Cyber security requirements for Management

Reference:
GSA-SEC-SREQ-SPE-237329

Issue/Version: 1.2

Date: 31/05/2018

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

Reviewed By:			
Name	Role	Signature	Date
Wieland Kuenzel	Quality Manager		12/6/2018
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
237329	1.0	First version approved at GSA EB#19	F. Belli	16/01/2018
	1.1	Updated after SAB-AT RIDs received for EnS review Approved at GSA EB 26.	F. Belli	27/02/2018
	1.2	Version updated after EC revision. Main differences from previous version: Added: • CYB-MNG-0220 • CYB-MNG-0410 Removed: • CYB-MNG-0270 Version approved at GSA EB#35.	F. Belli	31/05/2018

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This document defines requirements for cyber security Management of contracts and procurements awarded by GSA for the Galileo Programme.

The compliance to these requirements ensures that key roles and responsibilities are correctly defined and assigned according to the infrastructure security needs. This enables the Programme to manage cyber risk associated to the contract or procurement.

The intended audience of these requirements are the Project Managers of contractors and their subcontractors in charge of the infrastructure development, service operations or infrastructure maintenance.

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 the basis for the documents containing requirements for the infrastructure development [RD.02], maintenance requirements [RD.03], and the requirements for the operations [RD.01] which will use the infrastructure. Figure 1 Figure 1shows the relations between this document and the applicable Mission Requirement document [AD-02].

