Bundesamt
für Sicherheit in der
Informationstechnik

Orientation guide to documentation of compliance according to Section 8a (3) BSIG

Version 1.1
of 21/08/2020

Version history

Date	Version	Author	Remarks
15/05/2019	1.0	BSI	• Final agreement in BSI, creation of document accessibility
03/08/2020	1.1	BSI	• Harmonisation of the glossary and designations • Additions to newly registered systems • Additions to self-declaration • Presentation and adaptation of the audit topics; explanation of information on the audit process • Requirements for presenting the scope • Notes on the network structure plan • Assessment of maturity level of the ISMS and BCMS • List of deficiencies (the list of deficiencies should classify deficiencies by topic and severity)
21/08/2020	1.1	BSI	• Incorporation of comments from TAK AS

All job titles are to be understood in a gender-neutral way and are equally available for use for female, male and other gender identities.

Federal Office for Information Security

P.O. Box 20 03 63
53133 Bonn
Phone: +49 22899 9582-0

E-mail: kritische.infrastrukturen@bsi.bund.de

De-Mail: de-mail@bsi-bund.de-mail.de

Internet: https://www.bsi.bund.de

Table of contents

1 Overview

1.1 Introduction

A critical infrastructure within the meaning of the BSI Act (BSIG) and the BSI Regulation on the Determination of Critical Infrastructures (BSI-KritisV, BSI KRITIS Regulation) is operated by anyone who meets defined qualitative and quantitative criteria. Operators of critical infrastructures (KRITIS operators) must, in accordance with Section 8a (1) of the BSIG, provide the BSI with documentation in an appropriate manner of their precautions to avoid disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes which are crucial for the operability of the critical infrastructures they operate.

All operators of critical infrastructures covered by the BSI KRITIS Regulation are required to provide documentation, with the exception of those mentioned in Section 8d (2) BSIG.

KRITIS operators must submit compliance documents to the BSI for each infrastructure or system subject to documentation requirements. These shall include both general information on the nature and extent of the audits carried out and a list of the security deficiencies detected.

According to Section 8a (3) BSIG "[...] the BSI may also request the submission of the documentation on which the review was based. In the event of security deficiencies, in consultation with the competent federal regulatory authority or after consultation with the otherwise competent regulatory authority as necessary, the BSI may request that the security deficiencies be remedied." For issues that are not fully clarified, the BSI can also obtain its own impression of the KRITIS operator's security precautions through its own on-site audit in accordance with Section 8a (4) BSIG.

1.2 Objective of the orientation guide

The purpose of this document is to give guidance to KRITIS operators and auditing bodies on what is meant by "*in an appropriate manner"* in Section 8a (3) BSIG in relation to an audit and how the legal requirements under Section 8a (3) BSIG can be met. It describes the requirements for the participants as well as their tasks and responsibilities and provides a framework for appropriate documentation of compliance. It explains the procedure for the submission of documentation, the formal aspects to be observed and the due dates to be met.

This document provides answers to the following questions:

- What are the possible approaches for KRITIS operators when fulfilling the obligation to provide documentation according to Section 8a (3) BSIG? What information should be provided and to whom? (see Section 2)
- What are the tasks of the auditing bodies? What are appropriate auditing bodies? (see Section 3)
- What are the tasks of the audit team and what competencies does it require? (see Section 4)

- How should the audit be performed (audit basis, subject areas, methods, results)? (see Section 5)
- How are compliance documents submitted and what due dates must be observed (see Section 6)?

1.3 Definition of terms[1]

The orientation guide differentiates between the terms ***audit***, ***audit report, compliance documents*** and ***documentation of compliance***.

In this document, the term ***audit*** refers to "security audits, audits or certifications" according to Section 8a (3) BSIG. Audits are carried out by an auditing body with the help of an audit team and the results are presented to the KRITIS operator.

The ***audit report*** is the document containing the audit results. The audit report is drawn up by the auditing body and presented to the KRITIS operator. The BSI may request the submission of the documentation on which the review was based (e.g. IT security concepts, process documentation, audit report, business continuity management and contingency concepts).

The forms and their respective appendices that the KRITIS operator submits to the BSI **for each registered system (or grouped)** are referred to as ***compliance documents***.

These comprise the following:

- confirmation from the auditing body that the operator complies with the legal requirements of Section 8a (1) BSIG and that findings deviating from these are recorded as security deficiencies
- general information on the nature and extent of the audits carried out
- forms provided by the BSI
  - KI with information on the audited critical infrastructure and the contact person
  - P with details of the audit implementation with times and scope (Section PD), the audit result and the security deficiencies detected (Section PE) and the auditing body and audit team (Section PS) and
- the list of security deficiencies and the implementation plan.

The ***documentation of compliance*** comprises the complete ***compliance documentation***.

1.4 Roles and responsibilities in the documentation process

The framework conditions and implementation guidelines described within the scope of this orientation guide affect the roles "KRITIS operator", "auditing body", "audit team" and "BSI", which are illustrated in Figure **1**.

[1] Additional definitions of terms can be found in the glossary

Auditing bodies may declare their suitability on the basis of appropriate recognition or accreditation or in the form of a self-declaration. The graphic does not illustrate this aspect, since the BSIG does **not** introduce a new approval/accreditation process; it simply refers to existing processes.

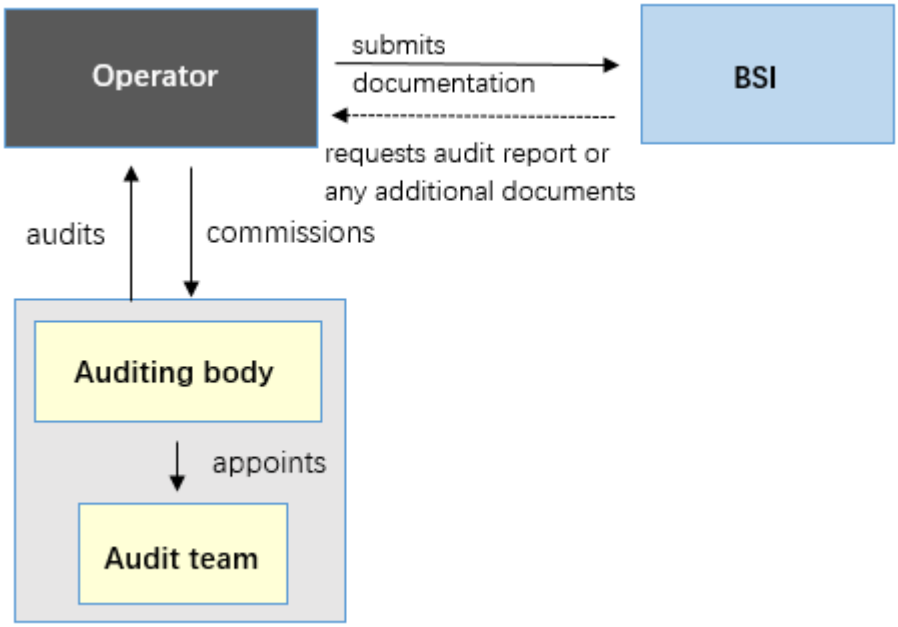

Figure 1: Roles in the documentation process, source: BSI

1.4.1 KRITIS operators

According to Section 8a (3) BSIG, the KRITIS operators covered by the BSIG are obliged to demonstrate compliance with the implementation of appropriate organisational and technical precautions according to Section 8a (1) BSIG every two years. Precautions are appropriate if the costs are in proportion to the possible consequences of a disruption to the supply of the population. The precautions serve to ensure the functionality of the essential services (kDL) and thus the maintenance of the supply service.

The KRITIS operator shall commission an auditing body to carry out the audit necessary to produce documentation of compliance.

1.4.2 Auditing body and audit team

The auditing body puts together an appropriate, qualified and independent audit team (see Section 4), which prepares and carries out the actual audit and documents it in an audit report. The responsibilities of the auditing body regarding audits and documentation are described in detail in Section 3.

The auditing body is responsible to the KRITIS operator for the correct execution of the audit (Section 6) as well as for the correctness of the audit report and the corresponding documents.

Due to the shared responsibility of the auditing body towards the KRITIS operator and the KRITIS operator towards the BSI, it is recommended that the obligations between the auditing body and the KRITIS operator are clearly agreed by contract.

1.4.3 BSI

The BSI receives documentation of compliance from the KRITIS operator, including a list of the security deficiencies with the associated implementation plan for dealing with these deficiencies. The documentation of compliance shall also include information on the audit carried out, such as a description of the audit object.

The BSI accepts the documentation of compliance of the KRITIS operator, checks it for completeness and evaluates it initially to see whether its contents are conclusive and informative enough to assess the degree to which requirements have been met. The BSI immediately requests any content and documents that is obviously missing. After submission of the complete documents (i.e. all documents required for the documentation check), the KRITIS operator will receive a confirmation of receipt by e-mail stating the new official due date for documentation of compliance (see also Section 6).

In principle, further documentation checks can be carried out up to the submission of the subsequent documentation depending on available capacities and at the discretion of the BSI. The BSI does not provide a confirmation the quality of the content of the documentation of compliance.

If no further enquiries are necessary for documentation of compliance or no further cooperation of the KRITIS operator is required for subsequent auditing, the KRITIS operator will not receive any further notification of the procedure after the confirmation of receipt detailed above. The BSI can, however, request further parts or the entire documentation on which the audit is based at any time, or schedule on-site audits, irrespective of the specific reason.

