Network Equipment Security Assurance Scheme Audit Guidelines

Version 1.0

18 February 2022

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

The GSMA operates the Network Equipment Security Assurance Scheme (NESAS) for Product Development and Lifecycle Processes Assessment and Network Equipment evaluation. For the assessment part, to fulfil the NESAS requirements, Equipment Vendors are audited by a GSMA appointed Auditor against all the Product Development and Lifecycle Processes Security Requirements, defined by NESAS.

This Audit Guidelines document is the supplement to the NESAS documentation and is published to ensure common standards across the Auditors and Auditing Organisations. It is not intended to replace the security requirements or any other documentation. It should also not be seen as training material for Auditors, but as a guideline that focuses only on aspects that may have an impact on the outcome of the audit and may require more clarification, such as the interpretation of certain security requirements and the type of evidence needed.

The guide is also intended to help Equipment Vendors to understand, interpret and apply the NESAS requirements.

The guide must be read and used in conjunction with the NESAS Development and Lifecycle Security Requirements document FS.16 [3]. Note that the guide is specific to the version of the requirements. Before using this guide, it should be ensured that the guide matches the version of the requirements in FS.16 [3] against which compliance is going to be claimed and the audit is performed. The version of NESAS documentation that this document refers to can be seen in section 2.3.

This document is part of the NESAS documentation. The NESAS Development and Lifecycle Assessment Methodology, containing the audit procedure, is defined in FS.15 [2]. For general information on the NESAS scheme, see the overview available in FS.13 – Network Equipment Security Assurance Scheme - Overview [1].

1.2 Scope

The Audit Guidelines are intended for both Equipment Vendors and Auditors to prepare and align themselves by providing guidance on the planning, preparation and conduct of the audit.

The Audit Guidelines also describe what evidence is considered sufficient to determine that a process complies with the security requirements. This is provided for each requirement in the NESAS Vendor Development and Product Lifecycle Assessment Requirements, FS.16 [3]. It also contains information on what evidence should be provided to NESAS Security Test Laboratories to validate that an audited Development and Product Lifecycle process was followed.

The purpose of the Audit Guidelines is to improve audit quality and consistency, reduce subjectivity, make audits more repeatable, reproducible, consistent, and comparable between Auditors and between Equipment Vendors.

The Audit Guidelines are limited to audit matters pertaining to the auditing aspects of the Vendor Development and Product Lifecycle Security Requirements. Note that the Audit Guideline document is only a complement, and does not substitute or contain any additional

requirements, so it is important to firstly read and understand the NESAS Scheme Overview FS.13 [1], the NESAS Development and Lifecycle Assessment Methodology FS.15 [2] and the NESAS Development and Lifecycle Security Requirements FS.16 [3].

Note that these Audit Guidelines apply to the Vendor Development and Lifecycle Processes Assessment of Equipment Vendors, performed by the appointed Auditor. They do not apply to the Network Equipment and Evidence Evaluation, performed by NESAS Security Test Laboratories.

1.3 Document Maintenance

This guide has been created and developed under the supervision of GSMA's Security Assurance Group comprised of representatives from mobile network operators, Equipment Vendors and NESAS Auditors.

The GSM Association is responsible for maintaining this security standard and for facilitating a review, involving all relevant stakeholders, which will take place every 12 months during the life of the scheme. Whenever the FS.16 [3] changes, this audit guide must also be reviewed and if necessary updated.

2 Definitions

2.1 Abbreviations

Term	Description
3GPP	The 3rd Generation Partnership Project
BOM	Bill of Materials
CA	Certification Authority
CERT	Computer Emergency Response Team
CM	Configuration Management
CPA	Commercial Product Assurance
CVE	Common Vulnerabilities and Exposures
DAST	Dynamic Application Security Test
FASG	Fraud and Security Group
FOSS	Free and Open Source Software
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
NCSC	National Cyber Security Centre
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
PDF	Portable Document Format
PKI	Public Key Infrastructure
RCA	Root Cause Analysis
SAST	Software Application Security Test
SCA	Software Composition Analysis

Term	Description
SCAS	Security Assurance Specification
SCAT	Source Code Analysis Tool
SDL	Software Development Lifecycle
SECAG	Security Assurance Group
SHA-512	Secure Hash Algorithm-512
TR	3GPP Technical Report
TS	3GPP Technical Standard
URL	Uniform Resource Locator

2.2 Glossary

Unless defined below all capitalised terms shall have the same meaning as in FS13:

Term	Description
Audit Guidelines	Document giving guidance to the Auditor and Equipment Vendor on how to interpret the requirements.
Audit Report	Document presenting the results of the audit conducted for the Equipment Vendor by the Auditor.
Audit Summary Report	A subset of the Audit Report created by the Auditor that summarises the key results.
Auditing Organisation	Organisation selected by Equipment Vendor to conduct Audits of Vendor Development and Product Lifecycle Processes, employs, or contracts Auditors.
Auditor	Organization appointed and contracted by GSMA and selected by the Equipment Vendor to conduct audits of Vendor Development and Product Lifecycle processes.
Conformance Claim	A written statement by the Equipment Vendor that confirms it meets the NESAS security requirements for the Development and Product Lifecycle Processes that are to be assessed.
Equipment Vendor	Network Equipment Vendor. Network equipment that is produced and sold by an Equipment Vendor is called a Network Product in NESAS.
Firmware	Binaries and associated data supporting low-level hardware functionality installed on non-volatile memory like ROM and EPROM usually not mountable to a running operating system's file system. Firmware is a specific type of Software, therefore in this document the term "Software" includes Firmware.
NESAS Oversight Board	The body overseeing NESAS, run by the GSMA. It is responsible for the governance of the Vendor Development and Product Lifecycle Process assessments and quality assurance of NESAS.
NESAS Security Test Laboratory	A test laboratory that is ISO 17025 accredited in the context of NESAS and that conducts Network Product evaluations. It can be owned by any entity.
Network Product	Network equipment produced and sold to network operators by an Equipment Vendor.

Term	Description
Network Product Class	In the context of NESAS, the class of Network Products that all implement a common set of 3GPP defined functionalities.
Network Product Development Process	The stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production, and delivery.
Network Product Lifecycle Processes	The stages through which developed Network Products journey to end of life including maintenance and update releases during their lifetime.
Release	Version of a Network Product being made available for deployment. The first Release of a Network Product is assumed to be a new Network Product.
Software	Binaries and associated data forming the basis of a Network Product's operating system and functionality. Software is commonly stored on hard disks or flash memory mass storage devices. In this document, the term "Software" includes "Firmware".
Vulnerability	In SP 800-30 [6], NIST defines a vulnerability as "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

2.3 References

Ref	Title
[1]	FS.13 -– Network Equipment Security Assurance Scheme – NESAS Overview v.2.1
[2]	FS.15 -– Network Equipment Security Assurance Scheme – Development and Lifecycle Assessment Methodology v. 2.1
[3]	FS.16 – NESAS Development and Lifecycle Security Requirements v. 2.1
[4]	3GPP TR 33.916, "Security assurance scheme for 3GPP Network Products for 3GPP Network Product classes". http://www.3gpp.org/DynaReport/33916.htm
[5]	"CPA Build standard", contains the NCSC's requirements for a Network Product developer's security engineering approach. https://www.ncsc.gov.uk/content/files/protected_files/document_files/The%20CPA%20Build%20Standard%201.3.pdf
[6]	NIST SP 800-30 Rev. 1, "Guide for Conducting Risk Assessments" September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
[7]	NIST FIPS PUB 180-4 "Secure Hash Standard (SHS)", August 2015. http://dx.doi.org/10.6028/NIST.FIPS.180-4
[8]	SEI CERT Coding Standards, Carnegie Mellon University, https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards.

