Bundesamt
für Sicherheit in der
Informationstechnik

Information security audit (IS audit)

- A guideline for IS audits based on IT-Grundschutz

German Federal Office for Information Security
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: isrevision@bsi.bund.de
Internet: http://www.bsi.bund.de

Table of contents

Table of figures

1 Introduction

1.1 Version history

Date	*Version*	*Changes*
September 2008	**1.0**	

1.2 Objective

Many business processes are supported electronically, and large amounts of information are stored digitally, processed digitally, and transmitted over IT networks, which means businesses, administrations, and citizens depend on the proper operation of the information technology used. For this reason, information security is a must for everyone today. For companies and government agencies, this means, among other things, that an appropriate information security management must be implemented to counteract the increasing threats to the availability, confidentiality, and integrity of information, business processes, applications, and systems. The information security audit (IS audit) is part of every successful information security management. Only by revision of the implemented safeguards and the information security process on a regular basis, it is possible to form an opinion on their effectiveness, up-to-dateness, completeness, and appropriateness, and therefore on the current status of information security. The IS audit is therefore a tool for determining, achieving, and maintaining a proper level of security in an organisation.

The main task of the IS audit is to provide the management, the IS management team, and in particular the IT Security Officer with support when implementing and optimising information security. The audits are intended to improve the level of information security, avoid improper information security designs, and optimise the efficiency of the security safeguards and security processes. This ensures the operability, reputation, and assets of the organisation. The result of an IS audit, the IS audit report, shows in compact form the security status in the organisation, possibly together with the actions required to be taken based on the existing security deficiencies, and is used as an aid during the subsequent optimisation process performed on the information security management system (ISMS). The IS audit report is a source of information for management and a tool that can be used by anyone responsible for security.

1.3 Target group

This document is intended to be read by all persons responsible for initiating or performing IS audits based on IT-Grundschutz. This group may include, for example, auditors, ISO 27001 auditors, the organisation’s management, the IT Security Officer, or any other persons responsible for IT security. The primary target audience is the group of office managers in federal agencies who are responsible for regular IS audits as well as the IS auditors who actually perform the corresponding audits.

For the IT Security Officer and any other persons responsible for IT security, this guide should serve in particular to provide an overview on the subject of IS audits, examine the security aspects to be tested, and familiarise these persons with the procedure to follow when performing an IS audit.

The guide provides IS auditors with concrete specifications for performing an IS audit. Chapter 4 ”Performing an IS audit” focuses on these specifications in particular.

1.4 Application

This guide for an information security audit on the basis of IT-Grundschutz is a module for implementing the ”National Plan for Information Infrastructure Protection”, referred to in the following as the ”National Plan” [BMI1], and the ”Implementation Plan for the Federal Administration” (RESTRICTED referred to in the following as the ”Federal Implementation Plan”). It forms the basis for performing IS audits in federal agencies. The goal of the Federal Implementation Plan is to establish medium-term and long-term information security at a high level throughout the entire federal administration to guarantee a reliable and functioning information infrastructure for the federal administration in the future. The Federal Implementation Plan and the National Plan were created by the German Federal Ministry of the Interior (BMI) and apply to all federal departments and their domains.

The goal of this document is to illustrate the importance of the IS audit in the security process and to explain in detail the tasks associated with the IS audit. On the one hand, the guide illustrates how an organisation can establish the IS audit in the organisation and which activities need to be carried out by the organisation in conjunction with the IS audit, for example evaluations of IS audit reports or the planning and co-ordination of the IS audits. On the other hand, the IS auditors are provided with a practical guideline containing concrete specifications and information on how to perform an IS audit as well as on how to produce the report. In addition, it is to be used as the basis for the call for tenders for IS audit services. Standardisation of the procedure used for an IS audit is intended to ensure a constant, high level of quality of the audits. Furthermore, the introduction of this audit procedure allows to assess the status of information security of the organisation and to retrace long-term developments.

In section 2.1, the relationship between the information security process and the IS audit is explained after providing a general overview of the IS audit procedure. In addition, different types of IS audits are presented, and general auditing principles are described. Chapter 3 explains the elements of the IS audit. This includes organisational instructions for the organisation, the illustration of each phase of an IS audit, descriptions of the tasks resulting from the introduction of regular IS audits, and information on evaluating and processing the results of the audit. Chapter 4 describes how to carry out an IS audit (which can be performed by internal personnel as well as by contracted IT security providers) as well as the reporting requirements. Chapter 5 closes with information on the auditing aids available.

1.5 The relationship between the IS audit and the IT audit

There are numerous publications of standards and guidelines as well as general literature available on the subject of audits, and in particular IT audits. Such publications are available from, for

example, the German Institute of Auditors (IDW), the German Institute of Internal Auditors (IIR), the Information System Audit and Control Association (ISACA), and international organisations such as the International Auditing and Assurance Standards Board (IAASB) or the Institute of Internal Auditors (IIA). These publications take IT, as an important component of a company, and its security into account in the test specifications.

The main object of an IT audit used to be the examination of the IT-supported accounting systems. This point of view is not taken any more today since it has been realised that current systems are highly networked and that numerous dependencies exist between the systems and the business processes. For this reason, the entire IT infrastructure of an organisation is now examined when performing an IT audit or an IS audit.

In contrast to the IS audit, in which the test criteria focus mainly on information security (including the appropriateness of the security safeguards), the IT audit examines information security as well as the efficiency (IT process, IT organisation, security safeguards) and correctness (following basic accounting principles such as completeness, correctness, timeliness, reproducibility, orderliness) of the IT. In the IT audit, the three test criteria of efficiency, security, and correctness are equally important. How these three goals are weighted is determined individually by the organisation or by the auditor and depends on the strategy followed by the company or government agency as well as on the concrete mission.

In contrast, the IS audit, as a ”new” auditing discipline, places emphasis on a holistic examination of information security. This means that all levels, from the establishment of an information security organisation through personnel issues to system configurations, are checked. The audit criteria efficiency and correctness are considered as secondary criteria in this context.

If an organisation already has implemented an IT audit process internally, the large number of common aspects allows to perform the IS audit together with the IT audit if the requirements in this guide are taken into account.

Section 2.2 deals with the interaction between the IS audit and certification according to ISO 27001 based on IT-Grundschutz.

1.6 Terminology

The following terms are used in this document:

The task of the **audit** [German: Revision] is in general to check business processes including the tools they apply with respect to their correctness, security, orderliness, lawfulness, and usefulness.

In contrast to a general audit, the **IS audit** [German: IS-Revision] focuses on information security in the organisation. The goal of an IS audit is to have an independent party determine the current level of security throughout the organisation and point out any existing security gaps and deficiencies. The IS audit is a special type of the (general) audit. The result is an IS audit report with recommendations for improving the level of information security.

In the IS audit, the **risk-based approach** to auditing is used (see [IDW]). This means that the areas subject to a higher level of risk are tested more intensively and more frequently than the areas with lower risk level. On this foundation, the testing strategy is developed, and the IS audit plan is then derived from this strategy.

The **IS audit plan** describes the entire examination procedure, from the initial selection of the module target objects to the documentation of the on-site examination. To prevent confusion with audit plans in other areas, the test plan used in conjunction with an IS audit is always referred to as the IS audit plan in this document.

The term **safeguard** in this document refers to the IT baseline safeguards as well as the additional security safeguards to be implemented based on a risk analysis and on any existing regulations.

The term **module target object** refers to a specific audit object or a group of audit objects as described in BSI Standard 100-2, section 4.2.1, to which a certain module is applied (e.g. module 3.209 ”Clients under Windows XP” is applied to a group of 10 Windows XP clients in the Personnel Administration Department).