2 The KRITIS operator

The KRITIS operator must guarantee compliance with the requirements according to Section 8a (1) of the BSIG (appropriate provisions in order to avoid errors in compliance with the state of the art) for their systems to the extent the operator is not exempted in line with Section 8d (2) of the BSIG. To do this, they must first define a suitable scope for the audit object, determine the underlying processes and plan, implement and document appropriate security safeguards.

They must then regularly (at least every two years) submit documentation of compliance with the implementation of the measures to the BSI.

In order to document the implementation of safeguards, they must commission an appropriate auditing body, which carries out the audit of one or more systems of the KRITIS

operator (audit or certification) and provides the results in writing to the KRITIS operator in an audit report listing the security deficiencies found.

In the next step, the KRITIS operator submits the documentation of compliance to the BSI. Documentation of compliance must be provided for each system in accordance with the BSI KRITIS Regulation. If several systems are comparable with multiple test steps carried out together, the information can also be summarised in one form (P or KI).

The following section includes answers to the following questions:

- What does the scope cover? (Section 2.1)
- What documents should the KRITIS operator provide the auditing body with in order to implement the audit? (Section 2.2)
- Which audit bases can be used? (Section 2.3)

2.1 Description of the audit object

An appropriate audit must include the entire and current scope[2] of the critical infrastructure as an audit object, i.e. the system according to BSI-KritisV. The scope must therefore be precisely defined and described in preparation for the audit (Section 5.2). In addition, essential points of this description may also be listed in the documentation (e.g. Annex to Form P).

For the implementation of the audit and the documentation of compliance, the following should be described:

- the system
- the parts of the essential service provided by the KRITIS operator
- the parts of the essential service provided by external service providers (e.g. outsourcing, provision through parent/subsidiary group)
- the interaction with other systems
- the interfaces and dependencies.

For the implementation of the audit, all of the following should be listed:

- IT systems
- components
- processes
- roles, persons and organisational units

insofar as these are necessary for the functioning of the essential service provided or which (may) influence its functioning. The connection between these objects should also be shown.

[2] See “Scope” in the Annex E

2.2 Standard security documentation

The audit team requires concrete documents and the option to carry out an on-site audit in order to properly carry out the audit for the documentation of compliance according to Section 8a (3) BSIG. The on-site audit needs to include an inspection of the technology and infrastructure as well as in-depth discussions with employees of the KRITIS operator (see Section 5).

Examples of documents the KRITIS operators should provide to the auditor[3]:

- Security concept (incl. presentation of implemented and planned safeguards, in particular industry-specific safeguards and KRITIS security objectives derived from the essential services)
- Description of the information security management system (ISMS)
- Contingency concept and description of continuity management
- Asset management documents
- Documentation of the processes for structural and physical security (e.g. site access control or fire protection safeguards)
- Documentation of the personnel and organisational security (e.g. records on employee training measures, awareness-raising campaigns, authorisation management)
- Concepts and documentation for incident identification and processing (e.g. description on incident management, detection of attacks, forensics)
- Concepts and documentation of reviews (e.g. audit reports of the internal audit and of other audits performed, drills, systematic log analyses, etc.)
- Guidelines on external supply of information (obtaining information on topics that are relevant to IT security)
- Guidelines on dealing with suppliers and service providers (e.g. service level agreements and other security-relevant agreements with service providers)

The auditing body may use additional documents as the basis of the audit.

2.3 Selection of the audit basis

In consultation with the auditing body, the KRITIS operator selects the audit basis. The following cases can be distinguished, among others, which are described in more detail in Section 5.1 on carrying out audits, whereby the cases are not mutually exclusive:

- audit based on a suitable industry-specific security standard (B3S) (Section 5.1.1)
- audit without using any industry-specific security standard (B3S) (Section 5.1.2)
- consideration of existing audits or other audit bases (Section 5.1.3)

[3] The "Guidelines on content and requirements for industry-specific security standards (B3S) according to Section 8a (2) BSIG" provides further information on the documents required.

3 The auditing body

An auditing body is an appropriate institution commissioned by the KRITIS operator to determine whether the operator has taken appropriate provisions in line with Section 8a (1) BSIG.

In order for an auditing body to be considered appropriate, it should meet the technical and organisational requirements described in this section. Specifically, the auditing body appoints the audit team performing the actual audit. The audit team should have the competencies described in Section 4.2.

This section includes answers to the following questions:

- What are the tasks of the auditing body? (Section 3.1)
- When is an auditing body appropriate? (Section 3.2)
- What kinds of auditing bodies are there? (Section 3.3)

3.1 Tasks

The auditing body must perform the following tasks:

- review compliance with the processes and methods
- ensure a consistent and equivalent implementation of the audit and audit results
- ensure quality management
- define framework conditions for the implementation of the audit (audit processes, etc.)
- assemble the audit team and ensure coverage of all areas of competence
- make sufficient personnel available so that the principle of dual control can be observed during the audit
- confirm the suitability of the auditors
- implement the communication with the KRITIS operator on the one hand, and with the audit team on the other

The auditing body assumes the responsibility for the audit results, signs the test documents and sends them to the KRITIS operator.

3.2 Qualification

An auditing body is suitable if the following criteria are met:

- The auditing body must prove to the BSI the additional documentation procedure competence for Section 8a BSIG (see Section 4.3) for at least one employee. If one of its employees is a member of the audit team, the documentation already provided is sufficient. However, in this case an indication that the person is a member of the audit team is required.

- The necessary processes (e.g. information security management system (ISMS), quality assurance procedures, documentation and recording procedures, archiving and backup concept, audit process) must be introduced, implemented and documented in concepts.
- The auditing body must carry out each audit in line with the documented audit process. The uniform understanding of deviations is absolutely essential for assessing the deficiencies. If a security deficiency is assessed as a severe deviation, the reasons must be analysed and documented transparently.
- It must be ensured that each audit is independent and impartial, neutral and free of instructions.
- Compliance with the ethical principles (see Annex A) must be ensured.
- The type and extent of the audit actions and results are documented uniformly, objectively and properly.
- Sufficiently competent human resources and suitable infrastructures are made available. An auditing body must meet the following criteria:
  - have at least one manager and one deputy in order to be able to compensate for planned and unplanned management absences
  - carry out the audit procedure within a reasonable period of time
  - be able to document secure infrastructure, systems, applications and a secure IT network structure
- The auditing body shall have a defined process in place to determine the competence of the audit team and other persons involved in conducting the audits (e.g. technical experts). The following competencies must be available in the audit team for this:
  - reliable knowledge of the field of information security
  - industry expertise and technical know-how in the field of providing the essential services of the audited KRITIS operator
  - reliable knowledge in the field of management systems and particularly information security management systems (ISMS)
  - detailed knowledge of the requirements of audits in line with Section 8a (3) BSIG

In order to provide for a comparable quality of the audit results, the audits should be performed within the documentation framework on the basis of common standards. Compliance with the requirements regarding the auditing body and the implementation of the processes should be checked by an independent authority.

In many cases the auditing bodies are subject to an accreditation scheme (see Section 3.3).

If an auditing body is not covered by the list in Section 3.2, individual documentation of suitability by means of a self-declaration for auditing bodies to the BSI is required (see Section 3.3.5).

3.3 Appropriate auditing bodies

The auditing body may document its qualification with the following, for example:

- an accreditation with the DAkkS (German National Accreditation Body) for ISO/IEC 27001 certification (accredited certification bodies of the DAkkS) (Section 3.3.1)
- a certification as IT security service provider or an approval as auditing body with the BSI (Section 3.3.2)
- an external quality assessment according to "International Standards for the Professional Practice of Internal Auditing" (IIA)[4] and/or DIIR auditing standard no. 3 "Examination of Internal Auditing Systems (Quality Assessments)" (DIIR)[5] (Section 3.3.3)
- an accreditation as an accounting institution by the IDW (Section 3.3.4)
- an individual documentation of suitability by self-declaration to the BSI (Section 3.3.5)

In addition, it should be demonstrated that the members of the audit team as a whole have all the necessary competencies (see Section 4).

The qualifications of the auditing body are described in more detail in the sub-sections below.

3.3.1 Accredited certification bodies of the DAkkS

Within the framework of an ISO/IEC 27001 certification procedure, the Deutsche Akkreditierungsstelle GmbH (DAkkS) as the national accreditation body of the Federal Republic of Germany assumes the function of an "independent body". A qualified certification body is accredited for the field of ISO/IEC 27001 and must document the implementation and compliance of the ISO/IEC 17021-1 and ISO/IEC 27006 standards to the DAkkS. These bodies thus fulfil the necessary quality requirements.

An overview of the bodies accredited for ISMS certification in Germany can be found on the website of the German National Accreditation Body (DAkkS).

3.3.2 Certified IT security service providers or approved auditing bodies of the BSI

The BSI offers certification of IT security service providers for various areas of application. Irrespective of the scope, the aim of recognition by the BSI is to ensure the professional competence, quality and comparability of the concepts, procedures and work results of the auditing bodies.

