DRAFT

GUIDELINES FOR INFORMATION SYSTEMS AUDIT

2019

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY

NITDA

Table of Contents

Definition of Terms

The following terms are used in this document:

1. **Audit -** the process by which a subject area is independently reviewed and reported on by one or more competent auditors on behalf of stakeholders.
2. **IS audit -** focuses on information systems in the organisation. The goal of an IS audit is to have an independent party that determines the current level of security throughout the organisation and points out any existing security gaps and deficiencies. The IS audit is a special type of (general) audit. The result is an IS audit report with recommendations for improving the level of information security
3. **Audit plan** - a project plan for an audit laying out the main audit activities and their timing.
4. **IS audit plan -** this describes the entire examination procedure, from the initial selection of the module target objects to the documentation of the on-site examination.
5. **Risk-based approach -** 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.
6. **Safeguard -** this 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.
7. **Module target object** - refers to a specific audit object or a group of audit objects to which a certain module is applied.
8. **Critical business processes** - special tasks that are very valuable to the organisation.

9. **Organisation -** a general term for government agencies, companies, and other public or private organisations.
10. 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.

Introduction

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 System 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, is it possible to form an opinion on their effectiveness, up-to-datedness, completeness, and appropriateness, and the status of information security. The IS audit is therefore a tool for determining, achieving, and maintaining a proper level of security in public organisations.

The main task of the IS audit is to provide the management, the IS management team, and particularly 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 organization. The result of an IS audit and the IS audit report, shows in compact form the security status within 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.

1.1 Power to Regulate

The National Information Technology Development Agency (NITDA) is empowered by Section 6 of its enabling Act (National Information Technology Development Agency Act 2007) to regulate and promote the use and development of Information Technology (IT) in all spheres of Nigeria through the development of IT framework, standards, guidelines, regulations, and policies.

In line with the above, NITDA hereby issues these guidelines for IS Audit in Nigeria.

1.2 Definition of IS Audit

IS audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations. IS audit can be considered as the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively and uses resources efficiently.

1.3 Objectives

The objectives of IS audits include assessment and evaluation of processes that ensure:

i Asset safeguarding which include the following five types of assets:

   a. Application system is understood to be the sum of manualand programmed procedures.
   b. Resources to house and support information systems, supplies etc.
   c. Data objects in their widest sense, (i.e., external and internal, structured and non-structured, graphics, sound, system documentation etc.).

d. Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

e. Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

ii. Ensures that the following seven attributes of data or information are maintained:

a. Confidentiality - concerns protection of sensitive information from unauthorized disclosure.

b. Efficiency - concerns the provision of information through the optimal (most productive and economical) usage of resources.

c. Effectiveness - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

d. Reliability of information

e. Integrity - relates to the accuracy and completeness of information as well as to its validity in accordance with the business' set of values and expectations.

f. Compliance - deals with complying with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria. This essentially means that systems need to operate within the ambit of rules, regulations and/or conditions of the organization.

g. Availability - relates to information being available when required by the business process, and hence also concerns the safe guarding of resources.

1.4 Target Group

This document is intended to be read by all persons responsible for initiating or performing IS audits based on NITDA requirements. This group may include, IS auditors, management of the organisation, the IT Security Officer, or any other persons responsible for IT security. The primary target audience is the group of office managers in organisations who are responsible for regular IS audits as well as the IS auditors who 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.

Information Systems Audit

Public Institutions in Nigeria are required to create and implement a security concept, they are also required to follow the specifications as well as to check the success of their implementation through IS audits; in order to maintain and continuously improve information security. Managements of organisations are responsible for initiation and management of information security process, including IS audits as an integral part of the information security management process.

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.

1. IS audits should be performed regularly;
2. Public agencies are obligated to perform a comprehensive IS audit at least every 3 years;
3. This audit must always examine all aspects of the organisation;

2.1 Basis of IS Audits

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 NITDA Implementation Plan should be carried out by performing the audit based on the following layers:

1. Layer 1 - Generic aspects;
2. Layer 2 - Infrastructure;
3. Layer 3 - IT Systems;

4. Layer 4 - Networks;
5. Layer 5 - Applications.

2.2 Performing IS Audit

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.

