurement of the system under development. Further roles are:

- **Cyber security Manager** (CSM), part of the contractor organization, and is responsible for the design and implementation of the technical solution to the requirements presented in this document. When not differently specified, within this document with CSM it is intended the prime contractor CSM. A part from the contractor CSM(s), the following CSMs are referenced in the document:
    - GSA CSM;
    - GSMC CSM;
    - Operator CSM, CSM of the organization which will operate the developed infrastructure;
    - Developer CSM, CSM of the organization in charge of development of the infrastructure.
- **Cyber security Internal Auditor** (CIA), is part of the contractor organization, and is responsible for verifying that requirements identified in this document are correctly implemented. Furthermore he/she is responsible to verify that all vulnerabilities or exposures present in the system are identified and reported. A part from the contractor CIA(s), the following CIAs are referenced in the document:
    - GSA CIA;
    - Operator CIA, CIA of the organization which will operate the developed infrastructure;
    - Developer CIA, CIA of the organization in charge of development of the infrastructure.

In some requirements the following project phases are referenced:

- **Development** – it includes all project phases, from design to deployment and acceptance. The production of any further minor or major version of the system is considered part of the development.
- **Maintenance** – it is the support provided by the contractor to address any infrastructure issues not resolvable through predefined maintenance procedures (e.g. patches application).

In this document, **Network Map** refers to a representation of networks and hosts within Galileo ground segment. This representation captures:

- For the system
    - Network architecture
    - Virtual architecture and separation
    - Operational entities (first and second level, including hosting services), including their interfaces
    - Technical facilities used by the operational entities (split from segment to element level) including their interfaces
- For each element

- Name and high level description of the function
- Network architecture (including IP list and used ports)
- Hardware list
- Hypervisors
- Software list and associated platform
- Operational configuration (including filtering rules, paths to all log files and human/non-human accounts list with associated identity and privileges)
- Asset configuration responsible: person in charge of maintaining the configuration status of each asset.

3 Network map management

The maintenance CSM has to maintain a copy of the "As Operated" network map, in order to have all required information when analysing vulnerabilities or patches, and avoid any potential regression of scheduled maintenance releases of the infrastructure.

The Operator is responsible for maintaining the network map "As Operated", communicating any change to GSMC. GSMC provides updates of the network map to the CSM. It should be noted that any change to the configuration during operations, is performed under the Configuration Change Board (CCB) process, and the update of the network map is triggered by an approved and implemented CCR.

Figure 2 presents the lifecycle of the network map, which is generated by the infrastructure provider during development, and after handed over to the operator at Acceptance.

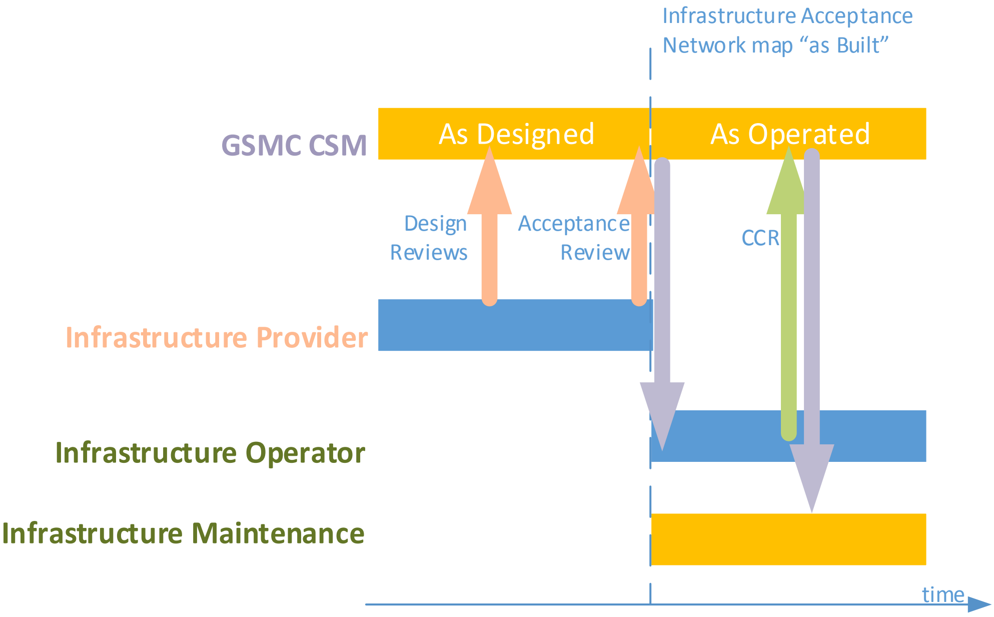

Figure 2 - Network Map responsibility

CYB-MNT-0010. Network map "as Operated"

