Network Equipment Security Assurance Scheme – Assessment Methodology for Vendor Development and Product Lifecycle Processes

Version 3.0

20 February 2025

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Contents

Licensing Statement

Foreword

This Technical Specification was produced by the GSM Association.

The contents of the present document are subject to continuing work within the GSMA NESAS Group and can change following formal GSMA approval. When the NESAS Group modify the contents of the present document, it will be re-released by the GSMA with an identifying change of release date and an increase in version number as follows:

Version x.y.

where:

x the first digit is incremented for all major changes

y the second digit is incremented for all changes of corrections, technical enhancements, updates, etc.

Modal verbs terminology

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

"**shall**" and "**shall not**" are confined to the context of normative provisions.

"**must**" and "**must not**" are not used as substitutes for "**shall**" and "**shall not**".

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

"**may not**" is ambiguous and is not used in normative elements.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "**can**" and "**cannot**" are not substitutes for "**may**" and "**need not**".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

Introduction

The present document forms part of the documentation of the Network Equipment Security Assurance Scheme (NESAS), which is described in the NESAS Framework document GSMA PRD FS.13 [2].

The present document describes the assessment and audit process for Vendor Development and Product Lifecycle Processes. The NESAS Audit process provides confidence and trust in an Audit, performed by an independent third party NESAS Auditing Organisation pertaining to the Equipment Vendor's compliance with the security requirements defined in GSMA PRD FS.16 [4]. The results are recorded in an Audit Report and published in an Audit Summary Report.

NESAS was originally created by GSMA and responsibility for its maintenance and development of the NESAS specifications rests with the NESAS Group, which comprises representatives from mobile telecom network operators, infrastructure and equipment vendors, security auditors and test laboratories. The NESAS Group is an Industry Specification Issuing Group, and as such, it is bound to GSMA PRD AA.35 [1] governance.

The NESAS Group is responsible for maintaining the NESAS specifications and for facilitating periodic reviews involving all relevant stakeholders.

The Scheme Owner using NESAS specifications can add additional documentation and will be responsible for development and maintenance of its own documents.

1 Scope

The present document sets out the NESAS Vendor Development and Product Lifecycle audit and assessment process.

A separate document, PRD FS.46 - NESAS Audit Guidelines [5] describes guidelines, tips and information on how to prepare for and perform a Vendor Development and Product Lifecycle Process audit. The present document may be used by Auditors and Equipment Vendors in preparation for an Audit.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, GSMA cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] GSMA PRD AA.35: “Procedures for Industry Specifications”

[2] GSMA PRD FS.13: “Network Equipment Security Assurance Scheme – Framework”

[3] GSMA PRD FS.14: “Network Equipment Security Assurance Scheme – Requirements for NESAS Auditing Organisations, Security Test Laboratories, and Associated Personnel”

[4] GSMA PRD FS.16: “Network Equipment Security Assurance Scheme – Security Requirements for Vendor Development and Product Lifecycle Processes”

[5] GSMA PRD FS.46: “Network Equipment Security Assurance Scheme – Audit Guidelines”

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, GSMA cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ISO 9001 2015: “Quality management systems – Requirements”

[i.2] ISO/IEC 27001 2022: “Information security, cybersecurity and privacy protection – Information security management systems – Requirements”

[i.3] NIST FIPS PUB 180-4 2015: “Secure Hash Standard (SHS)”, http://dx.doi.org/10.6028/NIST.FIPS.180-4

[i.4] NIST SP 800-30 Rev. 1 2012: “Guide for Conducting Risk Assessments”, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[i.5] TL 9000: “Quality for Excellence for Suppliers of Telecommunications Forum”

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Assessment Evidence: Evidence to be provided by the Equipment Vendor to the NESAS Security Test Laboratory, demonstrating that the Equipment Vendor's processes were internally assessed and independently audited by an Auditor. The Audit Report serves as Assessment Evidence.

Audit: A review and assessment that is performed and completed by an Audit Team against the NESAS Development and Product Lifecycle Security Requirements following the NESAS assessment methodology.

Audit Evidence: Evidence to be provided by the Equipment Vendor to the Audit Team in the course of the Audit, demonstrating that the NESAS Development and Product Lifecycle Security Requirements are sufficiently addressed by an Equipment Vendor's processes.