[4] https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Standards__Version_6.1__20180110.pdf

[5] https://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr__3.pdf

A prerequisite for certification as an IT security service provider is meeting the requirements of DIN EN ISO/IEC 17025 in the respective valid version. The procedure for certification or recognition of auditing bodies is laid down in a published description of the procedure, which is supplemented by an audit catalogue[6].

These bodies therefore meet appropriate quality requirements.

3.3.3 Internal audits

Internal audits can demonstrate an appropriate and efficient auditing system and compliance with the International Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors (IIA) by means of a quality assessment (QA). In this case, the independent authority is the body performing the QA audits. This procedure is based on DIIR[7] revision standard no. 3 "Audit of Internal Audit Systems (Quality Assessments)" and IIA standards 1300ff[8].

In order to assess the appropriateness and effectiveness when auditing the current state of the art, an internal auditing process must also meet certain quality criteria. Compliance with specific criteria is checked within the scope of a quality assessment. The following six minimum requirements must be met:

- An official written, appropriate regulation regarding the implementation of the audit (rules of procedure, audit guideline or similar).
- Neutrality, independence from other functions as well as unrestricted information rights of the internal audit are guaranteed and must be presented to the BSI.
- The internal auditing department has the appropriate quantitative and qualitative human resources.
- The Gap Analysis Plan for the internal audit is drawn up on the basis of a standardised and risk-oriented planning process.
- The type and extent of the audit actions and results are documented uniformly, objectively and properly.
- The implementation of the safeguards documented in the report is monitored by the internal auditing department using an efficient follow-up process.

The independence of the internal auditing department is particularly guaranteed through compliance with the international standards. Additionally, the code of ethics of the IIA is binding for the internal auditors. The requirements regarding integrity, impartiality, confidentiality and professional competence are described here[9].

---

6 https://www.bsi.bund.de/dok/128146

7 DIIR: German Institute of Internal Auditors

8 http://www.diir.de/zertifizierung/quality-assessment/

9 https://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2017_Standards__Version_6.1__20180110.pdf

3.3.4 Accounting institutions

Due to the high level of responsibility that an accounting institution assumes, it fulfils special professional obligations, which are summarised in the Public Accountant Act (WPO)[10].

These include independence, discretion and professional conduct.

3.3.5 Self-declaration to the BSI

If an auditing body is not subject to one of the recognised accreditation schemes described above, it may nevertheless demonstrate its suitability, provided that it fulfils the suitability criteria (see Section 3.2).

This can be recorded in a self-declaration and presented to the BSI.

This self-declaration is a binding statement of compliance with the necessary suitability criteria and must therefore be in writing and signed by an authorised signatory of the auditing body.

The required information can be provided on the form[11] provided by BSI. It is sent to the BSI together with the other documentation.

The self-declaration must relate to the concrete audit object. A global self-declaration by an auditing body is not sufficient.

4 The audit team

The auditing body puts together an audit team that is commissioned with the concrete audit at a KRITIS operator.

The audit team must meet all the requirements necessary to provide the appropriate documentation of compliance and possess the required competence specified in Section 4.2. In principle, an audit team should consist of at least two qualified employees in order to adhere to the two-person rule.

Depending on the extent of the audit, additional auditors and/or technical experts (e.g. to provide industry-specific or system-specific know-how) may be added to the team. All members of the audit team must comply with the "basic ethical principles" set out in the appendix.

4.1 Tasks

An audit team of the auditing body implements the audit according to a specified audit process and draws up an audit report documenting the audit results.

This audit can be performed

- as an individual audit of an appropriate (internal or external) auditing body

[10] http://www.gesetze-im-internet.de/wipro/index.html

[11] https://www.bsi.bund.de/dok/408976

- as an additional audit, e.g. within the scope of
  - an internal ISMS audit by internal, independent IS auditors (first-party audit)
  - an audit performed by qualified chartered accountants
  - an ISO/IEC 27001 certification, i.e. a certification, monitoring or re-certification audit (native or on the basis of IT-Grundschutz) by auditors

(third-party audit).

4.2 Competence and suitability

To enable the auditors commissioned by the KRITIS operator to perform the appropriate audits and thereby provide the appropriate documentation of compliance to comply with the legal requirements, they must be competent in the following fields:

- Additional audit process competence for Section 8a BSIG
- Audit competence
- IT security competence and information security competence, respectively
- Industry competence

An auditor does not have to have all these competences individually; the appropriate composition of an audit team covering all areas of competence is sufficient. If the auditors themselves do not possess the required competence, a technical expert with the appropriate knowledge can also be included in the audit team. Particularly with regard to industry competence, it can be helpful to call in different experts for different areas (e.g. as a member of the audit team or as part of interviews).

An auditor must carry out the audit impartially and free of instruction. The audit results must be documented transparently. Each audit team should consist of at least two auditors in order to guarantee independence and impartiality (“two-man rule”). For reasons of independence and neutrality, the members of the team must not have previously been directly involved in an advisory or executive capacity in the audited area, e.g. in the creation of concepts or the configuration of IT systems. The head of the audit team shall not perform more than two consecutive audits of the same system.

Employees of the KRITIS operator or its service provider entrusted with the operation or IT security of the system to be inspected are not eligible as members of the inspection team. Expert knowledge from this group of people can be collected by the audit team in the course of an interview. However, participation as part of the audit team and thus in the assessment of the facts established during the audit must be excluded.

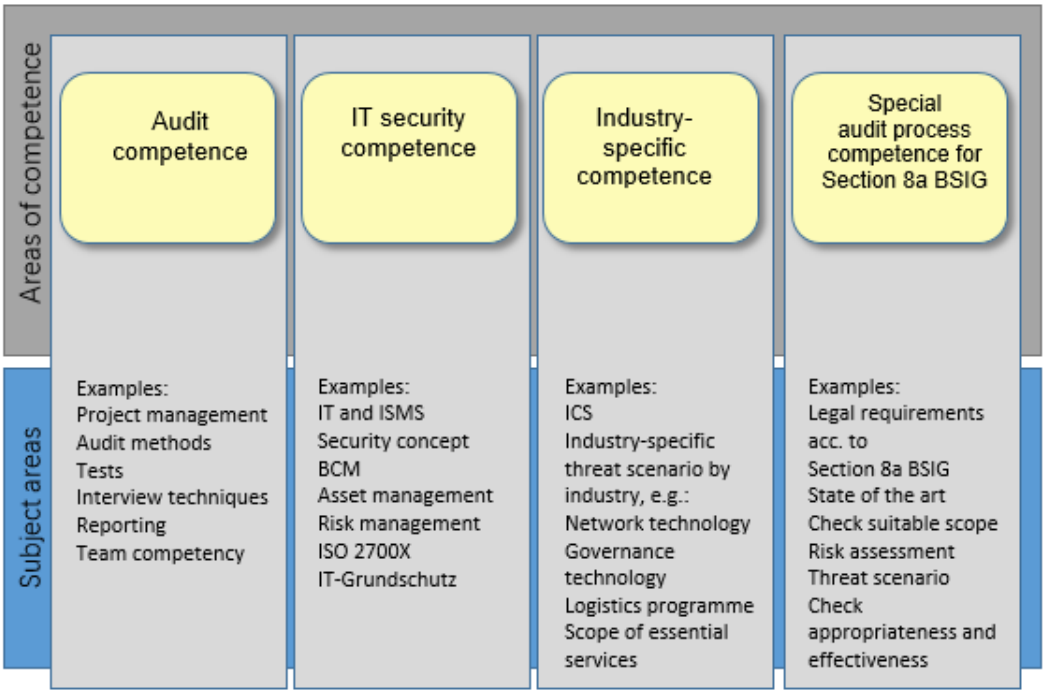

Figure 2: Subject areas of the areas of competence, source: BSI

Figure 2 shows the focal subjects that should be present in the individual areas of competence as a minimum requirement.

Note: The overall competence can be shared by several examiners. However, it is important that auditors with a sufficient level of competence are involved in every audit section.

4.3 Acquiring additional audit process competence

By additional audit procedure competence for Section 8a BSIG, we mean knowledge of the characteristics of a KRITIS-specific audit within the area of Section 8a BSIG. In particular, this concerns the evaluation of the scope, the protection of security of supply, restrictions in risk treatment, the consideration of the "state of the art" and other special aspects that are KRITIS-specific.

This competence can be acquired in a separate training course that deals in deal with the special aspects and requirements of an audit in line with Section 8a BSIG. This training is not an accreditation, recognition or certification of an auditor; it is an additional qualification.

Acquiring additional audit process competence can be proved to the BSI either by presenting a certificate of participation in an appropriate training course or by using the form “Self-declaration of the auditing person to document additional audit process competence”[12] provided by the BSI.

[12] https://www.bsi.bund.de/dok/408942

5 Performing the audit

The following section describes the matters to be taken into account when performing the audit. This includes the KRITIS operator, the auditing body and the audit team. The criteria of an appropriate audit will be listed, with equivalent alternatives possible according to the technical competence of the auditing body in particular. The following questions will be answered:

- What audit basis has been defined? (Section 5.1)
- Which audit subjects should be audited? (Section 5.2)
- Which audit techniques may be used? (Section 5.3)
- What is the expected time for the audit? (Section 5.4)
- How can the Gap Analysis Plan and random samples be drawn up? (Section 5.5)
- Which contents should be included in an audit report and the audit documentation, respectively? (Section 5.6)
- Which deficiencies must be documented and which deficiency categories should be used? (Section 5.6)

5.1 Audit basis

As a matter of principle, a plurality of audit bases is possible as long as they are appropriate to demonstrate compliance with Section 8a (1) BSIG.