2.4 Conventions

This is an informative document.

3 General Guidelines

The intention of this document is to advise the Auditor and the Equipment Vendor in the audit process and to align them in the delivery of the NESAS security audit.

3.1 Purpose of the Audit

The Audit is conducted in the context of the NESAS Vendor Product Development and Lifecycle Processes Assessment. The purpose of this assessment is for the Equipment Vendor to demonstrate that it is capable of developing secure products and maintaining product security until the product has reached end-of-life.

The key objective of the NESAS assessment is that Equipment Vendors have all necessary security controls, measures, and procedures in place and adhere to them at all times. For Equipment Vendors, in all their activities, comprehensive security should be as pervasive as product features are. In the highly digitised society of the 21st century, mobile networks can only be operated in a secure way, if its components – the network equipment – are secure. Equipment Vendors are responsible for delivering deliver secure products that can be securely operated by mobile network operators. This is particularly crucial due to the increasing connectedness of all sorts of equipment and networks. Attack surfaces are increasing, and stringent security is needed to combat attacks and unintentional malfunctioning.

Product security and the necessary activities to create and maintain secure products should become a #1 priority for all Equipment Vendors. The corporate philosophy should be arranged accordingly. All staff involved in developing and maintaining Network Equipment should take care of security as a standard activity. Tools, procedures, equipment, and training should be provided to make this possible and to maintain it on a high-quality level.

It needs to be demonstrated during the Audit, that the Equipment Vendor takes Network Equipment security seriously, and that the Equipment Vendor is using security focused methodologies at all stages of product design and development. The Auditor confirms this by signing the Audit Report.

3.2 Audit Scope

The scope of the audit should be clearly stated and agreed between the Auditor and Equipment Vendor to ensure there is a clear understanding and expectation for all stakeholders.

The audit scope should be agreed as early as possible in the audit preparation phase. Since the NESAS assessment process starts with an Equipment Vendor’s internal assessment, the Equipment Vendor must ensure the scope of the audit is consistent with the scope of the internal assessment and the conformance claim.

Important considerations when specifying the audit scope:

- How similar are the development processes for all products in the scope?
- Are all business groups/organisations relevant to the audited processes available?

- Can all necessary evidence be collected by different business groups/organisations in parallel?

3.3 Audit location

When choosing the site for on-site audit, the Auditor and the Equipment Vendor need to meet the requirements laid out in FS.15 [2] section 4.3.5.

3.4 Audit Evidence

Compliance with the NESAS requirements relies on the review of Audit Evidence to demonstrate that appropriate measures are in place and are effective, efficient, and sufficient. The Audit Evidence needs to demonstrate that the controls and security measures implemented meet the security objectives behind the requirements as stated in FS.16 [3] section 6.2.

In general, Equipment Vendors need to show two categories of Audit Evidence to prove their compliance with NESAS for each of the FS.16 [3] requirements:

1. Audit Evidence Category 1 – Company level or product line level product development/ lifecycle processes related evidence. For example, process evidence for version control, vulnerability management, test procedures, design guidelines or principles, test baselines, and threat modelling methodologies are required to be adhered to by the entire company or the relevant product line.

2. Audit Evidence Category 2 – Evidence such as records which demonstrate the implementation of the security measures described in Audit Evidence Category 1 by the product line to be audited. For example, design documentation, test reports, IT platforms, tools, completed checklists, review records, certificates, logs, repositories, etc. which are carefully checked by the Auditors to ensure compliance.

During the audit, the audit evidence as defined above needs to be assessed in terms of coverage, effectiveness, efficiency, and application to assess if the NESAS requirements have been implemented.

- Coverage: Whether the implemented measures are documented for the business groups/organisations in scope. For example, relevant process descriptions are provided for all NESAS requirements.

- Effectiveness: Whether the implemented measures are effective. For example, whether the Equipment Vendor has skilled staff, information is managed by IT systems, review mechanisms and issue resolution mechanisms are in place, continual improvement processes are in use, etc.

- Efficiency: Whether the implemented measures are efficient. For example, whether the Equipment Vendor has the capability of automatic code scanning, testing, and building, a shared knowledge base or checklists, integrated work platforms or desktops for the designer, developer, tester, etc.

- Application: Whether the implemented measures are being applied. For example, provision of evidence that demonstrates that the Equipment Vendor trains staff, applies automatic code scanning, and tests their Network Products.

3.5 Language

The language used during the audit is English. All Audit Evidence and documentation required to conduct the audit must be in English. The Equipment Vendor must submit an accurate translation of all Audit Evidence Category 1 that isn't in English to enable the Auditor to make the assessment of the provided documentation. Audit Evidence Category 2 (e.g., screenshots, tool output) can be presented in the original language; however, English translations should be provided if requested by the Auditor. In case of any conflict the English translation shall prevail.

3.6 Sampling methodology

Sampling in the context of this section refers to sampling of Audit Evidence Category 2 and sampling of product lines for each requirement demonstrated during the audit.

3.6.1 Audit Evidence Category 2 sampling

Audit Evidence Category 2 sampling means that a representative subset of the full evidence for a specific requirement is examined. It is used to gain sufficient confidence in the evidence without analysing the whole evidence. Sampling is used as a cost-effective measure to achieve confidence in the whole but shall only be used for evidence that is relatively homogeneous in nature, i.e., evidence produced by a well-defined process. Sampling may need to be justified based on the nature of the evidence to be sampled.

Some examples of how sampling may be used in this context are:

- witnessing the output of the Equipment Vendors software code review process to demonstrate that code reviews are being carried out consistently as per the defined development process;
- selecting items from the Equipment Vendors list of 3rd party components used in order to check how many known related vulnerabilities are present in these components, whether an old version is being used, or if any components are approaching end of life;
- identifying how many protocols have been fuzzed by the Equipment Vendor and then selecting a sample of these protocols to check the fuzzing tool used, fuzzing records, results, issues found, and any remedial plans to address any issues found.

The following rules must be followed by the Auditor when sampling the Audit Evidence Category 2:

1. Samples should be chosen such that they are representative of all the evidence and not be randomly chosen. The sampling must provide suitable coverage of the target group such that the sample set is representative of the items that are the target of the sampling.
2. The Equipment Vendor must not be informed ahead of the sample set involved.