The CSM shall keep an up-to-date copy of the "as Operated" network map (which is maintained by the Operator CSM). This version is derived from the "As built" network map, and takes in consideration all configuration changes implemented during the operational lifetime of the system.

End of requirement

Note: updates to the "as Operated" network map are provided by the operator of the infrastructure, which is in charge of configuration control.

Note: this version of the network map is important to avoid any regression in terms of patches between the operated infrastructure and a new minor/major release.

4 Vulnerability management

Vulnerability management process is required to keep under control the risk associated to the operated infrastructure .Figure 3 shows how during the operational lifecycle of the infrastructure, responsibilities on the different activities associated to vulnerability management are mapped to GSMC, Operations and Maintenance.

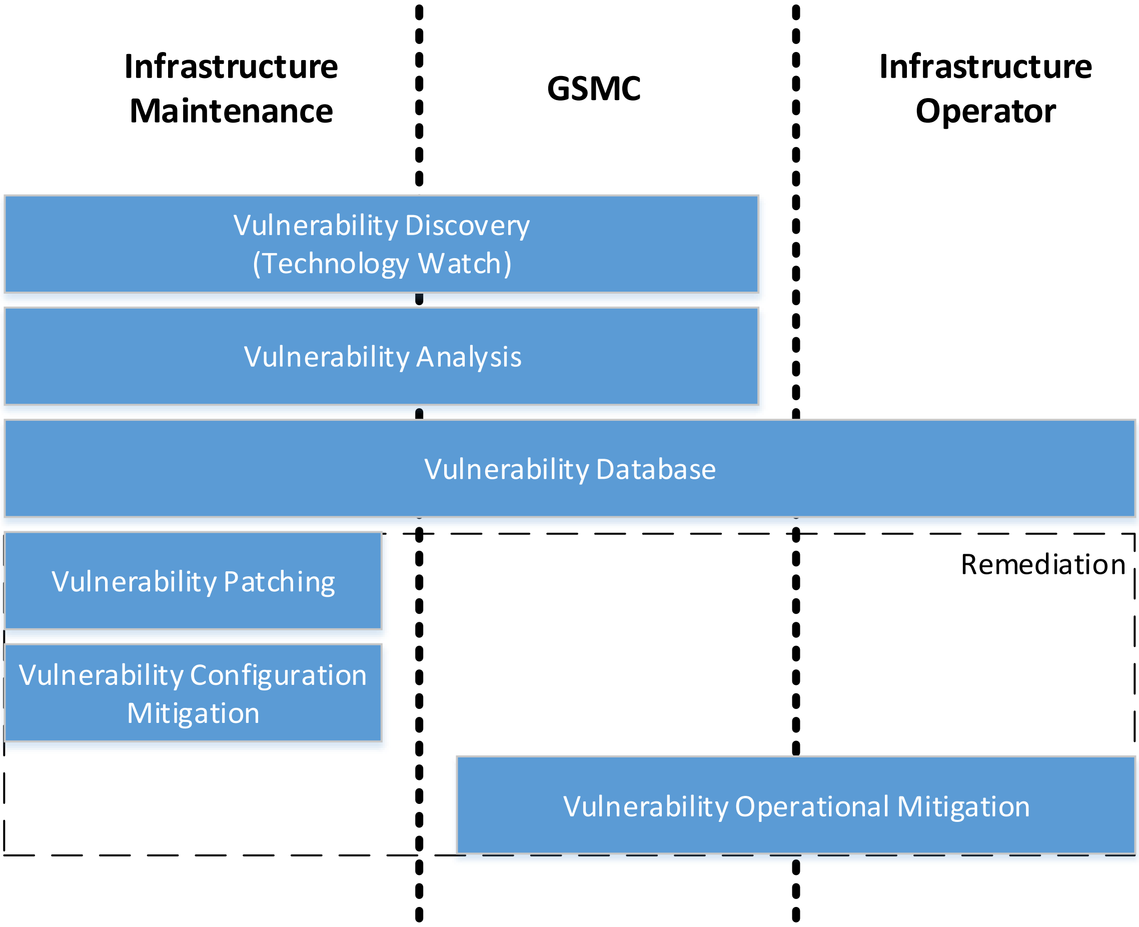
Infrastructure Maintenance
GSMC
Infrastructure Operator
Vulnerability Discovery (Technology Watch)
Vulnerability Analysis
Vulnerability Database
Remediation
Vulnerability Patching
Vulnerability Configuration Mitigation
Vulnerability Operational Mitigation

