Network Equipment Security Assurance Scheme - Development and Lifecycle Assessment Methodology

Version 2.0

05 February 2021

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

This document forms part of the documentation of the Network Equipment Security Assurance Scheme (NESAS). An overview of the scheme is available in GSMA PRD FS.13 – Network Equipment Security Assurance Scheme - Overview [1].

This document describes the assessment and audit process for Vendor Development and Product Lifecycle Processes.

1.1 Scope

The scope of this document is the NESAS Vendor Development and Product Lifecycle audit and assessment process.

A separate document entitled ‘Audit Guidelines’ describes guidelines, tips and information on how to prepare for and carry out a Vendor Development and Product Lifecycle Process audit. This document may be used by auditors and Equipment Vendors in preparation for an audit.

1.2 Document Maintenance

NESAS has been created and developed under the supervision of GSMA’s Security Assurance Group (SECAG) comprised of representatives from mobile network operators and infrastructure vendors.

This document can be used and referenced by other NESAS derivative schemes with the appropriate adaptation to suit their governance and operational constructs.

The GSMA, as the scheme owner, is responsible for maintaining NESAS and for facilitating periodic reviews involving all relevant stakeholders.

1.3 Vendor Development and Product Lifecycle Assessment

The evaluation of the provisions for security resilience of Vendor Development and Product Lifecycle processes is done as part of the Equipment Vendor assessment process by an appointed Auditor.

Lifecycle management controls are important during normal network product development and improvements, as well as for vulnerability/security flaw remediation.

The assessment of the Vendor Development and Product Lifecycle processes will provide assurance for these aspects in NESAS.

The Vendor Development and Product Lifecycle processes assessment covers an Equipment Vendor's engineering processes and thus is unlikely to apply to a single network product. Assessment results may apply to more than one network product at many different stages in the development lifecycle.

Under NESAS, Equipment Vendors submit their Development and Product Lifecycle processes, or a subset of them, for auditing. As different Vendor Development and Product Lifecycle processes could be utilised within a single organisation, for example due to mergers or acquisitions, participating Equipment Vendors must subject each Development

and Product Lifecycle process used for Network Products to be assessed under NESAS for assessment and audit.

Guidelines are available in Annex E that define the competencies expected of Auditors to conduct NESAS Vendor Development and Product Lifecycle processes audits.

When an Equipment Vendor's processes have been satisfactorily audited, the Audit Report can be used by the Equipment Vendor to inform customers and/or to initiate Network Product Evaluation with an accredited NESAS Security Test Laboratory.

At the beginning of a NESAS evaluation of a Network Product, the Equipment Vendor will have to confirm to the NESAS Security Test Laboratory which audited processes were used and provide evidence of their application. For that purpose, the Equipment Vendor creates the Compliance Declaration that contains all relevant Compliance Evidence.

2 Definitions

2.1 Common Abbreviations

Term	Description
3GPP	The 3rd Generation Partnership Project
CAB	Conformity Assessment Body
CPA	Commercial Product Assurance
FASG	Fraud and Security Group
NCSC	National Cyber Security Centre
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
PDF	Portable Document Format
SCAS	Security Assurance Specification
SECAG	Security Assurance Group
SHA-512	Secure Hash Algorithm-512
TR	3GPP Technical Report
TS	3GPP Technical Standard

2.2 Glossary

Term	Description
Audit	A review and assessment described in FS.15 that is undertaken and completed by an Audit Team against the requirements set out in FS.16.
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 at the Equipment Vendor by the Auditor

Term	Description
Audit Team	Collective group of Auditors, generally to consist of two or more people, that undertake a Vendor Development and Product Lifecycle Processes audit.
Auditing Organisation	Organisation selected by Equipment Vendor to conduct audits of Vendor Development and Product Lifecycle Processes, employs or contracts Auditors.
Audit Summary Report	A subset of the Audit Report created by the Auditor that summarises the key results.
Auditor	Individual that is qualified to perform Vendor Development and Product Lifecycle Processes audits and makes up part of the Audit Team.
Compliance Declaration	A written statement by the Equipment Vendor that confirms it adheres to the previously assessed development and lifecycle processes for the particular Network Product that is provided to a NESAS Security Test Laboratory for evaluation.
Compliance Evidence	Evidence to be provided by the Equipment Vendor to the NESAS Security Test Laboratory, demonstrating that the Equipment Vendor applied its previously internally assessed and independently audited development and lifecycle processes to build the Network Product under evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration.
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	Organisation that develops, maintains and supplies to network operators network equipment that supports functions defined by 3GPP.
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.
Interim Audit	An audit of an Equipment Vendor's Development and Product Lifecycle processes focussed only on security requirements revised or introduced since the Equipment Vendor's last full audit that allows the Equipment Vendor to demonstrate compliance with the new requirements. The report from the audit is treated as an addendum to the Audit Report from the last full audit of the Equipment Vendor.
Interim Audit Report	Document presenting the results of an interim audit conducted at the Equipment Vendor by the Auditor that is published as an addendum to an existing Audit Report.
NESAS Development and Product Lifecycle Requirements	The security requirements defined in this document that Equipment Vendor development and product lifecyle processes must comply with under NESAS and against which Audits are performed
NESAS Security Test Laboratory	An Equipment Vendor owned or third party owned test laboratory that conducts network product evaluations
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 products that all implement a common set of 3GPP defined functionalities.
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	Software is a physically intangible set of instructions, defined in a formal language, written in digital format. It is used by a machine to be interpreted or executed. Software can exist in various formats, such as binary software, which is only machine-readable, and scripts and source code, which is human readable and/or machine readable. Software is used for many purposes. It can be the instruction set of hardware, in which case it is called “firmware”. It can be (part of) an operating system, an application, a library, or anything else that is executed or interpreted by a machine. In this definition, the term is to be understood in its broadest possible sense.
Vulnerability	In SP 800-30 [5], 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 – Overview
[2]	FS.16 -– Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Security Requirements
[3]	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. http://www.ietf.org/rfc/rfc2119.txt
[4]	3GPP TR 33.916, “Security assurance scheme for 3GPP network products for 3GPP network product classes”. V15.0.0 (2018-06) http://www.3gpp.org/DynaReport/33916.htm
[5]	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
[6]	NIST FIPS PUB 180-4 “Secure Hash Standard (SHS)”, August 2015. http://dx.doi.org/10.6028/NIST.FIPS.180-4

