Cyber security requirements for service infrastructure

Reference:
GSA-SEC-SREQ-SPE-232364

Issue/Version: 1.5

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		12/6/2018
Andrea Scorzolini	PRS and Security Engineer		12/6/2018
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
	1.0	First Issue, endorsed at GSA EB#16	F. Belli	13/12/2017
	1.1	Scope clarified, according to comments received at GSA Project CCB	F. Belli	14/12/2017
	1.2	Document updated implementing comments from DCA and AAR and ESA implemented: • Recovered regression on Log forwarding requirement. • Extracted generic requirements in dedicated document. Extracted tender specifications in a dedicated document.	F. Belli	11/01/2018
236572	1.3	Version endorsed at GSA EB#19.	F. Belli	16/01/2018
	1.4	Updated after implementation of RIDs received during EnS phase 2 review. Approved at GSA EB 26.	F. Belli	27/02/2018
	1.5	Version updated after EC comments. Main differences from the previous approved version: Added (according to current numbering): • CYB-INF-0030 • CYB-INF-0130 • CYB-INF-0140 • CYB-INF-0150 • CYB-INF-0340 • CYB-INF-0350 • CYB-INF-0440	F. Belli	31/05/2018

Change Log:				
WFID	Issue/ Version	Changes & Pages Affected	Author	Date
		• CYB-INF-0680 • CYB-INF-0780 • CYB-INF-0880 • CYB-INF-0890 • CYB-INF-0960 • CYB-INF-1260 • CYB-INF-1420 • CYB-INF-1430 • CYB-INF-1670 • CYB-INF-1680 • CYB-INF-1980 • CYB-INF-2010 • CYB-INF-2160 • CYB-INF-2400 • CYB-INF-2430 • CYB-INF-2450 • CYB-INF-2580 • CYB-INF-2740 Removed (according to v1.4 numbering): • CYB-INF-0080 • CYB-INF-0090 • CYB-INF-0150 • CYB-INF-0870 • CYB-INF-0880 • CYB-INF-0960 • CYB-INF-1400 Version approved at GSA EB#35.		

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This document defines the cyber security requirements for a generic development project for Galileo infrastructure. It applies to all GSA infrastructure procurements, with the exclusion of procurements through the working arrangement between GSA and ESA. It is a general requirement document, not tailored for a specific procurement: depending on the security objectives of each specific procurement, a statement of applicability[1] will be prepared, defining the list of applicable requirements.

The intended audience of these requirements are the contractors and their subcontractors in charge of the infrastructure development.

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 hosting entities **Error! Reference source not found.**, where the infrastructure under development will be deployed, maintenance requirements [RD.09], and the requirements for the operations [RD.08], which will use the infrastructure.

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.

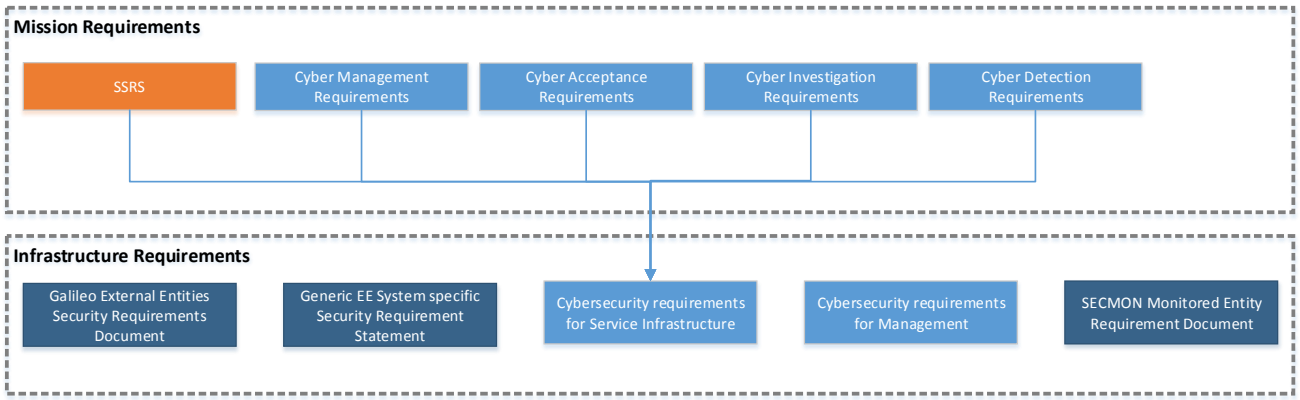

Figure 1 - Requirements break down

[1] The statement of applicability is also needed to ensure no overlapping with the SECMON MER [RD.10].

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
DMZ	Demilitarized Zone
DRB	Delivery Review Board
EC	European Commission
EU	European Union
EUCI	EU classified information, as defined in COMMISSION DECISION (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
GNU	GNU's Not Unix
GPL	General Public License

Abbreviation	Definition
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
GST	Galileo System Time
HIDS	Host Intrusion Detection System
ICD	Interface Control Document
IDS	Intrusion Detection System
INT	Integration Chain
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LSAA	Local Security Accreditation Authority
MAC	Medium Access Control
MCR	Main Control Room
MMI	Man Machine Interface
M-to-M	Machine to Machine
NIST	(United States) National Institute of Standards and Technology
NtK	Need to Know
OPE	Operational Chain
OPS	Operator. It intends the entity in charge of operating the infrastructure after its acceptance.
OS	Operating System

Abbreviation	Definition
PA	Product Assurance
PDR	Preliminary Design Review
PKI	Public Key Infrastructure
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
SNMP	Simple Network Management Protocol
SoC	Statement of Compliance
SQL	Structured Query Language
SSL	Secure Socket Layer
SSRS	System Security Requirements Specification
TBD	To be done
TLS	Transport Layer Security
UTC	Coordinated Universal Time
VAL	Validation Chain
VLAN	Virtual Local Area Network

Abbreviation	Definition
VPN	Virtual Private Network
WAN	Wide Area Network
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
[AD-07]	on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection	COUNCIL DIRECTIVE 2008/114/EC	N/A
[AD-08]	on the security rules for protecting EU classified information	COMMISSION DECISION (EU, Euratom) 2015/444	N/A
[AD-09]	on the security of communication and information systems in the European Commission	COMMISSION DECISION (EU, Euratom) 2017/46	N/A

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
[RD.06]	SACP Annex F - Security Vulnerability Management Requirements	GAL-PL-CIMC-SEC-X/7527	3.3
[RD.07]	Cyber security requirements for Management	GSA-SEC-SREQ-SPE-237329	1.2
[RD.08]	Cyber security requirements for service operations	GSA-SEC-SREQ-SPE-232365	1.4
[RD.09]	Cyber security requirements for service infrastructure maintenance	GSA-SEC-SREQ-SPE-237266	1.2
[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

Reference Documents:			
Type	Title	Reference	Issue
[RD.15]	IA Security Policy on Interconnection	IASP 3 6488/15	N/A
[RD.16]	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 for 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;
    - Maintenance CSM, CSM of the organization in charge of maintenance of the developed 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. When not differently specified, within this document with CIA it is intended the prime contractor CIA. 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;
    - Maintenance CIA, CIA of the organization in charge of maintenance of the developed infrastructure.

The following three actors have been used in order to make easier the understanding of the requirements; these are defined in the [AD-06] and are part of the OPS entity:

- **Security Equipment Administrator** –is an end user of the system; he/she is part of the organization which will operate the system after deployment. He/she is responsible to perform preventive and corrective maintenance of the infrastructure, manage operators accounts, and system security configuration using provided procedures.
- **Security Analyst**, is an end user of the system; is part of the organization which will operate the system after deployment. He/she is responsible for monitoring the security status of the system, using provided procedures.
- **System INFOSEC Officer,** they are responsible for the information security of operations. They are the point of contact with GSMC and the LSAA.

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** – when the infrastructure is in operation, it is the support provided to address any infrastructure issues not resolvable through predefined maintenance procedures (e.g. patches application).

The term **SECMON** refers to the Security Monitoring infrastructure operated by GSMC. It performs real-time raw data collection and analysis from the infrastructure. It also provides incident response support tools as for example forensic data extraction capabilities.

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.

Malware: is the short for malicious code, that can be defined as "software which interferes with normal operation of a computer system". Another definition might be "software which executes without the express consent of the user". Malicious code is therefore a threat for the integrity, availability and confidentiality of data.

3 Network map management

The CSM is in charge of maintain the Network map of the infrastructure, which is used for different activities. As an example, CSMs use it to identify and localise vulnerabilities and analyse their impact; CIAs use it to plan audits and vulnerability assessments, an report results.

Responsibility of maintaining the network map is owned by the infrastructure provider during development, and it is transferred to the operator when the infrastructure enters in operations. This is shown in Figure 2.

During the development phase, the Infrastructure CSM provides the Network Map "as Designed" for the different reviews (PDR, CDR, QR, OVR, AR). The Operator CSM will receive the network map from GSA, and he will receive it at least at OVR, in order to enable the handover of the responsibility at AR.

After entering in operation, the Operator CSM takes over the responsibility of maintaining the network map "As Operated", communicating any change to GSMC. 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.

Also the CSM appointed under the maintenance contract shall 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 major/minor releases of the infrastructure.

For major releases of the infrastructure, the infrastructure CSM shall instantiate a new instance of the "As Designed" network map.

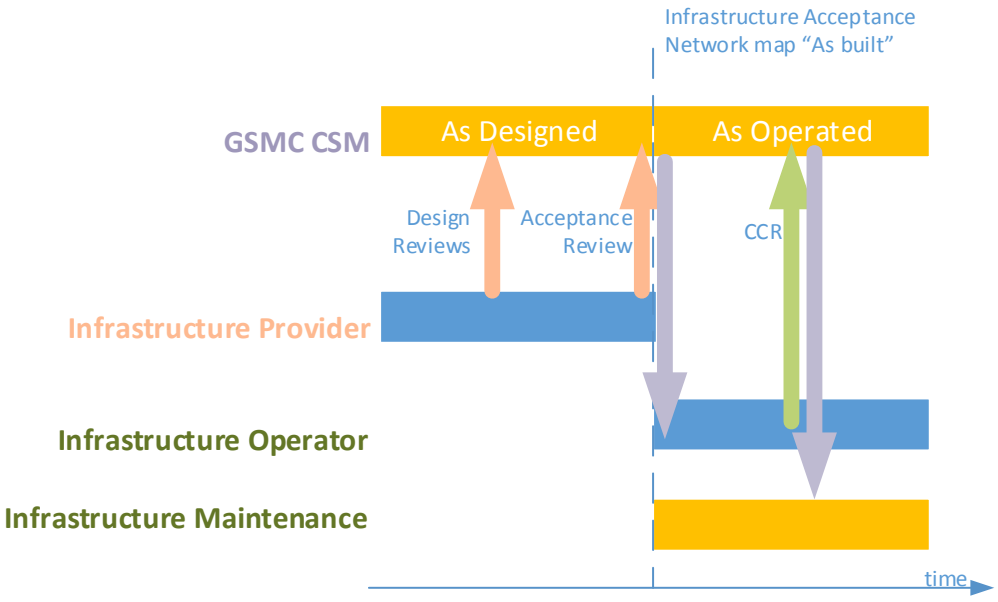

Figure 2 - Network Map responsibility

CYB-INF-0010 Network map "As Designed"

The CSM shall establish the network map “as Designed”. It describes the infrastructure as it is going to be deployed at acceptance. Its detail is expected to increase along with the maturity of the design and development. This version of the network map is also used for production of minor/major releases.