Figure 3 - Vulnerability management activities

The main objective of a vulnerability management process is to detect and remediate vulnerabilities in a timely fashion. Based on requirements on which the roles of CSM and CIA were defined, it is clear that this process will be continuous in an effort to capture as fast as possible vulnerabilities that might affect different elements of the infrastructure.

When implementing a vulnerability management process, regular scans should be scheduled to reduce the exposure time. Regular scanning ensures new vulnerabilities are detected in a timely manner, allowing for faster remediation.

A vulnerability management process is required to keep under control the risk associated to the infrastructure under development: it has to be concluded in a full cycle at least once before deployment of a new version of the infrastructure, in order to correct vulnerabilities before the acceptance. Vulnerability tracking should be done for each instance of the network map under responsibility of the CSM.

A report containing the list of vulnerabilities, associated analysis and corrections or mitigations need to be kept under configuration control, and provided to GSA, GSMC and operator CSM.

The vulnerability management process includes the following phases with a number of inputs and outputs per phase:

- Preparation
- Vulnerability detection
- Remediation identification
- Remediation implementation (Including patching were applicable)
- Validation of remediation

Preparation

The preparation phase is the first phase in a vulnerability management process. In this phase the scope has to be defined based on the network map and asset list available per segment. The preparation phase is mainly the responsibility of the CSM who should be at the end of this phase able to identify all the assets (network map) that will be in the scope of the vulnerability management process. After identifying the assets in scope and their characterization (vendor, model, owner etc), possible threats should also be identified.

Most common threats include (Galileo specific threats are defined in [AD-05]):

1. Unauthorized access (malicious or accidental).
2. Misuse of information (or privilege) by an authorized user.
3. Data leakage or unintentional exposure of information
4. Loss of data.
5. Disruption of service or productivity.

Determining inherent risk and impact are the next factors that need to be calculated based on controls in place and the likelihood of the given risk to materialize.

All the above mentioned steps will lead to defining the criticality of findings or the vulnerability baseline score defined in [CYB-MNT-0020]:

Impact (if exploited) * Likelihood (of exploit in the assessed control environment) = Risk Rating

Some indicative risk ratings can be:

- Severe – A significant and urgent threat to the organization exists and risk reduction remediation should be immediate.
- Elevated – A viable threat to the organization exists, and risk reduction remediation should be completed in a reasonable period of time.
- Low – Threats are normal and generally acceptable, but may still have some impact to the organization. Implementing additional security enhancements may provide further defence against potential or currently unforeseen threats.

Vulnerability Detection & Reporting

One of the most important phases is the detection of vulnerabilities that will later populate the vulnerability database [CYB-MNT-0030]. Detection can take place based on feedback from:

- the information retrieved from the providers of software and hardware deployed or foreseen in the concerned systems
- the information related to vulnerabilities retrieved from CERT-EU
- the information related to vulnerabilities from CERT of the Member States on the territory of which the GCC and the GSMC are being deployed
- the information related to vulnerabilities retrieved from the CVE Mitre database

In case of successful detection of a vulnerability, a new entry is created in the contractors vulnerability database. (Status of the vulnerability = IDENTIFIED)

Each vulnerability should be accompanied by an analysis [CYB-MNT-0060] covering important element later defined in this document. An important element of each vulnerability is the GSA Unique Vulnerability Identifier which can be used in order to track a vulnerability throughout its lifecycle.