Audit Guidelines: Document giving guidance to the Audit Team and Equipment Vendor on how to interpret the requirements.

Audit Report: Document presenting the results of the Audit performed at the Equipment Vendor by the Audit Team.

Audit Team: Collective group of Auditors, generally to consist of two or more people, that perform a Vendor Development and Product Lifecycle Processes Audit.

Audit Summary Report: A subset of the Audit Report created by the Audit Team that summarises the key results.

Auditor: Individual that performs Vendor Development and Product Lifecycle Processes Audits and makes up part of the Audit Team.

Authorisation: The procedures defined by the Scheme Owner of verifying and selecting Auditing Organisations and Security Test Laboratories which meet the requirements set out for NESAS Auditing Organisations and NESAS Security Test Laboratories.

Compliance Declaration: A written statement by the Equipment Vendor that confirms it adheres to the previously assessed Vendor Development and Product 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 Vendor Development and Product Lifecycle Processes to build the 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 Vendor Development and Product Lifecycle Processes that are to be assessed.

Equipment Vendor: Organisation that develops, maintains and supplies network equipment that supports functions defined by 3GPP or another SDO.

Evidence Evaluation: Activity in NESAS of evaluating if the Product under Evaluation (PuE) was developed in accordance with the previously assessed Vendor Development and Product Lifecycle Processes of the Equipment Vendor.

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 Audit that allows the Equipment Vendor to demonstrate compliance with the new requirements. The report from the Interim Audit is treated as an addendum to the Audit Report from the last Audit of the Equipment Vendor.

Interim Audit Report: Document presenting the results of an Interim Audit performed at the Equipment Vendor by the Audit Team that is published as an addendum to an existing Audit Report.

NESAS Auditing Organisation: Organisation that engages or contracts qualified Auditors and has Authorisation to perform Vendor Development and Product Lifecycle Processes Audits.

NESAS Development and Product Lifecycle Security Requirements: The security requirements that Vendor Development and Product Lifecycle Processes comply with under NESAS and against which Audits are performed.

NESAS Group: The Industry Specification Issuing Group of the GSMA that is tasked with the overall implementation, governance, maintenance and further development of NESAS specifications.

NESAS Security Test Laboratory: A test laboratory that is authorised to perform Network Product Evaluations and Evidence Evaluations under NESAS.

Network Product: Network Equipment developed, maintained and supplied by an Equipment Vendor, consisting of one or more Network Function(s).

Network Product Class: A class of products that implements a common set of functionalities.

Product under Evaluation: The Network Product for which an evaluation is sought by the Equipment Vendor.

Release: Version of a Network Product being made available for deployment.

Scheme Owner: Organisation or authority responsible for developing, maintaining or operating a specific security assurance or certification scheme that uses the NESAS specifications.

Security Assurance Specification: Specification containing security requirements and test cases for a defined Network Function or a group of Network Functions. It is created and maintained by a Standards Development Organisation (SDO).

Software: Physically intangible set of instructions, defined in a formal language, written in digital format.

Subject Matter Expert: Individual that is experienced in all NESAS related technical details, such as mobile networks, network and equipment security, and testing of network equipment and network services.

Vendor Development and Product Lifecycle Processes: The stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery and the stages to end of life including maintenance and update releases during their lifetime.

Vulnerability: 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.

NOTE: The term “Vulnerability” is as defined by NIST in NIST SP 800-30 [i.4].

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	The 3rd Generation Partnership Project
FASG	Fraud and Security Group
ISAG	Industry Specification Approval Group
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
PDF	Portable Document Format
PRD	Permanent Reference Document
PuE	Product under Evaluation
SCAS	Security Assurance Specification
SDO	Standards Development Organisation
SHA-512	Secure Hash Algorithm-512
TR	Technical Report

TS Technical Specification

4 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 NESAS Auditing Organisation.

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 Vendor 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 shall subject each Vendor Development and Product Lifecycle process used for Network Products to be assessed under NESAS for assessment and audit.