2.3 IS Audit Integration in Information Security Management Systems

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 system. 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.

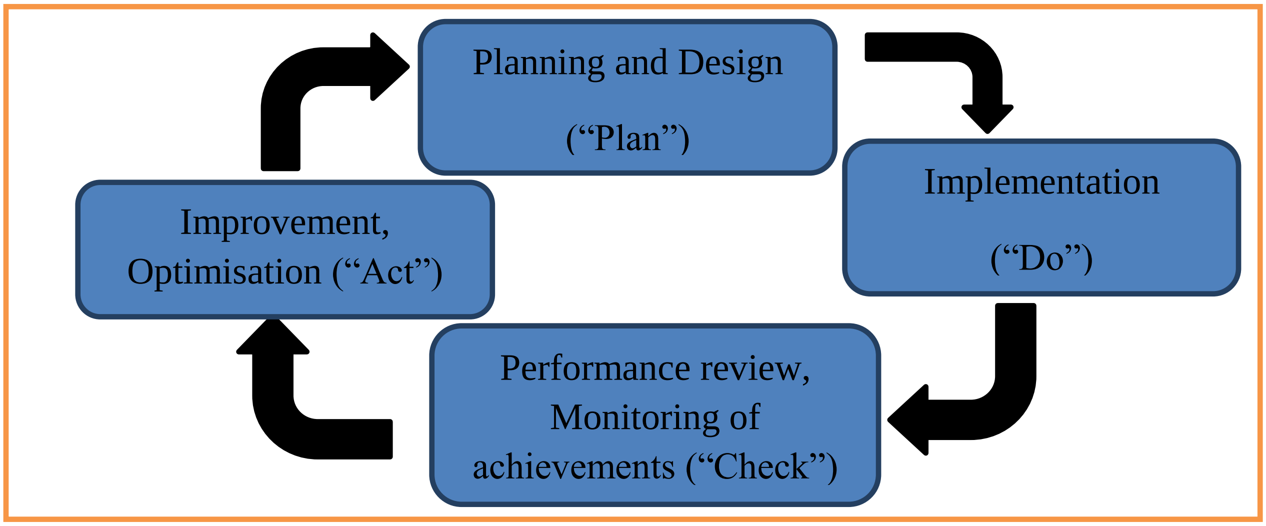
Planning and Design
(“Plan”)
Implementation
(“Do”)
Performance review, Monitoring of achievements (“Check”)
Improvement, Optimisation (“Act”)

Figure 1: IS Audit Process model according to Deming

The result of the ”Check” phase, e.g. the IS audit report, is evaluated and processed further according to the information security process in the subsequent ”Act” phase. This means that the business processes will be optimised and security gaps closed by implementing safeguards.

If fundamental or comprehensive changes are required as a result of the ”Check” phase, then the information security process starts again with the ”Plan” phase. The cycle of the methodology with the input and output documents influencing the process is shown in the following diagram:

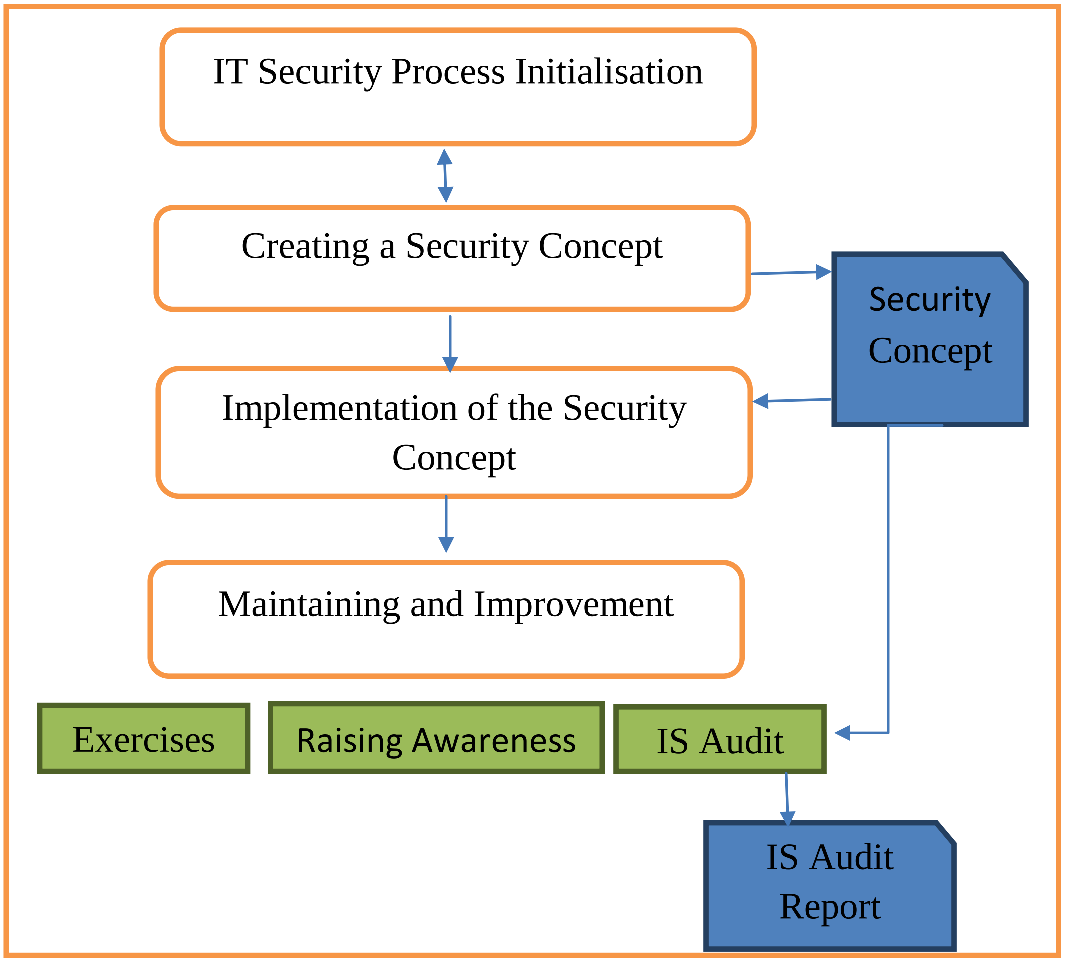
IT Security Process Initialisation
Creating a Security Concept
Security Concept
Implementation of the Security Concept
Maintaining and Improvement
Exercises
Raising Awareness
IS Audit
IS Audit Report

Figure 2: Embedding the IS Audit in the ISMS

The processes in the diagram 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 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.

2.4 Types of IS Audit

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

2.4.1 IS Cross-Cutting Audit

The 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 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 public organisations.

2.4.2 IS Partial Audit

The 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 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 an 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 applications 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 an IS partial audit.

Furthermore, the same rules and procedures apply to the IS partial audit as to the IS cross-cutting audit.

2.5 Requirements to become an IS Auditor

The most important skill for an IS auditor is understanding the business environment and related risk to determine; what to test and why. Developing meaningful IS audit programs depends on the ability to customize audit procedures according to the nature of the subject under review and the specific risk that must be addressed in the audit area/organisation. The following list describes some of the basic requirements / skills that can enable the IS auditor to develop good audit programs:

1. A bachelor's degree and/or a master's degree in Computer Science, Information Systems, Cyber Security or a related technical field;
2. Professional certifications such as Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM) etc.;
3. 5 years of cognate experience in general IT;
4. Good understanding of the nature of the enterprise and its industry to identify and categorize the types of risk and threat;
5. Good understanding of the IT space and its components and sufficient knowledge of the technologies that affect them;
6. Understanding of the relationship between business risk and IT risk
7. A basic knowledge of risk assessment practices;
8. Understanding of the different testing procedures for evaluating IS controls and identifying the best method of evaluation, for example:
    a. The use of generalized audit software to survey the contents of data files (e.g., system logs, user access list);
    b. The use of specialized software to assess the contents of operating systems, databases and application parameter files;

    c. Flowcharting techniques for documenting business processes and automated controls;
    d. The use of audit logs and reports to evaluate parameters;
    e. Review of documentation;
    f. Inquiry and observations.
9. Working knowledge of:
    a. ISO 27001/27002, ITIL and COBIT frameworks;
    b. Fidelis, Arc Sight, Niksun, Websense, Proof Point, Bluecoat and/or similar auditing and network defense tools;
    c. Firewall and intrusion detection/prevention protocols;
    d. Windows, UNIX and Linux operating systems;
    e. MSSQL and ORACLE databases;
    f. C, C++, C#, Java and/or PHP programming languages; and,
    g. ACL, IDEA and/or similar software programs for data analysis.

2.6 Key Aspects of the IS Audit

1. 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.
2. 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 regulating body.

3. Every IS audit team should consist of at least two IS auditors to guarantee the independence and objectivity of the audit.
4. Important IS audit meetings such as opening and closing meetings, as well as the interviews should be conducted as a team. This procedure ensures objectivity, thoroughness, and impartiality.
5. No member of the team, for reasons of independence and objectivity, should have participated directly in supporting or managing the areas to be audited. They must not have been involved in the development of concepts or the configuration of the IT systems.
6. The IS auditors should have wide range of knowledge and in-depth knowledge in the field of information security.
7. 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) are suitable for this purpose.
8. In general, IS Auditors should ensure that actual operations in the organisation are not significantly disrupted when initiating the IS audit.
9. IS auditors never actively intervene in systems, and therefore shall not provide any instructions for making changes to the objects being audited.

IS Audit Charter

The IS Audit Charter is a formal document that defines internal audit's purpose, authority, responsibility and position within an organization. The IS Audit Charter provides the organization with an agreement relating to the work internal audit will undertake and the support it will receive. It may also be seen as a benchmarking tool against which it can measure the effectiveness of the internal audit unit in fulfilling its commitment. The charter can act as a service level agreement with the board or audit committee so that there is a clear understanding of the role, purpose and position of IS Audit within the organization and the scope and nature of its work.

3.1 Mandate of the IS Audit Charter

1. The IS Auditor should have a clear mandate to perform the IS audit function. This mandate should be documented in an audit charter.
2. The Audit Charter should be formally accepted by all IS auditors.
3. Where an audit charter exists for the audit function as a whole, the IS Audit Mandate should be incorporated.

3.1.1 Contents of the Audit Charter

There is no right or wrong way to prepare an internal audit charter but it should be consistent with the mission of internal audit, the core principles for the professional practice of internal auditing, the code of ethics, the standards and the definition of internal. The IS Audit Charter should clearly address the aspects of purpose, responsibility, authority and accountability.

3.1.2 Responsibility

The IS Audit responsibilities should include any specific requirements relating to the sector as a service level agreement which the organization operates such as:

1. Risk assessment;
2. Independence;
3. Relationship with external audit;
4. Critical success factors;
5. Operating principles;
6. Key performance indicators;
7. Auditee requirements;
8. Other measures of performance.

3.1.3 Purpose

1. Objectives;
2. Scope;
3. Aims/goals;
4. Mission statement;
5. Role.

3.1.4 Accountability

1. Reporting lines to senior management;
2. Assignment performance appraisals;
3. Personnel performance appraisals;
4. Staffing/career development;
5. Auditee rights;
6. Independent quality review;
7. Assessment of compliance with standards;
8. Benchmarking performance and functions;

9. Assessment of completion of the audit plan;
10. Comparison of budget to actual costs;
11. Agreed actions, e.g., penalties when either party fails to carry out their responsibilities.