3.6.2 Selection of product lines

Selection of product lines is considered when there is more than 1 product line under the scope of the audit. In such cases, the following aspects must be considered:

- If there are no differences in the documented development process followed by the different product lines for a requirement, then the product lines for demonstration are chosen based on the differences that might exist in the tools used to follow the same process. Audit Evidence Category 2 is examined such that all tools are covered.

- If there are differences in the documented development process followed by the different product lines for a requirement, then all different processes must be chosen for demonstration during the audit. Audit Evidence Category 2 is examined such that all differences in the development process are covered.

- If there are no differences in the documented development process followed and associated tools used by the different product lines for all requirements, then one or more product lines are selected, and Audit Evidence Category 2 is examined such that all requirements are covered. The sample set must be agreed between the Auditor and the Equipment Vendor. A minimum threshold should be decided upon based on the number of product lines in scope.

3.7 Audit Report

The Audit Report must follow the Audit Report structure defined in FS.15 [2], Appendix B.

The Audit Report will include detailed audit steps performed for each NESAS requirement in Appendix A of the Audit Report. Records/examples showing the application of the process which are demonstrated to the Auditor by the Auditee during the audit should be recorded in the Audit Report.

Where sampling is performed then a sample plan must be documented in the Audit Report, which describes how the sample set was chosen from the target group, together with identification of the items sampled.

The Audit Report will include guidance on which kind of Compliance Evidence is to be considered as sufficient and provided to a NESAS Security Test Laboratory in Appendix A of the Audit Report. The format of any artefact that is required as evidence to be provided for Network Product evaluation should be specified in the Audit Report. The Audit Report should give some indication of the number of examples to provide as evidence.

3.8 Conformance claim

Before the start of the Audit, the Equipment Vendor provides the Auditor with all their Audit Evidence Category 1, including a signed conformance claim. The signed conformance claim also needs to be submitted by the Equipment Vendor to the GSMA.

3.9 Interim audits and Full audits

Requirements for the Interim Audit process are laid out in FS.15 [2], section 4.6.

Each Full Audit should essentially involve a complete review of the processes under audit and prior knowledge of those processes should not be a factor when determining the audit duration.

4 Application of requirements

The aim of the Guidelines for the NESAS requirements is to increase the audit quality and to provide consistent and comparable results between Equipment Vendors and Auditors. For each of the requirements there is general guidance, a description of the expected input, expected audit activity and evidence that the Security Test Laboratory should use to confirm that the audited processes have been applied for the product tested.

References to external documents and standards mentioned in the table below can be found in FS.16 [3], section 2.3.

Statements from NESAS FS.16		**Guidelines**
Design		
REQ-DES-01	**Security by Design**	

The Network Product shall implement security by design throughout the whole development and product lifecycles. Therefore, architecture and design decisions shall be made based on a set of security principles that are tracked throughout the development and product lifecycles.
The goal of security by design is to limit the impact of security risks through robust and consistently applied principles such as (but not limited to):
• Security architectural principles:
  ○ Domain separation
  ○ Layering
  ○ Encapsulation
• Security design principles:
  ○ Least privilege
  ○ Attack surface minimisation
  ○ Centralised parameter validation & centralised security functionality
  ○ Preparing for error & exception handling
  ○ Privacy by design
		General guidance
		Security-by-design covers all phases of the development lifecycle and the product lifecycle. Processes shall integrate security into all phases, in a comprehensible and effective way. Design decisions shall be made in favour of security and be documented.
		First, a requirement analysis or threat analysis should be carried out to identify which mitigations are required. Secondly, the design and implementation of these mitigations must take into consideration secure design principles.
		While there is flexibility as to how a requirements or threat analysis is carried out, there must be a clear basis for identifying all the necessary mitigations that are to be implemented. The second aspect focuses on implementation only. It may not be possible to redesign older products, however it is still possible to reduce attack surfaces. For newer products it is expected that many of the design principles given as examples in FS.16 would be implemented.
		The following aspects will be assessed:
		(1) How the principles are followed. The Auditor may need to interview the designer for verification.
		(2) For threat analysis, whether a representative threat landscape is identified through the methodology claimed, and whether corresponding mitigation measures have been introduced.

Statements from NESAS FS.16	Guidelines
Security principles such as the above should be considered and applied when appropriate. In the design phases, a threat analysis process for the Network Product shall be undertaken to identify the potential threats and related mitigation measures.	**Expected input** The Equipment Vendor is expected to demonstrate: • A description of the best practise guidelines used or publicly available security checklists (or benchmarks) that include detailed low-level guidance on setting the security configuration of operating systems and applications. • How the requirement and threat analysis has been carried out and that this is documented in the threat analysis reports. The threat analysis methodology could be applied per feature or/and per release. • A process description showing how and when network Product development processes and security architecture principles are considered. • A description/guidance of their design principles and when they are considered during the development process. Security by design supporting actions like designer platform, threat/mitigation library, tools, etc. • A description/guidance of design principles when using open-source software and components to include supporting actions, threat/mitigation library, analysis tools, etc. **Expected output** The Auditor shall verify: • Records/examples showing the application of the processes described above. **Evidence to Security Test Laboratory** • Provide the risk and threat analysis reports.
Implementation	
REQ-IMP-01 **Source Code Review**	
The Equipment Vendor shall ensure that new and changed source code dedicated for a Network Product is appropriately reviewed in accordance with an appropriate coding standard. If feasible, the review should also be implemented by means of utilizing a Source Code Analysis Tool and automation where appropriate.	**General guidance** First, the Equipment Vendor needs to declare what programming languages are used to develop the products in scope of the process audit. These are product specific; therefore, a representative sample of programming languages should be selected during the audit. Then, two aspects are important: the process for code review (that could be manual and/or automatic), and that there is a coding standard for these reviews.

Statements from NESAS FS.16	Guidelines
The goal is to help reduce the risk of software issues that could introduce vulnerabilities in the Network Product. An example of a best practice coding standard is Carnegie-Mellon, SEI CERT.	**Expected input** The Equipment Vendor is expected to demonstrate: • The coding guidelines (including any industry standards used) for all the programming languages used in the development of the products in scope of the audit. • A documented process which mandates a code review. The process can be manual/automatic and describe a process to resolve the bugs identified, and how to verify them. The process description shall include supportive materials (e.g., code review checklists) in accordance with an appropriate coding standard. • Description of the tools used to perform the source code analysis. **Expected output** The Auditor shall verify: • That the coding guidelines (and any industry standards used) are available for all the programming languages used in development. • That the coding guidelines (and any industry standards) are available and accessible to the developers. • The process followed to perform manual code reviews, resolution of the bugs, and reverification of the code before the code is merged. • The automatic code reviews performed with the help of the code analysis tools and how often the tools are updated. • How the results from the tools are dealt with, in case of false positives and in case of the true positive bugs found. • If there is any mandatory verification to ascertain that the bugs are resolved before the code is allowed to be merged. • Whether any free and open-source software (FOSS) used was reviewed by the Equipment Vendor using an automated industry security best practice tool(s) (e.g., SCA, SCAT, SAST, and/or DAST).