GSMA PRD FS.14 [3] defines requirements on NESAS Auditing Organisations to ensure that they perform meaningful, comprehensible, repeatable and complete assessments of the Vendor Development and Product Lifecycle Processes.

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 authorised NESAS Security Test Laboratory.

At the beginning of a NESAS evaluation of a Network Product, the Equipment Vendor shall 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.

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

5 Audit Guidelines and Evidence

5.1 Audit Guidelines Document

The way Equipment Vendors implement the NESAS Development and Product Lifecycle 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.

The Auditors have collaborated to create an Audit Guidelines document to ensure comparability between Audits, i.e. between different Equipment Vendors, different Auditors, and over time,.

The Audit Guidelines document GSMA PRD FS.46 [5] 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, GSMA PRD FS.16 [4]. 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 GSMA PRD FS.46 [5] is maintained by the NESAS Group. The guidelines defined are indicative only and are likely to evolve throughout the lifetime of NESAS.

5.2 Evidence

5.2.1 Overview - Types of Evidence

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.

Audit Evidence is evidence to be provided by the Equipment Vendor to the Audit Team in the course of the Audit, demonstrating that the NESAS Development and Product Lifecycle Security Requirements are sufficiently addressed by an Equipment Vendor's processes. The basis for the assessment is the requirements in the NESAS Vendor Development and Product Lifecycle Assessment Requirements document, GSMA PRD FS.16 [4]. Guidance on what evidence is considered adequate is provided in the Audit Guidelines document GSMA PRD FS.46 [5]. The Audit shall confirm that the Equipment Vendor meets the requirements. As a result, the Audit Report, as defined in clause 6.2.4, is produced and signed. It summarises what category of evidence the Equipment Vendor has demonstrated. NESAS distinguishes two categories of Audit Evidence:

- **Audit Evidence Category 1**: company level or product line level product development/lifecycle processes related evidence that demonstrates the Equipment Vendor has implemented controls to meet the NESAS Development and Product Lifecycle Security requirements.
- **Audit Evidence Category 2**: evidence which demonstrates the implementation of the security measures described in Audit Evidence Category 1.

Assessment Evidence is evidence to be provided by the Equipment Vendor to the NESAS Security Test Laboratory, demonstrating that the Equipment Vendor's processes were internally assessed and independently audited by an Auditor. The Audit Report serves as Assessment Evidence. The Audit Report, as defined in clause 6.2.4, is provided to the NESAS Security Test Laboratory upon Network Product Evaluation.

Compliance Evidence is 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 Vendor Development and Product Lifecycle Processes to build the Product under Evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration. Clause 5.2.2 specifies how Compliance Evidence is defined and what it is.

5.2.2 Compliance Evidence

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 Compliance Declaration shall 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 shall 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 clause 6.4.1 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 may require refinement after feedback from the Auditor during the course of the Audit.

The Auditor decides what type of evidence to be considered as suitable Compliance Evidence. The Audit Report, as defined in clause 6.2.4, contains details of which Compliance Evidence is deemed to be sufficient for each of the requirements defined in GSMA PRD FS.16 [4]. Auditors' determination in regard to Compliance Evidence is also described in the Audit Guidelines document GSMA PRD FS.46 [5].

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 necessary 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.

Creation of Compliance Evidence should not become an unnecessary burden for the Equipment Vendor. Therefore, creation of necessary 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 shall 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 version of the present document (GSMA PRD FS.15), or provide additional guidance in the Audit Guidelines document GSMA PRD FS.46 [5], if that is considered necessary in order to minimise the likelihood of the same issue occurring again in the future.

6 Assessment Process

6.1 General

In this clause 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 TL 9000, 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 audited process.

For NESAS, an Equipment Vendor's processes shall 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 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 Scheme Owner at the time the Equipment Vendor requests an Audit.

The Conformance Claim template is provided in Annex D.

The fundamental responsibility of the Auditor is to verify, in the course of the 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. A NESAS Auditing Organisation can be owned by any entity, but the Vendor Development and Product Lifecycle Processes assessment shall be performed by a NESAS Auditing Organisation that is impartial and independent of the Equipment Vendor that undergo a Vendor Development and Product Lifecycle Processes Audit.