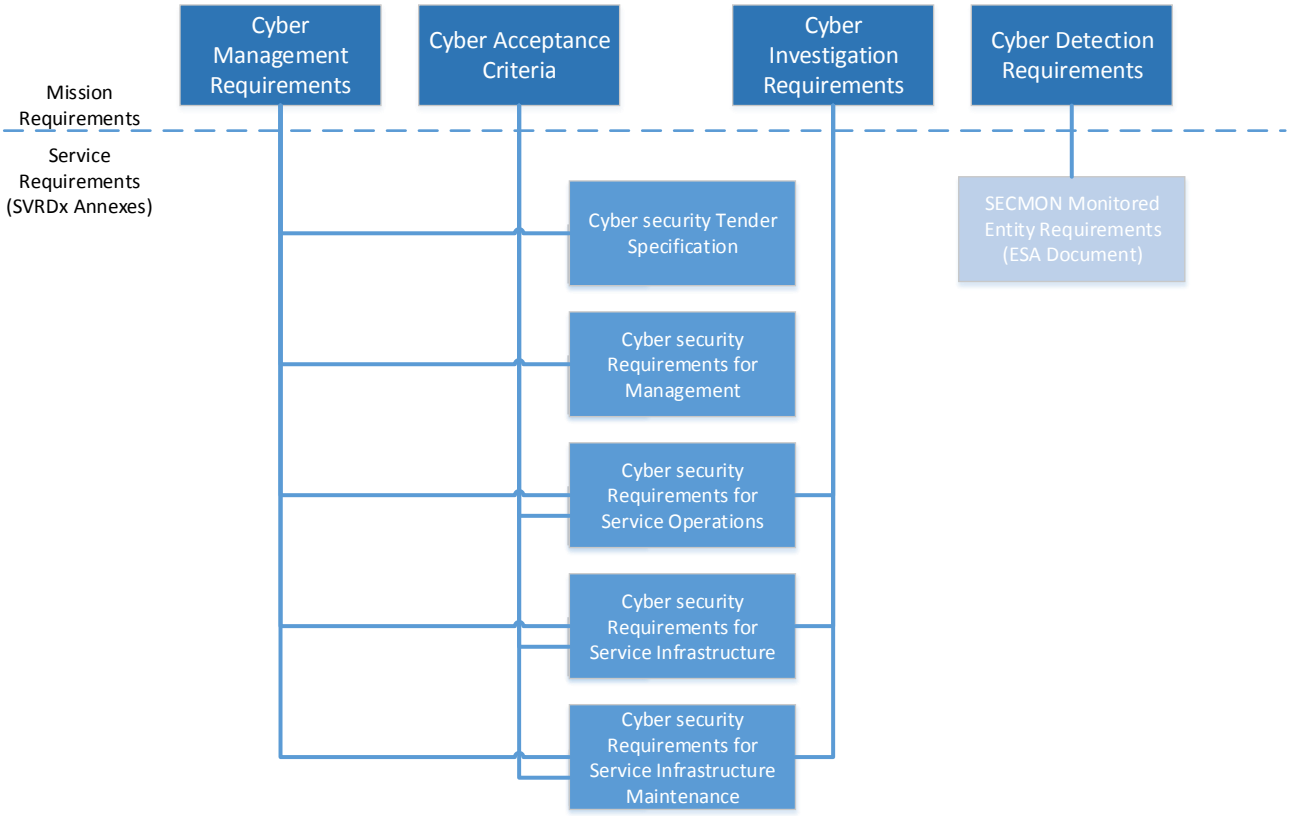

Figure 1 - Document tree.

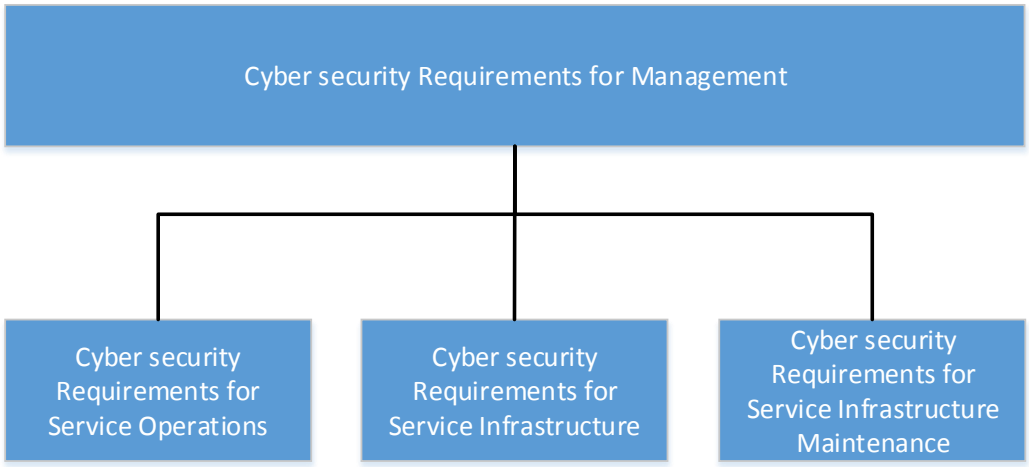

Figure 2 - Relationship between Management and technical requirements.

1.1 Acronyms and Abbreviations

Table 1 - Abbreviations

Abbreviation	Definition
AD	Applicable Document
AR	Acceptance Review
BYOD	Bring your own device
CDR	Critical Design Review
CEO	Chief Executive Officer
CIA	Cyber security Internal auditor
CSM	Cyber security Manager
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

Abbreviation	Definition
FTE	Full Time Equivalent
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
LSAA	Local Security Accreditation Authority
NtK	Need to Know
PDR	Preliminary Design Review
PM	Project Manager
QR	Qualification Review
RD	Reference Document
RfD	(cyber) Request for Deviation
RfW	Request for Waiver
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SoC	Statement of Compliance
SSRS	System Security Requirements Specification
WFID	Work Flow ID

1.2 Applicable and Reference Documents

The list of applicable documents contains 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
[AD-03]	System Security Requirements Specification	Galileo SSRS	3.9

Table 3 - Reference Documents

Reference Documents:			
Type	Title	Reference	Issue
[RD.01]	Security requirements for service operations	GSA-SEC-SREQ-SPE-232365	1.4
[RD.02]	Security requirements for service infrastructure	GSA-SEC-SREQ-SPE-232364	1.5
[RD.03]	Security requirements for service infrastructure maintenance	GSA-SEC-SREQ-SPE-237266	1.2
[RD.04]	Network Map Template	GAL-GSA-GSMC-TMP-238093	1.0
[RD.05]	Cyber security Report Template	GAL-GSA-GSMC-TMP-238092	1.0
[RD.06]	Security Operational Scenarios (SOS)	GSA-SEC-SREQ-TN-237908	1.0
[RD.07]	System Level Security Operating Procedures (secOps)	GAL-PRC-ALS-SYST-A-1000-x	6.4

2 Definitions

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

- **Cyber security Manager** (CSM), is part of the contractor organization, and is responsible for the design and implementation of the technical solution to the requirements presented in this document. Where not differently specified, "CSM" refers to prime contractor CSM.
- **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 present in the system are identified and reported. Where not differently specified, "CIA" refers to prime contractor CIA.