Network map shall follow the template in [RD.13].

If VAL chain network map is different from the OPE chain one, a dedicated instance shall be required.

End of requirement

CYB-INF-0020 Network map version control

All instances of the network map shall be under version control.

End of requirement

CYB-INF-0030 Network map responsibility

The prime contractor CSM is responsible in front of GSA for completeness and quality of the network map, including contributions from subcontractors. The prime contractor CSM is responsible to provide the complete network map to GSA CSM.

End of requirement

CYB-INF-0040 Network map “as Built” provision

At infrastructure qualification, the CSM shall provide the network map of the deployed infrastructure to GSA CSM and Operator CSM.

End of requirement

Note: quality and completeness of the network map will be reviewed by GSA and Operator CSM, and any identified issue may compromise infrastructure acceptance decision.

CYB-INF-0050 Network map reviews

The network map shall be submitted by the CSM for approval at each development review (e.g. PDR/CDR/QR/AR/DRB, for either segment and elements).

End of requirement

4 Vulnerability management

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 shall 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 has to be kept under configuration control, and provided to GSA, GSMC and operator CSM.

The vulnerability management process shall include 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 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 [CYB-INF-0060]:

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-INF-0070]. 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-INF-0100] 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-INF-0120] will be produced monthly including all vulnerabilities and their individual reports along with vulnerability metrics [CYB-INF-0140]. 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-INF-0210. Non vulnerable assets should also be identified [CYB-INF-0150].

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-INF-0170] 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-INF-0060 Vulnerability Baseline Score

The CSM shall define for each vulnerability in any 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-INF-0070 Vulnerability database

The CSM shall establish a vulnerabilities database, where are collected all the identified vulnerabilities affecting the infrastructure under development. For each vulnerability, results of the analysis shall be reported, as prescribed in CYB-INF-0110, and when available, the associated correction or mitigation.

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 may be a vulnerability notification.

CYB-INF-0080 Subcontractor vulnerability tracking responsibility

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

End of requirement

CYB-INF-0090 Vulnerability identification

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

- the network map
- the information related to vulnerabilities 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

In case of identification of new vulnerabilities the contractor CSM should update his local vulnerability database immediately.

End of requirement

CYB-INF-0100 Vulnerability analysis

The CSM shall analyse the risk associated to a vulnerability, in terms of exploitability and impact on service.

End of requirement

CYB-INF-0110 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 publication of the vulnerability ;
- Date of identification of the vulnerability
- Vulnerability identifier (e.g. CVE) if any;
- CSM in charge of the analysis;
- Element(s) affected, referencing the applicable network map;
- Source of information of the original vulnerability notification, and original report in appendix;
- Original criticality (e.g. CVSS)
- Assessed criticality based on deployed technical/operational mitigations (e.g. CVSS score including environmental and temporal metrics)
- Potential impact;
- Potential attack vectors and exploitation methods;
- Remediation (e.g. patch) availability;
- Correction/Patch impact analysis;
- 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-INF-0120 Vulnerability report

The vulnerability report shall list all the vulnerabilities in the vulnerability database, along with the associated analysis and details. The first version of the vulnerability report shall be provided to GSA at QR, in order to identify any required correction before AR. At infrastructure acceptance, the CSM shall provide the updated vulnerability report related to the deployed infrastructure to the GSA, Operational CSM and to GSMC.

End of requirement

Note: quality and completeness of the vulnerability report will be reviewed, and any identified issue may compromise infrastructure acceptance decision.

CYB-INF-0130 GSA vulnerability discrepancies

The contractor CSM shall receive from GSMC the list of known vulnerabilities affecting the infrastructure under maintenance. The CSM shall report any discrepancy from the vulnerability database they manage.

End of requirement

CYB-INF-0140 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 Cyber Security Board, or following the update of 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.

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

End of requirement

CYB-INF-0150 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-INF-0160 Configuration control of vulnerability list

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

End of requirement

Note: this requirement intends to track the evolution of the vulnerabilities within the database, and be able to recover the status at specific moments in time.

CYB-INF-0170 Vulnerability correction plan (Assurance Maintenance Plan)

At QR, the CSM shall provide a vulnerability correction plan, which will drive the correction of eventual vulnerabilities, deviation from baseline, and patch implementation. The Vulnerability Correction plan is updated and redelivered for AR, taking in consideration any further correction performed before Acceptance.

End of requirement

Note: the vulnerability correction plan is forwarded also to GSMC in order to enable preliminary risk analysis.

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, and it is also 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-INF-0180 Patch identification

The contractor CSM shall identify any new patch correcting vulnerabilities affecting the infrastructure to be delivered. 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 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

CYB-INF-0190 Subcontractor patch management responsibility

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

End of requirement

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

CYB-INF-0200 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-INF-0210 Patch report

Along with the Vulnerability report identified in [CYB-INF-0120], the CSM shall provide a patch report at QR for each instance of the network map. The report shall list all available and deployed patches, in relation with the associated vulnerability. For any non-applied software or firmware patch released by the vendor which is

older than 1 month, the CSM shall provide an analysis as specified in CYB-INF-0220 to GSA CSM, Operator CSM and GSMC.

The patch report shall be updated at AR, to ensure the coverage of any non-applied software or firmware patch released by the vendor which at Acceptance Review is older than 1 month.

End of requirement

Note: To enable compliance to CYB-INF-0240, CYB-INF-0250 and CYB-INF-0260, additional patches may be installed between QR and AR. When required by the operator and agreed by GSA CSM, patching may be delayed after AR, in order to do not disturb the Operational Validation activities.

CYB-INF-0220 Patch impact 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 and engineer(s) 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.

End of requirement

CYB-INF-0230 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

These metrics shall be organized by vulnerability criticality level.

End of requirement

CYB-INF-0240 Patching before infrastructure deployment - network and security elements

At infrastructure Acceptance Review, security and network elements of the infrastructure (firewalls, VPN, switches, routers, Anti-Virus, etc…) shall have installed the latest version of firmware and all available patches from the vendor.

End of requirement

CYB-INF-0250 Patching infrastructure assurance – services exposed through external interfaces

At infrastructure Acceptance Review, all servers accessible through external interfaces (e.g. web servers, SFTPs, etc.) shall have installed all the latest patches from the vendor.

End of requirement

CYB-INF-0260 Patching infrastructure assurance

Software and hardware (apart from the ones identified in [CYB-INF-0240 and CYB-INF-0250]) composing the infrastructure shall have installed, all the software and firmware patches released by the vendor which have been identified 9 months before the acceptance review.

End of requirement

CYB-INF-0270 Cyber Request for deviation associated to patches

At infrastructure Acceptance Review, the CSM shall provide a cyber request for deviation for each available patch which had not been implemented. The RfD shall have the same content as specified in [CYB-INF-0280]. RfDs can be in appendix to the vulnerability correction plan [CYB-INF-0170].

End of requirement

Note: the list of Cyber RfD will be reviewed by the Cyber Board and by the SAB. Ultimately the risk owner may decide to not accept the residual risk, and then the infrastructure.

CYB-INF-0280 Cyber Request for Deviation

To be valid, a cyber request for deviation shall include in any case at least:

- The justification for the statement of partial or non-compliance to a cyber requirement;
- An assessment of the security risks resulting from the partial or non-compliance to a cyber-requirement;
    - the description of the task(s), including impact in terms of schedule, budget and service provision, required to:

- recover completely the compliance to the concerned cyber requirement;
- mitigate operationally the assessed risk;
- identify potential attacks scenarios that may benefit from the partial or non-compliance to the concerned cyber requirement;

- A recommended way forward (operational mitigations, security monitoring or not-needed);
  - The justification for the recommendation;

- Expiration date for the deviation and a committed schedule for the complete recovery of the compliance to the concerned cyber requirement (action plan).

End of requirement

6 Obsolescence management

When selecting hardware and software, it is important to consider the support which will be provided during the lifetime of the infrastructure. It shall be avoided that patches for vulnerabilities are not provided because a 3rd party software is not maintained.

CYB-INF-0290 COTS provider selection

The contractor shall select COTS suppliers which provide maintenance for their products for at least 3 years after infrastructure acceptance.

End of requirement

CYB-INF-0300 Obsolescence plan

A segment obsolescence plan shall be delivered as part of the segment delivery. The obsolescence plan shall cover the whole operational life cycle of the infrastructure.

End of requirement

CYB-INF-0310 Maintenance of 3rd party software

When maintenance of 3rd party software is not guaranteed (e.g. GPL/GNU licences), the contractor shall perform a risk assessment, and where relevant confirm that it is possible to develop patches in house, or substitute the obsolete software.

All occurrences of this type of software shall be identified and reported to GSA.

End of requirement

Note: if support is discontinued, the risk is that a mitigation may not be possible for a critical vulnerability.

7 Infrastructure acceptance audit

At the moment of acceptance, the contractor shall demonstrate its compliance to these requirements, and the declared cyber risk level (calculated on the basis of non or partial compliances to these requirements, or exposed vulnerabilities). This demonstration is provided through the acceptance audit performed by the CIA.

Results of the acceptance audit are expected to be available at Qualification Review, in order to promptly identify any residual issue that shall be corrected before Acceptance Review.

CYB-INF-0320 Cyber acceptance audit plan

The CIA shall provide a cyber acceptance audit plan within the CDR data pack for GSA CIA review and approval, and will be updated in the relevant milestones.