6.2 Set-Up

6.2.1 Initiation of the Audit

When an Equipment Vendor wants its Vendor Development and Product Lifecycle Processes audited, the Scheme Owner is informed and the signed Conformance Claim is provided. The Scheme Owner refers the Equipment Vendor

to authorised NESAS Auditing Organisations. The Scheme Owner decides the selection process of the NESAS Auditing Organisations.

The selected NESAS Auditing Organisation and the Equipment Vendor agree on the Audit schedule, coordinate a kick-off meeting and manage subsequent exchanges of information.

6.2.2 Confidentiality

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

6.2.3 Language

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

6.2.4 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 versions of the NESAS documents under which the Audit was performed (i.e. reference to version of the present document and GSMA PRD FS.16 [4])
- Equipment Vendor defined process identifiers (and list of Vendor Lifecycle Process(es) audited)
- A date by which the Audit has been completed
- Audit Team and Equipment Vendor participants
- Audit summary and overall assessment
- Actions necessary
- 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 [i.3] hash over each of them.
- Confirmation that the completed and signed Conformance Claim is present.

6.2.5 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 versions of the NESAS documents under which the Audit was performed (i.e. reference to version of the present document and GSMA PRD FS.16 [4]).
- 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.

6.2.6 Validity

An Audit applies to the version of the NESAS documents 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 shall inform the Scheme Owner, and perform a full re-audit, 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 significant security breach of the Equipment Vendor environment that might reasonably have impacted the audited processes has occurred.

If there has been new or changed security requirements in GSMA PRD FS.16 [4], the current Audit Report continues to be valid for its two year validity period.

The Equipment Vendor has a choice:

- to perform an Interim Audit (refer to clause 6.7) based on the new security requirements subject to impact analysis performed by the Scheme Owner and noted in GSMA PRD FS.16 [4].
- or wait until the Audit Report expires and then do a full re-audit.

The Equipment Vendor also has the option of requesting a full Audit at any point during the two year validity period.

NOTE: The response time by a vendor to request a new Audit shall take into account factors such as the lead time for requesting and preparing for Audits or the impact of the new or changed GSMA PRD FS.16 [4] security requirements on the vendors development processes.

Customer or market requests shall ensure that Equipment Vendors initiate the re-audit of their Vendor 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 Vendor Development and Product Lifecycle Processes, which are the subject of the Audit, are in place.

6.2.7 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 clause 6.4, shall be completed within a time frame of at most three months.

The Equipment Vendor shall ensure that all necessary documents, information, and on-site visits are 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.

6.3 Audit Preparation

6.3.1 Initial arrangements

After audit dates have been agreed, the Audit Team and Equipment Vendor shall liaise to make 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 shall mutually agree on suitable technical means to validate the authenticity of submitted information and data encryption.

6.3.2 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. The scope should include:

- the Conformance Claim signed by the Equipment Vendor
- the exact version of the NESAS documents applicable for the Audit,
- the entities to 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 to be reviewed during the Audit,
- the location of the Audit,
- the business groups/organisations to be included in the Audit.

As each Audit is process specific, elements of previous Audits may not be reused and all Audits shall be performed 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.

Details of the items listed above are provided in the Audit Guidelines document GSMA PRD FS.46 [5].

6.3.3 Provisional Agenda

A provisional agenda shall 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 shall be mutually agreed between the Auditor and the Equipment Vendor.

6.4 Audit Proceedings

6.4.1 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 GSMA PRD FS.16 [4].

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.

6.4.2 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 GSMA PRD FS.16 [4]. 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.

6.4.3 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 shall 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 shall be at least four weeks (28 days) and not more than 8 weeks (56 days).

6.4.4 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 GSMA PRD FS.16 [4]. 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.

6.4.5 On-site Audit

The on-site Audit applies to each individual Vendor Development and Product Lifecycle process and does not intend 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 on-site Audit is to be performed, needs to be an engineering, development, or production site, at which the audited processes are actively applied by the Equipment Vendor.

When multiple sites exist, the Equipment Vendor and Auditor should discuss and agree to select at least one site at which engineering, development, or production of the Network Equipment within the scope of the assessment takes place.

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 are available for interview by the Auditor.

