Federal Office
for Information Security

Requirements for the selection of NESAS auditors

NESAS-Auditoren (courtesy translation)

Version 1.3 dated 2024-10-01

Federal Office for Information Security (BSI)
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 800 2741 000
Email: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Change history

Version	*Date*	*Name/Org. unit*	*Description*
1.0	2022-07-01	Division SZ 33	First edition
1.1	2022-12-14	Division SZ 33	Revision: • Concretisation of the selection process for NESAS auditors. • Addition of kick-off meetings at the beginning of the audits • Adjustments resulting from the use of the NESAS certificate and other referenced documents • Editorial changes and clarification of procedural steps
1.2	2023-11-01	Division SZ 33	Revision: • Editorial adaptions and corrections
1.3	2024-10-01	Division S 26	Revision: • Removal of fig. 1: Document index (certification and licensing programme) in Chapter 1.1 and the relevant amendment in the Chapter. • Additions to the data exchange in section 4.2.2 • Editorial adaptions and corrections

Table 1: Change history

Contents

1 Introduction

This document describes the requirements for selecting NESAS auditors.

NESAS auditors may be any natural person over the age of 18. Auditors are generally experts in audits of product development and lifecycle processes in the field of information and communication technologies.

1.1 Aim and integration of the scheme

This document contains detailed information as a supplement to the NESAS documents issued by the BSI, in particular [AIS N1]. It specifically identifies the requirements that auditors must take into account to comply with the regulations governing the scheme. Reference is made to forms or other resources, for example at the appropriate places in the document.

The document “Verzeichnisse” (Indexes) [Verzeichnisse] provides an index of all the essential sources of help and information (list of references) and contains a list of keywords and abbreviations (glossary).

2 NESAS auditors

The “Network Equipment Security Assurance Scheme” (NESAS) is a framework for assuring and improving security in mobile networks. NESAS is thus creating a basis for evaluating defined security properties of IT products that serve to provide a mobile network infrastructure, referred to below as network products.

To provide evidence of conformity, the corresponding network products must be developed by the vendor in accordance with pre-audited development and lifecycle processes. Subsequently, the application of the audited processes and the inclusion of product specific security requirements is assessed during the evaluation by the evaluation facility.

The task of the NESAS auditors is to carry out product development and product lifecycle audits as part of a NESAS certification.

2.1 Requirements for a NESAS auditor

2.1.1 The personal characteristics of NESAS auditors

Below is a list of the personal characteristics of NESAS auditors that are required to carry out the activities under the scheme, but which can only be evaluated to a limited extent as “soft skills” in the context of a selection process.

2.1.1.1 Management skills

- Structured and goal-oriented thinking and actions
- Leadership in a crisis situation
- Focus on solutions
- Flexibility and organisational abilities
- Assertiveness
- Organisational skills

2.1.1.2 Communication skills

- Conflict management
- Persuasion skills
- Expertise in moderation and auditing techniques
- Comprehensive and factual reporting

2.1.1.3 Didactic skills

- Clear and comprehensible statement of the facts and circumstances
- Objective presentation of results
- Clear listing of options for action

2.1.1.4 Methodological competence

- Analysis and evaluation methods
- Ability to motivate others

- Focus on the essentials
- Analytical skills
- Development of solution strategies

2.1.1.5 Social skills

- Resilience in stressful situations
- Open-mindedness and friendliness
- Quick to grasp facts
- Sound judgement
- Perseverance
- Calmness
- Self-confidence
- Psychological sensitivity/empathy
- Objectivity, particularly in sensitive matters
- Constructive handling of criticism and praise
- Responsible conduct
- Open-mindedness and friendliness
- Approachability
- Credibility
- Ability to work in a team
- Ability to operate as a partnership

2.1.1.6 Independence

- Independence from the audited parties and the evaluation facility/test laboratory
- Impartiality and immunity to influence
- Total confidentiality
- Incorruptibility
- Ability to argue based on objective evidence

2.1.2 Admission requirements for the selection of NESAS auditors

Auditors must be employed by an accredited body or be managed by such body as external auditors.

2.1.2.1 Academic qualifications

The applicant must have completed a technical/scientific degree or equivalent technical training in which they acquired the fundamental knowledge and skills for their subsequent activity as a NESAS auditor. This includes, for example, training or a degree in IT and/or communication technologies.

2.1.2.2 Professional experience

Auditors must have at least two years of practical experience in development projects in the area of IT and communication technologies.