Critical business processes are special tasks that are very valuable to the organisation. Classification into uncritical, less critical, critical, and highly critical business processes can proceed similarly as for given damage scenarios from the defining protection requirements determination (see [BSI2]). All business processes classified as critical or highly critical are entered into a list of critical business processes (for more detailed information, see BSI Standard 100-4 Emergency Management [BSI3]).

This document uses the term **”organisation”**. Organisation is used as a general term for government agencies, companies, and other public or private organisations.

All personal pronouns used in this document refer equally to men and women. If the male form of a term is used, it is to simplify readability.

1.7 References

[BMI1] German Federal Ministry of the Interior, National Plan for Information Infrastructure Protection (NPSI), July 2005, www.bmi.bund.de

[BMI2] German Federal Ministry of the Interior, National Plan for Information Infrastructure Protection in Germany, Federal Implementation Plan (“VS – Nur für den Dienstgebrauch” - RESTRICTED), September 2007

[BMI3] German Federal Ministry of the Interior, General Administrative Instructions for the physical and organisational protection of classified material, June 2006, www.verwaltungsvorschriften-in the-internet.de

[BMWI] German Federal Ministry of Economics and Technology, Handbuch für die Geheimschutz in der Wirtschaft (Mannual for Classified Information in Business), November 2004, www.bmwi.de

[BSI] German Federal Office for Information Security, IT Security Management and IT-Grundschutz - BSI Standards, 2008, www.bsi.bund.de/gshb

[BSI1] German Federal Office for Information Security, Information Security Management Systems (ISMS), BSI Standard 100-1, Version 1.5, May 2008, www.bsi.bund.de/gshb

[BSI2] German Federal Office for Information Security, IT-Grundschutz-Methodology, BSI Standard 100-2, Version 2.0, May 2008, www.bsi.bund.de/gshb

[BSI3] German Federal Office for Information Security, Notfallmanagement [Emergency Management], BSI Standard 100-4, Draft, 2008, www.bsi.bund.de/gshb

[BSI4] German Federal Office for Information Security, Risk Analysis based onIT-Grundschutz, BSI Standard 100-3, Version 2.5, May 2008, www.bsi.bund.de/gshb

[GSK] German Federal Office for Information Security, IT-Grundschutz Catalogues -Standard Security Safeguards, BSI, reissued annually, http://www.bsi.bund.de/gshb

[IDW] German Institute of Auditors, IDW PS 261 ”Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisken” (”Determination and evaluation of the risks of errors and the reaction of the final auditor to the error risks evaluated”), September 2006, www.idw.de

[SÜG] German Act on Security Clearance Checks (Sicherheitsüberprüfungsgesetz (SÜG)), February 2008, www.gesetze-im-internet.de

[ZERT] German Federal Office for Information Security, ISO 27001 Certification based on IT-Grundschutz – Audit Scheme for ISO 27001 Audits, Version 2.1, March 2008, www.bsi.bund.de/gshb

2 Introduction to the IS audit

2.1 Overview of the IS audit

Federal agencies in Germany are required to fully implement IT-Grundschutz according to the specifications of the Federal Implementation Plan. In addition to being required to create and implement a security concept, they are also required to follow the specifications in BSI standards 100-1 [BSI1] and 100-2 [BSI2] as well as to check the success of their implementation through IS audits. In order to maintain and continuously improve information security. The organisation's management is responsible for the initiation and management of the information security process, including IS audits as integral part of the information security management process.

Figure 1: Set of criteria and standards for the IS audit

The following overview illustrates the main set of criteria and standards for the IS audit.

The IS audit checks the effectiveness of the security organisation as well as the appropriateness and implementation of the organisation's security concept. The security strategy and the implementations of technical, organisational, and personal safeguards are examined (see [BMI2]).

IS audits should be performed regularly. Federal agencies are obligated by the Federal Implementation Plan to perform a comprehensive IS audit at least every 3 years. This audit must always examine all aspects of the organisation taking all IT-Grundschutz layers into account.

The existing information security documentation (for example the information security concept, network plan, and basic security check) is used as the basis for the IS audit.

The minimum requirements for IS audits according to the Federal Implementation Plan are fulfilled by performing the audit based on the following IT-Grundschutz layers:

- Layer 1 - ”Generic aspects”
- Layer 2 - ”Infrastructure”
- Layer 3 - ” IT Systems”
- Layer 4 - ”Networks”
- Layer 5 - ”Applications”

An IS audit can be performed by employees of the organisation itself (internal audit) or by third parties (external audit). It is important that the auditors performing the IS audit did not participate in the design, development, or implementation of the safeguards for the object under examination.

The result of the IS audit is the IS audit report, which contains information on the information security status and possibly recommendations for improvements or modifications to IT security safeguards, structures, and processes. The IS audit therefore supports the organisation’s management in its overall responsibility, as well as the security management as the IS audit report provides an additional tool indicating need for action.

2.2 Integration into the ISMS process

Practical experience has shown that comprehensive, company-wide or agency-wide information security oriented towards long-term fulfilment of requirements and sustainable limitation of the risks can only be achieved through information security management. BSI Standard 100-1 ”Information Security Management Systems (ISMS)” (see [BSI1]) describes the information security process. Within the ISMS, the IS audit is part of the information security process and is integrated into “Check” phase of the PDCA model by Deming.

The information security process is initiated by the management level and starts with the ”Planning” phase. The security organisation is planned in this phase.

In the subsequent ”Do” phase, the security concept is created and the necessary safeguards are implemented.

The following ”Check” phase serves to check the IT security strategy, the IT security organisation, the security concept, and the implementation of the safeguards. The security concept is always used as the basis for the tests for success in the ”Check” phase. One possible method for testing for success is the IS audit.

process. They point out to the organisation where urgent action needs to be taken and which security deficiencies should be handled with priority. If individual information systems of the organisation are ISO 27001-certified on the basis of IT-Grundschutz, then it is recommended to jointly conduct the re-certification and the IS audit if possible for these systems. Knowledge gained from surveillance audits or certification procedure can be used for the IS audit.

2.3 Different types of IS audits

There are different types of IS audits. This document distinguishes between IS cross-cutting audits and IS partial audits.

An IS cross-cutting audit has a holistic approach and a wide range of tests and examinations. In an IS cross-cutting audit, all layers of the IT-Grundschutz concept are tested based on spot checks or selected samples.

The object tested in the IS cross-cutting audit is always the entire organisation. The goal of a IS cross-cutting audit is to obtain a comprehensive impression of the information security status of the organisation. The IS cross-cutting audit is the IS audit required to be performed by federal agencies according to the Federal Implementation Plan.

A IS partial audit is limited to a certain section of the organisation and is initiated, when necessary, by the IS management team. The tests performed in this case are much more in-depth than those performed in the IS cross-cutting audit.

The IS partial audit is an IS audit triggered whenever necessary, for example after large scale restructuring, security incidents, or when new business processes or new technologies are introduced. The IS partial audit is particularly suitable for auditing critical business processes.

Since a IS partial audit is limited to certain business processes or IT procedures, only the systems used in connection with these business processes or IT procedures and the applicable IT-Grundschutz modules (for short: module target objects - section 1.6) are examined. This allows more rigorous testing. Depending on the scope of testing defined, it may make sense to examine selected samples or fully examine all applicable safeguards when performing a IS partial audit. Furthermore, the same rules and procedures apply to the IS partial audit as to the IS cross-cutting audit.