Statements from NESAS FS.16	Guidelines
	The Auditor will document in the Audit Report, the process followed by the Equipment Vendor for source code review, some examples of the code commits, and reviews performed (manual/automatic). **Evidence to Security Test Laboratory** • Provide a sample of the coding analysis performed (in case of manual reviews) or code review reports (in case of code review by tools).
REQ-IMP-02 **Source Code Governance**	
The Equipment Vendor shall ensure that no changes are introduced into the Network Product without appropriate governance. The goal is to prevent unauthorised changes and to reduce the likelihood of unintended or unauthorised changes. It is also to ensure that there are independent lines of control for any changes.	**General guidance** The source code governance requires both organisational and technical measures. It must be clear who should have access and who should be able to make changes to the source code. These rules must be enforced by processes for granting and denying access that are applied by technical means, such as access rights to the Configuration Management (CM) or version control system. **Expected input** The Equipment Vendor is expected to demonstrate: • The process of access control. How the access rights to the version control systems where source code is stored and developed is given, revoked, and regularly updated. • A documented and approved change process to identify and track who (internally or externally) made the changes and to identify the source (internally or externally) for the change. • A process to link the code commits to the reason for the change, e.g., the code commit is being made to fix a bug or to meet a new requirement etc. • A process that ensures that the code commit is successful only after it passes the code review process and that neither more nor less code is included in the commit. • A process that ensures that only the intended changes are included in any release. **Expected output**

Statements from NESAS FS.16	Guidelines
	The Auditor shall verify: • That controls are in place describing who can access the source code and submit a code change. • That the code commits can be tracked and linked to the reason for the change, and the product version which will include the submitted change. • That there are mandatory reviews to ensure that neither more nor less code is included in any particular commit. • That all code commits are only successful after passing the code review process • In any release the change commits leading to the release can be traced. The Auditor shall check a random selection of change commits to ensure the end-to-end traceability for that change and that any reviews (manual or automatic) were performed. The Auditor shall document in the Audit Report, the process followed by the Equipment Vendor for the source code management change process, some of the example changes committed, and whether there are any checks made to verify that only the intended changes are included in the product. The Auditor shall document all reports regarding updates or changes to source code, binaries, libraries, packages and/or files. **Evidence to Security Test Laboratory** • Provide a sample of source code change commits to demonstrate the process of change control.
Building	
REQ-BUI-01 **Automated Build Process**	
The Equipment Vendor shall utilise an automated build process with a minimum of manual intervention to build the software of the finished product and store the build logs. The goal is to ensure that the build is reproducible, deterministic and that it covers the security procedures defined by the Equipment Vendor.	**General guidance** Automated processes / tools shall be used where applicable to make sure that the way the product is assembled is consistent and repeatable. The build tool should be able to record any changes made to the build process itself, together with who made the change and when. **Expected input** The Equipment Vendor is expected to demonstrate: • The configuration management system and any build processes / tools used.

Statements from NESAS FS.16	Guidelines
	• For software, this may be demonstrated through the use of an automated build tool, build scripts and makefiles. If manual 'build' methods are used, then a justification must be provided by the Equipment Vendor as to why an automated system could not be used. • Evidence of an approval process for any changes to the build process should be provided by the Equipment Vendor. Example end-to-end audit trail evidence should be provided. **Expected output** The Auditor shall verify: • That an automated build management system is being used and will record the name of any tools used (e.g., Jenkins) in the Audit Report. • Evidence of documented approvals process for any changes to the build process. **Evidence to Security Test Laboratory** • Example end-to-end audit trail evidence of the build process should be provided.
REQ-BUI-02 **Build Process Management** All the data (including source code, building scripts, building tools, and building environment) of the build process shall come directly from a version control system. The goal is to ensure that the same binaries can be reproduced and that there is a clear audit trail for any modifications.	**General guidance** A version control system should be used to store all configuration items that go to make up the product. Access to any configuration items should be adequately controlled, with individuals having separate login accounts and an audit trail of activity being recorded. There should be an approval mechanism for any changes to the build process. As part of this overall requirement, consideration also needs to be given to the operational security procedures relevant to the build process, such as who has access to the required tools, and who can make authorised changes to the build process, together with the integrity of the input and output. **Expected input** The Equipment Vendor is expected to demonstrate: • A list of configuration items that are to be maintained under configuration management.

Statements from NESAS FS.16	Guidelines
	• How version control is achieved for each configuration item (for example in a source code version control repository such as Git, Subversion etc.). • That the product can be uniquely identified within the version control system, and that each release build is clearly identified as such. • That there are access control measures (e.g., individual logins) to the version control systems used to prevent any unauthorised changes from being made, and suitable auditing of changes is maintained. • All changes to configuration items should be suitably authorised. • Example audit trail evidence should be provided. **Expected output** The Auditor shall verify: • That version control system(s) is being used and record in the Audit Report the name of the tool being used (e.g., Git, Subversion). • There are access control measures (e.g., individual logins) to the automated build tool/platform and version control system to prevent any unauthorised changes from being made. • Individuals have separate login accounts to any such tools, and that any activity (changes) can be traced back to the individual making the change. • That all changes are recorded within the version control system. Evidence of a documented approvals process for any changes will be recorded by the Auditor in the Audit Report. • All FOSS sourced binaries, libraries, packages and/or files are documented and logged including download source (i.e., repository server information – Hosting Provider's Name, Primary FQDN, IP, URL Link to Download, etc.), versions, and results from analysis tools. **Evidence to Security Test Laboratory** • A list of all the data / configuration items being maintained and the methods by which they are version managed, together with the tool set than enables this.

Testing	
REQ-TES-01	**Security Testing**
Security testing should include the validation of security functionality, both positive and negative testing, as well as vulnerability testing of the Network Product. Network Products are to be tested from a security perspective within a fair representation of the operational environment. Vulnerability testing shall test for the robustness of the Network Product against undefined/unexpected input. The goal is to ensure that security functionality has been validated and that potential vulnerabilities are detected and mitigated before the Network Product is delivered.	**General guidance** The Security Testing requirement considers many aspects: (1) Security functionality testing should be performed on the Network Product and must contain both positive and negative test cases. (2) Vulnerability testing should be performed. (3) The test environment used must be similar to the operational environment. (4) Vulnerability testing shall include testing for robustness against undefined/unexpected input (e.g., Fuzz testing). (5) The testing process must also include a process to register problems found during both functionality and vulnerability testing as bugs which are then resolved and verified. (6) How the risk will be accepted for any bugs found that could not be resolved in the current version. **Expected input** The Equipment Vendor is expected to demonstrate: • A process description which mandates security functionality testing and vulnerability testing. • Security functional test cases which include both positive and negative test cases. • Activities that are part of the vulnerability testing. • That there is a test strategy (or test plan) developed for each project, and that any such test plan considers the risk assessment carried out during the project planning stage. • That the test plan or test cases are mapped to the security requirements to verify that all the security requirements are fulfilled. • That the testing performed is completely automated or whether there are any manual tests performed.

