Network Equipment Security Assurance Scheme - Development and Lifecycle Assessment Methodology

Version 1.1

13 August 2020

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 GSMA 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.

The GSMA 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.

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.

2 Definitions

2.1 Common Abbreviations

Term	Description
3GPP	The 3rd Generation Partnership Project
CPA	Commercial Product Assurance
DRC	Dispute Resolution Committee
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 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
Audit Summary Report	A subset of the Audit Report created by the Auditor that summarises the key results.
Auditor	Organisation appointed and contracted by GSMA and selected by Equipment Vendor to conduct audits of Vendor Development and Product Lifecycle processes.
Conformance Claim	A written statement by the Equipment Vendor that confirms it meets the NESAS security requirements for the Development and Product Lifecycle Processes that are to be assessed.
Firmware	Binaries and associated data supporting low-level hardware functionality installed on non-volatile memory like ROM and EPROM usually not

Term	Description
	mountable to a running operating system's file system. Firmware is a specific type of Software, therefore in this document the term "Software" includes Firmware.
NESAS Oversight Board	The body overseeing NESAS, run by the GSMA. It is responsible for the governance of the Vendor Development and Product Lifecycle Process assessments and quality assurance of NESAS.
NESAS Dispute Resolution Process	The process used by the NESAS DRC in Section 3.6 of FS.13 – Network Equipment Security Assurance Scheme – Overview [1].
NESAS Dispute Resolution Committee (DRC)	A panel established to adjudicate on disputes pursuant to Section 3.6 of FS.13 – Network Equipment Security Assurance Scheme – Overview [1].
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
Network Product Class	In the context of NESAS, the class of products that all implement a common set of 3GPP defined functionalities.
Network Product Development Process	The stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery.
Network Product Lifecycle Processes	The stages through which developed Network Products journey to end of life including maintenance and update releases during their lifetime.
Release	Version of a Network Product being made available for deployment. The first Release of a Network Product is assumed to be a new Network Product.
Software	Binaries and associated data forming the basis of a Network Product's operating system and functionality. Software is commonly stored on hard disks or flash memory mass storage devices. In this document, the term "Software" includes "Firmware".
Vulnerability	In SP 800-30 [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

Ref	Title
[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, FS.16 [2]. It also contains information on what evidence should be provided to NESAS Security Test Laboratories to validate that an audited Development and Product Lifecycle process was followed.

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

Should any involved party see the need to challenge any decision of an Auditor it may refer the matter to the NESAS Dispute Resolution Process. Similarly, should any party see the need to challenge the Audit Guidelines, it may refer the matter to the NESAS Oversight Board.

3.2 Evidence

3.2.1 Overview - Types of Evidences

TR 33.916 [4], section 7.2.1, requires the NESAS Security Test Laboratory to validate that assessed and audited Equipment Vendor processes were used to build the Network Product under test and refers to two categories of evidence to support this validation.

- Evidence that the processes were self-assessed and independently audited by an Auditor must be available to the NESAS Security Test Laboratory. This is the Audit Report as defined in section 4.1.6.
- Evidence that the self-assessed and independently audited processes were in fact implemented. This evidence is provided by the Equipment Vendor to the NESAS Security Test Laboratory. Section 3.2.2 specifies how this evidence is defined and what it is.

Although not explicitly defined in TR 33.916 [4], there is also the following type of evidence to consider, which is explicitly distinguished from other evidence.

- Evidence that the NESAS Development and Product Lifecycle requirements are sufficiently addressed by an Equipment Vendor's processes. This is evidence evaluated by the Auditor. This evidence shall be defined by the Audit Guidelines document.

3.2.2 Evidence for Application of Assessed Processes

An Equipment Vendor needs to provide a compliance declaration for the self-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 evidence in free form, showing that the self-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 self-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 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.

Auditor's requirements in regard to evidence which needs to be provided to NESAS Security Test Laboratories are also in scope of the Audit Guidelines document as discussed in section 3.1.

The Audit Report, as defined in section 4.1.6 contains details of which evidence is deemed to be sufficient for each of the requirements defined in FS.16 [2].

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 evidence. Evidence requirements shall be defined as loosely as possible to allow flexibility while concentrating on the actual need for proper 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.

It is not desired that creation of evidence becomes an unnecessary burden for the Equipment Vendor. Therefore, creation of required 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 evidence has been provided 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. The Auditor shall inform the NESAS Oversight Board about the issue providing detailed information and recommendations. The NESAS Oversight Board shall fix the requirement in a future NESAS release, 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 NESAS, an Equipment Vendor's processes will be self-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 a self-assessment by the Equipment Vendor, after which the Equipment Vendor will issue a conformance claim. The conformance claim, based on a template provided by the GSMA, is submitted to the GSMA at the time the

Equipment Vendor requests an audit. The conformance claim is structured as shown 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 GSMA logs the details and provides the contact details of the GSMA appointed Auditors from which the Equipment Vendor can choose one to conduct its audit.

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 Auditor chosen by the Equipment Vendor which then contacts 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 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.

4.1.7 Audit Summary Report

The Audit Summary Report, which may be published by GSMA, subject to agreement by 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 and Product Lifecycle Processes in scope of NESAS change.
- 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.

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 engineering and production departments of the Equipment Vendor 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 conduced 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

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.

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, the Audit Report 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, GSMA staff will review the reports to ensure the audit was undertaken in full compliance with the defined process.

The GSMA will seek permission from the Equipment Vendor that it can publish the Audit Summary Report on the 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 successful Vendor Development and Product Lifecycle processes audit. The GSMA only publishes the received Audit Summary Report to maintain a central list of all successfully audited Equipment Vendors.

Vendor Development and Product Lifecycle process assessments can only be considered successful 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 NESAS security requirements the overall audit result considers the Equipment Vendor to be non-compliant.