End of requirement

CYB-INF-0330 Infrastructure acceptance

The CIA shall plan and perform the acceptance audit, to demonstrate:

- Completeness of provided acceptance data package (as defined below);
- Correct implementation of cyber security technical requirements:
    - Features in support to incident detection (see section 8.20)
    - Feature in support to incident investigation and reaction (see section 8.18 and 8.19)
    - Accounts limitation, according with CYB-INF-0790 and CYB-INF-0820;
    - Software and Services limitation, according with CYB-INF-1350, CYB-INF-1360 and CYB-INF-1370.
    - Accounts inventory, according with CYB-INF-0780, CYB-INF-0790, CYB-INF-0830 and CYB-INF-1020;
    - Completeness of password list to be delivered at infrastructure handover, in accordance with CYB-INF-2760;
    - Security configuration, in accordance with CYB-INF-1400 and CYB-INF-1410;
    - Removal of development kits, in accordance with CYB-INF-1390;
    - Root accounts disabled, in accordance with CYB-INF-0430 and CYB-INF-0460;
    - Least privilege and separation of duties, in accordance with CYB-INF-0640, CYB-INF-0650, CYB-INF-0660 and CYB-INF-0670;
    - Installation and maintenance rights, in accordance with CYB-INF-0430;
    - Need to know principle for interfaces, according with CYB-INF-1980 and CYB-INF-2160;
    - Limitation of scripts, in accordance with CYB-INF-1330;

- Audit logs, in accordance with CYB-INF-2430 and CYB-INF-2500, or [RD.10];
- Virtualised environment, as required in CYB-INF-1630;
- Any other technical requirement;

- Completeness of network map, as required in CYB-INF-0010;
- Patching as documented in the patch report;
- Mitigations to vulnerabilities as described in the vulnerability report;
- Risk impacting the infrastructure is in accordance with the vulnerability report, and any cyber RfWs and cyber RfDs.
- Lockdown report, according with CYB-INF-2730 and CYB-INF-2740.

End of requirement

CYB-INF-0340 Independent audits and penetration tests

Audits and penetration tests shall be performed by the infrastructure supplier CIA with auditors recognised by EU NSAs.

End of requirement

CYB-INF-0350 Acceptance audit of architecture and configuration

System audits shall cover system architecture and configuration, to ensure cyber security hardening.

End of requirement

CYB-INF-0360 Acceptance penetration test

Audit and penetration tests shall be performed at Segment/Service Facility level and Galileo Global Component level, combining VAL and OPE chain audits with an incremental approach. Tests shall demonstrate at least that:

- There are no more vulnerabilities than the ones reported in the vulnerability report;
- Vulnerability exploitability and impact is in line with what had been declared in the vulnerability report;
- Risk due to non or partial compliances is as reported in terms of likelihood and consequences;

This shall be responsibility of the Contractor's CIA.

Both COTS and bespoke software shall be included in the audit plan. Audit shall be performed at architecture and configuration levels.

End of requirement

Note: if an element is provided by a subcontractor, the pen-test can be managed by the subcontractor CIA. The infrastructure pen-test has to be managed by the contractor CIA.

Note: due to a non-compliance, a function may be exposed to a risk. The pen test shall demonstrate that the risk likelihood and consequences are as reported in the RfW/RfD.

CYB-INF-0370 External interface penetration test

All external boundary devices, and external network connections of the infrastructure with external entities shall be pen tested to verify that no vulnerability is exposed.

End of requirement

CYB-INF-0380 Support to Program and SAB penetration tests

In the case of the Programme or SAB performing a security assessments (i.e. audit and or penetration test), the CIA shall support the tester providing required information and access to the infrastructure.

End of requirement

CYB-INF-0390 Cyber acceptance report

At the conclusion of cyber acceptance activities, the contractor CIA shall provide the cyber acceptance report to GSA CIA and PM. The report shall provide details of activities performed executing CYB-INF-0330, CYB-INF-0340, CYB-INF-0350, CYB-INF-0360, CYB-INF-0370 and CYB-INF-0380 highlight any cyber critical findings identified.

The acceptance audit report shall be available within the data package delivered at Qualification Review, in order to allow any required correction before Acceptance Review.

End of requirement

CYB-INF-0400 Cyber critical findings during cyber acceptance audit

The CIA shall prompt the CSM to include resolution of any cyber critical findings in the vulnerability correction plan, or raise an Cyber Request for Deviation, in accordance with CYB-INF-0280.

End of requirement

Note: the list of Cyber RfD will be reviewed by the Cyber Board and by the SAB. Ultimately the risk owner may decide to not accept the residual risk, and then the infrastructure.

8 Technical requirements

This chapter provides technical requirements applicable to new infrastructure developments, and infrastructure evolutions. Requirements are derived from EC Cyber requirements, SSRS, industry standards and applicable EU regulations.

Additional project specific requirements may be added. For example, in case of deployment of certified equipment.

8.1 User accounts and access control

Purpose of following requirements is to ensure that all users of the system are responsible for activities they perform, and that they can perform only activities for which they are entitled: user is authenticated and authorised at the moment of establishing a session, and its relevant activities tracked. Key roles are the security equipment administrator which manages authentication and authorisation, and the security analyst which performs audits (accounting).

Requirements in this section are applicable to network equipment, operating systems, COTS applications and any bespoke applications which require user authentication.

CYB-INF-0410 Authorised use of the infrastructure

Only authorised personnel are permitted to operate the Infrastructure.

End of requirement

Note: authorised personnel are part of the operational team, they have a role defined by the concept of operations (then a need to access the infrastructure).

CYB-INF-0420 Accountability

The Infrastructure shall enforce accountability of activities performed by users. Generic accounts (e.g. 'admin', 'guest', 'pippo' or 'operator') shall be disabled or removed, unless full accountability can be ensured. When generic accounts are used (e.g. legacy system), this shall be justified, and a risk analysis submitted.

End of requirement

Note: static credential hardcoding is not allowed.

CYB-INF-0430 Root access

Root access or use of administrative account shall not be used for nominal maintenance operations. In exceptional cases their use may be possible exclusively for L2/L3 corrective maintenance (e.g. installation of new software or patches), and while the Infrastructure is not operational.

End of requirement

CYB-INF-0440 Administrative privileges

Where for operational reasons it is needed the execution of a program or script requiring root privileges/ administrative privileges, its execution shall be enabled only for target users via dedicated accounts (i.e. sudoers file for Unix like OS, run-as on windows). Executables or scripts shall be owned by root, and not modifiable by any other users.

End of requirement

CYB-INF-0450 Root passwords

At acceptance, root/administrative passwords shall be provided in separated sealed envelopes to the system INFOSEC officer.

Passwords shall be protected during all their life cycle to avoid compromise of the infrastructure.

End of requirement

Note: after infrastructure handover to operations, the SIO is in responsible to protect the confidentiality of the password, and allow its use where required.

CYB-INF-0460 Remote access privileges

It shall not be possible to connect to a remote host using root or administrative accounts.

End of requirement

Note: requirement intends to avoid compromising accountability.

CYB-INF-0470 User account

The infrastructure shall identify univocally each user authorised to access its functions (each user shall have its own personal user account), for Operating Systems and any COTS or bespoke application.

End of requirement

CYB-INF-0480 Single account for whole infrastructure

An user shall have a single user accounts to access facilities of the infrastructure.

End of requirement

Note: multiple user accounts implies more maintenance effort, and increase the probability of the user mishandling authentication tokens.

Note: usually this is achieved using a single authentication service (e.g. LDAP) for the whole infrastructure.

Note: depending on operational needs, an account will have different level of access on different hosts.

CYB-INF-0490 Protection of identification and authentication credentials

The infrastructure shall protect identification and authentication credentials against unauthorised access.

It shall not be possible for an user of the system to get the list of users, or password hashes.

End of requirement

CYB-INF-0500 Protection of identification and authentication credentials over the network

The infrastructure shall protect identification and authentication parameters against interception and replay attacks when exchanged on a network.

End of requirement

CYB-INF-0510 User authentication and authorisation

When user accesses a function of the infrastructure he/she shall be prompted for login (authentication and authorisation). This establishes the start of an interactive session. After finishing work the user is expected to log-out and end his/her session.

End of requirement

CYB-INF-0520 Functionalities before authentication

Before being authenticated, only the authentication function shall be available to the user (i.e. it shall not be possible to power-off reboot etc.)

End of requirement

CYB-INF-0530 Automatic remote session termination

Once a remote session has been established, the infrastructure shall terminate the session after a definable time interval of user inactivity. A maintenance (L1) procedure to set the time interval shall be provided in the user manual.

End of requirement

CYB-INF-0540 User session locking

The Infrastructure shall allow user to lock his/her own interactive session, by disabling any activity of the user's data access devices other than unlocking the session. The Infrastructure shall require user re-authentication prior to unlock the session.

End of requirement

CYB-INF-0550 Automatic session locking

The Infrastructure shall lock an interactive session after a definable time interval of user inactivity by disabling any activity of the user's data access devices other than unlocking the session. The Infrastructure shall require user re authentication prior to unlocking the session. A maintenance (L1) procedure to set the time interval shall be provided in the user manual.

End of requirement

CYB-INF-0560 Access history notification

Upon successful session establishment, the Infrastructure shall display the date, time and location of the last previous successful and unsuccessful attempts to session establishment and the number of unsuccessful attempts since the last successful session

establishment.

End of requirement

CYB-INF-0570 User acknowledgement of access history

The Infrastructure shall require the user to acknowledge the displayed information.

End of requirement

Note: e.g. click "Ok" before closing the access history pop up.

Note: this requirement is to alert the user in case of malicious login attempts, so he can raise an alert to the SIO.

CYB-INF-0580 Unauthorised use warning

Before establishing a user session, the Infrastructure shall display a legal warning notice regarding unauthorised use of the system.

End of requirement

CYB-INF-0590 Credential expiring warning

The Infrastructure shall notify the user before expiration of its credentials. The notification period shall be configurable by the security equipment administrator.

End of requirement

CYB-INF-0600 Authentication credential renewal grace time

The infrastructure shall allow a last (single) "grace login" after password expiration. The only functionality allowed to the user shall be the password renewal.

End of requirement

CYB-INF-0610 Password reset

The security equipment administrator shall be able to reset the user account password.

End of requirement

CYB-INF-0620 Password renewal after password reset

The user shall be forced to renew his/her password at his /her first login, or after password reset.

End of requirement

Note: it is required in order to ensure that the password is known only by the user *. After user account creation, or password reset, the security equipment administrator knows the password in order to communicate it to the* user *.*

CYB-INF-0630 Two factor authentication

At least for security equipment administrator, two factor authentication shall be used.

End of requirement

Note: e.g.: smartcard, biometric, token, etc.

CYB-INF-0640 user roles

The infrastructure shall provide at least the following user roles:

- Operator – to perform operational activities of the infrastructure (depending on the infrastructure there may be different types of operators). Multiple operator roles shall be defined based on the different need-to-know. Each operational role shall be duly justified;
- Security Equipment Administrator – performs preventive and corrective maintenance of the infrastructure, configures security parameters, and manages user access and privileges;
- Security analyst – inspect audit logs, and system configuration. Shall not be able to modify anything on the infrastructure.

Each role shall be limited to the minimum set of required privileges to perform its activities on the infrastructure.

End of requirement

CYB-INF-0650 Security analyst segregation of duties

Referring to CYB-INF-0640, the infrastructure shall ensure that if a user has assigned the Security analyst role, he/she cannot have any other role associated. The security analyst shall have “read-only” access to the system.