A vulnerability report [CYB-MNT-0080] will be produced monthly including all vulnerabilities and their individual reports along with vulnerability metrics [CYB-MNT-0100], [CYB-MNT-0240]. This report will be forwarded to GSMC and will be introduced in the GSA's vulnerability database.

Reporting can happen ad hoc via urgent reports from the contractors CSM to the GSAs CSM and GSMC or in a scheduled manner via monthly reports.

Both contractors CSM and CIA are responsible for this phase.

Remediation identification

The remediation identification is part of the vulnerability analysis and should be already introduced in deliverables such as the monthly vulnerability report. The remediation may consist in the application of a patch, for which a patch analysis shall also be provided [CYB-MNT-0210]. Non vulnerable assets should also be identified [CYB-MNT-0110].

The proposed remediation mechanisms identified will be provided as part of the vulnerability report to GSA CSM and GSMC in order for later to evaluate each remediation, accept risk and approve implementation of remediation actions.

One of the options in order to remediate an identified vulnerability is via patching. A separate process for patch management will be described later in this document [5].

(Status of the vulnerability = ANALYSED)

This actions might have an effect in the vulnerabilities Criticality and Status.

Remediation implementation

The CSM will drive the correction of eventual vulnerabilities, deviation from baseline, and patch implementation.

(Status of the vulnerability = TESTED)

A vulnerability correction plan (assurance maintenance plan) [CYB-MNT-0160] should be defined for all vulnerabilities that will not be fixed immediately.

The vulnerability correction plan is forwarded also to GSMC in order to enable preliminary risk analysis.

Validation of remediation

The CSM should be able to validate that the remediation chosen for a specific vulnerability has been applied and is effective.

The contractor CIA is also responsible to test if the remediation chosen was sufficient and has properly mitigated the risk. (Status of the vulnerability = DEPLOYED)

GSA CIA and GSMC can and will perform separate audits in order to identify if a vulnerability has been remediated.

(Status of the vulnerability = CLOSED)

CYB-MNT-0020. Vulnerability Baseline Score

The CSM shall define for each vulnerability in system/software identified in the network map, a Vulnerability Baseline Score. This represents the sensitivity of the system/software to technical vulnerabilities.

This score shall be calculated under the CVSS 3.0 schema [RD.11].

End of requirement

Note: this score is used to determine the priority for the vulnerability correction.

CYB-MNT-0030. Vulnerability database

The CSM shall maintain an database of vulnerabilities affecting the infrastructure under maintenance, along with the associated analysis, as specified in CYB-MNT-0070.

The database shall be based on the vulnerability report provided by the infrastructure developer, which shall be reviewed by the CSM before acceptance in order to assess its quality and completeness.

End of requirement

Note: this task is performed collecting information from all possible sources; e.g.: COTS suppliers, vulnerability assessment reports, notifications from GSMC, information from CERTs, Mitre database, etc. Consider that also a patch announcement is a vulnerability notification.

CYB-MNT-0040. Subcontractor vulnerability database responsibility

The prime contractor CSM is responsible to GSA for completeness and quality of vulnerability management performed by subcontractors.

End of requirement

Note: GSA and GSMC have only the contractor CSM as interface.

CYB-MNT-0050. Vulnerability identification

The CSM shall review weekly information on vulnerabilities, in order to identify any new vulnerability affecting the infrastructure under maintenance. Inputs to this process are:

- the network map
- the information related to vulnerabilities, patches and obsolescence retrieved from the providers of software and hardware deployed or foreseen in the concerned systems
- the information related to vulnerabilities and obsolescence retrieved from CERT-EU
- the information related to vulnerabilities and obsolescence retrieved from CERT of the Member States on the territory of which the GCC and the GSMC are being deployed
- the information related to vulnerabilities retrieved from the CVE Mitre database
- Outcomes and lesson learned from security incidents

In case of identification of new vulnerabilities the contractor CSM should update his local vulnerability database immediately. If a vulnerability is deemed critical the GSA and GSMC should be informed immediately.