5.1.1 Audit when applying a B3S according to Section 8a (2) BSIG

If there is an industry-specific security standard (B3S)[13] with suitability determination from the BSI for the respective current scope of application and if it was applied by the KRITIS operator during the implementation of safeguards, it can be used as a reference document for creating the Gap Analysis Plan. A B3S describes both the scope and the minimum requirements of the safeguards to be implemented.

The KRITIS operator must determine an appropriate scope for the audit object. At the start of the audit, the auditor should check if the scope has been selected correctly. and is oriented to the individual conditions of the KRITIS operator on site. If the auditor's assessment differs significantly from that of the operator, the auditor must reach an agreement with the operator on the new audit object.

The scope of a B3S, however, is typically oriented to the conditions of the entire industry. It is therefore necessary to examine whether the scope of the B3S fully covers that of the audit or if further additional individual safeguards may be necessary. The specifications of the B3S should be mapped to the systems to be audited.

[13] https://www.bsi.bund.de/Stand-der-Technik

5.1.2 Audit without applying a B3S

If there is no B3S or if the audit is to be performed separately from a B3S, it must be ensured that the requirements according to Section 8a (1) BSIG are complied with differently. The audit must be suitable to demonstrate the aforementioned. Prior to performing the audit, the auditing body must define an appropriate audit process and must transparently document the defined audit process. This audit process will then serve as the audit basis.

Indications of an appropriate audit process may include the following:

- the orientation guide to industry-specific security standards (B3S) according to Section 8a (2) BSIG
- the catalogue for specifying the requirements of Section 8a (1) BSIG, [14]
- other B3Ss according to Section 8a (2) BSIG whose suitability has been determined (in this regard, the scope of the B3S should be adapted to the scope to be audited, if necessary
- relevant standards (e.g. certification schemes for ISO 27001 (native or on the basis of IT-Grundschutz), ISO/IEC 17021--1, ISO/IEC 27006)

5.1.3 Consideration of existing audits

As a matter of principle, existing, appropriate audits may be considered when furnishing the documentation, i.e. it is possible to cover aspects to be covered for Section 8a (3) BSIG within the scope of different audits. To ensure appropriate audits, they must be valid at the time of submission, i.e. the audit object must still exist in this form. In addition, the audits must be up-to-date, i.e. at the time of filing with the BSI they must have been carried out within one year. At best, older audit results may be incorporated into the audit in the form of a document analysis (see Section 5.3), but this does not take the place of the current audit (e.g. due to a changed risk situation and efficiency of measures). Aspects that are still missing must be included in the Gap Analysis Plan.

In particular, it must be ensured that the scope of application completely covers the critical infrastructure to be audited and takes account of additional framework conditions relevant to the critical infrastructure (e.g. dealing with service providers, limitations regarding the risk acceptance). The "Orientation Guide to Industry-Specific Security Standards" provides an indication of such framework conditions[15].

The responsibility to completely cover the scope rests with the KRITIS operator. The completeness is checked expressly by the auditing body.

5.1.3.1 Use of ISO 27001 certificates for documentation of compliance

A valid ISO 27001 certificate can be used as part of a documentation of compliance in line with Section 8a (3) BSIG, as long as some basic conditions are met. This applies both to native ISO 27001 certificates as well as ISO 27001 certificates based on IT-Grundschutz.

[14] https://www.bsi.bund.de/dok/408936

[15] https://www.bsi.bund.de/dok/408956

An ISO 27001 certification does not automatically cover the entire scope relevant for the documentation of compliance in line with Section 8a BSIG. The scope of the documentation of compliance must cover the critical infrastructure or the essential service fully (process layer).

In addition, the information security process with regard to the essential service must be viewed through "KRITIS glasses". Avoiding shortage of supplies in essential services is very important in the context of KRITIS. The essential service must therefore be considered with the focus on avoiding shortage of supplies for the population.

The following section will consider the general framework conditions for the use of ISO 27001 certificates for documentation of compliance in line with Section 8a (3) BSIG:

1. Defining scope

The scope must include the systems operated according to the BSI KRITIS Regulation. The interfaces should be suitably defined.

2. Extended scope

The scope must be extended to outsourced areas and a comprehensive security assessment carried out from the KRITIS perspective. This can be based on ISO 27001 or other comparable procedures.

In the case of an existing ISO 27001 certification, this can be extended to the previously unaudited parts of the scope for documentation of compliance in accordance with Section 8a (3) BSIG. In this way, a supplementary audit of the area already audited can be carried out with regard to the KRITIS protection objectives. This means the documentation can be examined on the basis of the audit of an initial certification, a monitoring or re-certification audit and synergy effects can be used. The test results form part of the documentation of compliance in accordance with Section 8a (3) BSIG.

3. Consideration of KRITIS protection objectives

The BSIG requires appropriate measures to be taken for the operation-relevant parts of the respective systems in accordance with the protection requirements.

Maintaining the security of supply of the population must be the central concern in information security risk management. The requirements placed on the provision of services are also referred to as KRITIS protection objectives. The KRITIS protection objectives of the operation-relevant parts are to be suitably defined. The KRITIS protection objectives (e.g. the availability of the essential service) are to be included in the proprietary risk analysis and additionally considered throughout all processes and safeguard implementations ("KRITIS glasses").

4. KRITIS protection needs

As part of risk management, the protection objectives of availability, confidentiality, integrity and authenticity must be assessed in terms of the extent to which the essential service is maintained.

A purely economic view of risks is not generally sufficient (see "Dealing with risks"). The impact on the functioning of the essential infrastructure and essential service should be considered as an indication of the level of risk to the public. For the risk treatment, it should also be considered that the effort required to implement the safeguards is proportionate to the level of risk for the population.

Note: Section 8a (1) BSIG requires “[...] Precautions to avoid disruption to availability, integrity, authenticity and confidentiality [...]”. Risk management based on the evaluation of confidentiality, integrity and availability, as is usual in ISO 27001 or IT-Grundschutz of the BSI, is possible as long as it is ensured that authenticity is considered in the risk assessment and selection of safeguards.

5. Dealing with risks

A purely economic consideration of the risks and the protection needs is not generally sufficient. In particular, the level of risk to the public, i.e. the impact on the functioning of the essential infrastructure and essential service, must be taken into account. In selecting safeguards, care must be taken to ensure appropriateness, i.e. the possible consequences of a failure or impairment of public services must be considered in relation to the cost of security precautions.

- Risk acceptance

  According to Section 8a (1) BSIG, risks in scope may not be accepted if state-of-the-art security precautions are possible and appropriate. Risk acceptance is only possible for the remaining residual risk.

- Insurability of risks

  A transfer of the risks, e.g. by insurance, is not a substitute for the security precautions in line with Section 8a (1) BSIG. In the case of insurance or other risk transfer, appropriate security precautions must also be taken in accordance with the state of the art. However, the KRITIS operator is free to take out additional insurance.

6. Implementation of safeguards

In principle, all the measures necessary for the maintenance of the essential service must be implemented as part of risk management. All safeguards that are only planned, for example in the continuous improvement process (CIP), in the implementation plan or in the risk treatment plan, must be included in the list of security deficiencies according to Section 8a (3) BSIG. In order to assess these deficiencies, explanatory documents such as the deficiency assessment, CIP documentation and implementation plan should also be submitted.

5.1.3.2 Use of an existing C5 attestation

The Cloud Computing Compliance Controls Catalogue (C5) is a minimum standard for IT security for Cloud Service Providers (CSPs). CSPs are classified as essential infrastructures within the “data storage and processing” essential service if the corresponding threshold of the BSI KRITIS Regulation is exceeded. A passed C5 attestation can be used as part of a

documentation of compliance according to Section 8a (3) BSIG, as long as some basic conditions (see FAQ to C5) are met during the testing.

1. Scope of application

The scope of application of the measures in accordance with Section 8a (1) BSIG as well as the object of documentation of compliance in accordance with Section 8a (3) BSIG must cover the entire operated system in accordance with the BSI KRITIS Regulation (e.g. server farm). In the case of cloud service providers (CSP), in order that the documentation of C5 is sufficient for their system as part of the documentation of compliance in accordance with Section 8a (3) BSIG, documentation of adequate protection under consideration of the state of the art must also be provided for all operationally relevant information technology services, systems, components or processes that are not audited via the C5 certificate. This can be done by extending the C5 audit to the previously unaudited parts of the CSP system or by an additional audit.

2. Consideration of KRITIS protection objectives and protection needs

The BSIG requires appropriate measures to be taken for the operation-relevant parts of the respective system categories (in consideration of availability, confidentiality, integrity and authenticity) in accordance with the protection requirements. Avoiding shortage of supplies in essential services is very important in the context of KRITIS. Therefore, the appropriate specification of the protection needs of the operationally relevant parts of the system category has to be examined (cf. Section 8a (1) BSIG and Section 8a (3) BSIG) and, in addition to the requirements of C5, care should be taken to ensure that the systems relevant to operations for essential services are based on a resilient architecture.