2.4 Key aspects of the IS audit

The IS audit team is independent and objective. The team provides the organisation with support to reach its goals by evaluating through a methodical and targeted approach, the effectiveness of the security process and by providing support to improve it.

A basic requirement for any audit, and therefore for the IS audit as well, is the unrestricted right to obtain and view information. This means that no information may be withheld from the IS audit team. This also includes the right to view sensitive or classified information related to the information security management and the IT operations provided that the IS audit team can provide plausible reasons for the need to know. In the latter case, the IS audit team must have an adequate

security clearance and be authorised in accordance with the ”General Administrative Instructions for the Physical and Organisational Protection of Classified Material” issued by the Federal Ministry of the Interior (VSA - see [BMI3]) and the ”*Handbuch für die Geheimschutz in der Wirtschaft*” (see [BMWI]), where the clearance level depends on the level of confidentiality of the corresponding information.

The IT-Grundschutz Catalogues (see [GSK]) and the BSI standards (see [BSI]) are the standard references for IS audits. If these references do not contain information relating to the implemented technologies you use, then other relevant regulations, laws, standards, or manufacturer specifications apply. The use of these references is to be documented and accounted for justified.

Every IS audit team should consist of at least two IS auditors to guarantee the independence and objectivity of the audit (”two-person rule”). Important IS audit meetings such as the opening and the closing meetings as well as the interviews should be conducted as a team. This procedure ensures objectivity, thoroughness, and impartiality. No member of the team, for reasons of independence and objectivity, should have participated directly in supporting or managing the areas to be audited, e.g. they must not have been involved in the development of concepts or the configuration of the IT systems.

The IS auditors require a wide range of knowledge as well as in-depth knowledge in the field of information security. Continuous further education and training of the IS auditors is a basic prerequisite for their work. Verification of such qualifications in the form of certificates (e.g. Audit Team Leader for ISO 27001 audits based on IT-Grundschutz) are suitable for this purpose.

In general, it should be ensured that actual operations in the organisation are not significantly disrupted by the IS audit when initiating the IS audit. IS auditors never actively intervene in systems, and therefore do not provide any instructions for making changes to the objects being audited.

2.5 Professional ethics

To gain trust in an objective audit, it is necessary to uphold a set of professional ethics. The professional ethics must be upheld by individual persons as well as by companies providing services in the field of IS auditing. The professional ethics consist of the following principles (see [ZERT]):

- **Honesty and confidentiality**
  Honesty is the foundation of trust and forms the basis for the reliability of an assessment. Since sensitive business processes and information are often found to be dependent on information security, the confidentiality of the information obtained during an audit and the discreet handling of the results and findings of the IS audit are an important basis for such work. IS auditors are aware of the value of the information they receive and who owns it, and will not disclose this information without the corresponding permission unless they are legally or professionally required to do so.
- **Expert knowledge**
  IS auditors only accept those jobs for which they have the requisite knowledge and skills as well as the corresponding experience and use these when performing their task. They continuously improve their knowledge as well as the effectiveness and quality of their work.

- **Objectivity and thoroughness**
  An IS auditor must demonstrate the highest possible level of expert objectivity and thoroughness when collecting, evaluating, and passing on information on the activities or business processes audited. The evaluation of all relevant circumstances must be performed impartially and may not be influenced by the auditor's own interests or the interests of others.
- **Objective presentation**
  An IS auditor has the duty to report the results of the examination precisely and truthfully to his client. This includes the impartial and understandable presentation of the facts in the IS audit reports, the constructive evaluation of the facts determined, and specific recommendations for improving the safeguards and processes.
- **Verifications and reproducibility**
  The rational basis for reliable and comprehensible conclusions and results is the clear and consistent documentation of the actual facts. This also includes that the IS audit team follows a documented and reproducible methodology (IS audit plan, IS audit report) to come to its conclusions.

3 IS audit in the organisation

IS audits should be performed regularly; in federal agencies in Germany at least every 3 years according to the Federal Implementation Plan. For this reason, it is advisable to integrate the IS audit procedure into the information security process of the organisation. The general organisational, personnel, and financial resources are to be ensured, and the corresponding tasks and responsibilities must be assigned accordingly.

3.1 Basics and responsibilities

Organisations should assess their ISMS regularly. This is done e.g. by establishing an IS audit procedure based on the information security concept adopted by the organisation. An ”overview” of the information security status of the organisation can be obtained through regular IS cross-cutting audits, amongst others.

The management level of an organisation always bears the overall responsibility for the IS audit. Management must be informed regularly about any problems as well as of the results and activities of the IS audit, but also on new developments, new or changed general conditions, or possibilities for improvement in order to fulfil their function as a control instance.

One person in the organisation (for example the IT Security Officer) must be named responsible for IS audits. He will then supervise the entire process and the actual execution of the IS audits. This person should have:

- an independent position in the organisational structure of the organisation (to prevent conflicts of interest),
- the right to speak directly to the organisation’s management, as well as
- sufficient knowledge in the field of information security, and in particular of the IT-Grundschutz methodology.

The task of the person responsible for IS audits in the organisation is, among others, to create a rough p**lanning** for the IS audit project based on this guide to be substantiated on an annual basis. Furthermore, this person is the main contact person for an IS audit team during the entire duration of the IS audit and is also responsible in particular for providing the reference documents (see section 4.4) and co-ordinating schedules and personnel/material resources during the on-site examination.

Each of the specifications relating to the IS audit procedure and the assignment of the tasks are to be documented individually in an IS audit manual. This manual should contain the following aspects:

- the strategic goals of the IS audit to be achieved,
- any possible legal regulations and ordinances,
- the organisation of the IS audit in the organisation,

- the resources (in terms of time, finances, and personnel),
- the special conditions and restrictions of the organisation and
- the archiving of the documentation

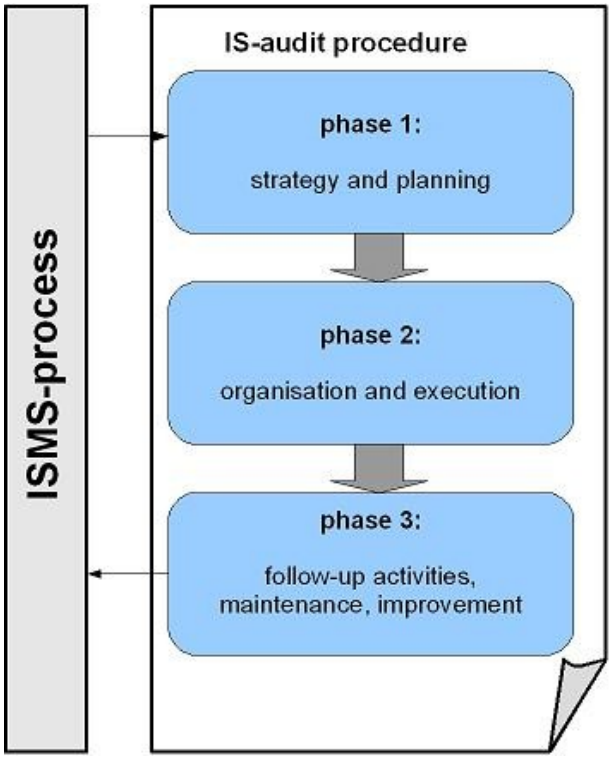

Figure 4: Phases of the IS audit procedure from the organisation's point of view

The IS audit manual is the main foundation and an instruction manual for the IS audit. Since it regulates, among other things, the rights and duties of the persons participating in the IS audit as well as the rights to view information and documents granted to the IS audit team, the personnel representative should be included in the process before it is adopted by the management.