2.4 Conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC2119 [3].”

3 Audit Guidelines and Evidence

3.1 Audit Guidelines Document

The way Equipment Vendors implement the NESAS security requirements in their development and product lifecycles might vary from one Equipment Vendor to another, or even for different Network Products by the same Equipment Vendor. Therefore, it is not feasible to precisely specify the evidence an Auditor has to look for when verifying that the requirements are sufficiently fulfilled.

To ensure comparability between NESAS Vendor Development and Product Lifecycle assessments, i.e. between different Equipment Vendors, different Auditors, and over time, the NESAS Auditors will collaborate to create an Audit Guidelines document.

The Audit Guidelines document describes what evidence is considered sufficient for an Auditor to conclude that a process complies with the security requirements. This is provided for each requirement in the NESAS Vendor Development and Product Lifecycle Assessment Requirements document, FS.16 [2]. It also contains information on what Compliance Evidence should be provided to NESAS Security Test Laboratories to validate that an audited Development and Product Lifecycle process was followed.

The Audit Guidelines document is drafted by the Auditors and is maintained by the GSMA. The guidelines defined are indicative only and are likely to evolve throughout the lifetime of NESAS.

3.2 Evidence

3.2.1 Overview - Types of Evidences

NESAS requires Equipment Vendors to be internally assessed and independently audited, and the NESAS Security Test Laboratory to validate that assessed and audited Equipment Vendor processes were used to build the Network Product under evaluation. To enable this, NESAS refers to three types of evidence to support this validation.

- Evidence that the NESAS Development and Product Lifecycle Requirements are sufficiently addressed by an Equipment Vendor’s processes. This is evidence provided by the Equipment Vendor and assessed by the auditor. The basis for the assessment are the requirements in the NESAS Vendor Development and Product Lifecycle Assessment Requirements document, FS.16 [2]. Guidance on what evidence is considered adequate is provided in the Audit Guidelines document. The audit shall confirm that the Equipment Vendor meets the requirements. As a result, the Audit Report, as defined in section 4.1.6, is produced and signed. It summarises what type of evidence the Equipment Vendor has demonstrated.
- Evidence that the Equipment Vendor’s processes were internally assessed and independently audited by an Auditor must be available to the NESAS Security Test Laboratory. The Audit Report, as defined in section 4.1.6, produced by the Auditor serves as such type of evidence. It is provided to the NESAS Security Test Laboratory upon Network Product Evaluation.

- Evidence that the internally assessed and independently audited processes were in fact applied when building a Network Product is provided to the NESAS Security Test Laboratory. This type of evidence is called ‘Compliance Evidence’. Section 0 specifies how this Compliance Evidence is defined and what it is.

Note: 3GPP TR 33.916 [4], clause 7.2.1 defines these types of evidence, which are the basis for NESAS.Compliance Evidence of Application of Assessed Processes

An Equipment Vendor needs to provide a Compliance Declaration for the internally assessed and independently audited processes that were used to develop the Network Product under evaluation to the NESAS Security Test Laboratory. The declaration is accompanied by the Audit Report and contains Compliance Evidence in free form, showing that the internally assessed and independently audited processes were effectively applied during the development of the Network Product.

For the avoidance of doubt, the development process Compliance Declaration must apply to the actual development processes under which the product to be evaluated was developed. Where more than one development process was used, each process should be declared and have been individually internally assessed and audited. It must be specified by the Equipment Vendor which audited processes were used to develop each individual product that is submitted for evaluation.

The NESAS Security Test Laboratory will review the development process Compliance Declaration for the Network Product and evaluate whether the Compliance Evidence provided by the Equipment Vendor is sufficient to prove that the Network Product development followed the audited processes.

The documentation provided by the Equipment Vendor to the Auditor before the start of the audit, as defined in section 4.3.1 contains the type of evidence the Equipment Vendor considers to be sufficient to demonstrate to a NESAS Security Test Laboratory that the security requirements, have been fulfilled in practice for a particular Network Product. It is possible that this documentation will require refinement after feedback from the Auditor during the course of the audit.

The Auditor decides what type of evidence can be considered as suitable Compliance Evidence. The Audit Report, as defined in section 4.1.6, contains details of which Compliance Evidence is deemed to be sufficient for each of the requirements defined in FS.16 [2]. Auditors’ determination in regard to Compliance Evidence is also described in the Audit Guidelines document as discussed in section 3.1.

As Equipment Vendors’ processes might allow for different options on how to implement a particular process, there can also be options for what constitutes the required Compliance Evidence. Compliance Evidence criteria shall be defined as loosely as possible to allow flexibility while concentrating on the actual need for proper Compliance Evidence. This is in order not to trigger any unnecessary re-audits if irrelevant and/or exchangeable details in the process change. Such details could be e.g. tools, names, file locations, etc.