End of requirement

CYB-MNT-0060. Vulnerability analysis

The CSM shall analyse the risk associated to a vulnerability, in terms of exploitability and impact on service. Preliminary prioritization of the analysis is done by the contractor. GSMC will reassess vulnerability criticality and reassign priority. Contractor CSM and GSMC shall agree on the timeline for the analysis, which in any case cannot be later than 6 weeks after vulnerability identification, even for low rated vulnerabilities.

End of requirement

CYB-MNT-0070. Vulnerability analysis content

As a result of the vulnerability analysis, at least following information shall be captured in a report:

- GSA Unique Vulnerability Identifier;
- Date of the analysis;
- Vulnerability identifier (e.g. CVE) if any;
- CSM in charge of the analysis;
- Applicability: clear description of the COTS affected and if the function is used in the system or not.
- Element(s) affected, referencing the applicable network map;
- Source of information of the original vulnerability notification, and original report in appendix;
- Date of publication of the vulnerability;
- Date of identification of the vulnerability;
- Original criticality (e.g. CVSS)
- Assessed criticality based on deployed technical/operational mitigations (e.g. CVSS score including environmental and temporal metrics)
- Functional impact on the infrastructure in case the vulnerability is exploited;
- Potential attack vectors and exploitation methods;
- Patch availability and application timeline;
- Proposed mitigation, where patch application cannot be immediately performed (e.g.: configuration change, patch, operational workaround, none);
- Potential obsolescence of the affected element.

End of requirement

Note: The GSMC will perform an independent assessment of impact, exploitability and likelihood of the vulnerability.

CYB-MNT-0080. Vulnerability report

The vulnerability report shall list all open vulnerabilities in the vulnerability database, along with the associated analysis and details. The CSM shall provide a monthly vulnerability report for each instance of the network map (each version of the system under development, or operated). All available analysis shall be provided in accordance with CYB-MNT-0060.

The vulnerability report shall be delivered last Friday of each months.

End of requirement

CYB-MNT-0090. GSMC vulnerability discrepancies

The CSM shall receive from GSMC the list of open vulnerabilities affecting the infrastructure under maintenance. He/she shall verify it against its own network map(s) and list(s) of cyber vulnerabilities. In the case of a discrepancy, he/she shall coordinate with GSMC or the CSM of GSA in order to update the information which is wrong.

End of requirement

CYB-MNT-0100. Vulnerability metrics

The vulnerability report shall contain vulnerability metrics. The CSM shall facilitate the data collection to support the development of new metrics when requested by GSA Cyber Review Board, or following the update of requirements for the vulnerability report.

At least following metrics shall be initially supported:

- Number of identified vulnerabilities.
- Number of open vulnerabilities, (pending for analysis, remediation, closure).
- Number of closed vulnerabilities.
- Time elapsed between identification and analysis.
- Time elapsed between analysis and closure.

Such metrics shall be reported as total number, and also grouped by vulnerability criticality, drilled down by segment/element, and distributed by timeline.

End of requirement

CYB-MNT-0110. Non-vulnerable assets

Referencing the network map, the systems not affected by potential cyber-vulnerabilities or obsolescence shall also be identified.

End of requirement

CYB-MNT-0120. Configuration control of vulnerability database

The CSM shall keep under configuration control the list of vulnerabilities and associated analysis affecting the infrastructure to be delivered and/or delivered.

End of requirement

CYB-MNT-0130. Critical vulnerability notification

When the preliminary assessment of a vulnerability affecting the deployed infrastructure is critical or high, the contractor CSM shall immediately provide a report to GSMC.

End of requirement

CYB-MNT-0140. Vulnerability notification from GSMC

The CSM shall accept notifications of new vulnerabilities from GSMC and GSA CSM, and forward to subcontractor CSM when required. In case of critical vulnerabilities the information should be forwarded immediately.

End of requirement

CYB-MNT-0150. Support to mitigation definition

The CSM shall support the GSMC in identifying the mitigation to vulnerability which cannot be immediately corrected.

End of requirement

Note: Also the Operator CSM is involved in this process.