Based on the IS audit manual, the IS audits planned are performed by an internal or external IS audit team (see section 3.3), and the audits are supervised by the person responsible for IS audits in the organisation. The resulting IS audit reports form the basis for follow-up activities intended to maintain and improve the level of information security.

3.2 Planning individual IS audits

An understanding of the business processes and risks of the organisation is the basis for planning and executing IS audits. The rough **planning** and detailed annual plans to be created must

take the protection requirements of the business processes in the organisation as well as the IT used into account. Free reserves should be included in the annual resource plan to allow for additional IS audits after unexpected security incidents.

Basically, it is also possible to split up a IS cross-cutting audit by tasks and locations. In this case, it must be ensured that the requirements of the Federal Implementation Plan and this guide are still fulfilled. When a IS cross-cutting audit is split up into several tasks, the resulting IS audit reports are to be integrated into a single final report by an independent party.

When planning IS audits, it must be noted that the audits can only be planned sensibly when there is a structure analysis according to IT-Grundschutz (see [BSI2]) available for the organisation. This means that:

- the business processes, applications, and information in the organisation have been documented,
- the network plan is available,
- IT systems and similar objects (e.g. routers, switches, printers, fax machines) have been documented,
- and the premises and locations have been documented.

These tasks are basic security management tasks and are part of the security concept. The creation and consistent implementation of the security concept is mandatory for federal agencies according to the Federal Implementation Plan.

The internal expenses incurred for an organisation by an IS audit performed by an external security service provider are generally limited to collecting the existing documents, of organising and co-ordinating the IS audit, allocating to interview the contact persons, and of evaluating the IS audit report.

IS audit cycles

- According to the Federal Implementation Plan, federal agencies are required to perform an IS cross-cutting audit at least once every **3 years**.
- In addition, IS partial audits for critical business processes must be planned.
  Critical business processes, especially those that require high availability according to the BSI compendium ”High Availability”, should be subjected to IS partial audits more often according to the Federal Implementation Plan. The audit interval must be appropriate for the particular criticality.
- Additional IS partial audits can be performed as well, for example as in-depth examinations, after security incidents, after introducing new procedures, or when planning to restructure.

Supervising an IS audit

The person responsible for IS audits is also the person to contact while performing an IS audit. He helps the IS audit team answer organisational and technical questions (for example when organising meetings, when collecting the documents, and when supervising the on-site examination).

The organisational tasks of the person responsible for IS audits in the organisation are shown in the following flow chart.

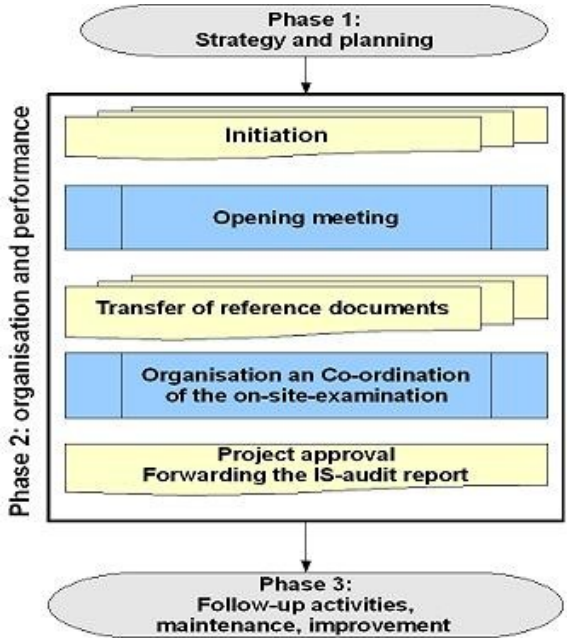

Figure 5: Performing the IS audit from the organisation's point of view

3.3 IS audit team

For each IS audit, a suitable IS audit team is to be assembled. The members of this IS audit team should possess the corresponding technical qualifications as well as the necessary personal qualifications. Aspects to consider when selecting people for an IS audit team are illustrated in sections 2.4 and 2.5. There are various ways to put together an IS audit team in an organisation:

Internal IS audit team:

Depending on the type and size of the organisation, it may make sense to create an internal IS audit team, i.e. to assign a group of people in the organisation to perform the IS audits. This has the

advantage that knowledge of complex organisational structures and procedures is available. However, many organisations do not have the necessary expertise and/or the necessary personnel resources to guarantee effective and independent execution of the IS audits. If the IS audit team is made up of internal employees, then it is recommended to integrate the team into the organisation as a staff function. The right to speak directly to management as well as independence must be guaranteed (see section 2.4).

Co-operations between IS audit teams:

Since not all organisations can afford to form a complete, internal IS audit team, a co-operation with other organisations may make sense. One possible solution to cover all required topics could be to sign co-operation agreements with other organisations to exchange security experts.

Department IS audit team:

Another alternative for federal agencies is to place the IS audit teams or competency centres in one department. The IS audit team could be established centrally in the top federal agency level. The government agencies would then have the ability to access competent IS audit teams with knowledge specific to their area. Information on whether or not an IS audit team already exists in a certain department can be obtained from the corresponding departmental IT Security Officer.

BSI IS audit team:

Federal agencies are entitled to use the corresponding free services provided by the BSI. When there are resource bottlenecks, federal security agencies are given top priority. More detailed information on the IS audit service is offered by the BSI on our web page (www.bsi.bund.de). The BSI can be contacted at sicherheitsberatung@bsi.bund.de to answer questions or co-ordinate schedules.

External ”IS audit” service provider:

External service providers also offer IS audit services. Federal agencies should use IT security service providers accredited by BSI. Information on the corresponding call for tenders procedure can be found in section 3.4.

The BSI is planning to publish a list of all IT security service providers accredited by BSI. In the accreditation process, these service providers are required to prove their trustworthiness and expertise to the BSI.

3.4 Call for tenders procedure

If the organisation to be audited decides to contract an external service provider, then the following aspects should also be taken into account when requesting for tenders in addition to the usual contract awarding rules. This applies especially to federal agencies:

- The IS audit is performed based on the current ”Guide for the IS audit based on IT-Grundschutz”.

- The type of audit, i.e. IS cross-cutting audit or IS partial audit, is to be stated.
  For a IS partial audit, the object to be audited must also be specified precisely (for example: procedure, IT-systems, network, branch office, information domain).

- The time frame in which the IS audit should be performed must be defined.

- Abort criteria are to be defined, where appropriate (see section 4.4).

The object to be audited should be described in detail. This description includes:

- A general description of the organisation (location, number of branch offices, number of employees, tasks / goals of the organisation)

- Naming of the main tasks and processes of the organisation / of the division to be examined / of the information domain to be examined

  - A list of the sites in the organisation to be examined, where applicable

  - A description of the IT systems, applications, and procedures used

  - The type of networking used in the audited division of the organisation

  - The number of critical processes

  - A list of outsourced business processes and IT systems belonging to the object to be examined

The following requirements should be met by the service provider or the IS audit team:

- A wide range of knowledge in the field of IT security

- In-depth knowledge of IT-Grundschutz

- Experience in performing information security audits

- Specific expert knowledge of the audit subject

Since sensitive data of the organisation may need to be disclosed during a call for tenders procedure for an IS audit, a restricted request procedure or limited competition should be performed, depending on the types of activities of the organisation, to guarantee the confidentiality of the information.

Depending on the protection requirements of the information, the service providers and IS auditors may need to verify their trustworthiness in accordance with the German ”Law on Security Clearance Checks” (SÜG - see [SÜG]). Authorisation to view classified materials must be provided, if necessary, by presenting a valid personal security clearance certificate.