The responsibilities of the above roles are later defined in the document, along to the ones of subcontractors CIA and CSM.

Any other role identified in the document (i.e. LSO, SIO) is defined in the SECOPS document [RD.07].

Vulnerability: A bug, performance issue or missing security functions representing a weakness in a software, or inadequate/incorrect operational process, enabling accidental scenarios or deliberate exploitations with potential impact on one or more of these criteria:

- Confidentiality (e.g. for software: disclosure of data or configuration)
- Integrity (e.g. for software: unauthorized modification of data)
- Availability (e.g. for software: unavailability or saturation of resources)
- Accountability (e.g. inability to identify a responsible for an action on the system)
- Non-Repudiation (where relevant)

3 Key personnel

This section defines requirements for the appointment of key personnel: Cyber security Manager and Cyber security Internal Auditor. These two roles are independent, having the CSM performing and driving the implementation and evolution of cyber security across the contract perimeter, and the CIA auditing and providing assurance that these activities are correctly performed.

Specific requirements for activities performed by the CSM and CIA are provided in the following two sections.

3.1 Key personnel appointment

CYB-MNG-0010. Appointment of CSM

The contractor shall appoint a Cyber security Manager (CSM), which will be responsible for the implementation of the applicable cyber requirements for the Galileo activities under the responsibility of his/her contracting entity, with the exclusion of requirements assigned to the CIA.

End of requirement

CYB-MNG-0020. Appointment of subcontractor CSM

When the contractor is subcontracting fully or partially its technical activity, where relevant, its sub-contractors shall appoint a CSM which will be responsible for the implementation of the applicable cyber requirements for the activities under the responsibility of the sub-contractor.

End of requirement

CYB-MNG-0030. Appointment of CIA

The contractor shall appoint a Cyber security Internal Auditor (CIA). The CIA is in charge of the implementation of the cyber requirements related to audit.

End of requirement

Note: The CIA is responsible for requirements within section 6 and "acceptance audit requirements" in [RD.02].

CYB-MNG-0040. Appointment of subcontractor CIA

A sub-contractor referred to in [CYB-MNG-0020] may decide not to appoint a CIA if it authorises the CIA of its customer to conduct continuously audits of cyber security for the activities in the perimeter of the cyber policy under its own responsibility.

End of requirement

Note: the scope of applicability is later defined in the document CYB-MNG-0230.

CYB-MNG-0050. CIA and CSM independence

Duties of CIA and CSM shall be segregated. The contractor shall be able to demonstrate an absence of conflict of interest between the two roles.

End of requirement

Note: it is expected that the reporting lines of CSM and CIA touches at executive director level.

3.2 Cyber security Manager

CYB-MNG-0060. CSM training

The person assigned as CSM shall be trained to fulfil this role (e.g. equivalent to ISACA CISM certification), and they shall be continuously updated to the latest security field development. His/her position shall be between senior management and the operative level.

End of requirement

CYB-MNG-0070. CSM responsibilities

The CSM shall ensure that the following activities are correctly performed:

- Produce the strategy to implement these cyber requirements, and submit it for GSA approval at relevant contract milestones;
- Supervise the performance of the planned tasks (i.e. track and verify the correct implementation of all requirements);
- Monitor of performance of information security management system and of effectiveness of security measures;
- Preparation of materials for the relevant reviews (i.e. GSA Cyber Review Board);
- Support to the System Architect to implement the technical requirements;
- Creation and/or maintenance of the network map;
- Report on activity planning, implementation status and performances of governance processes;
- Report on non-compliances and effectiveness of the security measures;
- Track vulnerabilities using the designated information resources;
- Define, implement and validate mitigations for discovered vulnerabilities;
- Report security incidents to GSMC according to [RD.06];
- Promote security culture across the contractor's team;
- Manage sub-contractors CSM activities.

End of requirement

Note: CSM will be required to provide the documentation supporting the above tasks.

CYB-MNG-0080. CSM reporting

CSM shall report the status of activities listed in CYB-MNG-0070 to the contractor's CIA, to contractor's PM, and to GSA CSM. A quarterly report is expected.