	• Tools used for automated tests and vulnerability testing or scans (e.g., vulnerability scan tools, breach detection tools). • Whether the testing includes robustness testing, fuzz testing, compliance to industry security best practises for secure configuration of operating systems and applications, etc. • Whether the test environment used reflects the customer operational environment, and if not, an explanation of how it differs and why this will not invalidate the test results. • How issue/bug tickets are raised, tracked, and subsequently resolved for any tests that fail. • The risk acceptance strategy for any unresolved problems found during testing. • Evidence of test plans, test reports, vulnerability scan reports, issue/bug tickets raised by the testing team. **Expected output** The Auditor shall verify: • If a test plan or test strategy has been created for the project under the scope of audit. • A sample of the test cases and check if they include both positive and negative functionality test cases. • A sample of the vulnerability scans performed, together with the tools used and the reports produced. • A sample of the issue/bug tickets raised during testing and walk through with the Equipment Vendor the resolution, tracking and risk acceptance process for any bugs found during testing. The Auditor shall document the process followed by the Equipment Vendor for security testing covering all the aspects discussed above and list the issue/bug ticket tracking numbers or ID’s, and any test reports that were examined in the Audit Report. **Evidence to Security Test Laboratory** • Security test plan or test strategy • Security test reports (manual/automatic)

Release	
REQ-REL-01	**Software Integrity Protection**
The Equipment Vendor shall establish and maintain methods to ensure that the delivery of Network Products is carried out under controlled conditions. The mobile network operator shall be provided with appropriate means to identify whether a received software package is genuine. The goal is for mobile network operators to be able to check the integrity of the software package and associated documentation.	• Vulnerability scan reports **General guidance** The requirement considers two aspects: (1) That the integrity of the software can be verified; and (2) That authenticity can be verified for both the software and associated documentation in any release. The Auditor shall check the security mechanisms deployed to ensure integrity and authenticity for software package delivery are strong. If cryptography is used, then state of the art algorithms and key lengths should be used. The following are examples for consideration: • Since anyone can generate a checksum this would not show that the software package is genuine. So, more evidence is needed such as a digital signature of the software, or by having a secure reference to that checksum: for example, on a suitably protected Equipment Vendor web page. • MD5 and SHA-1 functions are prone to collision attack and should be avoided. In case a weaker algorithm is used, there must therefore be additional measures to ensure a secure path is used to deliver the software - such as a VPN connection etc. An automated process shall be used where applicable if digital signatures are applied to the software package. This requirement applies to both the software and any associated product documentation. **Expected input** The Equipment Vendor is expected to demonstrate: • A process to apply a digital signature or checksums to both the software package and any associated documentation. • A documented process by which the customer can securely verify the digital signature or checksum.

	Expected output The Auditor shall verify: • That a process exists to ensure that all the software packages (software and the relevant documentation) are integrity protected before they are made available to the customer. • There is a process that can be followed by the customer to ensure the authenticity of the software package delivered. • The instructions for the verification of the software package are provided to customer. • The update process, being either manual or automated, must provide a mechanism by which the updates can be authenticated and checked for integrity before they are applied. The Auditor shall document the process followed by the Equipment Vendor in the Audit Report. **Evidence to Security Test Laboratory** • Provide the instructions for the verification of the software package for the product being tested by the evaluator.
REQ-REL-02 **Unique Software Release Identifier**	
All released software package versions shall bear a unique identifier that maps to a specific build version. The goal is to ensure that all software is identifiable, and that the exact same software uses the same unique identifier.	**General guidance** There are two aspects to verify: (1) There is a well-defined process for how the IDs are generated that ensure they will be unique when the software product changes. (2) That there are examples showing that processes have been correctly applied. **Expected input** The Equipment Vendor is expected to demonstrate: • That an automated process exists wherever applicable to ensure a unique identifier is assigned to the software package. • It is possible to identify the exact build that went into the release. • That there is a process to identify the source code of the released software package in the version control system used.

	Expected output The Auditor shall verify: • There is a process which ensures that the software package being released gets a unique identifier. • The exact build can be identified and can be traced to the source code level for any released software package. • The customer will be able to identify the build of the new software package/update received and will be able to differentiate from the earlier or the older release. The Auditor shall document the process followed by the Equipment Vendor to assign unique identities to the software. The Auditor shall document the examples that were examined. **Evidence to Security Test Laboratory** • Provide the unique release identifier of the software package.
REQ-REL-03 **Documentation Accuracy**	
Customer documentation shall be up-to-date in all security related aspects and reflect the current functionality of the Network Product at the time when both the Network Product, or software upgrades of it, and the customer documentation are shipped to the customer. The goal is to ensure that the Network Product documentation reflects the version of the Network Product delivered.	**General guidance** The Equipment Vendor should provide comprehensive documentation including user and administrator guides. The documentation provided should clearly explain any security enforcing functionality and give guidelines to the product's secure use and operation. This requirement will verify that there is a process in place to ensure that the Equipment Vendor documentation is accurate, for example: ■ When a new product requirement or feature is introduced in the design phase, the corresponding description should be added in the product documentation, ■ When a security vulnerability is fixed it should be described in the security documentation, Any changes to the documentation should be clearly highlighted to the reader (for example using a change log or history of changes within the document itself). Any documentation specifically describing the product should be examined to ensure their accuracy.

	Expected input The Equipment Vendor is expected to demonstrate: • A sample of the documentation to be supplied to the customer, including a subset of the user and administrator guides, and any guides to product security features. • It should be possible to easily identify the version of the product to which the documentation relates. **Expected output** The Auditor shall verify: • The sample of documentation provided to make sure that it is up to date in all security related aspects and reflects the current functionality of the Network Product at the time when both the Network Product, or software upgrades of it, and the customer documentation are shipped to the customer. • A sample of changes identified from REQ-GEN-02 below and ensure that product changes are reflected accurately in the customer documentation. The output of these checks will be recorded in the Audit Report. **Evidence to Security Test Laboratory** • Provide the up-to-date customer documentation which includes the documented instructions and commands that should be applied to the Network Product.
REQ-REL-04 **Security Documentation**	
The documentation delivered with the Network Products contains all up-to-date information necessary to securely configure and run the Network Product. The goal is to ensure that operators can configure the Network Products in a secure way, including clarifying if the default configuration is secure.	**General guidance** Compared with the previous requirement (REQ-REL-03), this requirement will verify on the completeness of any product security documentation. For example, the accuracy of any security feature descriptions, security feature configuration and commissioning processes, and secure operation instructions. Based on these documents, the customer should be able to configure and operate the Network Product securely. By ‘secure default configuration’ or ‘secure default settings’ it is understood to mean that the product configuration is secure ‘out of the box’ and that any settings that can be configured or changed by the user during deployment are defaulted to a ‘secure’ state when the product is initially installed. This interpretation differs to a product that ‘fails safe’ when a failure occurs – and which means that the product is not left in a vulnerable state.