It must also be specified in the contract which data used by the service provider must be destroyed, placed in safekeeping, or handed over after the IS audit is finished. A non-disclosure agreement should be signed by the organisation and the service provider.

The intended duration of the IS audit is to be specified in the call for tenders document by the organisation. The duration of a IS cross-cutting audit depends on the size as well as the complexity of the organisation. The size of the organisation is determined by the number of employees and locations, whereby each aspect by itself may lead to the necessity for a more extensive audit effort. The level of complexity is specified using one of three levels: ”normal”, ”high” or ”very high”.

The selection of the level of complexity of an organisation can only be performed on an organisation-by-organisation basis according to the following criteria, for example:

- What does the system landscape look like (number of systems and level of heterogeneity of the systems used)?
- How many network gateways are there?
- Which and how many IT applications are used in the organisation? Are they used to support critical business processes?
- Are higher-level procedures used that may affect realms outside of the organisation?
- How high is the protection requirement for the infrastructure, systems, and IT applications?
- Is the organisation active in areas critical to security (for example, is the organisation a security agency)?

The following values for the personnel resources of the IS audit team, obtained from experience, can be used as a basis for estimating the total time and expense of an IS cross-cutting audit according to the Federal Implementation Plan (see Chapter 4, ”Performing an IS audit”):

Complexity	***Size of organisation: small (up to 100 employees)***	***Size of organisation: medium (up to 500 employees)***	***Size of organisation: large (over 500 employees)***
”Normal”	30 person-days	50 person-days	60 person-days
”High”	50 person-days	65 person-days	80 person-days
”Very high”	60 person-days	80 person-days	100 person-days

Table 1: Standard values for personnel expenses for a IS cross-cutting audit

The times stated are initial rough estimates based on experience gained from previous audits performed by the BSI and other government agencies. The estimated times provided are continuously updated as new experience is gained.

When specifying the duration of an IS cross-cutting audit, no delays, for example due to waiting for documents or scheduling delays, are to be taken into account. The given times are only rough estimates and need to be adapted to reflect the actual conditions present in the organisation. It is assumed that the IS audit will only be performed by an experienced IS audit team. The estimated

times are only applicable in part to IS partial audits since the times for IS partial audits depend highly on the complexity of the section of the organisation to be examined, the audit techniques used, and the depth of testing performed. These estimates cannot be used for estimating the time and expense of ISO 27001 certification based on IT-Grundschutz either.

3.5 Evaluating an IS audit

The results of the IS audit are reported to the management of the organisation, the person responsible for IS audits, and the IT Security Officer (see section 4.9) and integrated into the ISMS process. A clearly defined procedure should be available for this purpose that is stated in a guideline for examining and improving the security process (see [BSI2]). Requirements for eliminating deficiencies and improving quality are the result of the evaluation of the IS audit report. The IT Security Officer derives the corresponding follow-up activities from these requirements. The follow-up activities also include updating the security documents, for example the security concept and the basic security check. In individual cases, additional IS partial audits may be necessary. The rough and detailed IS audit plans are to be adapted accordingly.

The IS audits performed, their results, and a summary of the activities required to eliminate deficiencies and improve quality are to be included into the regular reports provided to management by the IT Security Officer.

4 Performing an IS audit

The following sections explain the tasks of the IS audit team when performing an IS audit from initiation of the project until it is finished. The work required to be done by the organisation is described in detail in Chapter 3.

4.1 Overview

The audit procedure illustrated here should guarantee consistent, high quality IS audits and the ability to compare the results of audits. In all steps, the audit procedure is to be documented by the IS audit team in an orderly and understandable manner.

All working documents created to perform an IS audit for a Federal Agency are to be classified as ”VS – Nur für den Dienstgebrauch” (RESTRICTED). The individual classification is with the office head and the affected assistant advisors, and possibly in co-operation with the Data Protection Officer.

The management of the organisation to be examined initiates the IS audit procedure by awarding the contract.

The methodology is illustrated in the following diagram.

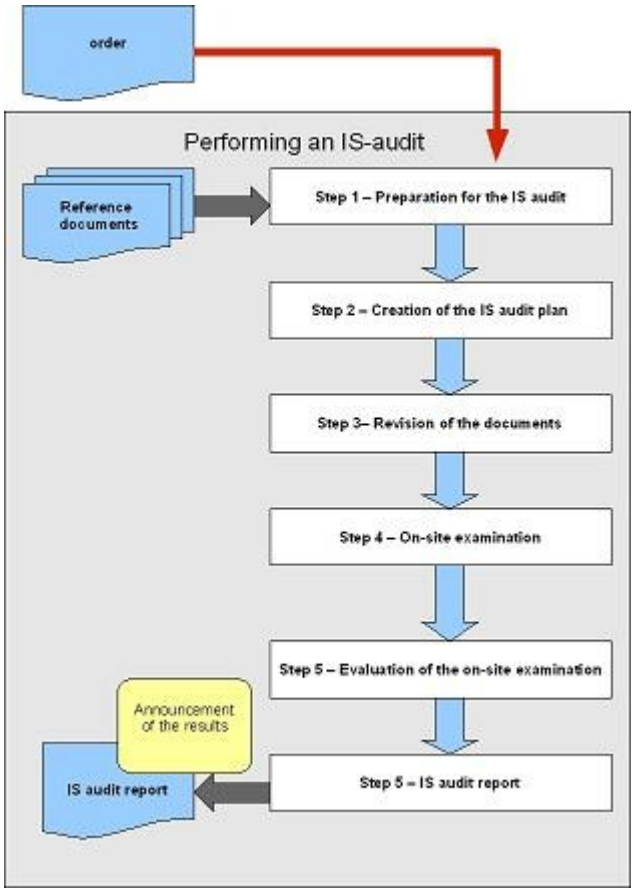

Figure 6: Steps when performing an IS audit

Step 1

At the beginning of the procedure, the most important general conditions are determined and the necessary documents are requested in an opening meeting between the organisation and IS audit team.

Step 2

Based on the documents then made available, the IS audit team gets a picture of the organisation to be examined and creates the IS audit plan.

Step 3

Based on the IS audit plan, the contents of the available documents are assessed. If necessary, additional documents are requested.

Based on the revision of the documents and the IS audit plan (which is updated during this time), the chronological and organisational terms of the on-site examination are co-ordinated together with the contact person in the organisation.

Step 4

The on-site examination starts with an opening meeting with the main participants. After that, interviews are conducted, the site is inspected, and a preliminary evaluation is performed. The on-site examination terminates with a closing meeting.

Step 5

The information obtained during the on-site examination is consolidated further and evaluated by the IS audit team.

Step 6

The results of the IS audit are summarised in an IS audit report at the end of the review. This report is provided to the organisation audited. The estimated amount of work required for each step should be based on the following schedule:

Phase	*Task*	*Time in %*
Step 1	Preparation of the IS audit	**5 %**
Step 2	Creation of the IS audit plan	**15 %**
Step 3	Revision of the documents	**20 %**
Step 4	On-site examination	**35 %**
Step 5	Evaluation of the on-site examination	**5 %**
Step 6	Creation of the IS audit report	**20 %**

Table 2: Relative times required for each step when performing an IS audit

The procedure described here applies to a IS cross-cutting audit as well as a IS partial audit.

4.2 Audit techniques

”Audit techniques” are understood to be all methods used to determine the facts of the matter. The following different audit techniques can be used during an IS audit:

- Verbal questioning (interviews)
- Visual inspection of the systems, locations, spaces, rooms, and objects
- Observations (e.g. things observed incidentally in the context of the on-site examination)
- Analysis of files (including electronic data)
- Technical examination (e.g. testing of alarm systems, access control systems, applications)

- Data analysis (for example of log files, database evaluations, etc.)
- Written questions (e.g. questionnaires).