End of requirement

CYB-INF-0660 Authorisation and least privilege principle

The Infrastructure shall enforce the least privilege principle: it shall provide the capability to logically control and restrict the access to processing functions (commands) and information according to user roles and associated need-to know.

System shall grant to the user access only to information and resources that are necessary for his/her legitimate purposes.

End of requirement

CYB-INF-0670 Need To Know and least privilege principle

While implementing CYB-INF-0660 and CYB-INF-0680 the need to Know policy shall be taken in account.

End of requirement

CYB-INF-0680 Rights for software installation and upgrade

Software installation and upgrade is an high level maintenance activity (L2/L3). (i.e. the security equipment administrator shall not be able to perform autonomously this type of activity).

End of requirement

Note: during operations of the infrastructure, software installation and upgrades are managed through the configuration change process.

CYB-INF-0690 Security function administration

The Infrastructure shall restrict the ability to disable, enable or modify the behaviour of the security functions to security equipment administrator only.

End of requirement

CYB-INF-0700 Secure operations workstations

The Infrastructure shall provide one (or more) dedicated workstations for security activities (management and auditing). It shall be possible to deploy this workstations outside of the MCR.

End of requirement

Note: these are used only by security equipment administrator and security analyst.

CYB-INF-0710 user account enabling/disabling

The infrastructure shall allow the security equipment administrator to enable/disable a user account.

End of requirement

CYB-INF-0720 User account creation

The infrastructure shall allow the security equipment administrator to create a user account. At least following information shall be associated to the account:

- user Id
- Name and Surname
- Badge Id
- Account creation timestamp
- Last account modification timestamp
- Account validity expiration
- List of roles
- Need to Know (if applicable)
- Comment
- Status (e.g. enabled, disabled, suspended, revoked);

End of requirement

CYB-INF-0730 user account management

The infrastructure shall allow the security equipment administrator to modify a user account.

End of requirement

CYB-INF-0740 Trigger for password renewal

The infrastructure shall allow the security equipment administrator to force an user to update his/her account's password.

End of requirement

CYB-INF-0750 User account lock-out

When the defined maximum number of unsuccessful authentication attempts has been surpassed, the Infrastructure shall disable the user account (account lock-out).

The security equipment administrator shall be able to un-lock the account status.

End of requirement

CYB-INF-0760 Audit of user list

The infrastructure shall allow the security analyst to have read only access to the list of users and available information. The security analyst shall be able to extract/print this list.

End of requirement

CYB-INF-0770 Accounts security logging

The infrastructure shall log at least the following security events:

- User account provisioning events (e.g. creation, suspension, deletion, etc…)
- User session events (successful login, unsuccessful login, session terminated, session timeout, etc…)
    - A specific focus shall be provided on root accounts (e.g. login attempts)

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

CYB-INF-0780 List of available user roles

Defined user roles shall be listed, providing details of access and execution rights and a justification for each operator role.

End of Requirement

CYB-INF-0790 User accounts list

The list of user accounts for each host shall be provided at acceptance. The number of user accounts shall be limited (i.e. proportioned to the test activities to be performed), and only to be used for qualification/acceptance testing activities. Unnecessary user accounts shall be removed or disabled after tests, before handover to operator.

End of requirement

CYB-INF-0800 user account passwords

At acceptance, passwords for user accounts shall be provided to the System INFOSEC Officer.

End of requirement

CYB-INF-0810 Initial Security Equipment Administrator Account

A security equipment administrator account shall be available to enable the security equipment administrator of the operating entity to configure the infrastructure after acceptance. The account password shall be provided to the System INFOSEC Officer.

End of requirement

8.2 Non-human account

CYB-INF-0820 Limitation of non-human accounts

The use of non-human accounts is not allowed.

In exceptional cases, where their use is needed, their privileges shall be strictly limited to what is needed to perform the functionality. Non-human accounts should not be allowed to log into the system in interactive sessions.

End of requirement

CYB-INF-0830 Non-human accounts list

At acceptance, the list of non-human accounts shall be provided, along with their justification.

It shall not be possible to create new non-human accounts in the operational chain.

End of requirement

Note: e.g. LDAP master account, MySQL root, etc.

Note: this list needs formal approval by the SAB (SSRS IdAuth-06).

CYB-INF-0840 Non-human account passwords

It shall not be possible to login with non-human accounts (CYB-INF-0820), then passwords should not be required.

In exceptional case where passwords are defined, after acceptance these passwords shall be provided in separated sealed envelopes to the System infosec officer.

End of requirement

CYB-INF-0850 Non-human account password renewal

The security equipment administrator shall be able to renew passwords for non-human accounts. Current non-human account password shall be needed for this operation.

End of requirement

CYB-INF-0860 Non-human account authentication credentials configuration

The password policy for non-human account shall be compliant with CYB-INF-0900. However non-human accounts shall not be locked out in case of high number of failed logins

End of requirement

Note: During lockdown, the operator will enforce the non-human account password policy, which will be in general more strict than the one for user *accounts.*

CYB-INF-0870 Non-human accounts logging

The infrastructure shall log at least the following security events:

- Successful session established (login)
- Session terminated
- Unsuccessful login
- Non-human account modified
- Non-human account password renewed

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

8.3 Password policy

This section specifies requirements for the infrastructure in order to allow enforcement of the password policy. The security equipment administrator is in charge of managing the password policy. When an user changes his/her password, the infrastructure shall ensure that it is of adequate quality.

CYB-INF-0880 Password renewal

It shall be possible to renew any defined password in the infrastructure. A maintenance (L1) procedure to renew password for each non-human account shall be provided in the user manual.

End of requirement

CYB-INF-0890 Password policy

The infrastructure shall enforce password policies for:

- User account
- Non-human accounts (if required)
- M-to-M accounts (if required)

It shall be possible to define a different password policy for each of the above types of accounts, and for each type of user (e.g. operator, security equipment administrator, security analyst).

End of requirements

CYB-INF-0900 Password policy configuration

The credentials used for authentication in the infrastructure shall be configurable by the security equipment administrator within ranges specified below:

- Length of authentication credential : [10..64]
- Characters sets :
  - At least 1 alphanumeric lowercase [a..z]
  - At least 1 alphanumeric uppercase [A..Z]
  - At least 1 numeric [0..9]
  - At least 1 special character [eg. '@','#',"$','%']
- As far as possible, check that no trivial passwords are used (e.g. contains the user id).
- Number of authentication credentials to remember to prevent repetition : 20
- Duration of authentication credentials validity [0..360 days]
- Authentication credential expiry warning [15..30 days] (*see CYB-INF-0590*)
- Number of failed logins before user account lock out: [3 10]

End of requirement

CYB-INF-0910 Default password policy

The default password policy shall be:

- Length of authentication credential : 12
- Characters sets :
  - At least 1 alphanumeric lowercase [a..z]
  - At least 1 alphanumeric uppercase [A..Z]
  - At least 1 numeric [0..9]
  - At least 1 special character [eg. '@','#',"$','%']
- Number of authentication credentials to remember to prevent repetition : 20
- Minimum duration of authentication credentials validity: 2 days
- Maximum duration of authentication credentials validity: 60 days
- Authentication credential expiry warning: 20 days
- Number of failed logins before user account lock out: 5 attempts.

End of requirement

CYB-INF-0920 Security equipment administrator password policy deviation

The security equipment administrator account cannot be locked out.
End of requirement

CYB-INF-0930 Password policy modification logging

The infrastructure shall log a security event when the password policy is modified, providing details of the change.

End of requirement

8.4 Information access control

CYB-INF-0940 Information access control

If the infrastructure contains sensitive resources (e.g. classified information, company sensitive, or personal details), it shall monitor access to these resources to detect unauthorised access or access attempts.

End of requirement

CYB-INF-0950 Information access control logging

The infrastructure shall log at least the following security events:

- Authorised access to sensitive resource;
- Unauthorised access attempt to sensitive resource;

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

CYB-INF-0960 Multi-layer environment protection

Where the infrastructure is handling EUCI, it shall provide multi-layer security levels segregation, with the use of accredited equipment (e.g. data diode, physical segregation, accredited hypervisors).

End of requirement

8.5 Machine to Machine interface

This section specifies authentication requirements for machine to machine interfaces. Use of shared secrets (passwords) for authentication can be easily exploitable and requires significant maintenance effort when

there are a large number of M-to-M interfaces (e.g. in the case of syslog or SNMP). The section requires to use certificate based authentication in order to authenticate and encrypt M-to-M communications.

CYB-INF-0970 Certificate based authentication

Machine to Machine interfaces shall use certificate based authentication, to authenticate both servers and clients.

End of requirement

Note: Existing ICDs take always priority over this requirement.

CYB-INF-0980 Certificate management

The security equipment administrator shall be able to manage certificates during their lifecycle.

End of requirement

Note: in case of crypto items, the crypto custodian is responsible for the certificates management.

CYB-INF-0990 Certificate protection

The infrastructure shall protect the certificates from unauthorised access.

End of requirement

CYB-INF-1000 Certificate expiry warning

The infrastructure shall notify the security equipment administrator and the security analyst 30 days in advance of certificate expiration.

End of requirement

CYB-INF-1010 M-to-M authentication in legacy systems

When using legacy system, unable to support certificate based authentication, username and password authentication can be used. In this case, it shall be possible to enforce an adequate password policy, according to CYB-INF-0900. The security equipment administrator shall be able to periodically renew passwords. Authentication credentials confidentiality shall be protected when stored and when transmitted over the network.

This type of account shall be treated as a non-human account.

End of requirement

Note: When using this type of authentication, a dedicated password policy shall be defined, according to CYB-INF-0900. However M-to-M accounts shall not be locked out in case of high number of failed logins. Logs shall be generated as per CYB-INF-0870.

CYB-INF-1020 List of M-to-M interfaces

At acceptance, the contractor shall provide the list of M-to-M interfaces, along with their details.

End of requirement

CYB-INF-1030 Certificate modification and logging

The infrastructure shall log a security event when:

- A certificate is due to expire in less than 30 days (one event per day)
- A certificate expired (one event per hour)
- A certificate had been renewed
- Certificate based M-to-M authentication failed
- Critical data transferred

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

Note: Critical data shall be defined case by case.

8.6 Host protection

CYB-INF-1040 Host security events logging

Each host of the infrastructure shall log a security event when:

- IT performances monitoring, e.g.:
  - CPU usage over a configurable threshold
  - Hard disk available space under a configurable threshold
  - RAM available space under a configurable threshold
  - Bandwidth utilisation on an interface over a configurable threshold
  - Any software or hardware failure
- Security related IT events, e.g.:
  - Start/stop of a service
  - Time synchronization problems
- Host security events, e.g.:

- Root privileges invoked
- Host-based firewall events
- Host intrusion detection system
- Antimalware events

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

CYB-INF-1050 Host Intrusion Detection System

Critical hosts shall deploy an host-intrusion detection system (HIDS).