Compliance Evidence will be evaluated by a NESAS Security Test Laboratory later in time, when the audit has finished and the Auditor is no longer involved. To enable the NESAS Security Test Laboratory to determine if Compliance Evidence, provided by the Equipment Vendor, is meaningful and convincing, the Auditor shall explain in the Audit Report, in an appropriate level of detail, what types of Compliance Evidence are expected.

It is not desired that creation of Compliance Evidence becomes an unnecessary burden for the Equipment Vendor. Therefore, creation of required Compliance Evidence should not exceed the extra effort outside of commonly employed industry practices, or significant alteration of existing processes otherwise adequate to fulfil the requirements.

If there are cases where the Auditor finds that, due to the nature of a requirement, no meaningful and suitable evidence has been provided, where appropriate, to prove that the requirement is sufficiently fulfilled nor could it be created or evaluated with reasonable effort, the requirement shall not trigger the need for an Equipment Vendor to create any evidence, or for the NESAS Security Test Laboratory to evaluate any. In the case that it is not possible to provide Compliance Evidence for a particular security requirement, where the absence of such suitable evidence is appropriate and reasonable, the Equipment Vendor must provide a rationale instead, giving reasons why evidence is not available. If this is considered, by the Auditor, to be an issue the Auditor, shall inform the scheme owner about the issue providing detailed information and recommendations. The scheme owner shall consider the issue raised and may fix the requirement in a future NESAS release, or provide additional guidance in the Audit Guidelines, if that is considered necessary in order to minimise the likelihood of the same issue occurring again in the future.

4 Assessment Process

In this section the Development and Product Lifecycle assessment process is described.

Stakeholders in NESAS should be made aware that the procedure of auditing the Equipment Vendor’s development and lifecycle processes is different to how schemes such as TL9000, ISO 9001 & ISO/IEC 27001 operate. For those latter schemes the auditors check both the processes and the implementation of the processes and in addition there are periodic surveillance audits by the auditor to ensure that the Equipment Vendor continues to comply with the accredited process.

For GSMA NESAS, an Equipment Vendor’s processes will be internally assessed and independently audited and then the NESAS Security Test Laboratory determines if the audited processes are implemented for products and their releases evaluated according to the scheme.

The GSMA NESAS assessment process starts with the Equipment Vendor undertaking an internal assessment of its processes and issuing a Conformance Claim. The Conformance Claim, based on a common form template, is signed by an authorised representative of the Equipment Vendor. The signed Conformance Claim is submitted to the GSMA at the time the Equipment Vendor requests a GSMA NESAS audit.

The Conformance Claim template is provided in Annex D.

The fundamental responsibility of the Auditor is to verify, in the course of the NESAS audit, that the documented processes are properly and fully applied to the Vendor Development and Product Lifecycle processes in accordance with the signed conformance claim.

4.1 Set-Up

4.1.1 Assessment Request

When an Equipment Vendor wants its Development and Product Lifecycle Processes audited, the GSMA is informed.

On receipt of the request along with the Conformance Claim, the details are logged and the contact details of the appointed Auditors that will conduct the audit are provided.

To ensure that the audit can be carried out in the requested timescales, the Equipment Vendor should be aware that sufficient notice is required in order to meet desired audit dates.

It always remains the responsibility of the Equipment Vendor to ensure that its NESAS participation status remains current to meet the requirements of any specific contract, customer, or bid. The Equipment Vendors should schedule their audits accordingly.

4.1.2 Confirmation of audit date

After logging the request details, the information is sent to the Auditors chosen by the Equipment Vendor which then contact the Equipment Vendor to agree audit dates.

4.1.3 Contract

The Equipment Vendor seeking an audit enters into an agreement with the chosen Auditor. Then, the Auditor carries out the audit and payment falls due based on the payment terms agreed between the parties.

4.1.4 Confidentiality

Ownership of all information communicated to the Auditor or otherwise gathered by the Auditor during the audit stays with the Equipment Vendor.

4.1.5 Language

The language used in the course of the audit is English.

4.1.6 Audit Report

Throughout the audit the Auditor summarises the results in a report which is structured as shown in Annex B:

- An identifier for the audit, unique within NESAS
- A reference to the NESAS release under which the audit was conducted
- Equipment Vendor defined process identifiers (and list of Development and Product Lifecycle Process(es) audited)
- A date by which the audit has been completed.
- List of Auditor and Equipment Vendor participants

- Audit summary and overall assessment
- Actions required
- Auditors' comments
- Details of products developed in accordance with the audited processes, as known at the time of the audit.
- Details of evaluation and result for each requirement with a list of audit steps performed.
- Details for each requirement which kind of Compliance Evidence is to be considered sufficient by a NESAS Security Test Laboratory.
- A reference to all Equipment Vendor input documentation and material audited, including a hexadecimal representation of the SHA-512 hash over each of them.
- Confirmation that the completed and signed Conformance Claim is present.

4.1.7 Audit Summary Report

The Audit Summary Report, which may be published by the scheme owner, with the agreement of the Equipment Vendor, is a subset of the Audit Report that records summary information as follows:

- An identifier for the audit, unique within NESAS
- A reference to the NESAS release under which the audit was conducted
- Equipment Vendor defined process identifiers
- Result for each NESAS security requirement.
- Details of products developed in accordance with the audited processes, as known at the time of the audit.

Its structure is shown in Annex C.

4.1.8 Validity

An audit applies to the NESAS release applicable at the time of the audit, and to the audited processes in place.