3. Dealing with risks

The central concern in dealing with risks must be to maintain the security of supply of the company or to comply with the Service Level Agreements (SLA) concluded with customers. As part of risk management, therefore, the protection objectives of availability, confidentiality, integrity and authenticity must be assessed in terms of the extent to which the essential service is maintained – a purely business management approach is usually not sufficient. The consequences of impairing the functionality of an operated critical infrastructure can be used as an indication of the extent of a risk to society.

Risks within the scope of Section 8a (1) BSIG may not be accepted if security precautions pursuant to Section 8a (1) BSIG are possible and appropriate. Even if risks cannot be completely eliminated, the risks must be adequately reduced as far as possible before acceptance is permitted.

Furthermore, an insurance of the risks does not replace the required security precautions. Appropriate safeguards pursuant to Section 8a (1) BSIG remain necessary. Even if risks cannot be completely eliminated, the risks must be adequately reduced as far as possible before an insurance on the risk treatment is permitted. Concluding additional insurance policies is unaffected.

In addition, there must be compliance with the requirements of C5 regarding the implementation of the measures. If further measures are to be adopted over and above the requirements of C5 with regard to the appropriate protection in accordance with Section 8a (1) BSIG for risk treatment, these must be implemented for the documentation of compliance in accordance with Section 8a (3) BSIG or be in an expected stage of progress at the time of documentation. These measures and deficiencies must be included in the list of security deficiencies.

4. Provision of documentation

Documentation of compliance pursuant to Section 8a (3) BSIG must be provided at least every two years. The underlying C5 certificates must be current at the time of submission of a certificate, i.e. not older than one year. Older documentation can be included in the documentation of compliance in the form of a document analysis if necessary. This documentation requirement can be easily integrated into the testing of the C5.

In addition to the current audit certificate, a list of detected security deficiencies must be submitted as appropriate documentation of compliance, see Section 5.7.

5.2 Audit topics and auditing of the scope

Generally, the audit topics are described in detail in a B3S; in particular, industry-specific requirements and/or safeguards may be listed there, the implementation of which must be ensured.

If no B3S is available or if no B3S is used for the audit, Annex E shows the audit topics that must be considered as a minimum.

If the documentation of compliance extends over several systems or sites, the respective audits topics and statements that refer to the systems and sites must be indicated.

In particular, checking that the scope has been chosen correctly is very important for the suitability of the documentation. The auditor must question whether the choice of scope is correct and fully includes the information technology systems, components and processes belonging to the critical infrastructure of the system to be audited, as well as those influencing the critical infrastructure.

In this regard, under the aspects to be examined, the auditor must examine and evaluate

- functionality of the essential service
- suitability and necessity and
- completeness.

The description of the system and the associated aspects of the essential service must be transparent and correspond in its characteristics to the registered system category.

The scope of application must be presented graphically and, where necessary for comprehension, described in writing. The graphic presentation is intended to provide a quick overview, while the textual description supplements this overview with the necessary depth of information. If there are dependencies or interfaces to areas or systems outside the scope of

application, these must be recognisable in the graphic overview and described in a comprehensible manner. The same applies to parts of the essential service which are provided by third parties on behalf of the operator.

If the presentation of the scope of application is embedded in a presentation of a larger area or overall network, the boundaries of the scope must be clearly indicated. A list of the requirements for the presentation and description of the scope shown here can be found in Annex C with the corresponding points from G01.

The central element of the graphic presentation is the network structure plan. In its function as an overview, it must map all areas of the critical infrastructure, as well as point out communication interfaces and dependencies to the outside world It must indicate the extent to which individual elements are relevant to the essential service. The choice of an appropriate level of abstraction is essential for this. In particular, the network structure plan covers all systems, components and, if applicable, applications that are decisive for the functionality of the essential service. Associated processes can be recorded in the network structure plan or displayed separately. In any case, however, it must be possible to assign processes to the corresponding necessary IT systems, components and applications. It is also important here that the interaction of the essential components with each other and with third parties is made clear.

Similar objects should be meaningfully combined into groups so that the network structure plan remains clear.

Objects may then be assigned to one and the same group if all the components

- are of the same type,
- have similar tasks,
- are subject to similar framework conditions, and
- have the same protection needs.

If the systems, constituents or other areas of the critical infrastructure are distributed over several sites, the scope shall reflect this distribution and identify the sites. It must also show the connections between the sites.

Outsourced parts of the essential service must be identifiable within the scope, along with the communication interfaces used. This also includes maintenance interfaces, provided they are permanently enabled.

This means that at least the following interfaces must be shown in the network structure plan:

- Communication interfaces with external networks
- Communication interfaces with networks at other sites
- Maintenance interfaces that are permanently enabled
- Interfaces to outsourced parts of the service

If elements of the network structure plan are represented by symbols to improve clarity, the elements used must be explained in a legend.

A list can also be used to provide a better overview to meet the requirements for presenting the scope in a network structure plan. A list of the requirements for the presentation and description of the network structure plan is given in Annex C with the corresponding points from N01.

Detailed explanations and examples of graphic scopes are published on the BSI website[16].

The auditing body shall examine the suitability of the scope within the meaning of Section 8a (3) BSIG and present the result in the audit report.

Note: As a matter of principle, it makes sense that the auditing body, together with the KRITIS operator to be audited, clarifies the scope of the audit prior to being engaged, and that the auditing body creates the cost assessment and the offer for the audit on this basis.

5.3 Possible audit techniques

The term "audit techniques" refers to all methods used to examine a situation. Different audit techniques can be used during an audit, such as the following:

- personal questioning (interview)
- (visual) inspection of systems, sites, premises and objects
- document analysis (this also includes electronic data)
- technical on-site examination and/or targeted observation (e.g. the functionality of alarm systems, site access controls, having applications demonstrated)
- penetration tests
- data analysis (e.g. log files, firewall configuration, analysis of databases, etc.)
- written questioning (e.g. questionnaire)
- incorporation of existing documentation of compliance (e.g. reviewing the audit report of an audit performed in a different context, see also Section 5.1.3).

The use of the different audit techniques depends on the specific case and must be defined by the audit team.

5.4 Audit effort

The determination of the audit effort for first-time audits includes, for example:

- the size of the scope to be audited, as measured by the number of employees of the organisation
- the criticality and the degree of supply, respectively, according to BSI-KritisV
- the complexity of the scope to be audited

[16] https://www.bsi.bund.de/dok/932836

- the IT dependence and the IT penetration, respectively, of the essential service
- the question of whether detailed investigations based on expert/technical tests or analyses should be carried out within the scope of the audit – this will normally be the case if the KRITIS operator does not carry out such tests regularly.

In order to estimate the complexity, the following questions may be used:

- How complex is the IT system environment (number of systems and heterogeneity of the systems used)?
- How many sites does the object of examination encompass (scope)?
- How many network transitions are there?
- Which and how many IT applications are being used in the organisation? Do they support critical business processes?
- Are superordinate methods being used that have an influence on areas outside of the organisation?
- How long has the topic of information security been established in the organisation and what is the organisation's level of experience in this respect? Have (partial) systems already been certified, if applicable?

The actual time required for the audit is difficult to estimate, since the systems of KRITIS operators can vary greatly.

Each audit should cover the six audit steps listed below. In general, these are to be adapted to the specific system and the industry-specific characteristics.

Audit steps	Activity
Step 1	Preparation of the audit as well as examination of the suitability of the scope
Step 2	Creation of the Gap Analysis Plan
Step 3	Checking of official documents
Step 4	On-site audit
Step 5	Follow-up of the on-site audit
Step 6	Drawing up of the audit report

Table 1: Basic guide to the relative time required to carry out an audit as documentation of the implementation of the requirements Section 8a (3) BSIG, source: BSI

5.5 Gap Analysis Plan and possible selection of random samples

Every audit must be based on a documented Gap Analysis Plan. This defines the audit team, the audit objects, the audit goals, as well as the intended audit technique prior to the actual audit. Likewise, the roles within the audit team and the necessary contact persons on part of the KRITIS operator as well as the schedule should be defined.

The compliance documentation includes information on the audit process including the audit topics and the audited sites (Annex PD.B). It must be possible to follow the audit process using this information.

As a minimum, the following information on the test procedure is required (an example of a table with information on the test procedure can be found in Annex B):

What?

- The concrete topics that were covered in the audit must be clear and transparent. Where this is meaningful, the topics can also be broken down into different levels.
- If the audit basis is made up of several standards/documents, each audit topic must be assigned to the corresponding standards/documents from the audit basis (ideally with reference to the corresponding chapter).
- The audit object (process, system, document, KRITIS etc.) must be presented transparently to the BSI

How?

- The methods used to achieve audit results must be transparent.

Who?

- It must be clear and transparent, which people within the audit team and which roles or departments of the KRITIS operator were involved in the (partial) audit.

When?

- A chronological sequence of the audit steps must be recognisable.
- It must be clear and transparent which topics were allocated more time in the audit.

Where?

- The audit site must be clearly presented to the BSI. In particular, if several systems are considered in an audit, it must be made clear to which systems/sites the respective topic relates.