The audit techniques actually used depend on the specific case and are to be specified by the IS audit team. The IS audit team must ensure during all examinations that the results obtained justify the amount of time and effort taken to obtain them.

If the IS audit team finds deviations from the documented status during the examination of a selected sample, then the number of samples must be increased accordingly to obtain an explanation. The examination is only finished once the deviation has been adequately clarified. Several audit techniques may be applied in combination to determine the reason for the deviation.

4.3 Evaluation scheme

The results obtained for each safeguard tested are to be included in the IS audit plan (see Chapter 5 ”Aids”), and the implementation status of each safeguard must be evaluated.

The evaluation is performed based on the basic security check according to a uniform evaluation scheme (see [GSK]):

- Safeguard implemented:
  ”All recommendations in the safeguard are completely, effectively, and adequately implemented.”
- Safeguard partially implemented:
  ”Some of the recommendations are implemented, others are only partially implemented or not implemented at all.”
- Safeguard not implemented:
  ”The recommendations in the safeguard are not implemented for the most part.”
- Safeguard unnecessary:
  ”The recommendations in the safeguard do not need to be implemented in the manner suggested because there are other adequate safeguards implemented to counteract the corresponding threats (e.g. safeguards that are not listed in IT-Grundschutz but have the same effect) or because the recommended safeguards are irrelevant (e.g. because the corresponding service is not activated)”.

When safeguards are only partially implemented or not implemented at all, the IS audit team must judge (no later than when creating the IS audit report) whether a ”security deficiency” or a ”serious security deficiency” exists in the organisation. A ”serious security deficiency” is a security gap that needs to be closed immediately since there is a great threat to the confidentiality, integrity, or availability of the information, and serious damage is to be expected if the gap is exploited. If there is a ”security deficiency”, then there exists a security gap that needs to be eliminated in the mid-term. The confidentiality, integrity, or availability of the information may be adversely affected. These deficiencies include, for example, documentation required according to the safeguard but which is inadequate or missing completely.

Security deficiencies are to be documented for the safeguards concerned in the IS audit report. If a security deficiency is evaluated and found to be ”serious”, then the reasons for this evaluation must be provided in an comprehensible manner in the IS audit report. In addition, there may be ”security recommendations” provided in the safeguards. These recommendations are suggestions for improving the implementation of safeguards.

Evaluation – Implementation Status (Step 1)	***Evaluation - Security Deficiency (Step 2)***
Safeguard is not implemented	Security deficiency or serious security deficiency
Safeguard is partially implemented	Security deficiency or serious security deficiency
Safeguard is implemented	No security deficiency or security recommendation
Safeguard is unnecessary	No security deficiency

Table 3: Evaluation according to the implementation status and security deficiency

With the two-part evaluation scheme (according to the implementation status and security deficiency), the IS audit team has an instrument at hand that allows to quickly visualise the current information security status in the organisation in detail. The organisation can determine the security status in the particular IT-Grundschutz layer by looking at the number of safeguards (sorted by layer and severity of the security deficiency) found to be deficient. From this information, the organisation must determine in which areas enhanced activity is required in terms of information security. Furthermore, the development of the status of information security in the organisation can be followed over a period of several years.

4.4 Preparing the IS audit (Step 1)

When initiating an IS audit (for example by the IT Security Officer or the person responsible for IS audits), the management of the organisation to be examined must participate. In this stage, the object to be examined is specified, the contract is awarded, and the IS audit team contracted is granted the necessary authorisations (for example authorisation to view documents).

The management of the organisation should inform the worker council or the personnel board of the planned IS audit.

The person responsible for IS audits in the organisation, however, should explain the core functions of the organisation to the IS auditors and provide a brief overview of the IT in use. The first set of general conditions for the on-site examination are to be co-ordinated (when, at which location, organisational questions, etc.). The following reference documents must be provided to the IS audit team by the organisation to be audited since they form the basis for the IS audit:

Organisational documents

- Organigram

- IT framework concept

- Schedule of responsibilities

Technical documents

- Security concept
  The security concept is the main document in the security process and contains, at a minimum, the structure analysis, network plan, defining protection requirements, model according to IT-Grundschutz, basic security check, and the supplementary security analysis. Likewise, the supplementary risk analyses and the implementation plans for the safeguards should be included (see [BSI2]).

- Export of the information security management database, if available (e.g. a GSTOOL database).

- The security policy
  The management is responsible for the efficient and proper functioning of an organisation and therefore for guaranteeing information security internally and externally as well. For this reason, management must initiate, control, and guide the information security process. This includes issuing strategic statements relating to information security, conceptual specifications, as well as general organisational conditions in order to be able to achieve the desired level of information security in all business processes.

- List of the critical business processes
  A list of the critical business processes must be presented. The list of critical business processes is of special importance for the selection of the target objects and the up-dating of the IS audit plan by following the risk-based approach.

- The IS audit reports from the previous six years (if available).

Independent of this list, the IS audit team can request additional documents in paper or electronic form.

If the structure analysis according to BSI Standard 100-2 (see [BSI2] Chapter 2) and a complete and up-to-date network plan are not existing, then it is impossible to perform the IS audit. It is therefore recommended to cancel the IS audit at this point and document the current status in the IS audit report. In such a case, the IS audit should be repeated within one year.

If a structure analysis is available but the defined protection requirements or the modelling are missing, then an auxiliary modelling is to be created by the IS audit team based on the existing documents available. This modelling is only intended for use as an internal aid and tool for the IS audit so that the IS audit can be structured according to the specifications in this guide.

The auxiliary modelling will proceed as instructed in BSI Standard 100-2 (see [BSI2] Chapter 4). Before that, the IS audit team must check the extent to which groups (collections of systems of the same type) have already been formed during the structure analysis to reduce the complexity of the organisation to be audited. If no groups have been formed yet, then the IS audit team is to form these groups to the extent permitted by the documents currently available. The auxiliary modelling

takes place in the next step. Modules in Layer 1 are selected as well as modules to be applied to the infrastructure, the IT systems documented, and the applications. When modelling, the modelling instructions in the IT-Grundschutz Catalogues according to section 2.2 ”Assignments based on the layer model” (see [GSK]) are to be followed. Defining protection requirements for individual systems and applications are not performed in this case. Instead, it is assumed for this audit that the protection requirements are normal. A ”IS basic audit” performed under these general circumstances can only provide an initial idea of where optimisation is required and is not a replacement for an IS cross-cutting audit as required by the Federal Implementation Plan. The audit cycles required by the Federal Implementation Plan (see section 3.2) must be maintained.

4.5 Creating the IS audit plan and screening documents (Step 2)

All reference documents are to be checked for completeness and up-to-dateness.

When evaluating the up-to-dateness of the documents, note that some documents are more generic than others so that updates in the documents may be required more or less often, depending on the document. However, the organisation must evaluate all documents regularly to see if they correspond to the current conditions. The IS audit team checks this procedure by screening documents and where appropriate by comparing them to the results of the on-site examination.

In terms of completeness, the contents of the documents are to be checked to see if all major aspects have been documented and if suitable roles have been assigned. The documents presented must be comprehensible for the IS audit team. In particular, decisions made should be justified comprehensibly.

By screening the documents, the IS audit team obtains an overview of the main tasks, the organisation itself, and the use of IT in the organisation to be examined.

Based on this, the IS audit team begins creating the IS audit plan. This plan is the main tool used throughout the entire audit, which documents all audit activities.