However, in order to maintain a valid and current audited status Equipment Vendors will need to have audits performed, if one or more of the following applies:

- A period of two years has lapsed since the previous audit.
- The Vendor Development Process of the Product Lifecycle Process in scope of NESAS changes.
- A new NESAS major release is issued and the Equipment Vendor wants to comply with that.
- A significant security breach of the Equipment Vendor environment that might reasonably have impacted the audited processes has occurred.

Customer or market requests will ensure that Equipment Vendors initiate the re-audit of their Development and Product Lifecycle Processes in order to demonstrate that their processes are aligned with the latest NESAS release. For renewal audits, Auditors may choose to visit different sites from those previously audited at which the same Development and Product Lifecycle Processes, which are the subject of the audit, are in place.

Whenever the Vendor Development and Product Lifecycle Processes in scope of NESAS change, the Equipment Vendor must inform the GSMA.

4.1.9 Timeline

It is in the interests of all involved parties to keep the overall time for the audit as short as possible. This allows the Equipment Vendor to be audited within a reasonable timeframe and it allows the Auditor to focus on the Equipment Vendor without delays and interruptions.

The entire audit, as outlined in section 4.3, shall be completed within a time frame of at most three months.

The Equipment Vendor must ensure that all required documents, information, and on-site visits can be provided accordingly. The Auditor shall ensure it has sufficient time within the necessary timeframe to perform the audit.

This timeline reflects the maximum lead time and not the actual labour time. The timeline already includes periods where one of the involved entities prepares for the next step and the other entity is inactive.

4.2 Audit Preparation

After audit dates have been agreed, the Auditor and Equipment Vendor will liaise to agree arrangements for the audit and prepare for parts of the audit process as needed.

To avoid misunderstandings on which input needs to be delivered by the Equipment Vendor, the exact versions of the NESAS standard documents (requirements, guidance, etc.) applicable for the audit shall be explicitly agreed between all parties.

The Auditor and Equipment Vendor will mutually agree on suitable technical means to validate the authenticity of submitted information and data encryption. For email communication the use of S/MIME with personal certificates is recommended for all parties.

4.2.1 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. The scope should include:

- the conformance claim signed by the Equipment Vendor
- the exact release of the NESAS documents applicable for the audit,
- the entities that will be involved in the audit (Auditor, Equipment Vendor and potentially any 3rd parties such as contractors that are employed by the Equipment Vendor),
- the processes that will be reviewed during the audit,
- the location that will be included in the audit,
- the business groups/organisations that will be included in the audit.

Details of the items listed above will be provided in the Audit Guidelines document.

4.2.2 Provisional Agenda

A provisional agenda will be agreed at least one week before the audit. A sample agenda is included in Annex A. The sample agenda includes guidance for Equipment Vendors on information that should be prepared and submitted for each element of the audit.

Changes to the agenda may need to be made during the audit itself. Changes will be mutually agreed between the Auditor and the Equipment Vendor.

4.3 Audit Proceedings

The Audit proceeds in order of the subsections given in this section.

As each NESAS audit is process specific, elements of previous audits may not be reused and all audits must be conducted in full.

In the case of Interim Audits, elements of previous audits may only be reused where the scope is restricted to modified or new requirements.

4.3.1 Presentation and Documentation for the Auditor

Before the start of the Audit, the Equipment Vendor provides the Auditor with written documentation regarding its processes, including its signed conformance claim, along with a reasoning of how it believes it complies with the security requirements laid out in FS.16 [2].

At the start of the Audit, the Equipment Vendor and the Auditor meet virtually or in person. During this meeting, the Equipment Vendor provides an overview of the information submitted and additionally supplies its signed conformance claim and descriptions of how it believes it complies with the NESAS security requirements. The Auditor may use the opportunity to indicate if and where further clarification might be needed. Additional documentation should be submitted by the Equipment Vendor within an agreed timeframe.

4.3.2 Documentation Review by the Auditor – First Round

The Auditor evaluates that the processes described in the submitted documentation are sufficient to fulfil the requirements as laid out in FS.16 [2]. This is done according to the timeframe defined in the agreed agenda.

If applicable during the progress of the first round of document audit, the Auditor may indicate to the Equipment Vendor which documentation is still missing and which requirements are not fulfilled by the information provided. The Equipment Vendor may communicate the missing information to the Auditor.

4.3.3 Intermediate Audit Result Meeting

An intermediate audit result meeting is held after the Auditor has evaluated all initially provided documentation, and supplementary information that may have been provided during the first round of the audit.

In this meeting, the Auditor informs the Equipment Vendor which requirements may not be fulfilled according to the information it has available.

The findings in the intermediate version of the Audit Report will classify issues in terms of major or minor issues, or observations. Observations (positive or negative in nature) are merely for information.

It is mutually agreed within which timeframe the missing or modified documentation is handed over from the Equipment Vendor to the Auditor. If requested by the Equipment Vendor, this timeframe must be at least four weeks (28 days) and not more than 8 weeks (56 days).

4.3.4 Documentation Review by the Auditor – Second Round

The Auditor evaluates whether the documentation provided by the Equipment Vendor is sufficient for the Auditor to assess if the Equipment Vendor fulfils the requirements, as laid out in FS.16 [2]. This is done according to the timeframe defined in the agreed agenda.

If applicable during the progress of the second round of document audit, the Auditor may indicate to the Equipment Vendor which documentation is still missing and which requirements are not fulfilled by the information provided.

4.3.5 On-Site Audit

The On-Site Audit described in this section applies to each individual Development and Product Lifecycle process and is not intended to be Network Product specific.

After the documentation has been reviewed and considered complete by the Auditor, the audit continues on-site at the Equipment Vendor’s premises.