End of requirement

CYB-MNG-0090. Subcontractor CSM reporting

The sub-contractor's CSM shall report the status of activities (relevant to the subcontractors) listed in CYB-MNG-0070 to its PM, to the prime contractor's CIA, to prime contractor's PM, and prime contractor's CSM.

End of requirement

CYB-MNG-0100. CSM security incident reporting

CSM shall communicate to GSMC occurrences of any cyber security incidents related to non-operational activities, according to [RD.06];

End of requirement

Note: this requirement is in addition to the already established incident management procedures defined in the LSOP for the operational environment.

Note: A cyber security incident, is any issue may affect integrity, availability and confidentiality of the system under production, related documentation or EUCI. For example malware on development workstations, unauthorised access on production repositories, public disclosure of detailed design, etc.

Note: This requirement has to be read in conjunction with, and not a replacement of applicable EU regulations.

CYB-MNG-0110. Segregation of duty

The CSM role cannot be shared by the same person having the CIA role. CSM and CIA roles shall be without prejudice to the roles and responsibilities of the Local Security Officer and of the Security Accreditation Authority as defined by the applicable security rules.

End of Requirement

3.3 Cyber Internal Auditor

CYB-MNG-0120. CIA training

The person assigned as CIA shall be trained to fulfil his role (e.g. equivalent to ISACA CISA certification), and they shall be continuously updated to the latest security field development.

End of requirement

CYB-MNG-0130. CIA responsibilities

The CIA is responsible for ensuring that the following activities are correctly performed:

- Plan, schedule and perform audits in the perimeter of the cyber policy under the responsibility of his/her entity to:
  - Evaluate the level of compliance of the implementation of cyber requirements;
  - Identify vulnerabilities;
  - Identify non compliances;
  - Evaluate the compliance level of the information security management system and implemented security measures with defined requirements, security policies in place and the appropriate safety standards;
  - Provide independent feedback on the effectiveness and efficiency of information security management system and security measures.
- Reporting on audit results.

End of requirement

CYB-MNG-0140. CIA reporting

CIA shall report the status of activities listed in CYB-MNG-0130 to contractor's PM, its CEO, and to GSA CIA. A quarterly report to CIA GSA is expected.

End of requirement

CYB-MNG-0150. Subcontractor CIA reporting

Subcontractor CIA shall report the status of activities (relevant to the subcontractors) listed in CYB-MNG-0130 to contractor's PM, its CEO, and to contractor's CIA and contractor's CSM.

End of requirement

CYB-MNG-0160. CIA Independence

A CIA shall carry out his/her role impartially. The person fulfilling the role of CIA shall not have a conflict of interest between their organizational function and those functions running the procurement contract.

End of requirement

CYB-MNG-0170. CIA access to project resources

The contractor shall ensure that the CIA has access to any project documentation necessary to perform his role.

End of requirement

CYB-MNG-0180. CIA removal for conflict of interest

The contractor shall immediately revoke the appointment to a person fulfilling the CIA role, in case of a conflict of interest raises after the appointment.

End of requirement

CYB-MNG-0190. GSA requiring CIA removal

Upon the GSA discovering a conflict of interest the contractor shall immediately revoke the appointment to person fulfilling the CIA post.

End of requirement

CYB-MNG-0200. CIA security incidents reporting

CIA shall immediately report to GSMC occurrences of any cyber security incidents, and to its CSM. If the CSM is the cause of the security incident, the reporting has to be done only to the GSMC.

End of requirement

Note: A cyber security incident, is any issue may affect integrity, availability and confidentiality of the system under production, related documentation or EUCI. For example malwares on development workstations, unauthorised access on production repositories, public disclosure of detailed design, etc.

Note: This requirement has to be read in conjunction with, and not a replacement of applicable EU regulations.

CYB-MNG-0210. Cyber security within Security Management Plan

The CSM shall contribute to the contract Security Management Plan, describing how cyber security requirements shall be implemented.

The contractor should follow guidelines defined in *ISO/IEC 27002 – Information technology — Security techniques — Code of practice for information security controls* or equivalent.

End of requirement

3.4 Participation to cyber security meeting

CYB-MNG-0220. Support to cyber security meetings

On GSA request, the CSM and CIA shall support the preparation of documentation to submit, and participate to cyber meetings on request (i.e. cyber board, cyber review board, SAB-AT cyber check points).