CYB-MNT-0160. Vulnerability correction plan (Assurance Maintenance Plan)

The CSM shall take over the vulnerability correction plan delivered along with the infrastructure to be maintained. It will drive the correction of eventual vulnerabilities, deviation from baseline, and patch implementation. The vulnerability correction plan shall be reviewed every 3 months, and at minor/major releases of the infrastructure.

Any update to the vulnerability correction plan shall be forwarded also to GSMC in order to enable preliminary risk analysis.

End of requirement

5 Patch management

Patch management process is needed to correct existing vulnerabilities. The benefit of a patch compared to another type of mitigation of the risk (e.g. workaround, affected by operational risk) is that the patch fixes the vulnerability on long term, removing the risk. It is important to identify and prioritize patches based on severity of the vulnerabilities mitigated. Wherever is possible batch patching can speed up the process leaving the infrastructure exposed for a smaller time frame. It is very important to state that patches should be applied only when it is verifies that they fix a vulnerability and at the same time do not introduce a new vulnerability or destabilize the infrastructure in any way.

The contractor has to ensure that the infrastructure is adequately patched, to guarantee an acceptable level of risk.

CYB-MNT-0170. Patch identification

The CSM shall identify any new patch correcting vulnerabilities affecting the infrastructure to be delivered and/or in operations. The CSM shall be responsible to analyse and test if the patch indeed fixes a vulnerability without introducing a new vulnerability or destabilizing the already deployed infrastructure. Test shall only be performed in a testing environment.

This task shall be performed collecting information from the certified COTS suppliers. The patch shall be obtained using a certified supply chain.

End of requirement

Note: this process of patch identification is required when a patch or a correction is not available at the moment of discovery of the vulnerability.

CYB-MNT-0180. Subcontractor patch management responsibility

The prime CSM is responsible in front of GSA for completeness and quality of patch management performed by subcontractors.

End of requirement

CYB-MNT-0190. Patch identification frequency

The CSM shall review weekly information about available patches.

End of requirement

Note: frequency of this task is not considered overloading: usually patch availability notifications are provided via emails by COTS providers.

CYB-MNT-0200. Vulnerabilities associated to patches

If a patch is announced, and it is associated to a not previously analysed vulnerability, then it shall also be considered as an input to the vulnerability database.

End of requirement

CYB-MNT-0210. Patch analysis

On any security patch published by a COTS developer, the CSM shall analyse it on a timeframe agreed with the GSMC based on the vulnerability severity ranting performed by the GSMC and in any case no later than 6 weeks even for low rated vulnerabilities.

End of requirement

Note: in some cases, a patch may modify functionalities of a COTS, affecting its correct integration with the rest of the infrastructure.

Note: this analysis shall be performed in INT chain where available. The in general the patch shall be analysed before deployment in VAL and OPE.

CYB-MNT-0220. Patch analysis content

As a result of the patch analysis, at least following information shall be captured in the report:

- GSA Unique Vulnerability Identifier (to be mitigated)
- Date of the analysis;
- CSM in charge of the analysis;
- Associated vulnerability identifier (e.g. CVE);
- Assessed criticality of associated vulnerability;
- Current vulnerability mitigation;
- Applicability: Element(s) affected, referencing the applicable network map (patch applicability), and a clear description of the functionality on the COTS affected and if the function is used in the system or not;
- Date of publication of the patch;
- Potential impact of the patch in other functional areas of the system;
- Potential impact of the patch on operations;
- Set of non-regression tests proposed to be performed as part of the validation of the security patch.
- Proposed schedule for patch implementation, including validation testing, and deployment strategy in the operational chain without impacting the service provision. This plan is reviewed and agreed with GSA CSM.

End of requirement

Note: The GSMC will perform an independent assessment of impact, exploitability and likelihood of the vulnerability.

CYB-MNT-0230. Patch report

Along with the Vulnerability report identified in [CYB-MNT-0080], the CSM shall provide (monthly) a patch report for each instance of the network map. The report shall list all available patches; an analysis shall be provided for all patches announced 5 weeks before issuing the report, and of the patches prioritized by GSA.

End of requirement

Note: GSMC supports GSA PM and CSM in the prioritization.