3.1.5 Authority

1. Right of access to information, personnel, locations and systems relevant to the performance of audits;
2. Scope or any limitations of scope;
3. Functions to be audited;
4. Auditee expectations;
5. Organizational structure, including reporting lines to board and senior management;
6. Grading of IS audit staff.

3.2 Communication with Audited Organizations

Effective communication with organizations' being audited involves:

1. Describing the service, its scope, its availability and timeliness of delivery;
2. Providing cost estimates or budgets if they are available;
3. Describing problems and possible resolutions for them;
4. Providing adequate and readily accessible facilities for effective communication;
5. Determining the relationship between the service offered and the needs of the auditee.

3.2.1 Basis for Communication

The audit charter forms a sound basis for communication with auditees and should include references to service level agreements for such things as:

1. Availability for unplanned work;

2. Delivery of reports;
3. Cost;
4. Response to auditee complaints;
5. Quality of service;
6. Review of performance;
7. Communication with auditees;
8. Needs assessment;
9. Control risk self-assessment
10. Agreement of terms of reference for audits;
11. Reporting process;
12. Agreement of findings.

3.3 Quality Assurance Process

The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys) to understand auditees' needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary.

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:

4.1 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.

1. IS auditors should be aware of the value of the information they receive and who owns it;
2. Should not disclose this information without the corresponding permission unless they are legally or professionally required to do so;
3. Information obtained during the course of auditing shall not be used for personal benefit or released to inappropriate parties.

4.2 Expert Knowledge

1. IS auditors should 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;

2. They should continuously improve their knowledge as well as the effectiveness and quality of their work.

4.3 Objectivity and Thoroughness

1. 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;
2. 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.

4.4 Objective Presentation

An IS auditor has the duty to report the results of the examination precisely and truthfully to his client. This include:

1. The impartial and understandable presentation of the facts in the IS audit reports;
2. The constructive evaluation of the facts determined;
3. Specific recommendations for improving the safeguards and processes.

4.5 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: The IS audit team follows a documented and reproducible methodology (IS audit plan, IS audit report) to come to its conclusions.

Failure to comply with this Code of Professional Ethics shall result in an investigation into an IS auditor's conduct and ultimately, in disciplinary measures.

IS Audit in Public Sector

IS audits should be performed regularly; at least every 3 years. 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.

5.1 Basics and Responsibilities

1. Organisations should assess their ISMS regularly 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;
2. The management level of an organisation should always bears the overall responsibility for the IS audit;
3. Management must be informed regularly about any problems as well as 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;
4. 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:

    a. An independent position in the organisational structure of the organisation (to prevent conflicts of interest);
    b. The right to speak directly to the organisation's management;
    c. Sufficient knowledge in the field of information security;
    d. To create a rough planning for the IS audit project based on this guide to be substantiated on an annual basis;
    e. He should be the main contact person for an IS audit team during the entire duration of the IS audit;
    f. He is responsible in particular for providing the reference documents and co-ordinating schedules and personnel/material resources during the on-site examination.
5. 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:
    a. The strategic goals of the IS audit to be achieved;
    b. Any possible legal regulations and ordinances;
    c. The resources (in terms of time, finances, and personnel);
    d. The special conditions and restrictions of the organization;
    e. The archiving of the documentation.

5.2 IS Audit Manual

The IS audit manual is the main foundation and instruction manual for the IS audit. Since it regulates, among other things:

1. 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;
2. The personnel representative should be included in the process before it is adopted by the management;

3. Based on the IS audit manual, the IS audits planned should be performed by an internal or external IS audit team;
4. The audits should be supervised by the person(s) responsible for IS audits in the organization;
5. The resulting IS audit reports form the basis for follow-up activities, which is intended to maintain and improve the level of information security.