A complete audit of the entire scope at reasonable cost is not normally possible. That is why the auditor must define an appropriate selection of random samples within the Gap Analysis Plan. This selection must at least include all critical processes. The selection of the random samples must be risk-oriented (consideration of likelihood and effects on the provision of the essential service; however, it must be ensured that comprehensive random samples provide good coverage of the system or systems of the critical infrastructure as well as coverage of the network topology. Areas with higher risks should be taken into account more severely. In particular, the risk assessment should include the impact on the supply of the population with the essential service according to the size of the KRITIS operator (How many people would be affected by a failure? How serious would a failure or malfunction be?) The selection of the random sample must be justified.

Establishing a multi-year auditing concept is recommended so that each IT system, each IT component and each IT process is audited at least once in the foreseeable future. The random sample must be selected by the auditor or the auditing body, respectively. It is not appropriate to use the same random sample for several audits. The Gap Analysis Plan should take into account previous audits in order to achieve a complete coverage of all components/processes

in the long run. In particular, the list of deficiencies from the last audit result (audit reports) must be taken into account in the Gap Analysis Plan when selecting the random samples.

Note: The standards ISO 19011, ISO/IEC 27007 and ISO/IEC 27008 may include information for planning and implementing an audit.

5.6 Documentation of the audit result in the audit report

The audit report on the implementation of the requirements under Section 8a (1) BSIG should

- be a separate document
- be drawn up in German or English
  all contents must be comprehensible
- have an unambiguous denomination and version control
- include all meta information relevant to the evaluation (e.g. scope of the examination, audit goal, time, place and duration of the audit, auditing body and audit team, audit results, etc.)
- document all audit steps on a comprehensible and repeatable basis and set out the audit decisions on a substantiated basis

In particular, security deficiencies and recommendations must be documented in the audit report. A description of the minimum requirements for the description of security deficiencies and a template for a list of deficiencies is provided by the BSI on its website[17] and in Table 3 in Section 5.7.4 List of Deficiencies.

5.6.1 Assessment of maturity level of the ISMS and BCMS

Within the framework of the provision of documentation, an assessment of the effectiveness of the information security management system (ISMS) of an organisation should be performed regularly. This can be performed by using a maturity model. A maturity model makes it possible to transparently document the advancement of the ISMS during the years without providing too much detail on individual safeguards. It represents another potential key figure for controlling the information security in an organisation.

Likewise, the Business Continuity Management System (BCMS) and the resulting requirements and measures must be regularly reviewed for their efficiency and effectiveness.

Section PE of the supporting document P therefore provides for a designation of the maturity level of ISMS and BCMS.

The information on the maturity levels only relates to a superficial assessment by the audit team. In this context, the maturity levels of ISMS and BCMS specifically should only be assessed within the scope of the audit, i.e. with a view to ensuring the essential service. The classification into maturity levels in this documentation form is based on traditional maturity models; a maturity level determination using scientific methods is not required. Rather, the

[17] https://www.bsi.bund.de/dok/158698

audit team should provide a rough assessment of how strongly the processes for the ISMS and BCMS are already anchored and actively integrated in the company, in the form of maturity levels.

The following list should be used to assess the maturity level of the ISMS and BCMS audited.

ISMS maturity level

- Maturity level 1: an ISMS is planned, but not yet established.
- Maturity level 2: an ISMS is largely established.
- Maturity level 3: an ISMS is established and documented.
- Maturity level 4: in addition to maturity level 3, the ISMS has been checked regularly for effectiveness.
- Maturity level 5: in addition to maturity level 4, the ISMS has been improved regularly.

BCMS maturity level

- Maturity level 1: an BCMS is planned, but not yet established.
- Maturity level 2: an BCMS is largely established.
- Maturity level 3: an BCMS is established and documented.
- Maturity level 4: in addition to maturity level 3, the BCMS has been checked regularly checked and tested.
- Maturity level 5: in addition to maturity level 4, the BCMS has been improved regularly.

To assess whether maturity levels 4 or 5 are reached, it is necessary to look at the measures or reviews carried out in the past. This implicitly means that a newly established ISMS or BCMS, in which processes for measurement and continuous improvement are anchored but have not yet been run through several times, cannot yet reach these levels of maturity.

5.7 Security deficiencies, implementation plan and list of deficiencies

5.7.1 Security deficiency

For each tested security precaution in accordance with Section 8a (1) BSIG, the established facts shall be included in the audit report and evaluated with regard to the implementation status. If a deviation from the requirements according to Section 8a (1) BSIG is found, it is a security deficiency which has to be documented in the list of deficiencies and evaluated with regard to the provision of the essential service. As a matter of principle, all determinations representing a risk or requiring corrective action that cannot be implemented without any time or resource effort must be included in the audit report and in the list of deficiencies.

The security deficiencies and their assessment in relation to the provision of the essential service shall be recorded by the auditing body.

5.7.2 Deficiency categories

The security deficiencies shall be classified by the auditing body in two dimensions:

1) IT security issue concerned (see Annex E)

2) severity of the deficiency

To classify the severity of security deficiencies, deficiency categories shall be defined and used uniformly throughout the audit report. In this respect, each auditing body may select an evaluation scheme that is standard for its audits. However, uniform deficiency assessments must be made in the list of deficiencies of the compliance documentation sent to the BSI. If the auditor's deficiency categories deviate from the deficiency categories of this orientation guide, the auditor must map their categories to the categories defined in table 2.

For all security deficiencies, the causes have to be analysed and documented in a transparent way.

Category	**Definition**	**Audit report / list of deficiencies**
Severe or significant deviation/security deficiency	A "severe deviation" is a **serious** threat and a serious risk, respectively. A "significant deviation" is a huge threat or a high risk. There is urgent need for action. The deviation must be **eliminated** immediately or as soon as possible, since the confidentiality, integrity, authenticity or availability of the essential service is severely threatened and significant damage is to be expected.	Incorporation into the audit report and into the list of deficiencies in the documentation of compliance
Minor deviation/security deficiency	A "minor deviation" is a threat and a risk, respectively. There is no urgent need for action. The underlying deviation must be eliminated in the medium term. The confidentiality, integrity, authenticity or availability of the essential service might be impaired.	Incorporation into the audit report and into the list of deficiencies in the documentation of compliance
Recommendation	A "recommendation" is a suggestion for improvement. By implementing the recommendation, the security can be increased.[18] Examples of recommendations: - improvement suggestions for the implementation of safeguards - additional safeguards that have been successful in practice - comments regarding the appropriateness and effectiveness of safeguards.	Incorporation into the audit report Incorporation into the list of deficiencies is recommended

[18] A partially or not implemented measure or requirement may only be classified as a security recommendation if the audit team have reason to believe that, in the medium term, no impairment of the confidentiality, integrity or availability of the essential service data is expected.

Category	Definition	Audit report / list of deficiencies
No deviation	There is no security deficiency if the requirements are complied with in their entirety and if all safeguards have been implemented completely, efficiently and appropriately. There is no supplementary information.	Incorporation into the audit report Not incorporated into the list of deficiencies

Table 2: Deficiency categories

5.7.3 Risk assessment and implementation plan

Each security deficiency must be subject to a risk assessment. The concrete safeguards to be implemented, the persons responsible for them, the planned dates for rectifying the deficiencies, and their implementation status must be specified in an implementation plan.

The measures to be implemented, the persons responsible for them, the planned deadlines for eliminating the deficiencies and their implementation status are described by the KRITIS operator.

5.7.4 List of deficiencies

Finally, the list of deficiencies summarises the security deficiencies and their classification, the risk assessment and the implementation plan in a clear manner and also shows the status of implementation.

Minimum requirements for a list of deficiencies like this are described below. A template for a list of deficiencies including an implementation plan can be found in Annex D.

The list of deficiencies is part of the compliance documentation according to Section 8a (3) BSIG and must be sent by the KRITIS operator to the KRITIS office of the BSI as an attachment to the documentation forms.

The auditor or KRITIS operator must provide the BSI with sufficient information to assess the respective security deficiencies and to eliminate them (see Section5.7.4.1 "Minimum requirements for a list of deficiencies").

In principle, the list of deficiencies, which is provided to the BSI as part of the documentation of compliance, must describe the deficiencies in a transparent manner without further documents. In particular, care must be taken to avoid abbreviations or to explain them adequately.

The list of deficiencies in the implementation plan may also be extended by the operator by a Comments column for the operator to detail any possible divergences.

Example: No automatic screen locks are activated for medical devices in the operating area of a hospital. The auditor has classified this as a minor deviation. However, the operator can then comment that this is a particularly access-protected area, where an automatic screen lock can even be counterproductive.

5.7.4.1 Minimum requirements for a list of deficiencies

It is essential that the BSI is provided with sufficient information to assess the respective security deficiencies so that the BSI can decide whether the steps provided by the operator in the implementation plan to remedy the deficiencies are appropriate and sufficient.

a. Every security deficiency must be described in a comprehensible manner. It must be clear to the BSI why the circumstance described represents a security deficiency. For common security deficiencies a simple description is usually sufficient; for security deficiencies in more "exotic" systems, more detailed explanations are often required.
b. The BSI must be able to understand the (potential) impact of the security deficiency on the availability, integrity, authenticity or confidentiality of the information technology systems, components or processes necessary for the functioning of the critical infrastructure.
c. The assessment of the risk to the availability, integrity, authenticity or confidentiality of the IT systems, components or processes necessary for the functioning of the critical infrastructure must be transparent to the BSI. The list of deficiencies must follow the classification described in Table 2: Deficiency **categories** in order to assess the risk.
d. The BSI must be able to trace whether a security deficiency is properly addressed by the operator. The operator must therefore provide a time schedule and an action plan.