2.1.2.3 Practical experience

Auditors must have at least two years of practical experience in audits in the area of IT and communication technologies, focusing on the following:

- Quality audits
- Security audits
- Product development or product lifecycle audits

2.1.3 Requirement in professional competence

2.1.3.1 Formal requirements

For NESAS auditors, the following formal requirements are assumed:

- Qualification as an auditor (ISO 9001, TL 9000 or ISO/IEC 27001)
- At least three audits in the role of lead auditor
- Ability to communicate (C1 level) complex technical issues for German administrative procedures in the official language
- Ability to communicate (C1 level) complex technical issues and manage audits in English
- Willingness and ability to gain an understanding of the NESAS documents published by the BSI and to implement their requirements

2.1.3.2 Advanced specialist knowledge

The following specialist knowledge in NESAS certification is required:

- Understanding of the principles and methods of NESAS
- Extensive knowledge of the concepts and “best practices” regarding product development and product lifecycle in IT and communication technologies
- Knowledge of the security requirements to be inspected in the audit within NESAS

3 Selection process for NESAS auditors

The NESAS auditors are selected by the certification body via a mini competition. As described in document [AIS N1], this mini competition is organised by the BSI in collaboration with the Procurement Office of the Federal Ministry of the Interior (BeschA). The certification body is responsible for the expert assessment of the audit services submitted.

4 Special framework conditions

4.1 Duties of the NESAS auditor

The persons conducting the audits ensure that they will

- Treat all activities in strict confidence, and will observe and comply with the applicable requirements
- Comply with the NESAS lines of communication
- Report longer absence to the certifier
- Provides content-related feedback within 48 hours (on weekdays)
- Conduct professional coordination with their co-auditor
- Essentially carry out commissioned audits within three months

4.2 Cooperation between auditors and the certification body.

4.2.1 Assignment of an audit to an audit team

The selection of an audit team by the certification body of the BSI is regulated in document [AIS N1]. A new person selected for the audit will be elected if the persons selected for the audit fail to respond to the acceptance of an audit in a timely manner.

Upon acceptance of the audit, the certification body will inform the vendor of the selected auditors. In justified cases, the vendor may express an objection against a person assigned to the audit. The certification body will examine the objection, agree on how to proceed, and then announce the decision to the vendor and the person selected for the audit. If the objection is upheld, a new person selected for the audit will be appointed.

If there are no more objections in the process, the final decision will be communicated to the auditors and to the vendor.

Typical audit procedure:

Tasks of the auditor	*Resources*	*Tasks of the vendor*	*Tasks of the certification body*
• Confirm the audit • Reject the audit if applicable	• -	• Reject the audit if applicable	• Select the audit team
• -	• -	• -	• Notify the vendor and the auditor of the audit team

Table 2: Tasks in the preparation phase

4.2.2 Audit process

The evaluation and certification concept is based on close cooperation between the parties involved, the applicant, the assigned auditors and the assigned certifier in the certification body. Communication is generally in text form (e.g. documents, email, formal letter) or in the ongoing process by telephone or via web-based conference systems (e.g. telephone conferences regarding the status of the audit, clarification of minor technical issues that are not critical in terms of confidentiality) or in joint meetings. Emails exchanged between the vendor, audit team and the certification body must be encrypted using OpenPGP at all times. The public keys required for this purpose must be exchanged in advance of the procedure.

All the parties must adhere to the schedule agreed at the start of the process. The audit team leader is responsible for ensuring the timely conduct of the audit (within three months from the day of the audit kick-off meeting). If it is apparent that the process will be delayed or is already delayed, the other parties must be notified to then agree on an updated process schedule. The updated schedule must be approved by the certification body.

The exchange of documents within the audit takes place via the data exchange platform specified by the certification body (currently bscw.bund.de). Data that is provided on the data exchange platform shall be individually end-to-end encrypted for each recipient using OpenPGP. The certification body shall be included as a recipient for each data exchange by using the valid process key. Additional requests for documents to respond to queries will also be sent to the auditors via this channel.

The applicant must clarify and rectify any supplementary requirements/errors/inconsistencies in the vendor's verifications identified during the audit.

The certifier may subject the vendor's documents to a random, internal review and may attend the meetings between the applicant/vendor and the auditors to gain a better understanding of the auditors' evaluation statement and, if necessary, highlight any aspects that require clarification. The scope of the random inspection shall be at the discretion of the certification body. The certifier may also participate in on-site audits with the audit team and to gain an insight into the implementation of the processes described.