CYB-MNT-0240. Patch metrics

The patch report shall contain patch metrics. At least following metrics shall be provided:

- Total number of available patches
- Number of patches applied
- Average time between patch announcement and patch application

These metrics shall be organized by vulnerability criticality level.

End of requirement

CYB-MNT-0250. Patching during maintenance (operational lifecycle)

During maintenance, the contractor shall ensure that the vulnerabilities correction plan referred in [CYB-MNT-0160] is correctly implemented. Specific patches implementation may be prioritized by GSA based on criticality.

End of requirement

CYB-MNT-0260. Patch validation

During maintenance, the contractor shall test and validate all patches before their deployment. The CSM is responsible to analyse and test if the patch indeed fixes a vulnerability without introducing a new vulnerability or destabilizing the already deployed infrastructure.

End of requirement

Note: outcome of this activity is reported within the patch analysis CYB-MNT-0210.

CYB-MNT-0270. Patch associated to critical vulnerability notification

When a patch becomes available for the maintained infrastructure, and it is associated to a vulnerability assessed as critical or high, or it had been prioritized by GSMC, the CSM shall immediately provide an analysis according to CYB-MNT-0210 to GSMC.

End of requirement

CYB-MNT-0280. Support to patch decision

The CSM shall support GSA in taking the decision to apply the patch. This is based on the patch impact analysis, and patch test results.

End of requirement

Note: GSMC is closely involved in the decision making process.

CYB-MNT-0290. Patches bundles

The CSM shall rationalize the patch implementation process. It shall maximize the number of patches to be deployed together, in order to reduce the time required for testing and patching.

Patches contained in the bundle shall be individually and collectively tested before deployment in OPE chain.

End of requirement

Note: it is preferable to deploy all relevant patches for a specific element in the same maintenance activity.

CYB-MNT-0300. Phased patch management implementation

When implementing patch management on complex legacy systems, a phased approach shall be considered, prioritizing critical patches. This shall be documented in the Vulnerability correction plan.

End of requirement

6 Patch deployment

CYB-MNT-0310. Patch deployment

The contractor shall apply patches accordingly to the correction plan established in CYB-MNT-0160.

End of requirement

CYB-MNT-0320. Patch automation

In general, patches shall be implemented via manual activities. However, when the risk is limited (e.g. operators workstations), and the approach is duly justified, an automated method to deploy patches could be used. This is in order to reduce the effort of patch deployment.

End of requirement

Note: even if automated, all the procedure of patch application is under the responsibility of L2/L3 maintenance.

Note: for critical servers patches can be implemented only manually. Automated patching implies the deployment of agents, or remote administrative connections which are not considered secure.

CYB-MNT-0330. Patch automation architecture

If patch automation is foreseen, all possible architectures shall be carefully analysed. The chosen solution shall be duly justified.

End of requirement

CYB-MNT-0340. Patch automation resources consumption

If patch automation is used, in any case it should not negatively impact service performances. (e.g. resources overload).

End of requirement

Note: in general, patches are expected to be applied when the system is not in an operational state.

CYB-MNT-0350. Patch testing

During maintenance, the contractor shall test and validate all patches before their deployment. The CSM is responsible to analyse and test if the patch indeed fixes a vulnerability without introducing a new vulnerability or destabilizing the already deployed infrastructure.

End of requirement

Note: this requirement is in accordance with [CYB-MNT-0260]

CYB-MNT-0360. Correction evidences

After installation of a correction (e.g. patch), the CSM shall provide to GSA CSM and Operator CSM evidences of correct installation and effectiveness in terms of risk reduction of the correction.

End of requirement

CYB-MNT-0370. Patch impact on security hardening

When testing a patch, it shall be ensured that it doesn’t impact any baseline security configuration.

End of requirement

Note: some patches may restore software configuration to its default.

CYB-MNT-0380. Patch effectiveness

The patch application is considered complete after that it is taking effect.

End of requirement

Note: some patches may need system or service reboot before entering in effect.

CYB-MNT-0390. Patch integrity

Patch integrity shall be verified at each step (e.g. after download, before testing, before implementation).

End of requirement

Note: this is required in order to avoid a patch compromise; patches may be used as an infection vector.