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

6.4.6 Remote Audit

The preference and expectation is that Audits are performed by Auditors being physically present at the Equipment Vendor's nominated site at which product development activity is performed (on-site Audit). However, Scheme Owners can define circumstances, which qualify Audits to be performed remotely using information and communication technologies (ICT). In this context, the term remote Audit refers to each of the following scenarios:

- Full remote Audit: None of the Auditors are on-site for the entire duration of the Audit.
- Partially remote Audit: All Auditors are on-site for part of the Audit and off-site for other parts.
- Hybrid Audit: At least one, but not all, Auditors are on-site for the entire duration of the Audit.

It is also recognised that not all Equipment Vendor participants can be present on-site; therefore, also some interviews with participants from different locations may be performed using ICT, both in on-site and remote Audits.

The Scheme Owner shall approve each remote Audit on a case-by-case basis. When seeking approval for a remote Audit, the Equipment Vendor shall consult with the Scheme Owner in advance and provide at least the following information, as agreed with the Audit Team, to the satisfaction of the Scheme Owner:

- The specific circumstances that justify a remote Audit and the specific reasons why a remote Audit is considered more effective or necessary by the Equipment Vendor. The alternatives to a remote Audit, which were considered, including reasons that may make a remote Audit more effective than being physically present at the Equipment Vendor's nominated site for the entire duration of the Audit;
- Description of the arrangements to be put in place to support a remote Audit;

Statement from the Audit Team that a remote Audit is feasible and the Audit Team considers it appropriate. The Scheme Owner shall then decide whether to approve the remote Audit, and inform the Equipment Vendor of the decision.

For each remote Audit, the Audit Team shall ensure:

1. The feasibility of performing a remote Audit;
2. The ability of the Auditors to assess all Vendor Development and Product Lifecycle Processes appropriately.

The Audit Team shall indicate in the Audit Report and Audit Summary Report when an Audit was performed remotely, and which Auditors and Equipment Vendor participants were present on-site or participated remotely.

6.4.7 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 clause 6.2.4. Guidance on Compliance Evidence for the NESAS Security Test Laboratory is to be included as defined in clause 5.2.2.

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 Scheme Owner.

The preferred file format is PDF.

6.4.8 Record Retention

NESAS requires that the defined period for which reports and relevant records shall be retained by the NESAS Auditing Organisation is at least ten (10) years after the Audit Report has been issued by the Auditor.

6.5 Publication of Audit Summary Report

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

Permission shall be sought from the Equipment Vendor to publish the Audit Summary Report, while reserving the right to publish or remove an Audit Summary Report as circumstances may require.

6.6 Completion of the Audit

The Equipment Vendor, who has performed a Vendor Development and Product Lifecycle Processes assessment, shall only be considered fully compliant, if all requirements defined in GSMA PRD FS.16 [4] 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 GSMA PRD FS.16 [4], the Equipment Vendor should consult the Auditor to determine the improvements necessary to be introduced by the Equipment Vendor to meet the requirements.

If an Audit has been performed and it is determined during the Audit that the Equipment Vendor does not meet all the requirements defined in GSMA PRD FS.16 [4], the Equipment Vendor and the Auditor may agree on performing an additional re-audit, after the Equipment Vendor has introduced the necessary 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 clause 6.2.7.

6.7 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 an 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 perform 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 GSMA PRD FS.16 [4] 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 dictate how the changed requirements are subject to an Interim Audit and how the Audit works in practical terms. As a guide, an Interim Audit is deemed appropriate where the changed security requirements are less than five in number. However, this is just a guide and other factors should be taken into account when deciding on whether an Interim Audit is adequate or if a full Audit is necessary to assess compliance to the security requirement changes under consideration. Such a determination shall be made by the Scheme Owner.

When there are changes to the NESAS requirements in GSMA PRD FS.16 [4] an impact analysis shall be carried out by the Scheme Owner and a statement shall be added to GSMA PRD FS.16 [4] to clarify if Interim Audits may be allowed for the latest revision of GSMA PRD FS.16 [4].

Where an Interim Audit is performed 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 against a previous major version of the NESAS document GSMA PRD FS.16 [4] then a full Audit is necessary.