	The Equipment Vendor should therefore provide guidance on how to securely configure and run the product. The documentation should clearly explain any security enforcing functionality of the product and give guidelines to the product's secure use and operation. All settings (including any default values) that could affect the security of the configuration should be clearly described, together with the implications of changing such settings from their default values. If security settings can be deactivated, then the implications of taking such action must be clearly explained. There should be guidance on how to restore the product to a secure state, should a failure occur. **Expected input** The Equipment Vendor is expected to demonstrate: • A copy of the secure configuration guide (which describes any secure default configuration settings), together with examples of any diagnostic output and audit logging that takes place after failure / during startup and while in operation. • Configuration profiles that securely enable features for deployment. **Expected output** The Auditor shall verify: • The documentation provided to make sure that it contains information necessary to securely configure and run the Network Product. • The documentation provided to ensure it explains how configuration parameter changes can impact the security posture. • The documentation provides a process or a description of a tool to verify the security configurations were properly enabled for each Network Product feature. • That the Equipment Vendor only allows the required services, processes, ports, and protocols associated with product features to be enabled. These checks will be recorded in the Audit Report. **Evidence to Security Test Laboratory** • Security documentation which includes relevant security guidelines and instructions to the user.

Operation	
REQ-OPE-01	**Security Point of Contact**
The Equipment Vendor shall provide a point of contact for security questions/issues and communicate this point of contact to its customers and 3rd party vulnerability disclosers. This point of contact shall be able to find the right person/department inside the Equipment Vendor organisation to deal with security concerns raised by a customer/3rd party vulnerability discloser. The goal is to ensure that the Equipment Vendor forwards incoming requests to the relevant department in a timely and secure manner and that the requesting or informing party receives a timely and appropriate response.	• Hardening guidelines for the Network Product. **General guidance** There are several aspects here to consider: (1) There must be a point of contact that is known to the (supported) customers and also if any 3rd party vulnerability discloser needs to initiate contact; (2) There must be a process behind this point of contact that actually handles the security questions/issues, usually based on the type of request and the product affected; (3) There must be timely and appropriate reaction to these requests; (4) The communication must be secure so that no sensitive information about the customer or vulnerability gets disclosed that could be used for an attack against the customer or any other users of the same or similar products. **Expected input** The Equipment Vendor is expected to demonstrate: • There is a point of contact who can be approached by customers and 3rd party vulnerability disclosers. • There is a process which ensures that the received problems are escalated to the appropriate development team or personnel depending on the type of issue. • There is a process which is used to address and communicate the fix based on the agreed timeframes with the customer. • That the reporter of the issue is instructed to use a secure communication method to report the issue and appropriate means are provided to enable this. **Expected output** The Auditor shall verify: • There is point of contact information available to customers and 3rd party vulnerability disclosers. • The evidence for a selection of problems received from different external sources.

	• The use of secure communication methods, the presence of a define timeframe to resolve the problems, the escalation procedure followed, and the tools used (if any) to track the issues from the point of receiving to resolution and communication of the fix. The Auditor must describe the process followed with some end-to-end examples in the Audit Report. **Evidence to Security Test Laboratory** • End-to-end examples of this process having been implemented and followed.
REQ-OPE-02 **Vulnerability Information Management**	
The Equipment Vendor shall have reliable processes in place to ensure it can become aware of newly revealed potential vulnerabilities in used 3rd party components and to evaluate whether they result in vulnerabilities in the Network Product. The goal is to reduce the impact on the Network Product of 3rd party components becoming unsupported, unavailable, or vulnerable.	**General guidance** Vulnerability management is primarily not about finding vulnerabilities, but rather about collecting information about already known vulnerabilities in products, e.g., CVE entries for the product itself or 3rd party components used by the product, reports from customers, academia, etc. **Expected input** The Equipment Vendor is expected to demonstrate: • How they monitor vulnerabilities in the 3rd party components. The Equipment Vendor should demonstrate that they have a centralized repository of the components used, or they might be tracking the components for each product separately. • That they are subscribed to organizations like CERT or have maintenance contracts with the 3rd party component vendors to get notified about any potential vulnerability. • A process where the vulnerabilities received are analysed and the products affected are identified. • A process of how the vulnerability is tracked through to resolution or details of how any workaround solutions (if applicable) are sent before a fix is made available. **Expected output** The Auditor shall verify:

	• The Equipment Vendor process of how the 3rd party components are monitored and tracked for vulnerabilities. If there is a central repository, it is easier to apply a fix to the vulnerability. However, if the components are maintained individually per product line, the Auditor must check if there is a process to roll out any finding about a vulnerability or fix to other product lines that might be impacted. • Whether the Equipment Vendor receives notifications about any potential CVE's and if so, that the information is analysed to find out if there is any impact on their products. • The process of customer notification and in the case of a critical vulnerability whether a workaround solution is sent before a fix is available. The Auditor must document the process followed and record some CVEs examined in the Audit Report. **Evidence to Security Test Laboratory** • Examples of CVEs or other third party notified vulnerabilities that have resulted in the process being implemented. • Provide the 3rd party component vulnerability analysis report and release notes.
REQ-OPE-03 **Vulnerability Remedy Process**	
The Equipment Vendor shall establish a process to deal with vulnerabilities found in, or in relation to, released Network Products (including 3rd party components). Vulnerabilities shall be dealt with appropriately and, if applicable, patches/software upgrades shall be distributed to all affected mobile network operators, to honour existing maintenance contracts within an agreed schedule. The goal is to reduce the impact on the Network Product becoming vulnerable or 3rd party components becoming unsupported, unavailable, or vulnerable.	**General guidance** A vulnerability remedy process shall be used not only to address the vulnerabilities during the development process of a product, but also to fix vulnerabilities in a released Network Product. There must be an overall process which commences from the time the vulnerability information is received to the delivery of a fix as a patch or software upgrade. The process must ensure the delivery of the fix to all affected mobile network operators (with maintenance contracts). **Expected input** The Equipment Vendor is expected to demonstrate: • A documented process on how vulnerabilities can be received and resolved in a timely manner. • A process for analysing and identifying the affected products.