Typical audit procedure:

Tasks of the auditor	*Resources*	*Tasks of the vendor*	*Tasks of the certification body*
• The lead auditor contacts the vendor	• -	• -	• -
• Planning, invitation and implementation of the audit kick-off meeting	• -	• Participation in the audit kick-off meeting	• For acknowledgement • Optional: participation in the kick-off meeting
• Planning/coordination of the audit process with the vendor	• AIS N1	• Coordination of the audit process with the audit team/lead auditor	• -
• Notification of the audit process to the certification body: • Scheduled duration of the audit • Scheduled date of the completion of the first document audit • Scheduled date of the completion of the document audit • Scheduled duration of the on-site audit • Proposed site of the audit • Scheduled date of submission of the audit report	• -	• -	• For acknowledgement

Tasks of the auditor	*Resources*	*Tasks of the vendor*	*Tasks of the certification body*
• Receipt of the relevant documents provided	• AIS N1, data exchange platform provided by the certification body	• Submission of the necessary documents to the audit team and the certification body	• Submission of a folder with the appropriate authorisations and receipt of the relevant documents.
• Document audit round 1	• AIS N1	• -	• -
• The results of the first document audit are sent to the vendor for quality assurance and comments	• -	• Quality assurance and comments on the result of round 1 of the document audit	• -
• Decision on acceptance of the comments and their potential incorporation	• -	• The comments on the results are sent to the auditor for a decision on the comments and their incorporation. The certification body receives the comments for acknowledgement.	• Acknowledgement of the comments and necessary follow-up submissions by the vendor.
• Discussion on the results from round 1 of the document audit	• -	• Discussion on the results from round 1 of the document audit	• -
• -	• Data exchange platform provided by the certification body	• Fulfilment of the subsequent requirements arising from the discussion on the results	• -
• Document audit round 2	• AIS N1	• -	• -
• The results of the second document audit are sent to the vendor for quality assurance and comments	• -	• Quality assurance and comments on the result of round 2 of the document audit	• -
• Decision on acceptance of the comments and their potential incorporation and definition of priorities for the on-site audit	• -	• The comments on the results are sent to the auditor for a decision on the comments and their incorporation. The certification body receives the comments for acknowledgement.	• Acknowledgement of the comments
• Update on the date of the on-site audit • Notification of further instructions for subsequent steps	• -	• Coordination of the audit process with the audit team/lead auditor	• -

Tasks of the auditor	*Resources*	*Tasks of the vendor*	*Tasks of the certification body*
• Notification to the certification body of the precise date for the on-site audit	• -	• -	• For acknowledgement
• On-site audit	• AIS N1	• Provision of the necessary resources and data for the audit (e.g. personnel, time, workspace for auditors)	• Optional: • participation in the on-site audit

Table 3: Tasks in the audit process

4.2.3 Completion of the audit

In this phase, the audit report and all the annexes are created, and the audit summary is prepared for publication.

By signing the audit report, the auditors guarantees the completeness, correctness and technical suitability of the audited processes.

Typical audit procedure:

Tasks of the auditor	*Resources*	*Tasks of the vendor*	*Tasks of the certification body*
• Creation of the audit report and all the relevant annexes	• AIS N1	• -	• -
• Submission of the audit report to the vendor for quality assurance and comments	• -	• Quality assurance and comments on the audit report	• -
• Submission of the audit report with comments to the certification body for acknowledgement	• -	• -	• Acknowledgement of the comments
• Incorporation of the comments at the vendor's discretion, taking into account the referenced documents	• -	• -	• -
• Submission of the audit report to the certification body • Incorporation of the comments from the certification body where applicable	• -	• -	• Comments on the audit report • Acceptance of the audit report and notification to the audit team
• Finalisation of the audit report • Preparation of the audit summary	• AIS N1	• -	• -
• The audit report, annexes and audit summary are sent to the vendor and the certification body	• -	• Acknowledgement and confirmation of receipt	• Acknowledgement and confirmation of receipt
• Costs incurred by the auditor are sent to the certification body	• -	• -	• Review of the plausibility of costs

Table 4: Tasks upon completion of the audit

5 References and glossary [Verzeichnisse] (Indexes)

The document “Verzeichnisse” [Verzeichnisse] (Indexes) is a reference work for interested persons and those involved in certification and licensing procedures and provides an overview of all the necessary requirements, sources and resources with a glossary and list of abbreviations.

The lists with respect to requirements, sources and resources shall be understood as a master list and include information about current source references for all the requirements and documents.