The scope of activities to be performed 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 shall not extend the scope of a full Audit to different vendor processes.

6.8 Interim Audit process

In general, the Interim Audit process should mirror the steps necessary for a full Audit.

The process for applying for an Interim Audit is similar to a full audit as described in 6.2. A vendor completes an application, performs 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 NESAS Auditing Organisation, confidentiality and language agreements 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 shall 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 shall be met in order to be deemed fully compliant.

The Interim Audit shall be provided as an addendum to the original Audit Report. The addendum shall refer to the original Audit Report identifier and it shall 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 shall be produced for the existing Audit Summary Report recording similar details confined to the newly audited security requirements.

6.9 Impact of changes to the Vendor Development and Product Lifecycle Assessment Methodology

When there are changes to the present document an impact analysis shall be carried out by the Scheme Owner and a statement will be published to indicate if the change requires a new Audit or an Interim Audit in order to demonstrate compliance to the current version of the present document.

Annex A (informative): 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 and lifecycle management 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 [REQ-GEN-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 (normative): Audit Report Structure

B.1 First Page:

- Headline: NESAS Audit Report or NESAS Interim Audit Report, as appropriate
- An identifier for the Audit, assigned by the Scheme Owner
- A reference to the NESAS document versions under which the Audit was performed (i.e. reference to versions of GSMA PRD FS.15 (the present document) and GSMA PRD FS.16 [4])
- 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 shall 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)
- Audit team participants
- Names and roles of Equipment Vendor personnel involved in the Audit (these details may 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 necessary (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 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 X: access rights of developers to VC system *Test artefacts: test02-X.zip (hash: XXXXX)* 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 Classification and Handling	C / NC	+ comment		
REQ-GEN-05	Continual Improvement				
…					

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 Audit Team.

B.4 Appendix B

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

Annex C (normative): Audit Summary Report Structure

C.1 First Page:

- Headline: NESAS Audit Report or NESAS Interim Audit Report, as appropriate
- Audit identifier, assigned by the Scheme Owner
- Reference to applicable NESAS document versions under which the Audit was performed (i.e. reference to versions of GSMA PRD FS.15 (the present document) and GSMA PRD FS.16 [4])
- 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 shall be maintained by the Scheme Owner
- Name of the Equipment Vendor
- Date of the original audit and of the Interim Audit (if applicable)
- Audit team 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 Process Management	C / NC
REQ-TES-01	Security Testing	C / NC
REQ-REL-01	Software Integrity Protection	C / NC
…		

Annex D (normative): 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 Document Versions Under which Assessment is Done:	
GSMA PRD 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 performed an assessment of its level of compliance with, and conformance, to the NESAS security requirements defined in NESAS Document GSMA PRD FS.16 for the Vendor Development and Product Lifecycle 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 Process Management	
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 Classification and Handling	
REQ-GEN-05	Continual Improvement	
REQ-GEN-06	Sourcing and Lifecycle Management of 3rd Party Components	

History

Version	Date	Brief Description of Change
1.0	Aug 2019	Release 1 approved by NESASG
1.1	Aug 2020	Minor clarifications added
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 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 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
2.1	Jan 2022	The changes to FS.15 remove references to NESAS releases and add provisions pertaining to the licensing of NESAS documentation. An update of the Annexes reflects changes to FS.16: change of title of REQ-GEN-04. Definitions of different types of evidence used in NESAS have been added and references to NESAS Audit Guidelines have also been added.
2.2	Oct 2022	Changes made to correct editorials and reflect revised contractual arrangements.
2.3	Sep 2023	Definitions updated to align with other scheme documents and updates made pertaining to NESAS Group. Additional changes include the following: References to defunct TR 33.916 removed Clarification added that product evaluations must be performed by independent test labs Record retention requirement addedThis document update is not material to the scheme and does not require vendors to undergo an audit to maintain the validity of their NESAS status.
3.0	Feb 2025	Guidance on site selection for on-site audits. Text added on independence of the NESAS Auditing Organisations. Clarity of descriptions and consistent use of terms improved. Definitions updated. Separation of NESAS specifications from scheme run by GSMA. Details of GSMA NESAS have moved to new FS.51.