The site to be chosen at which the NESAS on-site audit is to be conducted, needs to be an engineering, development, or production site, at which the audited processes are actively applied by the Equipment Vendor.

During the on-site audit, the Auditor assesses:

- If the processes that are documented are actively applied in the day-to-day business of the Equipment Vendor;
- If the Equipment Vendor has the staff, skills, equipment, working practices and resources to follow the processes defined in the documentation;
- If the staff is sufficiently trained on the processes and if the staff understands them.

During the on-site audit, the Equipment Vendor provides evidence to the Auditor that the departments of the Equipment Vendor involved in the processes within the scope of NESAS effectively apply the processes defined in the provided documents.

NESAS expects an on-site audit period of 4 days under average conditions, but sets no maximum value for this time. The precise duration of the audit is to be discussed and agreed between the Equipment Vendor and the Auditor before the on-site audit. The Auditor and/or Equipment Vendor may choose to terminate the process if no progress is being made, with any requirement remaining unfulfilled. The Equipment Vendor shall provide information on which employees are within the scope of the assessment and shall ensure that individuals selected by the Auditor will be available for interview by the Auditor.

It is at the discretion of the Auditor how to conduct the on-site audit. It is recommended to the Auditor to witness day-to-day product development activities and product maintenance activities, including interviews with architects, developers, engineers and other personnel as needed. The Auditor should limit its activities to samples. It is not intended to audit the processes to their full extent.

The preference and expectation is that audits are conducted by Auditors being physically present at the Equipment Vendor's nominated site at which product development activity is undertaken. However, it is recognised that exceptional circumstances, such as health pandemics, natural disasters, etc., could arise that restrict the ability of auditors to travel to Equipment Vendor sites. Subject to;

i. the feasibility of conducting remote audits;
ii. the ability of Auditors to assess if the Equipment Vendor has satisfied each of the NESAS requirements referred to above;

audits may be performed remotely with prior consultation with, and approval from, GSMA.It should be indicated in the Audit Report and Audit Summary Report where it is decided that an audit is performed remotely.

In seeking approval for a remote audit the Equipment Vendor must provide the following details to the satisfaction of the GSMA;

- Why the request for a remote audit is deemed necessary
- What obstacles to travel exist
- What alternatives to a remote audit were considered
- Description of the arrangements to be put in place to support a remote audit
- Statement from the chosen Auditors that a remote audit is feasible
- Estimation of when in the future an on-site visit will be possible

4.3.6 Presentation of the Results and Completion of the Audit Report

At the end of the audit, the Auditor presents its findings to the Equipment Vendor. The Auditor also creates the Audit Report that contains all the results and reasoning. This report is structured as defined in section 4.1.6. Guidance on Compliance Evidence for the NESAS Security Test Laboratory is to be included as defined in section 3.2.

The Auditor reaches agreement with the Equipment Vendor that the draft Audit Report reflects the observations and results of the audit. Following agreement on the Audit Report, which is signed by the Equipment Vendor and the Auditor, the Auditor produces the Audit Summary Report, which is derived from the Audit Report, and provides both to the Equipment Vendor and the GSMA.

The preferred file format is PDF.

4.4 Publication of Audit Summary Report

On receipt of an Audit Report and Audit Summary Report, the reports will be reviewed to ensure the audit was undertaken in full compliance with the defined process.

Permission will be sought from the Equipment Vendor to publish the Audit Summary Report on the relevant NESAS web site, while reserving the right to publish or remove an Audit Summary Report as circumstances may require.

Publication of the Audit Summary Report indicates the Equipment Vendor has undergone a Vendor Development and Product Lifecycle processes audit that resulted in full compliance with all security requirements defined in GSMA PRD FS.16 [2]. The received Audit Summary Report may be published to maintain a central list of all successfully audited Equipment Vendors.

The GSMA maintains publication of all the received Audit Summary Reports it is permitted to publish.

The relevant web site will show for each Audit Summary Report, the NESAS Release, the validity status, a link to the Audit Summary Report for download, and a link to a list of Network Products that were produced under the assessed Vendor Development and Product Lifecycle processes. Validity is defined in section 4.1.8. As soon as the Equipment Vendor requests an expired Audit Summary Report to be removed from a web site, the site owner erases the corresponding Audit Report from its records.

For other NESAS schemes it is for the scheme owner to decide how, if at all, to publicise Audit Reports and results.

4.5 Completion of the Audit

The Equipment Vendor, who has undergone a Vendor Development and Product Lifecycle processes assessment, can only be considered fully compliant, if all requirements defined in FS.16 [2] are deemed by the Auditor to have been met by the Equipment Vendor. If the Equipment Vendor is found to be non-compliant with any one of the security requirements, the overall audit result considers the Equipment Vendor to be non-compliant.

Should the Equipment Vendor not meet all the requirements defined in FS.16 [2], the Equipment Vendor should consult the Auditor to determine the improvements required to be introduced by the Equipment Vendor to meet the requirements.

If an audit has been conducted and it is determined during the audit that the Equipment Vendor does not meet all the requirements defined in FS.16 [2], the Equipment Vendor and the Auditor can agree on conducting an additional re-audit, after the Equipment Vendor has introduced the required improvements. This is only possible if the full audit and the subsequent re-audit do not exceed the maximum total duration of an audit, as defined in section 4.1.9.