End of requirement

4 Compliance

CYB-MNG-0230. Perimeter of applicability

The perimeter of applicability of cyber requirements shall include any operational platform in the infrastructure (i.e. OPE chains) and any validation chain (e.g. VAL) where available, in the perimeter of the contract.

End of requirement

Note: In case of conflicting schedules, priority is always given to implementation of cyber requirements on the operational chains.

CYB-MNG-0240. Statement Of Compliance (SoC)

During execution of the contract, the CSM shall ensure that all cyber requirements are correctly implemented, and provide updates to the statement of compliance. The Statements of Compliance is expected for the prime contractor, including contributions from all sub contracts.

Following statement of compliance shall be provided:

- SoC as Contracted (at KO);
- SoC as Designed (updated at every relevant milestone);
- SoC as Build (after requirements validation, i.e. AR or OVR close out);

End of requirement

Note: Possible compliance status are "Compliant" "Partially Compliant" with an explanation of the limitation, "Non-Compliant" with justification and "Not Applicable" with justification.

Note: the CIA is indirectly involved on the building of the SoC, due to their role of compliance auditing.

CYB-MNG-0250. Cyber Request for Deviation/Waiver

During execution of the contract, if a deviation from the provided and justified SoC is required, the CSM shall present justifications for non-compliances or partial-compliances in Cyber Request for Deviation/Waiver.

End of requirement

Note: in certain cases, multiple organizations may be involved in the preparation of a deviation (i.e. operations and maintenance). These cases are coordinated by GSA CSM through the GSA Cyber Review Board.

Note: Cyber Requests for Deviation may be prepared in the technical cyber board (GSA Cyber Review Board), but recommendation for approval are made at the Galileo Cyber Board.

Note: Cyber Request for Waiver are prepared in case a remediation of a vulnerability is proposed to not be implemented.

CYB-MNG-0260. Cyber Request for Deviation/Waiver content

A cyber request for deviation/waiver 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 the compliance to the concerned cyber requirement;
        - mitigate operationally the assessed risk;
        - monitor the attacks that may benefit from the partial or non-compliance to the concerned cyber requirement;
        - 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/waiver and a committed schedule for the complete recovery of the compliance to the concerned cyber requirement (action plan).

End of requirement

5 Cyber awareness

This section identifies minimum requirements for the cyber security training. It is not related to or an alternative to training for EUCI management, which is regulated by national laws.

CYB-MNG-0270. Security awareness program

The contractor shall define the security awareness program. This document shall specify:

- Training objectives;
- Training audience, for example training for:
    - Management
    - Developers, Testers, etc.

- IT Administrators
- Support (e.g. PA, Legal, etc.)

- Training frequency;
- Trainers (outsourced, in house);
- Training methodology;

End of requirement

CYB-MNG-0280. Security awareness frequency

The contractor shall ensure that all employees and subcontractors involved in the GSA contract have at least an annual security awareness program session.

End of requirement

CYB-MNG-0290. Security awareness topics

As a minimum, the security awareness program shall cover the following aspects:

- Security policy of the organization
- Physical security
- Access controls (Password and account management)
- BYOD
- Social engineering avoidance
- Secure e-mail practices
- Security Incident Management Plan
- Classification data management

End of requirement

CYB-MNG-0300. Security awareness evidences

Evidence of attendance for contractor and sub-contractor staff on the Security awareness programme shall be provided annually to GSA (security awareness record).

End of requirement

6 Internal audit requirements

This section provides requirements applicable to the Cyber security Internal Auditor activities. The auditor shall regularly monitor via audits the activities of the CSMs, to verify correct requirements implementation, and risks raised by vulnerabilities are correctly treated through the vulnerability and patching processes. In case any problem is identified, it shall be promptly reported to the CSM, GSA CIA, GSA PM, and contractor CEO.

The reporting to the CEO (or Board of Directors) is necessary due to their legally accountability for any security breach that may happen. It is clear that in large organizations, this reporting may be delegated by the CEO to other actors, however the legal responsibility cannot be delegated.

CYB-MNG-0310. Cyber Security Auditing

A CIA shall conduct continuously his/her auditing function and shall plan his/her activities in order to cover at least every year all aspects related to cyber security, and under the responsibility of his/her entity.