The IT-Grundschutz modelling as well as the defining protection requirements (see [BSI2] and [BSI4]) form the basis for creating the IS audit plan. They should be available as part of the security concept and in the export of the information security management database (e.g. GSTOOL).

If they are not available or do not have the level of quality required, then the IS audit can be only performed with a limited scope based on the network plan and possibly any other information available (see also section 4.4). Assignments of IT-Grundschutz modules (including user-defined modules) to certain target objects (referred to in the following as ”module target objects”, see section 1.6) result from the IT-Grundschutz modelling.

IS cross-cutting audit procedure

When performing an IS cross-cutting audit, the audit is performed based on samples. A selection of module target objects is chosen, and then a limited number of safeguards are examined based on this selection. The IS audit team makes the selection and provides reasons for the selection in writing. The module target object for information security management (Module 1.0) including all associated safeguards must always be tested completely. From the number of remaining module target objects, another 30% are selected at a minimum, whereby at least one module target object is

to be selected from each layer. Note in this case that a group of target objects of the same type is added to the selection as a single module target object.

The module target objects to be examined are selected according to the risk-based audit approach. The following questions in particular will help you obtain a risk-based module target object selection:

- What are the main or critical business processes in the organisation? Which procedures support these business processes? Which module target objects affect these procedures?
- Which module target objects are particularly prone to error according to experience?
- Which module target objects have a high or very high protection requirement according to the protection requirements determination in the security concept?
- Has the target object / document ever been examined before in an IS audit or has the target object / document not been included in an IS audit for a long time?

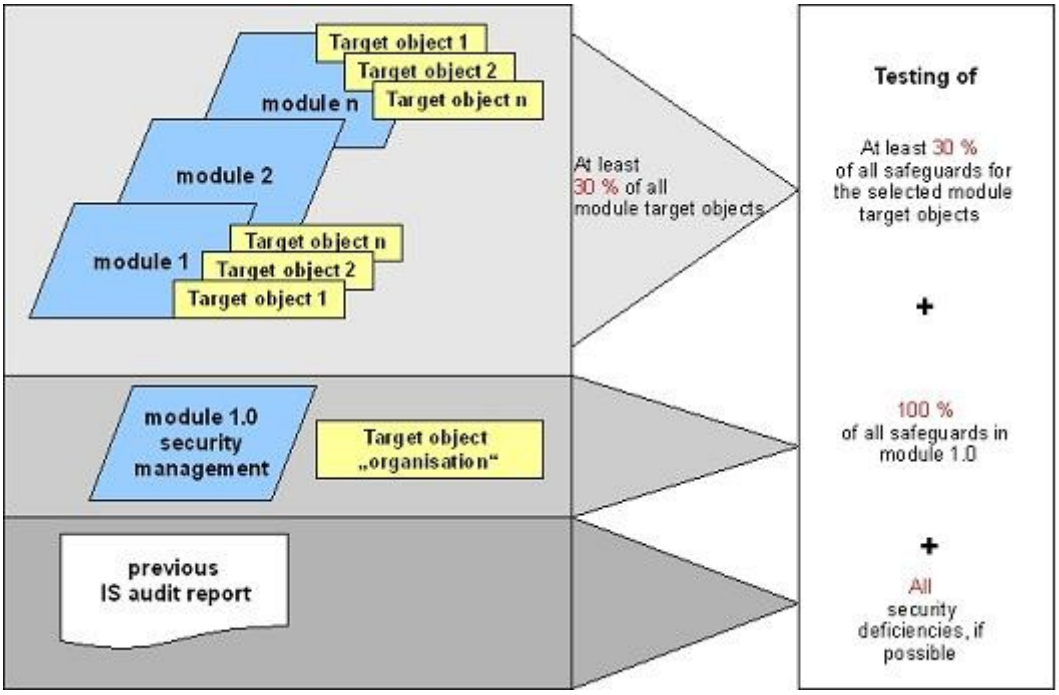

Figure 7: The assorted samples of an IS cross-cutting audit

Even previously certified or audited information domains in the organisation are to be reviewed in the framework of the IS audit, but due to the risk-based audit approach (see [IDW]) and the fact that an audit has already been performed, they are not the focus of the IS audit. Results from audits can be taken into account in the IS audit when the specifications in this guide were followed for the audits and the data was obtained within the current IS audit cycle (maximum of 3 years).

The selection of the module target objects should change in subsequent audits to ensure the best possible audit coverage of the entire information domain. In an additional reduction step, at least

30% of the safeguards are selected for examination for each module target object. Only the mandatory safeguards are subject to testing, meaning the A, B, and C safeguards and the safeguards resulting from the supplementary security analysis.

Regardless of which module target objects were selected, all safeguards found to be deficient in the previous IS audit must also be reviewed, if possible. If not all can be tested, then at least all safeguards with serious security deficiencies should be reviewed.

The safeguards, like the module target objects, should be selected according to the risk-based audit approach. The criteria for selecting the safeguards are to be documented comprehensibly for each IT-Grundschutz layer.

IS partial audit procedure

The procedure for an IS partial audit corresponds in principle with the procedure for an IS cross-cutting audit. Basically, the IS partial audit is a significantly wider ranging (possibly even a full) examination of the module target objects and safeguards.

4.6 Examining documents and updating the IS audit plan (Step 3)

The document examination is performed based on the safeguards specified in the IS audit plan. The examination of the documents focuses primarily on the completeness and understandability of the documents. If possible, the appropriateness of the safeguards to be examined should be evaluated.

In terms of completeness, the documents must be examined to ensure all major aspects (for example systems, networks, IT applications, and rooms) were documented and if the roles described were actually assigned.

The evaluation of the appropriateness includes an evaluation of the personnel, organisational, and technical safeguards in terms of their effectiveness. To evaluate the appropriateness of a safeguard, the following questions should be answered, if possible (see [BSI2] - Chapter 4):

- Which threats should be reduced by implementing the safeguard?
- What is the residual risk taken by the organisation? Is this level of residual risk bearable for the organisation according to the current documents?
- Is the safeguard suitable and can it actually be implemented in practice?
- Is the safeguard applicable, easy to understand, and not prone to errors?

The documents presented must be comprehensible for the IS audit team. Reasons for the decisions made in the organisation should be provided in the documentation to be examined.

A small part of the safeguards to be examined can be completely evaluated already within the document examination phase. The remaining safeguards are to be examined further during the on-site examination. The IS audit plan is to be complemented by safeguards result from the discrepancies found while examining the documents.

For each safeguard in the IS audit plan, the main questions to be answered are collected with specifications of the intended audit techniques (see section 4.2) and of the interview partners in the organisation (if these can be derived from the documents available) for the on-site examination.

Afterwards, these questions are to be consolidated. This means that questions about the safeguards are to be sorted, if possible, according to the interview partner, summarised according to the systems to be examined, and redundant questions eliminated.

This makes the IS audit procedure easier to perform, improves the understandability of the results, and serves to document the test actions taken.

In co-operation with the contact person of the organisation to be examined, the IS audit team works out the time schedule for the on-site examination (times and dates of the opening meeting, interviews, system inspections, and closing meeting) included in the IS audit plan. The contact person in the organisation to be examined is responsible for co-ordinating the schedules and possibly for reserving the necessary rooms.

The IS audit plan at this time consists of the following items:

- Specifications of the module target objects and safeguards to be examined
- Additional safeguards to test arising in conjunction with the deficiencies discovered during the document examination
- Selection of the audit techniques for the particular safeguards
- If possible, specification of the interview partners, including their roles
- Specification of the schedule

4.7 On-site examination (Step 4)

The goal of the on-site examination is to compare and check the documents presented, for example the concepts and guidelines, with the actual conditions on-site to see if information security is guaranteed in an adequate and practical form with the selected safeguards.