End of requirement

Note: host are considered critical where their compromise may have an immediate impact on service provision. These shall be identified by PDR.

CYB-INF-1060 Host intrusion detection system signature update

When signature based HIDS are used, the security equipment administrator shall be able to update the signature. Signature update shall be possible using a centralized management tool.

End of requirement

CYB-INF-1070 Host-based Firewall

Each host shall have an host-based firewall enabling only inbound or outbound connections required to provide or use allowed services.

End of requirement

CYB-INF-1080 Time synchronisation

All infrastructure hosts and equipment shall be automatically synchronized on Galileo System Time (GST).

End of requirement

CYB-INF-1090 Antimalware selection justification

The contractor shall define an antimalware strategy, and based on this, justify the choice for the selected antimalware solution.

End of requirement

CYB-INF-1100 Antimalware protection

All servers and workstations of the infrastructure shall be protected by antimalware software. It shall not be possible to disable antimalware protection.

End of requirement

CYB-INF-1110 Antimalware update

The security equipment administrator shall be able to update antimalware signatures locally and remotely using a centralized management tool.

End of requirement

CYB-INF-1120 Antimalware signature retrieval

The security equipment administrator shall be able to retrieve signature updates from internet, and verify signature integrity. This activity shall be performed on a workstation segregated by an airgap from the rest of the infrastructure.

End of requirement

CYB-INF-1130 Local antimalware update

The security equipment administrator shall be able to manually update the antimalware signature locally on the server/workstation, in a secure way, and verify their integrity.

End of requirement

CYB-INF-1140 Remote antimalware update server

All antimalware instances shall get their updates automatically from a signature server inside the Infrastructure. The security equipment administrator shall be able to load on the signature server new signatures in a secure way, and verify their integrity.

End of requirement

CYB-INF-1150 Antimalware real-time protection

Antimalware real-time protection shall be always enabled.

End of requirement

CYB-INF-1160 On-demand antimalware scan

The security equipment administrator and the security analyst shall be able to perform on-demand antimalware scan. It shall be possible to perform these scans remotely.

End of requirement

Note: scans can be triggered from the workstation identified in CYB-INF-0700.

CYB-INF-1170 Schedule of on-demand scans

The security equipment administrator shall be able to schedule on-demand scans. Scheduled scans can be recurrent or isolated.

End of requirement

CYB-INF-1180 Antimalware impact on performances

The Infrastructure shall be dimensioned in order to minimize impact of malware real-time protection or on-demand scans on service performances.

End of requirement

CYB-INF-1190 Antimalware quarantine

The antimalware shall put in quarantine compromised files.

End of requirement

CYB-INF-1200 Extraction from quarantine

The security equipment administrator and the security analyst shall be able to securely extract the content of the quarantine.

End of requirement

CYB-INF-1210 Antimalware dynamic analysis

Along with static analysis, the antimalware shall perform also dynamic analysis (heuristic/behavioural).

End of requirement

CYB-INF-1220 Antimalware crisis

The contractor shall provide crisis procedures to manually isolate the malware, in case the antimalware is not able to quarantine it.

End of requirement

CYB-INF-1230 Antimalware support

The antimalware shall be supported by the COTS provider for at least one year longer than the expected lifetime of the Infrastructure.

End of requirement

CYB-INF-1240 Antimalware signature at acceptance

At acceptance, all instances of the antimalware shall be updated to the latest available signature.

End of requirement

CYB-INF-1250 Antimalware events

The infrastructure shall log at least the following security events:

- Changes of antimalware configuration
- New signature uploaded on the updates server
- Antimalware signature updated
- Antimalware signature expired
- On-demand scan started
- Scan scheduled
- Malware detected
- Malware successfully quarantined
- Failure to remove malware
- Quarantine exported
- Any change in status of real-time protection
- Any type of antimalware error

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

8.7 Encryption

CYB-INF-1260 Deprecated encryption and hashing algorithms

Use of deprecated encryption or hashing algorithms is forbidden.

End of requirement

Note: At the moment of writing this document, examples of deprecated algorithms are SSL and MD5, while effective algorithms are AES and SHA-256.

8.8 Integrity

The infrastructure shall be able to detect if there was a change (intentional or unintentional), using an automated integrity detection system.

CYB-INF-1270 Integrity check

The infrastructure shall provide functions to automatically verify integrity of data used, scripts and code executed in any host and equipment.

End of requirement

CYB-INF-1280 Integrity check execution at start-up

Every host and equipment of the infrastructure shall perform an integrity check at start-up.

End of requirement

CYB-INF-1290 Integrity check on demand

The security equipment administrator, security analyst and any other user which has an operational need, shall be able to trigger integrity checks.

End of requirement.

CYB-INF-1300 Integrity check information

The security analyst shall be able to review the list of files/directories checked for integrity, and files which are in the whitelist.

End of requirement

Note: for whitelist is intended the list of files and directories excluded by the integrity check.

CYB-INF-1310 Integrity check maintenance

The modification of list of files and directories checked for integrity, and of whitelist, shall be a L2 maintenance activity performed while the infrastructure (or sub-system) is not operational.

During nominal operations of the infrastructure, it shall be forbidden to modify integrity check configuration and behaviour.

End of requirement

CYB-INF-1320 Protection of integrity check database

The Infrastructure shall protect the integrity check database from unauthorised access and modification. Only the security analyst and the security equipment administrator can access in read-only this database.

End of requirement

CYB-INF-1330 Script integrity

Execution of scripts shall be forbidden on any host of the infrastructure. If the infrastructure foresees the use of scripts in support to operational tasks, these shall be included in the integrity check database. In this case, the security equipment administrator shall be able to add/remove operator's scripts in the integrity check database. A script deployed in the infrastructure which is not in the integrity database shall raise a security event (script is not authorised).

End of requirement

Note: the security equipment administrator can manage integrity of operator's scripts only (e.g. not OS level scripts). Installation of additional scripts follows the Configuration Change Control process.

CYB-INF-1340 Integrity check events logging

The infrastructure shall log at least the following events:

- An integrity check is performed
- An integrity check fails
- The integrity check database is corrupted
- Access to integrity check database had been attempted
- Integrity check configuration had been modified
- Unexpected file had been found

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

8.9 COTS Hardening

CYB-INF-1350 Authorised software

The CSM shall ensure that only software effectively required for the delivery of the service are installed across the infrastructure. Any other software shall be removed.

End of requirement

CYB-INF-1360 Authorised services

The CSM shall ensure that only services and processes required for the delivery of the service are enabled across the infrastructure. Any other service shall be removed or disabled.

End of requirement

Note: the authorised service list may be a subset of the authorised software.

CYB-INF-1370 List of authorised software and services

At acceptance, the contractor shall provide the list of software installed and services enabled across the infrastructure (this information is included in the network map). Each software and service needs to be justified.

End of requirement

CYB-INF-1380 List of authorised scripts

At acceptance, the contractor shall provide the list of authorised scripts deployed across the infrastructure (this information is included in the network map), and the user privileges required for execution.

End of requirement

CYB-INF-1390 Development tools

The system shall be delivered without development tools that allow the production of executables (compilers, development kits, etc).

If not required and justified, development tools shall never be installed, even before deployment.

End of requirement

CYB-INF-1400 COTS secure configuration baseline

Where applicable, for each OS and COTS used in the system, security approved configurations shall be deployed (for example for classified systems). If not, all security hardening recommendations from the vendor shall be followed and applied unless dully justified.

The security configuration shall be proposed by the CSM and agreed at KO.

End of requirement

Note: for COTS it is intended any software and hardware, including OS, firewall, VPN, antimalware, IDS etc.

CYB-INF-1410 OS and COTS secure configuration baseline document

At acceptance, the contractor shall provide documentation of security guidelines used for OS and COTS security hardening.

End of requirement

Note: examples are Red Hat security hardening checklist, Oracle security checklist and recommendations.

CYB-INF-1420 Security features health check

The infrastructure shall enable the security equipment administrator and security analyst to verify nominal operation of security enforcement services (e.g. HIDS, antimalware, etc.)

End of requirement

CYB-INF-1430 Boot loader hardening

The boot loader shall be adequately protected. It shall allow only the normal system boot (e.g. no single user or recovery modes allowed)

End of requirement

8.10 Bespoke software

CYB-INF-1440 Infrastructure resilience

The infrastructure shall be designed to minimize the impact of failures or attacks.

End of requirement

CYB-INF-1450 Input data validation

The infrastructure shall validate input data, entered either manually or automatically (e.g. range checking, limit on input size, etc.).

End of requirement

CYB-INF-1460 Control of internal processing

The infrastructure shall validate data used for internal processing.

End of requirement

CYB-INF-1470 Message confidentiality, authenticity and integrity

Confidentiality, authenticity and Integrity of messages exchanged between infrastructure subsystems shall be provided.

End of requirement

CYB-INF-1480 Output data validation

Where relevant, generated output data shall be validated (e.g. plausibility checks, completeness).

End of requirement

CYB-INF-1490 Error messages

The infrastructure shall not disclose error, processing or configuration information to unauthorised operators/users.

End of requirement

Note: these information may be used by malicious users.

CYB-INF-1500 Bespoke software logging

The infrastructure shall log at least the following security events:

- Execution of critical commands
- Attempts to execute critical commands without authorization
- Invalid input data
- Invalid internal data
- Message integrity error
- Output data invalid

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

CYB-INF-1510 Test data

Test data shall be carefully selected in order to simulate also incorrect inputs, and peaks/overload situations. Test data integrity shall be verified.

End of requirement

CYB-INF-1520 Development environment

The contractor shall ensure security of the development environment. Following controls shall be established:

- Operating systems security hardening
- Development environment change management

- Patching and updating of OS and development tools
- Security event logging

End of requirement

CYB-INF-1530 Review process

The contractor shall establish a formal process and associated plan for in-house software review. At least the following areas shall be under review:

- SQL injection
- Cross-site scripting
- Input/output data validation
- Authentication
- Authorisation
- Handling of sensitive data
- Password security
- Exception management
- Data access
- Cryptography
- Use of uncontrolled code (e.g. external libraries)
- Configuration
- Threading
- Undocumented but accessible interfaces (backdoors)

End of requirement

8.11 Web portals

Operational chains used for service provisions cannot be exposed to Internet. However there may be cases in which is needed to provide access to users via Internet. In these specific cases the web portal shall be isolated from the operational chain used for the service (air gap).

CYB-INF-1540 Isolation of web portal

Web portals exposed to internet shall be appropriately segregated (e.g. data diodes) from operational chain used for service provision. Segregation approach shall be defined and justified against operational chain criticality during infrastructure design.

End of requirement

CYB-INF-1550 Web portals certificates and encryption

Web portal shall use encryption. Adequate certificates shall be used for this purpose.

Self-signed certificate are not adequate and not allowed.