	• The process followed to fix the vulnerability, the ticketing system used, and how it can be tracked until a fix is delivered. **Expected output** The Auditor shall verify: • That vulnerability alerts can be received not only for the products under development but for the released products too. • The process followed to fix a vulnerability and release a patch in a timely manner. • Whether the Equipment Vendor provides the fixed bug information in the release notes of the software package or patch release at the time of release or on demand to the customer. The Auditor shall document the end-to-end process followed for receiving and fixing a vulnerability, the timelines taken to release a patch and a sample of issue tickets that were examined. **Evidence to Security Test Laboratory** • Examples of such issues raised in the ticketing system. • Provide the vulnerability analysis report and product release notes.
REQ-OPE-04 **Vulnerability Remedy Independence**	
For ease of deployment, the Equipment Vendor shall have the facility to provide patches/software upgrades that close security vulnerabilities independently from unrelated patches/software upgrades that modify functionality of the Network Product. The goal is to ensure that security remedies can be delivered swiftly and independently from the functional delivery schedule.	**General guidance** This requirement is used to address the ability to provide a quick software upgrade or patch when there is a critical security vulnerability. This patch is expected to be an independent release to fix a security bug which is not part of a planned release. This independent patch is expected to fix the critical vulnerability and shall not contain any other update to modify or add functionality to the Network Product. **Expected input** The Equipment Vendor is expected to demonstrate: • A process is followed to release an emergency patch depending on the criticality of the vulnerability present in the Network Product. • A defined timeframe by which to provide an independent patch for critical security vulnerabilities.

	• A process description where it can be shown that a specific critical security vulnerability fix or patch can be independently released. • A process description to provide a workaround solution (where possible) if a fix is delayed. • A description of the process followed in the development and testing of the independent patch and the fix communication that is sent to the customer. **Expected output** The Auditor shall verify: • That a process exists to release an independent patch to fix a critical vulnerability which is separate from the scheduled release process. • How workarounds are provided to the customer when a fix for a critical security vulnerability is delayed. • The method of communication used to inform the customer about the availability of an independent patch and any associated release notes. (Also, see REQ-OPE-05). The Auditor shall document a sample of the examined independent patches, including a description of the communication method used to deliver the patch. **Evidence to Security Test Laboratory** • A sample of independent patches, communications and release notes that have been issued to fix security vulnerabilities.
REQ-OPE-05 **Security Fix Communication**	
A process shall ensure that information regarding available security related fixes is communicated to mobile network operators that have maintenance agreements in place at the time the fix is released. The goal is to ensure that mobile network operators are informed in a timely way to apply any security fixes**.**	**General guidance** This requirement checks to confirm there is a method to inform the customer of any security related fixes or workarounds available. This communication is to be sent to all customers who have a maintenance agreement in place and will take place within the defined timeframes agreed in the contract. **Expected input** The Equipment Vendor is expected to demonstrate: • That security related fix information can be communicated to all customers that have maintenance agreements, within defined timeframes. This information is

	provided along with a probable date of the fix availability and any workaround available. • Communication is sent to the customer to inform them of the availability of the vulnerability fix or the release of the patch. **Expected output** The Auditor shall verify: • The communication method used to notify customers about security vulnerabilities in the Network Products. • A sample of the communication notifications sent to the customer to ensure that the defined timeframes are being followed. • Whether any workaround solutions are provided, in case of a critical vulnerability before a fix is available. The Auditor shall document in the Audit Report the different types of communication methods used. A random selection of customer notifications sent for some of the CVE's or vulnerabilities in the Network Product will be selected, and a sample of notifications sent about the availability of the fix or when a patch will be released shall be documented in the Audit Report. **Evidence to Security Test Laboratory** • A sample of customer communications, and where appropriate interim workaround solutions, that have been issued in response to CVEs or security vulnerabilities.
General Requirements	
REQ-GEN-01 **Version Control System**	
During the entire lifetime of a Network Product, the Equipment Vendor shall utilise a version control system on hardware, source code, build tools and environment, binary software, 3rd party components, and customer documentation ensuring accountability, authorisation and integrity of all changes. The goal is to be able to trace all the above elements together in a finished Network Product.	**General guidance** This requirement is needed to establish discipline and control in the development and modification of products and related information. This is to both prevent accidental as well as unauthorized changes from being made. Both tools and processes are necessary to ensure the integrity of the configuration items. The tools will provide a method of tracking for any changes and ensure that all changes are authorised. Different tools may be used for different types of configuration items.

	Expected input The Equipment Vendor is expected to demonstrate: • All types of configuration items that must be controlled, such as software, hardware, third party components, test cases, test plans, design documentation, user documentation, etc. are captured in a version control system. • The version control systems being used for each configuration item type. • The processes which describe how to use these version control systems, such as how patches, branches, upstream changes are made in a well-defined manner. • How access control is enforced by the version control systems ensuring that only authorized users are eligible to make changes to their configuration items and that changes are audited to provide individual accountability of changes made. **Expected output** The Auditor shall verify: • That all processes and tools are used in a consistent manner by performing sampling. Sampling should be based on the representative types of configuration items identified. The sampling should consider types of configuration items identified, the different types of version control systems used and cover different types of changes made. **Evidence to Security Test Laboratory** • A list of all the data / configuration items being maintained and the methods by which their versions are managed, together with the tool set than enables this.
REQ-GEN-02 **Change Tracking**	
The Equipment Vendor shall establish a comprehensive, documented and cross Network Product line procedure to ensure that all requirements and design changes, which may arise at any time during the development and product lifecycles, and which impact the Network Product(s) (this includes all aspects of requirement REQ-GEN-01), are managed and tracked in a systematic and timely manner appropriate to the life cycle stage of all affected product components in all Network Products.	**General guidance** This requirement is needed to ensure that the Equipment Vendor uses an audit mechanism that identifies the author of a change to any of the configuration items at both the design and implementation stage of product development. There should be a documented approval process for all changes. **Expected input** The Equipment Vendor is expected to demonstrate: • A process to identify changes to the Network Equipment.

The goal is to ensure that all changes are made in a consistent way through the development of all affected Network Product components in all Network Products.	• An audit mechanism that identifies the author of any change to a configuration item. Change history will include a timestamp/date when the change was approved and will identify the author of any change to a configuration item. • That for the implementation of software/firmware changes a configuration management (or version control) system is used. • That for the implementation of hardware modifications a documented product modification process using Engineering Change Requests and/or change logs are used. • A documented 'approvals' process for changes, and that these processes are being followed in practice. **Expected output** The Auditor shall verify: • Traceability of changes to a configuration item to the individual making the change. A random selection of changes to configuration items will be chosen, and these will be documented in the Audit Report. **Evidence to Security Test Laboratory** • A sample of hardware and software changes that have been made during the design stage, together with evidence of their 'approval'. • A sample of hardware and software changes that have been made during the implementation stage, together with evidence of their 'approval'.
REQ-GEN-03 **Staff Education**	
Continuous education of all staff involved in Network Product design, engineering, development, implementation, testing and maintenance shall be provided to ensure knowledge and awareness on security matters, relevant to their roles are up-to-date. The goal is to ensure that all staff have knowledge and awareness on security matters relevant to their role, maintained to a consistently high level.	**General guidance** All staff should receive suitable training to ensure they are trained in the relevant development process and tools and understand how to apply them to the products they work with. This should be part of an 'onboarding' process, so employees have a basic awareness before they start work. All staff should have security awareness training and be fluent with secure coding methodologies and practices where this is relevant to their role. Training for source code developers should take place on an ongoing basis, to make sure that staff are knowledgeable in the latest security vulnerabilities and are knowledgeable on how to avoid them.