The procedure follows the IS audit plan. This does not mean, though, that the IS auditor absolutely must stick to the IS audit plan at all times. It may be reasonable and make more sense to skip some sections of the IS audit plan. This is already the case when it is discovered that the safeguards for the first samples reviewed were not adequately implemented, which means that more in-depth tests are therefore to no avail. On the other hand, it may be necessary to expand some tests to obtain more evidence for security gaps or security deficiencies. The IS audit plan must be updated accordingly. The decision to abort or extend the examination of a module target object or safeguard is at the discretion of the IS audit team. Extensions of examinations must, however, remain restricted to the audit objects specified in the contract.

Opening meeting

At the beginning of the on-site examination, the IS audit team holds an opening meeting with the management of the organisation to be examined, the person responsible for IS audits, the head of

IT, and the IT Security Officer. Additional persons, such as the head of the personnel department, administrators, and additional interview partners may also participate in the opening meeting, if required. In addition to the basic procedure for an IS audit, the audit objects and audit procedures are also explained. The IS audit team must present and document the type of support they expect from the organisation audited for a smooth IS audit. Support in this context means providing any information or documents requested and making the necessary communication resources (e.g. Intranet, telephone) available for the duration of the audit. It is also just as important that the IS auditors are announced by name in the organisation and that they are able to become familiar with the general external conditions, for example the office hours and access regulations.

The on-site IS audit procedure

The IS audit plan is used by the IS audit team as an aid to structure the on-site examination to perform the audit quickly, and should also be used to document the test actions taken.

The tests are performed initially using the intended audit techniques, usually the interviews and the inspections. For technical aspects a demonstration by the administrator responsible or his representative is recommended. The IS audit team itself never intervenes with the system. When the systems and methods are complex or there is a large amount of data, it is not always possible to evaluate the information directly on-site. In this case, additional information can be requested by the IS audit team in electronic or paper form for later evaluation. The IS audit plan must be updated accordingly.

If the IS audit team finds deviations from the documented status during the examination of a selected sample, then the number of samples must be increased accordingly to obtain an explanation. The examination is only finished after the deviation is adequately clarified (e.g. is there a problem with the procedure or was it just a one-time error?).

During the on-site examination, all facts as well as specifications of the sources and information on requests for information and documents as well as the interviews conducted are to be documented in writing. Technical aids such as photos and screen shots can also be used for documentation purposes. All technical documentation resources are to be approved by the management of the organisation and may only be used with the permission of the participants.

At the end of the on-site examination, the course of the examination so far, the determinations made (without an evaluation), and the remaining parts of the procedure are presented to the organisation audited in a closing meeting (minutes mandatory). The IT Security Officer, the person responsible for IS audits, and the head of IT in the organisation audited should participate in the meeting. Other participants can be included, if required.

4.8 Evaluating the on-site examination (Step 5)

After the on-site examination, the information obtained is consolidated further and evaluated. The evaluation can also be performed by external experts if the required expert knowledge is not covered by the IS audit team. If external experts are contracted, then it is necessary either to obtain the permission of the organisation audited, or to make the information anonymous so that no conclusions can be drawn regarding the organisation or its personnel. The evaluation of the information is incorporated into the overall evaluation of the safeguard tested.

After the evaluation of the documentation requested and the additional information, a final evaluation of the safeguards tested is performed and the results are summarised in an IS audit report.

4.9 Producing the IS audit report (Step 6)

The IS audit report, including the reference documents, is to be provided in writing to the management of the organisation audited or the client, the person responsible for IS audits, and the IT Security Officer.

A draft version of the IS audit report should be given to the organisation audited in advance in order to verify that the facts established by the IS audit team were recorded correctly.

The organisation audited is responsible for ensuring that all affected organisational units receive the relevant parts of the IS audit report important to them within an appropriate time frame. The "need to know" rule should be applied.

The IS audit report consists at a minimum of a management summary, a graphical evaluation of the information security status determined, and a detailed description of the facts found, as well as an evaluation of each fact for each safeguard tested.

Part 0

This part contains the organisational information, for example the basis of the audit, the chronological order of the steps in the IS audit, and a short description of the audit contract.

Part 1

Part 1 is the management summary. This summary should consist of a maximum of two pages. It should contain the main facts discovered in a brief and comprehensible form as well as the recommendations resulting from the facts determined.

Part 2

In addition to the management summary, it is also recommended to provide a graphical representation of the results of the audit (see also section 4.3). This part should contain, in particular, graphical overviews of the implementation status and security deficiencies based on the layers of IT-Grundschutz.

Part 3

This part of the IS audit report contains the detailed descriptions of the subject areas tested and the facts determined together with the technical details and recommendations. It is recommended to sort this part according to the module target objects and safeguards tested. Only the deficient safeguards and the safeguards with security recommendations should be entered here. To enable the evaluation of the security safeguards to be recognised quickly, it is recommended to use the following colours to indicate the evaluation results in the report:

Security Evaluation	*Visualisation in the IS audit report*
Serious security deficiency	red
security deficiency	yellow
Security recommendation	grey

Table 4: Visualisation of security deficiencies

Formal aspects

When creating the IS audit report, the following formal aspects must be taken into account. All tests conducted, their results, and the evaluations of the results must be documented reproducibly and understandably.

- The table of contents should contain the actual report as well as all appendices (for example screen shots, log files, etc.). Each appendix must be easily identifiable so that it is possible to check the IS audit report and the appendices for completeness.

- All reference documents used must be listed.

- Recorded data, for example notes from meetings or log file evaluations referred to in the report, must be included as an appendix.

- The pages must be designed so that every page can be uniquely identified (for example using page numbers as well as version numbers and the title and date of the report).

- If software tools are used to support the auditing activities, e.g. analysis tools, then these tools must be listed together with their name and version number.
  If the audit report refers to information recorded with these tools, then the corresponding reports (printouts) must be included in the audit report as additional notes.

- Special terminology or abbreviations not commonly used that appear in the report must be collected in a glossary or an index of abbreviations.

Management report

In order for the company or government agency management to make the right decisions when managing the information security process, they need an overview of the current state of information security. This also includes the results of the IS audit as edited by the IT Security Officer (see [BSI2]). Management should regularly receive reports on the following

- the main results of the IS audit report,

- the security status and the development of the security status determined in the IS audit reports and

- the necessary follow-up activities.

Storage and archiving

The IS audit report and the reference documents it is based on must be stored in revision-proof form by the organisation audited for a duration of at least 10 years after delivery of the report. They form the basis for the selection of the module target objects and safeguards to be examined in future audits (for the long-term, complete examination of the organisation and to track down security deficiencies, etc.).

Requirements for revision-proof archiving can be found in IT-Grundschutz module 1.12 ”Archiving” and in § 239 of the German Commercial Code:

- Correctness
- Completeness
- Protection against changes and falsification
- Securing against loss
- Use by authorised persons only
- Maintenance of the archiving periods
- Documentation of the procedure
- Testability
- Reproducibility

Upon delivery of the IS audit report, the IS audit is terminated for the commissioned IS audit team.

5 Aids

To help you when applying this IS audit guide, the German Federal Office for Information Security has developed aids that are updated regularly. The latest versions of these aids, such as sample templates for the IS audit manual, the IS audit plan, or the IS audit report, are available for downloading at the following link:

http://www.bsi.de/fachthem/is-revision/hilfsmittel.htm