The GSMA neither assesses, reviews nor interprets the received Audit Report and Audit Summary Report in any way. The GSMA keeps the Audit Report confidential in case a dispute is filed by an involved stakeholder which could lead to the invocation of the NESAS Dispute Resolution Process.

The GSMA maintains publication of all the received Audit Summary Reports it is permitted to publish. The GSMA 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 **Error! Reference source not found.**. As soon as the Equipment Vendor requests the GSMA to remove an expired Audit Summary Report from the GSMA Web site, the GSMA erases the corresponding Audit Report from its records.

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 delta audit, after the Equipment Vendor has introduced the required improvements. This is only possible if the full audit and the subsequent delta audit do not exceed the maximum total duration of an audit, as defined in section 4.1.9.

5 NESAS Dispute Resolution Process

The NESAS Dispute Resolution Process is described in section 3.6 of FS.13 [1].

5.1 Potential Dispute Scenarios

The following table illustrates a number of possible dispute scenarios that could arise within the Vendor Development and Product Lifecycle element of NESAS that involve a variety of parties. The table merely captures example scenarios and is not intended to be exhaustive.

	Operator	Vendor	Audit Team	NESAS OB
Operator		NP or development and lifecycle process security inconsistency	Vendor assessment undertaken by auditor and challenged by operator	Operator believes SCAS is inadequate or challenges auditor assessment
Vendor	NP or development and lifecycle process security inconsistency		Auditor assessment disputed by vendor	SCAS documentation ambiguous or not fit for purpose
Auditor	Vendor assessment undertaken by auditor and challenged by operator	Auditor assessment disputed by vendor		Auditor unhappy with document quality and NESAS with audit work
NESAS Oversight Board (OB)	Operator believes SCAS is inadequate or challenges auditor assessment	SCAS documentation ambiguous or not fit for purpose	Auditor unhappy with document quality and NESAS with audit work	

Table 1 Example Dispute Scenarios

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 and Implementation** [REQ-01] Security by Design [REQ-02] Version Control System [REQ-03] Change Tracking	

Schedule Day 2

Time	Requirement	Participants
09:00-17:00	**Design and Implementation (cont.)** [REQ-04] Source Code Review [REQ-05] Software Security Testing [REQ-06] Staff Education	
17:00-17:30	Closing meeting and summary of the day	All

Schedule Day 3

Time	Requirement	Participants
9:00-17:00	**Build and Delivery** [REQ-10] Automated Build Tool [REQ-11] Build Environment Control [REQ-13] Software Integrity Protection [REQ-14] Unique Software Release Identifier	

Schedule Day 4

Time	Requirement	Participants
09:00-15:00	**Maintenance** [REQ-07] Vulnerability Remedy Process [REQ-08] Vulnerability Remedy Independence [REQ-09] Information Security Management System [REQ-12] Vulnerability Information Management [REQ-15] Security Fix Communication [REQ-16] Documentation Accuracy [REQ-17] Security Point of Contact [REQ-18] Source Code Governance [REQ-19] Continuous Improvement [REQ-20] Security Documentation	
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: GSM Association NESAS Audit Report
- An identifier for the audit, unique within NESAS
- A reference to the NESAS release under which the audit was conducted
- 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 GSMA[1]
- Name of the Equipment Vendor
- Date of the audit
- 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 GSMA)

B.2 Following Pages:

- 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 evidence is to be considered as sufficient by a NESAS Security Test Laboratory (column 6).

REQ-#	Requirement	Result	Auditor remarks	Audit steps performed	Evidence to be provided for Network Product Evaluation
REQ-01	Security by Design	C / NC			
REQ-02	Version Control	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	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	

[1] Product details need to provide sufficient information to allow a customer to determine if a specific product is covered by the audited process.

REQ-#	Requirement	Result	Auditor remarks	Audit steps performed	Evidence to be provided for Network Product Evaluation
			NC: not documented; only some docs are controlled in there; processes are not clear; no individual user accounts	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-03	Change Tracking	C / NC			
REQ-04	Source Code Review	C / NC	- comment		
REQ-05	Software Security Testing	C / NC	+ comment		
REQ-06	Staff Education				
REQ-07	Vulnerability Remedy Process				
…					

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

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: GSM Association NESAS Audit Report
- Audit identifier, unique to NESAS
- Reference to applicable NESAS release
- 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 GSMA
- Name of the Equipment Vendor
- Date of the audit
- Auditor participants

C.2 Following Pages:

- Result for each NESAS security requirement.

REQ-#	Requirement	Result
REQ-01	Security by Design	C / NC
REQ-02	Version Control	C / NC
REQ-03	Change Tracking	C / NC
REQ-04	Source Code Review	C / NC
REQ-05	Software Security Testing	C / NC
REQ-06	Staff Education	
REQ-07	Vulnerability Remedy Process	
…		

Annex D Conformance Claim

D.1 First Page:

- Headline: GSM Association NESAS Conformance Claim
- Name of the Equipment Vendor
- Equipment Vendor defined process identifier
- Reference to applicable NESAS release
- Details of products developed in accordance with the assessed process
- Date of the claim
- Signatory

D.2 Following Pages:

- Assessment of level of compliance with each NESAS security requirement.

REQ-#	Requirement	Assessment
REQ-01	Security by Design	C / NC
REQ-02	Version Control	C / NC
REQ-03	Change Tracking	C / NC
REQ-04	Source Code Review	C / NC
REQ-05	Software Security Testing	C / NC
REQ-06	Staff Education	C / NC
…		

Annex E Document Management

E.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

E.2 Document and NESAS Release Mapping History

Document Version	Applicable NESAS Release
1.0	NESAS 1.0
1.1	NESAS 1.1

E.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.