BSI provides a template for list of deficiencies in addition to the template in Annex D in the download area on its KRITIS website[19].

6 The documentation process in line with Section 8a (3) BSIG

Under Section 8a (3) BSIG, KRITIS operators shall demonstrate compliance with the requirements of Section 8a (1) BSIG in an appropriate manner at least every two years.

6.1 Calculating the official due date for documentation of compliance

The BSIG stipulates that KRITIS operators must take precautions and measures to implement Section 8a (1) BSIG. Corresponding documentation of this must be submitted to the BSI every two years.

6.1.1 First documentation of compliance after exceeding the thresholds

For operators of critical infrastructures that fall under the regulations of the BSIG for the first time, the documentation of compliance according to Section 8a (3) BSIG must be provided within two years. On the other hand, the obligation to implement the security measures pursuant to Section 8a (1) BSIG and the obligation to report incidents pursuant to Section 8b (4) BSIG is immediate.

[19] https://www.bsi.bund.de/dok/158698

If, in addition to the systems already registered, the KRITIS operator registers new systems during the annual audit, they may combine all systems in one inspection, provided that the respective official due dates for documentation of compliance are not exceeded.

6.1.2 Subsequent documentation and implementation due dates

Operators of critical infrastructures that are already covered by the BSIG and have at minimum provided documentation of compliance in accordance with Section 8a BSIG must continue to provide subsequent documentation every two years. In principle, the documentation process is ongoing, i.e. the submission of documentation of compliance immediately leads to the obligation to provide subsequent documentation. When calculating the time periods, the date of the previous submission is definitive.

If any documentation of compliance proves to be incomplete in the course of the BSI review and additional submissions are required, this does not affect the due date calculated initially for the subsequent documentation.

Calculating the due date for additional documentation:

If documentation of compliance is submitted, the due date for the subsequent documentation is always calculated to the day, based on the date of submission. The date of submission is communicated to the operator in the confirmation of receipt. The official due date for submitting the additional documentation is calculated from the date of submission (e-mail receipt or postmark) plus two years. Whether all necessary compliance documentation was actually submitted at the time of submission (see Section 6.2.2 "Which supporting documentation must be submitted?") or whether documentation is submitted subsequently does not affect the calculation of the due date.

Example:

- Expiry of the period for providing the documentation of compliance according to Section 8a (3) BSIG 1: 01/04/2020
- Submission of the compliance documentation: 16/03/2020
- Expiry of the period for providing the subsequent documentation according to Section 8a (3) BSIG: 16/03/2022

A KRITIS operator can submit the compliance documentation at any time before the end of the official due date for documentation of compliance. If, for example, a KRITIS operator wishes to adapt its obligation to provide documentation of compliance in accordance with Section 8a (3) BSIG to its annual ISO 27001 audit cycle and carry out the audits jointly, it may also submit its documentation annually. The statutory two-year regulation is a minimum requirement.

6.2 Submission of the compliance documentation

KRITIS operators must confirm to the BSI that the requirements of Section 8a (1) BSIG have been met by submitting the corresponding documentation of compliance. In order to assess the appropriateness of the audit, the suitability of the provisions for the prevention of errors and the severity of the security deficiencies identified, the compliance documentation must contain all the required information.

6.2.1 Who submits compliance documentation?

The KRITIS operators provide the BSI with information on the type and scope of the audit carried out for each system and a list of the security deficiencies discovered during the audit. This compliance documentation must be submitted to the BSI in writing. A digital, machine-readable copy must be made available to BSI.

6.2.2 Which supporting documents are to be submitted?

In order to clearly present all necessary information on the type and scope of the audit carried out and to simplify the process of recording, the BSI provides documentation forms (forms KI and P) and recommends their use when submitting compliance documentation. The forms, including the necessary attachments, comprise the cornerstone of the documentation of compliance sent by the KRITIS operators to the KRITIS office of the BSI.

Form KI contains information on the audited critical infrastructure and the contact person at the operator. Form KI must be completed and signed by the KRITIS operator.

Form P includes details of the audit implementation (Section PD), the audit result and the security deficiencies detected (Section PE) as well as the auditing body and audit team (Section PS). Form P is completed and signed by the auditing body.

When submitting the documentation, it must be ensured that the system designation corresponds to the systems previously registered with the BSI.

The forms listed, the minimum requirements for a list of deficiencies and any necessary self-declarations are published on the BSI website[20].

Note: In principle, it makes sense to provide the systems (documents) to be submitted together with Form P with the operator ID and their designation. Files should be named accordingly. *Suggested file name structure: <Operator-ID>_System_PD.A).*

KRITIS operators with several systems can submit compliance documentation to the BSI grouped together for all systems. If the fields provided in the forms are not sufficient for system designation, the systems can be collated on a separate sheet. It is important that the systems are named as registered with the BSI. The supporting documents for individual systems can also be submitted separately.

[20] https://www.bsi.bund.de/dok/128146

A KRITIS operator must always provide and submit the compliance documentation for all its systems that are currently in the documentation process.

The submission of the audit report is not a mandatory requirement when submitting the compliance documentation initially. A KRITIS operator is only required to submit the detailed audit report to the BSI as an additional submission when this is requested by the BSI.

6.2.3 How can compliance documentation be submitted?

Compliance documentation must be submitted to the BSI KRITIS office as the central point of contact. This compliance documentation must be submitted in writing. A digital, machine-readable copy must be made available to BSI. In principle, documentation can be sent by post or e-mail to the KRITIS office (kritis-buero@bsi.bund.de). The BSI recommends encrypting the compliance documentation for confidential transmission by e-mail. The required public S/MIME certificate or the PGP key of the KRITIS office are provided in the download area on the BSI website[21].

6.2.4 Response and confirmation of receipt from the BSI

KRITIS operators will receive a confirmation of receipt from the BSI for submitted compliance documentation as soon as these have been successfully checked for completeness. The confirmation of receipt shall state the date and the systems for which compliance documentation was submitted and shall be deemed formal proof that the KRITIS operator has complied with its legal obligation to submit the compliance documentation in accordance with Section 8a (3) BSIG. It also contains the date on which the KRITIS operator must provide subsequent documentation (see Section 6.1.2).

If no further enquiries are necessary for documentation of compliance or no further cooperation of the KRITIS operator is required for subsequent auditing, the KRITIS operator will not receive any further notification of the procedure after the confirmation of receipt detailed above. The BSI can, however, request further parts or the entire documentation and the audit report on which the audit is based at any time, or schedule on-site audits, irrespective of the specific reason.

In principle, further documentation checks can be carried out up to the submission of the subsequent documentation depending on available capacities and at the discretion of the BSI. As this procedure does not provide for the completion of the documentation check, the BSI does not issue any confirmation of the completion of the documentation check.

6.2.5 Additional submissions

In the course of documentation checks, the BSI may request certain documents. The BSI reserves the right to request additional documents at any time even after the confirmation of

[21] https://www.bsi.bund.de/dok/126450

receipt has been sent. Subsequent requests are generally associated with a submission due date that depends on the type and scope of the additional submission.

Additional submissions do not affect the official due date calculated for the subsequent documentation of compliance.

6.2.6 Audits by the BSI

In accordance with Section 8a (4) BSIG, the BSI can check if the KRITIS operators meet the requirements of Section 8a (1) BSIG. An audit may be triggered by discrepancies in the documents submitted pursuant to Section 8a (3) BSIG which the BSI would like to clarify with the operator, or by the selection of the system as an audit object within the framework of a random sample selection. An on-site audit at the operator's premises is an essential part of these reviews.

7 Document/system overview

The complete documentation of compliance in line with Section 8a (3) BSIG should include the following documents:

- Compliance documentation KI signed by the operator
- Compliance documentation P signed and stamped by the auditing body
- Annex PD.A: Description and graphic presentation of the scope of the audit in a network/system plan
- Annex PD.B: Gap Analysis Plan
- Annex PE.A: List of security deficiencies including implementation plan to eliminate them
- Annex PS.A: Documentation of additional audit process competence for Section 8a BSIG
  - **a)** for (at least) one auditor from the audit team
  - **b)** for an employee of the auditing body responsible for the audit (if not already covered by a))
- Annex PS.B: Declaration of independence for all members of the audit team (no prescribed form)

Optional Annexes

- Annex PD.C: Description of the audit basis (insofar as no or only a partial B3S is used)

Annex A

Basic ethical principles

In order to create confidence in an objective audit, compliance with the "basic ethical principles" is necessary. Both the individual auditors and the auditing body must comply with the "basic ethical principles". They include the following principles:

- **Integrity and confidentiality**
  Integrity establishes trust and thereby creates the basis for the reliability of a decision. Since sensitive business processes and information can often be found in the environment of information security, the confidentiality of the information obtained within the scope of an audit and the discrete handling of the information and results of the audit are essential. Auditors appreciate the value and the ownership of the information obtained and do not disclose this information without the corresponding authorisation, unless there are legal or professional obligations to do so.
- **Professional competence**
  Auditors only assume those tasks they have the necessary knowledge, skills and the corresponding experience for and use the aforementioned when doing their work. They continuously improve their know-how and the efficiency and quality of their work.
- **Impartiality and diligence**
  An auditor must demonstrate the utmost expert impartiality and diligence when merging, evaluating and forwarding information about audited activities or business processes. All relevant circumstances have to be assessed on a balanced basis and may not be influenced by the auditor's own interests or by third parties.
- **Objective reporting**
  An auditor is obliged to provide the customer with true and accurate reports of the examination results. This includes objective and comprehensive reporting of the circumstances in the audit reports, constructive evaluation of the circumstances reported and specific recommendations for improvement of the safeguards and processes.
- **Documentation of compliance and comprehensibility**
  The rational basis necessary in order to arrive at reliable and comprehensible conclusions and results is the unambiguous and logical documentation of the circumstances. This also includes a documented and comprehensible methodology (Gap Analysis Plan, report) used by the audit team in order to arrive at its conclusions.
- **Independence and neutrality**
  An auditor must carry out the audit impartially and free of instruction. The audit results must be documented transparently. Each audit team should consist of at least two auditors in order to guarantee independence and impartiality ("two-man rule"). For reasons of independence and neutrality, the members of the team must not have previously been directly involved in an advisory or executive capacity in the audited area, e.g. in the creation of concepts or the configuration of IT systems.