End of requirement

Note: at the moment of writing this document, it would be requested to use at least TLS 1.2, with appropriated cypher suites.

CYB-INF-1560 Virtual Patching

A web application firewall, capable of virtual patching shall protect the webserver.

End of requirement

Note: This requirement enables to deploy fast mitigations (virtual patches) while the vulnerability is properly fixed.

CYB-INF-1570 User management

Users shall be registered, collecting all relevant information for legal identification.

End of requirement

CYB-INF-1580 Password policy

Requirements for password policy apply to web portal users.

End of requirement

CYB-INF-1590 Administration access

It shall be possible to access administration interfaces only from dedicated networks/workstations.

End of requirement

Note: the web portal can be managed only within the local network.

CYB-INF-1600 Protection of user data

Infrastructure shall protect confidentiality and integrity of user data and information.

End of requirement

CYB-INF-1610 Web portal logging

The web portal shall log at least the following activities:

- User session event
- User created/deleted/modified
- Administration session events
- Content modification
- Management access to databases or other support services
- Modification of configurations
- Any software error
- Changes in the status of the web portal or other support services
- Any security relevant event

If possible (e.g. diode): if the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise logs shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

CYB-INF-1620 OWASP top 10

Any web portal of the infrastructure shall be reviewed at least (but not limited to) with respect to the OWASP Top 10 security risks, and ensure that it is not exposed to these risks before deployment.

End of requirement

Note:

8.12 Virtualization

CYB-INF-1630 Virtualized environment security

Security of guests (virtual) and hosts (physical) shall be at the same level. (The set of technical requirements provided in this document applies to both virtual and physical environments). Following are some of the aspects that shall be taken in to account:

- Integrity of the virtualised environment, on top of the virtualised servers.
- Dataflow control and encapsulation between the virtualised servers.

- Resource control and limitation of the virtual servers in the virtualised environment.
- Continuity plan.
- Administration of the physical systems.
- Administration of the virtualised systems (different from the above).
- Specific training and documentation foreseen for virtualised environment.

End of requirement

CYB-INF-1640 Virtualization hardening guidelines

The contractor shall implement security hardening guidelines according to CYB-INF-1400.

End of requirement

CYB-INF-1650 Patching of off-line virtual images

The contractor shall ensure that patches are maintained for every OS image and snapshot used for virtualization.

For example, when patching a virtual machine, also its offline instances (used for example for recovery) shall be patched, in order to avoid regression.

End of requirement

8.13 Back-ups

Back-ups of data stored electronically are a cornerstone of information security, providing the possibility of recovery from a very wide range of risks, both known and unknown. Backing up information helps to protect it against breaches of availability and integrity, and is useful in protecting against almost all such threats. Back-ups are an essential component of any business continuity plan. Ensure security of back-ups (that these are not compromised). Backups are a major component of business continuity plan.

Target of the following requirements is to drive the identification of the data that should be backed up, and that it is treated adequately.

CYB-INF-1660 Identification of back-up data

The contractor shall identify for each host of the infrastructure the data that should be backed up. Data shall be identified in the following categories:

- Configuration
- Security Configuration
- Application data

- Security Data
- Security Keys
- Operators data

It shall be possible to restore OS and programs from installation disc, virtual images or other media.

End of requirement

Note: For service infrastructures it is not expected the need of backup programs, test data, programme code, or emails. Backup of logs is treated in [CYB-INF-2500].

Note: backup of security logs (accounting information) is addressed in CYB-INF-2500.

CYB-INF-1670 Security Configuration and Data back-up

Referring to CYB-INF-1660, backup of security configurations and security data shall be performed on separated media from the ones used for other types of data.

End of requirement

Note: this requirement intends to enable the operator to enforce additional protection (i.e. physical) to backups containing security related information, and longer duration in time.

CYB-INF-1680 Backup of security keys

Referring to CYB-INF-1660, backup of security keys shall be performed on separated media from the ones used for other types of data. The infrastructure shall enable the operator to store these types of data offline for at least 20 years. Media used for this purpose shall achieve this target reducing the required storage space and operational effort.

End of requirement

CYB-INF-1690 Backup

The security equipment administrator shall be able to perform the backups. It shall be possible to perform the backup of a single host, or of multiple hosts.

End of requirement

CYB-INF-1700 Backup automation

The backup process shall be automated, to reduce maintenance effort.

End of requirement

CYB-INF-1710 Backup information

The backup procedure shall generate at least the following information:

- Backup timestamp
- Directory three of the backup
- Identification of the host
- Classification label

These information shall be stored within the backup data.

End of requirement

CYB-INF-1720 Backups integrity

The infrastructure shall guarantee backups integrity.

End of requirement

Note: for example hash calculation, CRC etc.

CYB-INF-1730 Backup integrity verification

The Infrastructure shall allow the verification of the integrity of a backup.

End of requirement

Note: e.g. generation of checksums for each backup bundle.

CYB-INF-1740 Backup restore

The security equipment administrator shall be able to restore one or more hosts (or data on the host) from backup. The operator shall be able to test periodically the restore function.

End of requirement

Note: different solution may be proposed; for example OS and application can be restored from installation disc, or virtual image, and after restore their configuration and application/ user *data via backup.*

8.14 Network

This section capture some basic network design best practices. The contractor is expected to adapt and extend network security, adapting it to the infrastructure under development.

CYB-INF-1750 Defence in depth

The network design shall use a defence in depth approach.

End of requirement

Note: this is a design principle.

CYB-INF-1760 Network security maintainability

The system design shall take into account the need of maintaining up-to-date the security status of the infrastructure during its whole lifetime.

End of requirement

CYB-INF-1770 Network segmentation

Internal networks of the infrastructure shall be segmented using firewalls, defining different networks for different purposes.

End of requirement

Note: network segregation is used to prevent attacker lateral movements and extend compromise.

Note: example: deploying a network for administration, a network for operator workstations, a network for critical servers, etc. These network are connected only in specific points via firewalls.

CYB-INF-1780 Authentication and integrity

Communication within internal networks shall enforce integrity and authentication.

Confidentiality shall be enforced only when explicitly required by SSRS [AD-05], in order to ensure integration with the SECMON [RD.10].

End of requirement

CYB-INF-1790 Network boundary firewalls

When is needed to connect two separate networks, these shall be connected via a network security filtering device, or when possible a data diode. The firewall shall allow only the data traffic strictly needed for service provision.

End of requirement

CYB-INF-1800 Segregation of virtual networks

In case of using virtual infrastructures, networks shall be segregated using physical equipment.

End of requirement

CYB-INF-1810 Network probes enabled networks

Each network shall provide the possibility to deploy network probes in relevant inspection points. For example at high risk locations (e.g. system perimeter, cross domains boundary,…).

End of requirement

Note: this can be used to perform audit or to connect IDS.

Note: If [RD.10] is applicable to the contract, then this requirement is replaced by SEC-SECMONMER-1937.

CYB-INF-1820 Switch Access Control Lists

Switches shall deploy Access Control Lists to allow connection only to authorised hosts.

End of requirement

Note: Access Control Lists for VLAN, MAC, Ports etc.

CYB-INF-1830 Intrusion detection system

Intrusion detection system shall be deployed to monitor external interfaces, and internal interfaces towards critical networks.

A network is considered critical where its compromise may have an immediate impact on service provision. Critical networks shall be identified by PDR.

End of requirement

CYB-INF-1840 Intrusion detection system engine

Intrusion detection system shall use heuristic and signature based engines. If only one type is used, it shall be justified at PDR.

End of requirement

CYB-INF-1850 Intrusion detection system tuning

Before acceptance, the contractor shall demonstrate correct tuning of the intrusion detection systems, in terms of reduced false positive and detection of events generated by activities prescribed in CYB-INF-0340 and CYB-INF-0370 (penetration tests).

End of requirement

CYB-INF-1860 IDS signature at acceptance

When using signature based IDSs, at acceptance the contractor shall ensure that all IDS instances are updated at the latest available signature.

End of requirement

CYB-INF-1870 IDS signature update

When using signature based IDSs, The security equipment administrator shall be able to update the IDS signature.

End of requirement

CYB-INF-1880 Network probes at boundaries

It shall be possible to deploy a network probe at the interconnection between networks.

End of requirement

Note: this can be used to perform audit or to connect IDS.

Note: If [RD.10] is applicable to the contract, then this requirement is replaced by SEC-SECMONMER-1937.

CYB-INF-1890 Protection of configuration

The infrastructure shall protect integrity configuration of all network equipment.

End of requirement

CYB-INF-1900 Network configuration management

During operations, the modification of switches, firewalls or other network equipment shall be a L2 maintenance activity.

End of requirement

Note: L2 maintenance activity undergoes CCB approval. Access to the equipment is provided by the System *INFOSEC Officer.*

CYB-INF-1910 Network logs inspection

The security analyst shall be able to review local logs of network equipment.

Log and configuration inspections shall be the only activities allowed for the security analyst on network equipment.

End of requirement

CYB-INF-1920 Audit of network configuration

The security analyst shall be able to inspect network equipment configuration.

End of requirement

CYB-INF-1930 Network security logging

All network devices (included ones defined in section 8.14.1) shall log at least the following security events:

- Any cable or accessory (e.g. expansion card) connected/disconnected
- Unexpected device connected to network (or attempted connection)
- Equipment configuration modified (e.g. firewall policy, switch configuration etc.)
- Firewall security events
- All packed denied by specific firewall rules and the default “clean-up” rule
- VPN session established/closed
- Antimalware and Antivirus events (e.g. reverse proxy or DMZ)
- Any other type of security related event generated by network equipment.
- All user related logs (see CYB-INF-0770)
- M-to-M communication events (see CYB-INF-1010 and CYB-INF-1030)

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

8.14.1Interfaces with external network (WAN)

Following requirements aim to protect the internal infrastructure network from threat raising from external connections, and also protect against intentional or unintentional unauthorised disclosure of information from the internal system to external systems.

Connections towards the Galileo Core Infrastructure (e.g. GMS, GCS and GSF) are not considered external infrastructures. Requirements for these interfaces are addressed in [RD.04] and [RD.05].

CYB-INF-1940 EU regulation on interconnections and security best practices

Interfaces should be designed based on EU regulations on interconnections and security best practices [RD.15]. In case of conflict with requirements in this document, EU regulations takes priority.

End of requirements

CYB-INF-1950 External interfaces design

A risk analysis of cyber threats on and from systems connected to the infrastructure and managed by 3rd parties shall be performed by the CSM. Results shall be taken into account during the design and development in order to minimize identified risks through the interfaces allowing those interconnections. The risk analysis

on external interfaces shall be provided at PDR, along with the identified risk mitigations. The report shall be consolidated and delivered at CDR.

End of requirement

Note: example of this type of interfaces are: web portals, or the RLSP interface to the SGS.