End of requirement

CYB-MNG-0320. Cyber audit plan

The CIA shall produce a cyber audit plan, defining the audit strategy and covering the whole security perimeter under contractor responsibility (including sub contracts). The cyber audit plan and the defined strategy shall be regularly updated (at least every 6 months), in order to take in consideration results from performed audit campaigns, and variation to the audit perimeter.

The contractor should follow guidelines defined in *"ISO/IEC 27007 – Guidelines for information security management system auditing"* or equivalent.

End of requirement

CYB-MNG-0330. Cyber audit plan review

The CIA shall provide the cyber audit plan to his/her CEO, and to his/her customer CIA (GSA CIA or Prime contractor CIA) for review.

The audit plan shall also be provided for information to the CSM and any other entity which will be subject to the audit.

End of requirement

CYB-MNG-0340. Audit scope

The cyber audit plan shall include at least:

- Confirmation of correct implementation of technical requirements;

- Confirmation of correct implementation and execution of governance processes;
- Verification of effectiveness of patches and mitigations (treatments);
- Identification of new vulnerabilities;

End of requirement

CYB-MNG-0350. Potential extension of audit scope

A CIA shall include in his/her audit plan and implement any request of audits issued by its director or by the CIA of GSA.

End of requirement

Note: if required, this type of audits shall take precedence over planned audit activities.

CYB-MNG-0360. Cyber audit report

The CIA shall provide quarterly cyber audit report to his/her CEO, and to his/her customer CIA (GSA CIA or Prime contractor CIA), describing performed activities and outcomes.

The first complete audit report shall be delivered 6 months after PDR, and in any case a first complete version of the report shall be available before CDR.

End of requirement

CYB-MNG-0370. Cyber critical findings

When during his duties, the CIA identifies a critical finding, this shall be immediately reported to his/her customer CIA (GSA CIA or Prime contractor CIA).

Any unexpected non-compliance to these cyber requirements shall be considered a critical finding.

End of requirement

Note: this requirement intends to provide immediate notification for critical vulnerabilities and non-compliances, without having to wait for the report defined in CYB-MNG-0360.

CYB-MNG-0380. Findings content

For each finding, at least the following information shall be provided:

- **Finding description**: description of the finding, including the method used for identification;
- **Root cause**: it is that which gives rise to the risk;
- **Impact**: deviation from the expected provision of the service or system functionalities;
- **Likelihood**: it is the chance of the risk materializing;

- **Proposed remediation**: proposed action to be put in place to remediate the finding;

Each finding shall be reported in writing, and signed by the CIA.

End of requirement

CYB-MNG-0390. CIA cyber request for deviation

When during an audit, the CIA identifies a non-conformance to a cyber requirement, he/she shall prompt the CSM to recover the non-conformance. When this is not possible, they shall request the CSM to produce an RfD.

End of requirement

CYB-MNG-0400. Inputs to the risk register

The CIA shall provide the finding contained in the cyber audit report as inputs to the project risk register.

End of requirement

CYB-MNG-0410. Program and independent security assessment

When requested by the Program or the SAB, the contractor and CIA shall facilitate and support the execution of security assessment performed by 3rd parties.

End of requirement

7 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
Inputs to Security Management Plan	CSM	CYB-MNG-0210	KO	PDR, CDR Or any operational relevant review (OVR, etc)
Statement of Compliance	CSM	CYB-MNG-0240	KO	PDR, CDR, QR, AR Or any operational relevant review (OVR, etc)

Cyber audit plan	CIA	CYB-MNG-0320 CYB-MNG-0330 CYB-MNG-0340 CYB-MNG-0350	PDR	Every 6 months
Cyber audit report	CIA	CYB-MNG-0360	after PDR and in any case first release before CDR	Quarterly
Cyber critical findings notification	CIA	CYB-MNG-0370	N/A	As soon as they are identified
(Requirements) Cyber Request for Deviation/Waiver	CSM	CYB-MNG-0250 CYB-MNG-0260 CYB-MNG-0390	N/A	As soon as they are identified
Security incident report	CSM	CYB-MNG-0100 CYB-MNG-0200	N/A	As soon as they are identified
Security awareness programme	PM	CYB-MNG-0270	KO	Each relevant milestone, if necessary.
Security awareness report	PM	CYB-MNG-0300	PDR	Yearly

Table 4 - Deliverables documents

End of Document