Annex B

Example of a table with information on the audit procedure

Date	**Time (from-to)**	**Location (site)**	**Audit topics**	**Reference to audit basis**	**Audit technique**	**Audit object *(functions / departments / areas / processes / systems / IT system)***	**Auditors involved**	**Process owner**
Audit day	*Duration of audit topics*	*Site of the audit object The site/system must be allocated to the scope*	*Audited topic/topic area*	*List of the concretely used sections/modules of the audit basis*	*A list of the audit techniques use: e.g. inspection, document check, interview...*	*Audit object 1-n* *A new line should be completed for each topic area*	*A list of the auditors involved in the audit topics*	*KRITIS operator process owner for the audit topic*
02/12/2019	11:00-12:00	Operations control centre, City X	Technical information security	ISO 27001 A.7.1, B3S Section 5	Visual inspection, checks of official documents	Documents: • Absicherung_von_Netz-übergängen.docx (Protection of network gateways) • Zonenkonzept.docx (zone concept) Systems: • VPN concentrator • Firewall Cluster	Joe Bloggs	Network Administrator

Annex C

Requirements for the description and presentation of the scope (to assist with Section 5.2)

- G01: The system is described in a recognisable and transparent way.
- G02: The parts of the essential service provided by the operator are described in a recognisable and transparent way.
- G03: The presentation contains all essential features of the system category.
- G04: All processes relevant to the essential service are recorded.
- G05: All systems, components and applications relevant for the essential are recorded.
- G06: All areas of KRITIS can be seen from the submitted scope.
- G07: The limits of the scope are clearly visible.
- G08: The interfaces to processes, systems, components and, if applicable, applications outside the scope are described in a recognisable and transparent manner.
- G09: The dependencies on processes, systems, components and, if applicable, applications outside the scope are described in a recognisable and transparent manner.
- G10: The parts of KRITIS operated by third parties are described in a recognisable and transparent manner.
- G11: The scope enables an assignment between processes and associated necessary systems, components and, if applicable, applications.
- G12: The scope is presented in a network structure plan.
- G13: Additions to the network structure plan that are necessary for comprehensibility have been made in writing.

Requirements for the presentation of the scope through a network structure plan (to assist with Section 5.2)

- N01: The network structure plan provides an overview of the scope.
- N02: All relevant systems, components and applications are shown.
- N03: The level of abstraction has been chosen appropriately.
- N04: The relevance of individual elements of the network structure plan for the essential service is clearly presented.
- N05: All external communication interfaces are shown.
- N06: Maintenance interfaces are mapped if they are permanently enabled.
- N07: The network structure plan shows any existing division into sites.
- N08: The IT connections between different sites are shown.
- N09: Outsourced services are shown.
- N10: Functional designations and legends are available if necessary and are comprehensible.

Annex D

Template of a list of deficiencies

List of deficiencies						Implementation plan[22]				Assessment of the safeguard by the auditor(s)	
ID[23]	**Deficiency description[24]**	**Classification of the deficiency: Topic[25]**	**Classification of the deficiency: Severity[25]**	**KRITIS-reference[26]**	**KRITIS-risk[27]**	**Safeguards**	**Persons responsible**	**Time period**	**Status**	**Suitability of the safeguard**	**Reason for non-suitablity of the safeguard**
1	The corporate policy on password complexity is not applied to ERP systems. Users, especially administrators, are obliged to use complex passwords for organisational reasons. However, this is not technically enforced.	Technical information security	Minor deviation	ERP system for treatment/ ordering/ distribution/ circulation	Taking over a privileged account can have a significant impact on the availability of the essential service, but administrative access is only possible from an isolated and secured administration network. Non-privileged accounts have limited rights and can only cause minor disruption. Anomalies would be detected and promptly controlled by a SIEM.	The adoption of the password guidelines is commissioned as a change by the ERP manufacturer	IT-SiBe, ERP manufacturer, ERP administration	Q3 2018	50 %	the safeguard is suitable	
2	...	...	...	...	...	...	...	...	...	...	...

[22] Implementation plan: action plan and timetable for remedial action; with responsibility if required
[23] A unique reference or identifier to facilitate communication of deficiencies
[24] Deficiency description: A comprehensible description of the security deficiency with a summary heading
[25] Classification of the deficiency: The categories set out in Annex E are used for the classification of the deficiency by topic; multiple selection is possible
[26] Reference to the part of KRITIS, including a specific reference to the audited system on which the security deficiency has or could have a concrete effect. Limited to the most important subsystems or an overview-like description if there are far-reaching effects
[27] An assessment of the security deficiency, described in words or as a classification, for the provision of the essential service

Annex E

The following categories should be used for the classification of deficiencies by topic:

1. Information Security Management System(ISMS)
2. Asset management
3. Business continuity management for the essential service
4. Technical information security
   - 4.1 Protection of network gateways
   - 4.2 Secure interaction in the Internet
   - 4.3 Secure software (avoidance of open vulnerabilities in particular)
   - 4.4 Secure and reliable hardware
   - 4.5 Secure authentication
   - 4.6 Encryption
   - 4.7 Miscellaneous
5. Personnel and organisational security
6. Structural/physical security
7. Incident identification and processing
8. Review during live operation
9. Suppliers, service providers and third parties
10. Industry-specific technology and (core) components (procurement, development, use, operation and maintenance)

Glossary

Term	Definition
appropriate	Organisational and technical provisions shall be appropriate if the time and expense required are not disproportionate regarding the consequences of failure or an impairment of the critical infrastructure concerned.
audit	The appropriate documentation that the safeguards have been implemented by the KRITIS operator. It is performed by independent and qualified auditors of an auditing body. The term “audits” includes audits and certifications according to Section 8a (3) BSIG.
audit object	The audit object comprises the IT systems, components and processes, roles and persons, respectively, that are key for the functionality of the critical infrastructures operated and which influence these.
audit processes	The method according to which the auditing body provides the documentation of compliance.
audit report	Document of the auditing body containing the entire audit or certification results.
audit team	Team put together by the auditing body which has the necessary competence to check whether the KRITIS operator has implemented the measures in line with Section 8a (1) BSIG.
auditing body	Organisation that assembles the audit team that provides part of the documentation of compliance by checking whether the KRITIS operator has implemented the measures according to Section 8a (1) BSIG.
competence	A trained skill allowing a person to perform certain work.
compliance documentation	The compliance documentation consist of the KI and P forms and the associated annexes, the results of the audits, tests or certifications carried out, including the security deficiencies detected and the information required for processing.

Term	Definition
critical infrastructure	See definition in BSIG or specification in the BSI KRITIS Regulation
deviation	Non-conformity Indicated security deficiencies are considered deviations.
documentation of compliance	The documentation of compliance comprises the complete compliance documentation.
essential service (kDL)	Essential services are important, sometimes essential goods and services for the population. An impairment of these essential services would cause significant shortage of supply, disruptions to public order, safety and security or other comparable dramatic consequences.
Gap Analysis Plan	Document in which the auditor defines the framework conditions for the audit before starting the audit. The contents include the audit process and the audit methods, respectively, and defined random sampling.
industry-specific security standard (B3S)	According to Section 8a (2) BSIG, operators of critical infrastructures and their industry associations have the option to propose industry-specific security standards (B3S) to guarantee the requirements according to Section 8a (1) BSIG.
KRITIS operators	Operator of a critical infrastructure according to Section 2 (10) BSIG, Section 1 (2) BSI-KritisV).
safeguards	The appropriate organisational and technical provisions which must be implemented to meet the requirements of the BSIG to avoid disturbances to the availability, integrity, authenticity and confidentiality of IT systems, components or processes according to Section 8a (1) BSIG. These provisions also include infrastructural and personnel safeguards. Particularly critical processes require specialist security safeguards.
scope	The scope of the documentation of compliance covers the critical infrastructure or the essential service fully (see Section 2 “Audit object”). It describes all related processes, systems, components and organisational units.

Term	Definition
security deficiencies identified	Necessary measures identified within the scope of the audit that are not or only partially implemented. Security deficiencies identified must be assigned “degrees of severity” accordingly (see deficiency categories).
system	Critical infrastructure as defined in the BSI KRITIS Regulation