CYB-INF-1960 VPN protection

Connections with systems outside of the infrastructure shall be protected at network layer by means of VPN gateways (IPSec). The VPN shall provide confidentiality, authentication, integrity and anti-replay protection.

End of requirement

CYB-INF-1970 Protection for EUCI communication over external network

If the interface is used for communication of classified information, then it shall be protected by adequate encryption. Cryptographic products used for the protection of EUCI shall be selected and implemented according to the rules laid out in the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 [AD-08].

End of requirement

CYB-INF-1980 Need to Know Principle for network interfaces

Accesses to network ports shall be restricted using the need to know principle.

End of Requirement

CYB-INF-1990 Paired firewalls protection

External interfaces shall be protected using at least an EAL3 double-level certified firewall structure implementing network (3/4) and application (7) level filtering. Two different firewalls models shall be used.

End of requirement

Note: see NIST 800 82r2

CYB-INF-2000 Demilitarized Zone (DMZ)

The double/level firewall structure shall implement the following Security Domains:

a. External Networks Domain:
   - This area is formed by the system connected towards a wide area network link via the appropriate network equipment. This area is considered as Untrusted.
b. Demilitarized Zones (DMZ):
   - DMZ-Untrusted: this area contains the Application level filtering, typically placed between inner and outer firewalls.

- DMZ-Services: this area contains the Applications Servers accessible from outside.

c. Internal Network Domains:
   - This is the secured area composed by the trusted infrastructure internal networks.

End of requirement

CYB-INF-2010 Separation of external entry points

The infrastructure shall provide different access interfaces to different user communities.

End of requirement

Note: for example for GSC, different interfaces for internet user, and high accuracy service provider.

CYB-INF-2020 Firewall filtering rules

The paired firewalls structure shall implement filtering rules able to prevent and detect unauthorized access attempts towards the internal network domains, and discard any malformed or out of order packet (e.g. according to their timestamp).

End of requirement

CYB-INF-2030 Network probes

It shall be possible to deploy network probes at the intersection of every domain defined in CYB-INF-2000.

End of requirement

Note: If [RD.10] is applicable to the contract, this requirement is replaced by SEC-SECMONMER-1937.

CYB-INF-2040 Application firewall

Any service exposed through an external interface shall be protected an application firewall (or reverse proxy). This proxy shall provide antimalware facilities.

End of requirement

Note: For web portals, this requirement is similar to CYB-INF-1560

CYB-INF-2050 Forward proxy

Any service used by the infrastructure through an external interface shall be protected by a forward proxy.

End of requirement

Note: in some cases this can be eventually embedded in an application layer firewall.

CYB-INF-2060 Services over external interfaces

Services exposed via external interfaces shall:

- Authenticate and authorize the client
- Validate the data exchanged

End of requirement

CYB-INF-2070 Service over external interfaces logging

Services over external interfaces shall log at least the following events:

- Authentication successful/unsuccessful
- Unauthorised access attempted
- Invalid data
- Critical data transferred

If the infrastructure is integrated with the SECMON, logs shall be forwarded according to [RD.10]. Otherwise these shall be stored in the centralised security logging system (see CYB-INF-2420).

End of requirement

Note: Critical data shall be defined case by case depending on the risk assessment of the infrastructure.

CYB-INF-2080 Firewall rules inventory

At acceptance, the contractor shall provide the inventory of firewall rules used across all deployed Firewalls, with their justification.

End of requirement

CYB-INF-2090 Switch and routers configuration inventory

At acceptance, the contractor shall provide the inventory of switch and router configurations (e.g. ACLs, VLANs, etc.).

End of requirement

8.15 Bios configuration

CYB-INF-2100 BIOS protection

At acceptance, all server BIOS shall be protected by password. Each system shall have a different password.

End of requirement

CYB-INF-2110 Bios password

At acceptance, the contractor shall provide in a sealed envelope passwords used to protect servers and workstation BIOS to the System INFOSEC officer.

End of requirement

CYB-INF-2120 BIOS password renewal

The security equipment administrator shall be able to renew BIOS password.

End of requirement

CYB-INF-2130 Boot on media

When operational, the Infrastructure shall not allow boot from external media (e.g. USB stick, CD ROM, DVD, etc) or network on all equipment (e.g. firewalls, switches, workstations, servers …).

End of requirement

Note: during installation or troubleshooting, this feature may be temporarily enabled by L2 maintenance.

CYB-INF-2140 Wake On LAN and other BIOS aspects

The Infrastructure provider shall ensure that following functionalities are deactivate on all workstations and on all servers:

- Wake on LAN
- Unused ports (e.g. USB, Ethernet etc.)
- Media drivers (e.g. CD/DVD ROM)
- Sound cards (e.g. microphone)
- Any other unused hardware peripheral

End of requirement

8.16 Hardware security

CYB-INF-2150 Physical lock down

All unused interfaces of servers, workstations and any other equipment shall be physically locked (e.g. USB, spare Ethernets, HDMI, etc.). Tampering prevention/detection measures shall be in place.

End of requirement

Note: example of interfaces

CYB-INF-2160 Need to Know Principle for physical ports

Accesses to enabled physical ports shall be restricted using the need to know principle.

End of Requirement

CYB-INF-2170 Rack lock

It shall be possible to lock racks to prevent physical access to contained equipment.

End of requirement

CYB-INF-2180 Rack keys

At acceptance, racks keys shall be provided to the System Infosec Officer.

End of requirement

CYB-INF-2190 Rack door open event

When a rack door is opened or closed, security event shall be generated.

End of requirement

CYB-INF-2200 Start-up and power-off events

Each server, workstation and equipment shall generate an event when starting-up, turning off or rebooting.

End of requirement

CYB-INF-2210 Temperature events

The infrastructure shall generate a critical event when the temperature inside a rack reaches a predefined threshold.

End of requirement

CYB-INF-2220 Cables labelling

All cables of the infrastructure shall labelled. Each label shall identify the two connected hosts and ports.

End of requirement

CYB-INF-2230 Physical lock down report

At acceptance, the contractor shall verify the physical lock down of the system, and provide an inspection report, detailing physical assets inspected and inspection results.

End of requirement

8.17 Removable media

In general it shall not be possible to connect any devices to the infrastructure. However it shall be possible to use CD-ROM for data extraction and if there are operational needs also USB media. However the use of USB media shall be restricted only to known authorised devices, from dedicated gateway workstations.

CYB-INF-2240 Active interfaces inventory

At acceptance the contractor shall document the physical interfaces to be used with removable media (if any).

End of requirement

Note: E.g. CD-ROM, USB, Tapes.

CYB-INF-2250 Removable media

All removable media interfaces shall be disabled. If removable media are required for operational activities, these shall be allowed only to the specific role (e.g. security equipment administrator). Only a predefined set of devices shall be allowed to be connected.

End of requirement

CYB-INF-2260 Authorised devices

If USB removable media are required, the infrastructure shall allow connection of only authorised devices, from dedicated gateway workstations.

End of requirement

CYB-INF-2270 Provision of authorised devices

Authorised USB devices shall be provided at acceptance. The operator shall not be able to enable further devices.

End of requirement.

CYB-INF-2280 Removable media logging

Insertion and ejection of removable media shall generate a security event. If the media is not authorised, a CRITICAL event shall be generated.

End of requirement

Note: E.g. USB connection, CD-ROM inserted etc.

CYB-INF-2290 USB serial

Events associated to USB devices shall report the USB serial number.

End of requirement

CYB-INF-2300 Audit of removable media

The security analyst shall be able to inspect logs related to removable media activities.

End of requirement

CYB-INF-2310 Authorised devices handover

At acceptance, the contractor shall provide to the SIO the authorised removable media, and a report on their security assurance (e.g. antimalware check, no tampering evidences, etc.).

End of requirement

CYB-INF-2320 List of authorised devices

The security analyst shall be able to inspect the list of authorised USB devices.

End of requirement

8.18 Support to incident response

In case of suspect or confirmed compromise of the infrastructure, the System Infosec Officer or the National Security Authority shall be able to collect and protect forensic evidences. The infrastructure shall continue being operational as far as possible during these activities.

CYB-INF-2330 Forensic data extraction

The Infrastructure shall include the necessary tools to allow the System Infosec officer to extract complete or partial content of the data stored in the system ensuring its integrity. This includes operating system related data (e.g. event logs, configuration parameters, etc), application related data (e.g. databases, files, etc).

End of requirement

Note: this requirement is superseded where forensic data extraction capabilities are already provided by other means (e.g. SECMON tools).

CYB-INF-2340 Forensic support

The Infrastructure shall allow the System INFOSEC officer to create physical copies of the data of any machine of the system. This shall include both the hard disks and their non-persistent memories (running memory). The copy shall be protected in terms of integrity.

End of requirement

Note: this requirement is superseded where forensic data extraction capabilities are already provided by other means (e.g. SECMON tools).

CYB-INF-2350 Compromised equipment segregation

The Infrastructure shall allow the segregation of equipment from the redundant operational chain to allow its sanitisation. The redundant equipment shall continue service provision while the segregation is performed.

End of requirement

CYB-INF-2360 Segregation of compromised equipment

The Infrastructure shall logically protect the compromised equipment from unauthorised access.

End of requirement

Note: target of this requirement is to prevent forensic evidences tampering.

8.19 Core of trust

In case of compromises impacting the service provided by the infrastructure, or the security functions, the infrastructure shall be able to quickly recover from the compromise.

CYB-INF-2370 Definition of core of trust

The contractor shall define the core of trust of the infrastructure, and it shall be provided at PDR.

End of requirement

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

CYB-INF-2380 Reinstallation of core of trust

The security equipment administrator shall be able to perform a complete re-installation of the core of trust of the infrastructure over a short timescale (e.g. a weekend) and in a single operation.

End of requirement

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-INF-2390 System sanitisation

In case of compromise, the system shall facilitate its sanitation, enabling the eradication of 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.

8.20 Logging and monitoring

Preventive controls can go a long way in assuring the security of information and systems, but they cannot guarantee absolute security. Systems must also be supervised to check whether information security breaches have taken place so that corrective measures can be taken. This supervision is performed through logging and monitoring.

Not only security events has to be collected, but also operational events, as for example service start/stop, or operational activities performed by an operator (e.g. issuing a telecommand).

In order to prevent log tampering, all events shall be forwarded to a dedicated server within the infrastructure.

When [RD.10] is applicable to the contract, events are forwarded to the SECMON infrastructure, which centralize them at GSMC. In case [RD.10] is applicable, some of the following requirement are superseded, and to be considered not applicable.