4.6 Interim Audits

NESAS is a living scheme so it is to be expected that security requirements will be added or changed. These significant changes could impact an Equipment Vendor that has already

completed a NESAS audit against the previous version of the security requirements insofar as its Audit Report and related material will reference an out of date version of the security requirements. In order to allow the Equipment Vendor to maintain and demonstrate compliance to the current security requirements it may be possible for it to undertake an audit that is focussed only on the changes included in the security requirements update rather than having to undergo a full audit. Such a focussed audit is called an Interim Audit and it allows the Equipment Vendor to keep its compliance to NESAS security requirements current, where the vendor's processes have not changed substantially, until the next full audit of its development and product lifecycle processes falls due.

Interim Audits shall be deemed allowable when the NESAS security requirements have been updated and they result in a major revision to FS.16 [2] but the changes are considered small in terms of number and/or impact. When changes are made to the NESAS security requirements consideration needs to be given to the following;

- The impact and effect of the change(s) on the vendor's processes
- The impact the change(s) may have on other security requirements
- How compliance with the changed requirement(s) is to be assessed
- If the changed requirements can be audited independently of all other requirements or if dependencies exist that require other requirements to be audited

These factors will dictate how the changed requirements can be subjected to an Interim Audit and how the audit will work in practical terms. As a guide, an Interim Audit can be deemed appropriate where the changed security requirements are less than five in number. However, this is just a guide and other factors may be taken into account when deciding on whether an Interim Audit is adequate or if a full audit is required to assess compliance to the security requirement changes under consideration. Such a determination will be made by the scheme owner.

Where an Interim Audit is conducted it does not extend the validity period of an already completed Audit Report, which remains at two years from date of completion of the original full audit. If a vendor does not have a valid Audit Report for a previous release of NESAS then a full audit is required.

The scope of activities to be undertaken for the preparation and performance of an Interim Audit shall be the same as per the previous full audit and as recorded in the original Audit Report i.e. An Interim Audit is not a means to extend the scope of a full audit to different vendor processes.

4.6.1Interim Audit process

In general, the Interim Audit process should mirror the steps required for a full NESAS audit.

The process for applying for an Interim Audit is similar to a full audit as described in 4.1.1. A vendor completes an application, undertakes an internal assessment of the new or changed process requirements, produces a conformance claim highlighting the new or changed process requirements to which it now claims compliance, etc.

As per a full audit, the Interim Audit date scheduling, agreement of contracts with the auditor, confidentiality clauses and language remain the same.

Other aspects of the Interim Audit such as the agenda, preparation, material to be provided as evidence and proceedings remain the same but will only be focussed on the specific security requirements that are the subject of the Interim Audit.

The same rules around compliance apply for Interim Audits in that all process requirements must be met in order to be deemed fully compliant.

The Interim Audit will conclude with the production and agreement of a report that will be an addendum to the original Audit Report. The addendum will refer to the original Audit Report identifier and it will record similar details as those found in a full Audit Report but just for the security requirements that were the subject of the interim audit. An addendum will also be produced for the existing Audit Summary Report recording similar details confined to the newly audited security requirements.

Annex A Sample Audit Agenda

Schedule Day 1

Time	Topic / Requirement	Participants
8:30-10:30	**Introduction and opening meeting** Presentation of the teams, Approval / changes to schedule, Identification of the scope, Comments on the documentation review (provided in advance)	All
10:30-17:30	**Design** [REQ-DES-01] Security by Design [REQ-GEN-01] Version Control System [REQ-GEN-02] Change Tracking [REQ-GEN-06] Sourcing of 3rd Party Components	

Schedule Day 2

Time	Requirement	Participants
09:00-17:00	**Implementation and Testing** [REQ-IMP-01] Source Code Review [REQ-IMP-02] Source Code Governance [REQ-TES-01] Software Security Testing	
17:00-17:30	Closing meeting and summary of the day	All

Schedule Day 3

Time	Requirement	Participants
9:00-17:00	**Building and Release** [REQ-BUI-01] Automated Build Process [REQ-BUI-02] Build Environment Control [REQ-REL-01] Software Integrity Protection [REQ-REL-02] Unique Software Release Identifier	

Schedule Day 4

Time	Requirement	Participants
09:00-15:00	**Release and Operation** [REQ-REL-03] Documentation Accuracy [REQ-REL-04] Security Documentation [REQ-OPE-01] Security Point of Contact [REQ-OPE-02] Vulnerability Information Management [REQ-OPE-03] Vulnerability Remedy Process [REQ-OPE-04] Vulnerability Remedy Independence [REQ-OPE-05] Security Fix Communication [REQ-GEN-03] Staff Education [REQ-GEN-04] Information Security Management System REQGEN-05] Continual Improvement	
15:00-17:00	Internal review and analysis	–
17:00-18:00	Closing meeting and summary of the audit	All

Annex B Audit Report Structure

B.1 First Page:

- Headline: NESAS Audit Reportor NESAS Interim Audit Report, as appropriate
- An identifier for the audit, unique to NESAS
- A reference to the NESAS release under which the audit was conducted
- Identifier and date of the original Audit Report (in the case of an Interim Report)
- Equipment Vendor defined process identifier
- Details of products developed in accordance with the audited processes, as known at the time of the audit, and a master list will be maintained by the scheme owner. Product details need to provide sufficient information to allow a customer to determine if a specific product is covered by the audited process.
- Name of the Equipment Vendor
- Date of the original audit and of the Interim Audit (if applicable)
- Auditor participants
- Names and roles of Equipment Vendor personnel involved in the audit (these details can be removed or redacted in copies provided to stakeholders other than the scheme owner)

B.2 Following Pages:

- Security requirements audited (in the case of an Interim Audit)
- Audit summary and overall assessment
- Actions required (what to do and maybe also how)
- Auditors' comments (how conduct of audit went)

B.3 Appendix A

- Details of evaluation and result for each requirement with the list requirement audit steps performed (column 5) and guidance on which kind of Compliance Evidence is to be considered as sufficient by a NESAS Security Test Laboratory (column 6).