	In general, depending on their role, staff should be trained regularly on matters that are relevant to them, and the Equipment Vendor shall ensure that staff attend this training and apply what they have learnt in their work. Basic security awareness training should also be provided to all staff in support roles such as customer support and technical writers to ensure at least a basic level of awareness of security issues. **Expected input** The Equipment Vendor is expected to demonstrate: • A sample of evidence of the different types of training provided to staff for both general information security awareness, and secure development practices (where applicable to their job role). **Expected output** The Auditor shall verify: • The training program is relevant and up-to-date. • The security awareness training exists and is performed regularly. • The training is mandatory, and staff participate in the training. The Auditor will document the training provided in the Audit Report. **Evidence to Security Test Laboratory** • Samples of training records, and/or course materials where available. • Samples of evidence that show staff have participated in the training.
REQ-GEN-04 **Information Classification and Handling**	
In the entire lifecycle, the Equipment Vendor shall employ an information classification and handling scheme to avoid sensitive information, such as security flaws, signing keys, etc., being leaked. The goal is to ensure that sensitive information is identified, classified, and managed appropriately.	**General guidance** This requirement is needed to ensure that sensitive information that could be used to compromise the Network Equipment is identified and protected from unauthorized access. **Expected input** The Equipment Vendor is expected to demonstrate: • That a process is followed that identifies the sensitive information, for example, signing keys if they are used, security flaw information etc.

	• How security flaw information found or received from both internal or external sources is protected in the issue ticketing system used (e.g., Jira), or in any customer support applications. • The access control mechanism in place to restrict access on a need-to-know basis for any systems where sensitive information is stored. • The protection of the PKI infrastructure, Root CA server including the physical protection of the server, backup protection and access restrictions to the servers. **Expected output** The Auditor shall verify: • That the sensitive information is identified. • That the sensitive information is protected in all systems used to resolve or store vulnerabilities (internal bug tracking systems and any external customer support applications). • There is an access control mechanism to all systems where sensitive information is stored, and access is only given on a need-to-know basis. The access rights are updated/verified periodically. • The private keys are protected if signing keys are used for integrity protection of software. • The Root CA is protected both physically and logically. The Auditor shall document identified types of sensitive information in the Audit Report and explain how this information is protected. **Evidence to Security Test Laboratory** • List of the sensitive information identified. • Examples of how the identified sensitive information is protected in all the systems used.
REQ-GEN-05 **Continual Improvement**	
The Equipment Vendor must have a continual improvement process for its development and product lifecycle and this process must include a root cause analysis of the security	**General guidance** This requirement is needed to ensure continuous improvement in the development and lifecycle processes, based on the lessons learnt from earlier problems. This process may include identification of what to learn from, if there is a security flaw etc., including the

flaws. The resulting improvements shall be incorporated into the relevant design or processes. The goal is to improve processes and to reduce the likelihood of vulnerabilities re-occurring by continual improvement.	identification of the source of the problem. For example, if it is a systematic issue the developers should be able to identify what could be changed to prevent this flaw and make any changes based on the root cause analysis. Most important is that there should be a process for improvement. Overall, it is about reducing the likelihood of flaws, not about eliminating them. Some security issues may be unique and not re-occurring or systematic and may therefore not be caught by this process. **Expected input** The Equipment Vendor is expected to demonstrate: • Information about a process to continuously improve the security design quality. For example, the use of a continuous integration (CI) and continuous deployment (CD) solution to automate their development, deployment, and testing pipeline • A documented process to describe when a root cause analysis (RCA) is performed, and which types of problems it applies to. • A process for incorporating the findings from the RCA into the development lifecycle across product lines to reduce the likelihood of introducing the same vulnerability again. **Expected output** The Auditor shall verify: • The process is followed to constantly improve the product and the development and lifecycle process. • That a continual cycle of root cause analysis is performed for any security flaws and improvements made to the design or process. The Auditor shall document examples of the root cause analysis performed by the Equipment Vendor and any resulting improvements made. **Evidence to Security Test Laboratory** • Examples of root cause analysis having been carried out. • Examples of where this process has resulted in a change to the development lifecycle/processes to prevent a reoccurrence (for example, the introduction of new regression tests, or an update to any coding standards used).

REQ-GEN-06	Sourcing of 3rd Party Components
The Equipment Vendor shall have processes in place to ensure the quality of 3rd party components during the product lifecycle. The Equipment Vendor shall select supported 3rd party components and shall avoid using those reaching the end of life. The goal is to decrease the possibility of the Equipment Vendor sourcing and using vulnerable, tainted, and unsupported 3rd party components within its supply chain.	**General guidance** This requirement is needed to ensure that any third-party components (or any upstream components) are well selected and kept up to date so as to not unwittingly introduce any vulnerabilities into the product. Care should be taken as to where third-party components are sourced, and how they are maintained during the lifetime of the product. Support agreements should be made with third-party suppliers where this is possible, and consideration given (for example, if open-source components are used) on how any flaws will get fixed in an adequate and timely manner. **Expected input** The Equipment Vendor is expected to demonstrate: • They hold a list of third-party components used. • Documented procedures for selecting, onboarding, and maintaining any third-party components used. • Procedure (or on-boarding process) to prevent vulnerabilities in third party software entering their products, e.g., by performing security assessments of the third-party components. • Any checks that are carried out as part of this 'on-boarding' process and provide examples of these checks having been carried out. • Documented procedures for dealing with flaws found in third party components that are part of their product. Examples, of support agreements, should be provided to the Auditor as evidence of these relationships. **Expected output** The Auditor shall verify: • That documented procedures concerning the selection and use of third-party components exist, and that there is a method of flaw remediation that can be used for any flaws found in third-party software. • Where applicable the Auditor should check there is ongoing maintenance during the lifetime of the product. This will be documented in the Audit Report.

	Evidence to Security Test Laboratory • The list of third-party components for the Evaluator to consider. • Evidence of any 'on-boarding' checks having been carried out for a sample of these third-party components. • Sample support agreements in place with third-party vendors.

Table 1: Product Development Process

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	Feb 2021	Release 1 approved by GSMA ISAG	Rasma Araby, atsec Paula Burgess, NCC

A.2 Licensing of NESAS Documentation

This GSMA document and its content is:

i. the exclusive property of the GSMA; and
ii. provided “as is“, without any warranties by the GSMA of any kind.

Any official government (or government appointed) body wishing to use this GSMA document or any of its content:

i. for the creation of; or
ii. as referenced in;

its own documentation regarding the same or a similar subject matter, is hereby granted a licence to the copyright in this document.

This grant is subject to and upheld, as long as the above body:

a) informs the GSMA about the use of the GSMA document prior to commencing work on;
b) provides the GSMA with the finalised, i.e. most up-to-date version of; and
c) properly references the GSMA document and any extracts thereof in;

its own documentation.

A.3 Other Information

Type	Description
Document Owner	GSMA, NESASG
Editor / Company	James Moran, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at nesas@gsma.com. Your comments or suggestions & questions are always welcome.