CYB-INF-2400 Events sources

As minimum the following sources shall create audit logs which shall be possible to collect:

- security equipment: network firewalls, application firewalls, encrypting devices, probes approved by an EU NSA at the appropriate level, antivirus software, authentication servers, VPN concentrators, SSL gateways, proxies, reverse proxies;
- network equipment: routers, switches, netflow, DNS servers, load balancers, time servers;
- infrastructure servers: authentication, directories, software distribution, remote management, supervision, virtualisation, file servers, backups, mail, print;
- business servers: web servers, databases, file servers, collectors;
- workstations: main operating systems

End of Requirement

Note: this requirement complements detailed requirement previously identified for logging: CYB-INF-0770, CYB-INF-0870, CYB-INF-0930, CYB-INF-0950, CYB-INF-1030, CYB-INF-1040, CYB-INF-1250, CYB-INF-1340, CYB-INF-1500, CYB-INF-1610, CYB-INF-1930, CYB-INF-2070 and CYB-INF-2280.

Note: This requirement is superseded where [RD.10] is applicable to the contract.

CYB-INF-2410 Events synchronisation

Events shall be synchronized on GST, in order to ensure logs timestamps correlation accuracy.

End of requirement

Note: in some cases UTC may be used instead of GST. This will be specified case by case.

CYB-INF-2420 Logs centralization

Events generated by all hosts (servers, workstations, network and any other equipment) shall be forwarded and stored in a centralized and redundant server.

End of requirement

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2430 Log protection

Logs shall be protected against deletion and modification. In hosts generating events, and in the log centralization server.

End of Requirement

CYB-INF-2440 Configuration of events forwarding frequency

The equipment shall be configurable in seconds on the time rate to forward the event to the destination from 0 (as soon as event is created) to 24 hours (daily). This configuration is an extraordinary maintenance (L2/L3) activity.

By default, events shall be forwarded as soon as created (near real-time).

End of Requirement

Note: during operations this configuration change can be approved only by GSMC.

CYB-INF-2450 Protection of events in transit

The communication channel for forwarding events shall ensure confidentiality, authentication, integrity and anti-replay protection.

End of requirement

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2460 Enabling/disabling event accounting

Enabling/disabling the accounting of specific event types from specific sources, shall not be allowed. It can be performed only after GSMC request by extraordinary maintenance (L2/L3).

End of requirement

CYB-INF-2470 Log centralization access

Only the security analyst has read-only access to logs contained in the log centralization server (via a dedicated workstations).

End of requirement

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2480 Security events to control room

If the infrastructure security is not monitored by GSMC, and the infrastructure foresees a control room, security events shall be reported to the on-shift operator. Events to be reported shall be agreed with GSMC during the design phase.

End of requirement

Note: after FOC it is expected that the security monitoring will be performed only at GSMC.

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2490 Log extraction

The security analyst shall be able to export logs (e.g. on DVDs or tapes).

End of requirement

Note: this requirement is applicable only in the cases where the applicable regulation doesn't require the Registry control office to perform the export.

CYB-INF-2500 Security Logs backup

The security analyst shall be able to perform backup of the logs, and consequently clear storage space. This activity shall generate an event.

End of requirement

Note: consider that the operator has a requirement of storing the logs for 20 years [SECOPS-902] [AD-06].

CYB-INF-2510 Log retention

The infrastructure shall be able to store at least 6 months of logs on-line.

End of requirement

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2520 Off-line archive

The infrastructure shall enable the operator to store security logs offline for at least 20 years. Media used for this purpose shall achieve this target reducing the required storage space and operational effort.

End of requirement

CYB-INF-2530 Warning on full logs

The infrastructure shall generate security event when free storage space is less than 20% on the log centralization server. One event every hour shall be generated along with an acoustic alarm.

End of requirement

CYB-INF-2540 Full logs

The infrastructure shall have a circular buffer for logs storage, this shall be used when the nominal storage space is full. This buffer shall log only events with criticality WARNING and above.

End of requirement

Note: it is expected that the operator takes action before reaching the full log.

CYB-INF-2550 Logs processing

The security analyst shall be able to perform log analysis (sorting, filtering etc.). He shall be able to produce his/her own processing scripts (e.g. Perl, python). Scripts shall be available only in a dedicated sandbox.

End of requirement

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2560 Events analysis and statistics MMI

The infrastructure shall provide to the security analyst a dedicated data processing and reporting MMI for events statistics and analysis. Following are listed the minimum capabilities:

- Filtering of auditing events based on attributes including at least: event type, user account, event source, time window, message, IP addresses

- Disable event display based on attributes including at least: event type, user account, event source, message, IP addresses
- Events sorting based on event fields
- Reporting of isolated events
- Reporting of most common events

End of requirements

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2570 Event details

Each event shall have the following information associated:

- Event type,
- Event criticality,
- Security event (yes or not)
- Date and time of event,
- Outcome (success or failure) of the event,
- Identity of the entity that caused the event (workstation, terminal, facility, security module, satellite),
- Identity of the current operator or maintenance personnel log-in (for audit records generated on workstations/terminals),
- Description

End of requirement

Note: all events required in this document are security events.

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2580 Network security event details

For network related events, the following information shall also be provided in addition to the ones in CYB-INF-2570:

- Source/destination IP address (prior to any address translation)
- Source/destination port number
- Where possible, details of the payload of rejected packets
- Where used, HTTP transactional data (URL, Status code, Filtering performed at any proxy server)
- Where used, Electronic Mail transactional data (Sender and recipient addresses, subject line, message identifier, Mail gateway processing).

End of requirement

CYB-INF-2590 Event severity

Security events shall be categorized following the Syslog severity levels (RFC 5424):

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

End of requirement

Note: This requirement is superseded where [RD.10] is applicable.

CYB-INF-2600 False alarm rate

The infrastructure shall minimize false alarm rate. A target threshold shall be agreed at PDR with GSA CSM.

End of requirement

CYB-INF-2610 False negative rate

The infrastructure shall minimize the false negative rate. A target threshold shall be agreed at PDR with GSA CSM.

End of requirement

CYB-INF-2620 Events flooding avoidance

Transient statuses shall not generate continuous events. An event shall be generated for each change in status. For critical events, the se can be repeated in defined intervals (no less than 5 minutes period).

End of requirement

Note: example is the rack door opening. An event is generated when the door is opened, and another when the door is closed.

CYB-INF-2630 Monitored Entity Requirements

Where [RD.10] is applicable, a dedicated SoC to this requirement document shall be provided.

End of requirement

Note: this set of requirements are needed to allow monitoring of the infrastructure from GSMC.

8.21 Patching

CYB-INF-2640 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 can be used. This 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-INF-2650 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-INF-2660 Patch automation resources consumption

If patch automation is used, in any case it should 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-INF-2670 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-INF-2680 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.

When this is not possible, adequate countermeasures to reduce the risk shall be put in place on the OPE chain, until the patched and certified system is installed.

End of requirement

8.22 Procedures

CYB-INF-2690 Procedures

The contractor shall provide procedures for the OPS team to perform security maintenance.

End of requirement

9 Lock down report

The lockdown report demonstrates the correct hardening of the system, and its complete documentation in terms of security. The Operator receives this report as a baseline, and it is in charge of maintaining it during the lifecycle of the system. This paragraph identifies the required information which shall be provided by the contractor to the operator.

CYB-INF-2700 Lock down report classification

The lockdown report shall be classified at least as RESTREINT UE/EU RESTRICTED, or up to the same classification of the equipment associated.

End of requirement

CYB-INF-2710 Lock down report audience

The lockdown report shall be provided to the System Infosec Officer, Security analyst, Cyber security Manager, Cyber security internal auditor.

End of requirement

CYB-INF-2720 Lock down report and network map

Lockdown information shall be provided referencing the network map.

End of requirement

CYB-INF-2730 Lock down report content

The lock down report shall provide at least the following information:

- Network Map [CYB-INF-0040]
- Operator profiles [CYB-INF-0640]
- List of available users and privileges [CYB-INF-0790]
- Non-human accounts list [CYB-INF-0830]
- Machine to Machine interfaces list [CYB-INF-1020]
- Default password policy [CYB-INF-0910]
- Antimalware signature date [CYB-INF-1240]
- IDS signature date [CYB-INF-1860]
- List of authorised software and services [CYB-INF-1370]
- List of authorised scripts [CYB-INF-1380]
- COTS secure hardening baseline [CYB-INF-1410]
- Results from last code review [CYB-INF-1530]
- Virtualisation security hardening baseline [CYB-INF-1640]
- List of authorised USB devices [CYB-INF-2150]
- Firewall rules [CYB-INF-2080]
- Network devices security configurations [CYB-INF-2090]
- List of cables [CYB-INF-2145]
- List of exceptions to the security baseline
- Physical security audit inspection report [CYB-INF-2230]
- Procedures for lock down maintenance [CYB-INF-2690]

End of requirement

Note: the lockdown report is handed over to OPS, which becomes responsible to maintain it after infrastructure acceptance.

CYB-INF-2740 Lock down report reviews

The first issue of the lock down report shall be at CDR, defining the structure of the document, and how it will be compiled for acceptance review.

The lock down will be updated at QR and submitted for acceptance audit, and finalized for Acceptance Review, and handover to the operator.

End of requirement

10 Security credentials delivery

Security token shall not be disclosed to anyone; these shall be provided during acceptance at the System Infosec Officer. Depending on their types, these will be provide to relevant operators, or stored in the safe.

CYB-INF-2750 Security credentials classification

Security credentials listed in CYB-INF-2760 shall be classified at least as RESTREINT UE/EU RESTRICTED, or up to the same classification of the equipment associated.

End of requirement

CYB-INF-2760 Security credentials delivery

At acceptance, the contractor PM shall handover to the OPS System INFOSEC Officer the following items:

- Users passwords [CYB-INF-0800]
- Root passwords [CYB-INF-0450]
- Non-human account passwords [CYB-INF-0840]
- BIOS passwords [CYB-INF-2110]
- Rack keys [CYB-INF-2180]
- Authorised removable media [CYB-INF-2310]
- Any other relevant authentication or security token (e.g. USB token)

End of requirement

11 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
Cyber acceptance audit plan	CIA	CYB-INF-0320 CYB-INF-0330	CDR	CDR, QR, AR

Cyber acceptance report	CIA	CYB-INF-0390	QR	QR, AR
Network Map(s)	CSM	CYB-INF-0050 CYB-INF-0040	PDR	CDR, QR, AR, DRB
Vulnerability report **(for each network map instance)**	CSM	CYB-INF-0120 CYB-INF-0150	QR	QR, AR
Vulnerability correction plan **(for each network map instance)**	CSM	CYB-INF-0170 CYB-INF-0270 CYB-INF-0400	QR	QR, AR
Patch report (for each network map instance)	CSM	CYB-INF-0210	QR	QR, AR
Cyber Request for Deviation	CSM	CYB-INF-0270	N/A	As soon as they are identified
Lockdown report	PM	CYB-INF-2730 CYB-INF-2740	CDR (template)	CDR, QR, AR
Security Credentials	PM	CYB-INF-2760	After acceptance	After any maintenance activity impacting security tokens

Table 4 - Deliverables documents

End of Document