REQ-#	Requirement	Result	Auditor remarks	Audit steps performed	Compliance Evidence to be provided for Network Product and Evidence Evaluation
…					
REQ-GEN-01	Version Control System	C / NC	C: no comment C+: a robust VC system is there and access control to individuals is maintained strictly and timely	Test X: access rights of developers to VC system *Test artefacts: test02-X.zip (hash: XXXXX)*	

REQ-#	Requirement	Result	Auditor remarks	Audit steps performed	Compliance Evidence to be provided for Network Product and Evidence Evaluation
			C-: version control is not applied in all cases NC: not documented; only some docs are controlled in there; processes are not clear; no individual user accounts	Test Y: comparison between files and resources used in the build process and present in the VC system *Test artefacts: test02-Y.zip (hash: XXXXX)* Synthesis of REQ-02 testing and evaluation *artefacts: test02-synthesis.pdf (hash: XXXXX)*	
REQ-GEN-02	Change Tracking	C / NC			
REQ-GEN-03	Staff Education	C / NC	- comment		
REQ-GEN-04	Information Security Management	C / NC	+ comment		
REQ-GEN-05	Continual Improvement				
REQ-GEN-06	Sourcing of 3rd Party Components				
…					

A reference to all Equipment Vendor input documentation and material audited, including a hexadecimal representation of the SHA-512 hash over each of them.

Confirmation that the completed and signed Conformance Claim is made available to the auditor.

B.4 Appendix B

Signature page to include authorised signatures on behalf of the Auditor and the Equipment Vendor indicating acceptance of the Audit Report.

Annex C Audit Summary Report Structure

C.1 First Page:

- Headline: NESAS Audit Report or NESAS Interim Audit Report, as appropriate
- Audit identifier, unique to NESAS
- Reference to applicable NESAS release
- Identifier and date of the original Audit Report (in the case of an Interim Report)
- Equipment Vendor defined process identifiers
- Details of products developed in accordance with the audited processes, as known at the time of the audit, and a master list will be maintained by the scheme owner
- Name of the Equipment Vendor
- Date of the original audit and of the Interim Audit (if applicable)
- Auditor participants

C.2 Following Pages:

- Result for each NESAS security requirement audited.

REQ-#	Requirement	Result
REQ-DES-01	Security by Design	C / NC
REQ-IMP-01	Source Code Review	C / NC
REQ-IMP-02	Source Code Governance	C / NC
REQ-BUI-01	Automated Build Process	C / NC
REQ-BUI-02	Build Environment Control	C / NC
REQ-TES-01	Security Testing	C / NC
REQ-REL-01	Software Integrity Protection	C / NC
…		

Annex D Conformance Claim

Network Equipment Security Assurance Scheme Conformance Claim

Vendor Name:	
NESAS Contact Name:	
NESAS Contact Email and Tel No.:	
Vendor Assessed Process Identifier:	
NESAS Release Under which Assessment is Done:	
FS.16 Security Requirement(s) Subjected to Interim Audit (if applicable)	
Products Developed in Accordance with Assessed Process:	

This statement confirms the named vendor has undertaken an assessment of its level of compliance with, and conformance, to the NESAS security requirements defined in NESAS Document FS.16 for the vendor development and product lifecycle management processes and the Conformance Claim represents an honestly held view that is provided in good faith.

Date of Claim _____

Signatory Job Title _____

Authorised Signature _____

Compliance Assessment against NESAS Requirements

Req#	Requirement	Compliance C/NC
REQ-DES-01	Security by Design	
REQ-IMP-01	Source Code Review	
REQ-IMP-02	Source Code Governance	
REQ-BUI-01	Automated Build Process	
REQ-BUI-02	Build Environment Control	
REQ-TES-01	Security Testing	
REQ-REL-01	Software Integrity Protection	
REQ-REL-02	Unique Software Release Identifier	
REQ-REL-03	Documentation Accuracy	
REQ-REL-04	Security Documentation	
REQ-OPE-01	Security Point of Contact	
REQ-OPE-02	Vulnerability Information Management	
REQ-OPE-03	Vulnerability Remedy Process	
REQ-OPE-04	Vulnerability Remedy Independence	
REQ-OPE-05	Security Fix Communication	
REQ-GEN-01	Version Control System	
REQ-GEN-02	Change Tracking	
REQ-GEN-03	Staff Education	
REQ-GEN-04	Information Security Management	
REQ-GEN-05	Continual Improvement	
REQ-GEN-06	Sourcing of 3rd Party Components	

Annex E NESAS Auditor Competency Requirements and Guidelines

E.1 Introduction

It is required that NESAS Vendor Development and Product Lifecycle processes audits are performed by GSMA or Certification Body appointed Auditors. The NESAS Auditors must demonstrate their competencies to undertake NESAS Vendor Development and Product Lifecycle processes audits against the requirements defined in FS.16 -– Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Security Requirements [2].