CYB-MNT-0400. Patching of certified systems

The contractor shall ensure that patches do not impact certification of systems. When certification is compromised, then the patched system shall get recertified before deployment on operational chain. Recertification shall be achieved within 9 months from definition of the patch.

While the certified system is not patched, adequate measures to reduce the risk shall be put in place.

End of requirement

7 Support to incident response

In case of compromises impacting the service provided by the infrastructure, or the security functions, the maintenance team shall support GSMC to deploy a reaction, and ensure service recovery.

CYB-MNT-0410. Forensic extraction

Where required by GSMC, the maintainer shall provide support to GSMC and the operator to execute forensic data extraction.

End of requirement

CYB-MNT-0420. Reinstallation of core of trust

Where required by GSMC, the maintainer shall provide support to GSMC and the operator to recover the Core of Trust of the maintained infrastructure, over a short timescale (e.g. a weekend).

End of requirement

Note: the timing part of the requirement may be subject to Infrastructure limitations.

Note: the Core of Trust includes services with high privileges over the system's resources, especially infrastructure services (e.g. authentication, remote installation, remote management, remote control, supervision, antivirus, etc.) and the associated administration machines.

Note: the expected time frame will be defined according to the business continuity needs, which will take in account the nature and extent of the compromise.

CYB-MNT-0430. System sanitisation

Where required by GSMC, the maintainer shall provide support to GSMC and the operator to perform sanitation of the maintained infrastructure, eliminating the attacker's means of accessing the system.

End of requirement

Note: For example changing the set of secrets, suppressing accounts used by the attacker, replacing the compromised machines.

8 Obsolescence

These requirements apply specifically to cyber maintenance of 3rd party software, and may be duplicated of general obsolescence requirements. These are captured here in order to stress the importance of having a cyber maintenance of all COTS deployed on the infrastructure across its lifecycle.

CYB-MNT-0440. Obsolescence plan

The contractor shall maintain and implement the obsolescence plan, to ensure adequate patching of software deployed across the maintained infrastructure.

End of requirement

CYB-MNT-0450. Maintenance of 3rd party software

When maintenance of 3rd party software is not guaranteed (e.g. GPL/GNU licences), the contractor shall confirm that it will be able to autonomously develop patches, or substitute the obsolete software.

End of requirement

9 Maintenance

CYB-MNT-0460. Non-regression

Maintenance activities shall not compromise original compliance of the infrastructure with respect to security requirements for service infrastructure [RD.04], [RD.05], [RD.08] and [RD.10].

End of requirement

CYB-MNT-0470. Approval of maintenance activities

Maintenance activities shall be approved by the infrastructure operator, and tracked via Configuration Change Requests (CCRs).

End of requirement

CYB-MNT-0480. Certified equipment maintenance

Maintenance activities of certified equipment shall ensure to have no impact on the certification validity.

End of requirement

CYB-MNT-0490. Maintenance impact on service

Maintenance shall not impact critical activities. Maintenance activities shall be planned in order to reduce impact on service.

End of requirement

CYB-MNT-0500. Extraordinary maintenance

When extraordinary maintenance is required on the operational system, a plan shall be provided for approval along the CCR, identifying risks on operations and service provisions, and their mitigations.

End of requirement

CYB-MNT-0510. Planning of maintenance

Maintenance activities shall be planned to have enough time to recover from any unpredictable event that may happen during the activity.

End of requirement

Note: e.g. planning maintenance on Fridays, is a risk, because for any inconvenient the system may be left in an inconsistent status for the weekend.

10 Deliverable list

Table 4 lists deliverable documents specified in this requirement document. For each deliverable it is stated its applicability and frequency of delivery.

	Responsible	Requirement	First release	Release frequency

Vulnerability report **(for each network map instance)**	CSM	CYB-MNT-0080 CYB-MNT-0110	QR	Monthly
Vulnerability correction plan **(for each network map instance)**	CSM	CYB-MNT-0160	QR	Quarterly
Patch impact analysis	CSM	CYB-MNT-0210 CYB-MNT-0220	N/A	As soon as performed
Patch report (for each network map instance)	CSM	CYB-MNT-0230	QR	Monthly

Table 4 - Deliverables documents

End of Document