E.1.1. Purpose

This annex is primarily intended to guide organisations that;

I. Apply to be NESAS Auditors under the NESAS rules or

II. Act as the body appointing NESAS auditors.

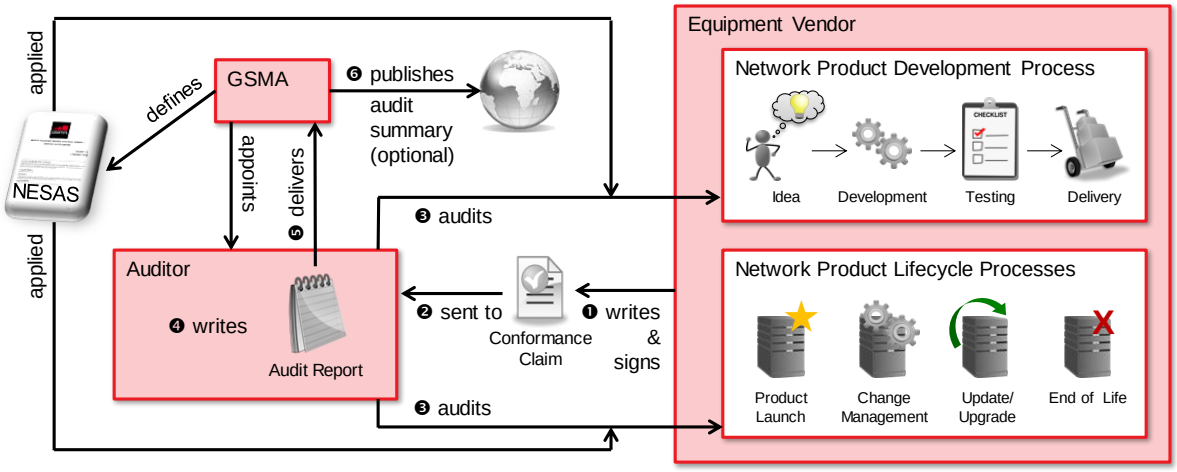
E.2 Overview

The process for appointing NESAS Auditors is designed to ensure that the candidate Auditors have sufficiently demonstrated that they are technically competent in the specific field of performing NESAS Vendor Development and Product Lifecycle processes audits.

The NESAS process includes the need for candidate Auditors to demonstrate that they have the ability to undertake NESAS Vendor Development and Product Lifecycle processes audits against the requirements defined in FS.16 Network Equipment Security Assurance Scheme - Vendor Development and Product Lifecycle Security Requirements [2].

E.3 Auditor Competency

The requirements and guidelines provided below are intended to be helpful to candidate Auditors and also to those “subject matter experts” appointing auditors to ensure that high quality NESAS Vendor Development and Product Lifecycle processes audits take place as described in FS.13 ‘NESAS Overview’ [1]) and as depicted below.



Auditors need to demonstrate relevant knowledge of the tasks they are assigned. The Auditors, working within the definition of NESAS, are required to:

- Understand the principles and methods used in NESAS,
- Understand the relationship between the 3GPP Security Assurance Specification documents and other NESAS documents used by the scheme,
- Demonstrate an understanding of the overall audit methodology as described in this document,
- Be able to independently document the audit results of their work objectively, precisely, correctly, unambiguously, and at the level of detail required by NESAS. The NESAS Audit Report must ensure that the level of detail allows for reproducibility of the audit results,
- Ensure that the NESAS Vendor Development and Product Lifecycle processes Audit Report indicates the type of evidence that should be provided to the NESAS Product Evaluators to facilitate the 'evidence evaluation' task,
- The Auditors are expected to be knowledgeable to a high degree with concepts and industry best practises behind product development and product lifecycle processes especially related to ICT and telecommunications equipment.
- The Auditors should demonstrate their understanding of the requirements in FS.16 -– Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Security Requirements [2]. including:
    - How NESAS process requirements are defined,
    - How to interpret the NESAS process requirements in conjunction with the vendor development and product lifecycle processes to determine the evidence that needs to be provided during an audit,
    - How to identify evidence and document it in the Audit Report that will indicate to the NESAS Product Evaluator that the audited process has been used to develop a product,

It is the GSMA NESAS Auditor's responsibility to determine the competencies needed by the individual auditors for each vendor audit and to appoint auditors accordingly.

Although not especially specified in NESAS, it is expected that:

- The Auditors have a team leader who is highly experienced to supervise, oversee and monitor the activities of less experienced Auditors.
- The Auditors are expected to provide proposals to the scheme owners to enhance the current NESAS methodology, standard, guidelines and/or other supporting documentation.

Guidance for identifying relevant knowledge, experience, skills or educational qualifications for individual auditors includes:

- Several years (2-3+) experience performing ICT quality or security auditing tasks
- Several years (2-3+) experience working on ICT product development projects in a Quality Management System role
- External auditing qualifications (such as ISO9000, TL9000 or ISO27001 auditors).

Annex F Document Management

F.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Aug 2019	Release 1 approved by SECAG	GSMA TG	James Moran / GSMA
1.1	Aug 2020	Minor clarifications added	GSMA FASG	James Moran / GSMA
2.0	Feb 2021	Audit participants and software definitions updated Unused terms removed from definitions Compliance Declaration object and definition added Conformance Claim signature requirement added Document updated to apply more generically to GSMA NESAS Clarification added that requirements are not defined in Guidelines Document Term 'successful' audit changed to 'fully compliant' Provision made for situations in which Compliance Evidence may not be available Removed references to GSMA dispute resolution and NESAS Oversight Board Conformance Claim template added Auditor competency requirements and guidelines added Interim audits provided for and defined Re-mapping of templates to reflect revised security requirements	GSMA FASG	James Moran / GSMA

F.2 Document and NESAS Release Mapping History

Document Version	Applicable NESAS Release
1.0	NESAS 1.0
1.1	NESAS 1.1
2.0	NESAS 2.0

F.3 Other Information

Type	Description
Document Owner	GSMA SECAG
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.