5.3 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. IS partial audits should be included in the annual resource plan to allow for IS audits after unexpected security incidents. Basically, it is also possible to split up an IS cross-cutting audit by tasks and locations. When an 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 available for the organisation. This means that:

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

5.4 IS Audit Cycles

1. Organisations are required to perform an IS cross-cutting audit at least once every 3 years;
2. In addition, IS partial audits for critical business processes must be planned;
3. Critical business processes, especially those that require high availability should be subjected to IS partial audits more often;
4. The audit interval must be appropriate for the particular criticality;
5. IS partial audits can be performed as well, for example as in-depth examinations, after:

a. Security incident;
b. Introducing new procedures;
c. When planning to restructure.

5.5 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 such as:

1. Organising meetings;
2. Collecting documents;
3. Supervising the on-site examination.

5.6 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. There are various ways to put together an IS audit team in an organisation:

5.6.1 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 and independence must be guaranteed

5.6.2 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.

5.6.3 Departmental IS Audit Team

An organisation can place the IS audit teams or competency centres in one department. The IS audit team could be established centrally at the top level in the organization. The organization would then have the ability to access the 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.

5.6.4 External IS Audit Service Provider

External service providers also offer IS audit services. Organisations' should use IT security service providers accredited by NITDA.

NITDA shall publish a list of all IS Audit service providers accredited by NITDA, these service providers are required to prove their trustworthiness and expertise to NITDA.

5.7 Call for Tenders

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

1. The IS audit should be performed based on this guideline for IS audit.
2. 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:
    a. Procedures,
    b. IT-systems,
    c. Networks ,
    d. Branch offices,
    e. Information domain.
3. The time frame in which the IS audit should be performed must be defined.
4. Aborted criteria are to be defined, where appropriate.
5. The object to be audited should be described in detail. This includes:
    a. A general description of the organisation (location, number of branch offices, number of employees, tasks / goals of the organisation);
    b. Naming of the main tasks and processes of the organisation / of the division to be examined / of the information domain to be examined;
    c. A list of the sites in the organisation to be examined, where applicable;

   d. A description of the IT systems, applications, and procedures used;
   e. The type of networking used in the audited division of the organization;
   f. The number of critical processes;
   g. A list of outsourced business processes and IT systems belonging to the object to be examined.

6. The following requirements should be met by the service provider or the IS audit team:
   a. A wide range of knowledge in the field of IT;
   b. Experience in performing information security audits;
   c. Specific expert knowledge of the audit subject.

7. 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;
8. Depending on the protection requirements of the information, the service providers and IS auditors may need to verify their trustworthiness in accordance with the law;
9. Authorisation to view classified materials must be provided, if necessary, by presenting a valid personal security clearance certificate;
10. It must also be specified in the contract that; data used by the service provider must be destroyed, placed in safekeeping, or handed over after the IS audit is finished;
11. A non-disclosure agreement should be signed by the organisation and the service provider;

12. The intended duration of the IS audit is to be specified in the call for tenders document by the organisation. The duration of an 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: very high, high or normal;

13. 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:

    a. How many network gateways are in the organization?
    b. What does the system landscape look like (number of systems and level of heterogeneity of the systems used)?
    c. Number of IT applications used in the organisation. Are they used to support critical business processes?
    d. Is the organisation active in areas critical to security (for example, is the organisation a security agency)?
    e. Which and how many IT applications are used in the organisation? Are they used to support critical business processes?
    f. Are there higher levels of IS audit procedures used that may affect other departments outside of the organisation?
    g. How high is the protection requirement for the infrastructure, systems, and IT applications?

5.8 Evaluating an IS Audit

1. The results of the IS audit should be reported to the management of the organisation, the person responsible for IS audits, and the IT Security Officer and integrated into the ISMS process;
2. A clearly defined procedure should be available for this purpose that is stated in a guideline for examining and improving the security process;
3. The IT Security Officer should derive the corresponding follow-up activities from these requirements;
4. The rough and detailed IS audit plans are to be adapted accordingly;
5. 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.

Performing an IS Audit

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 should be classified as "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 as shown in the chart below.

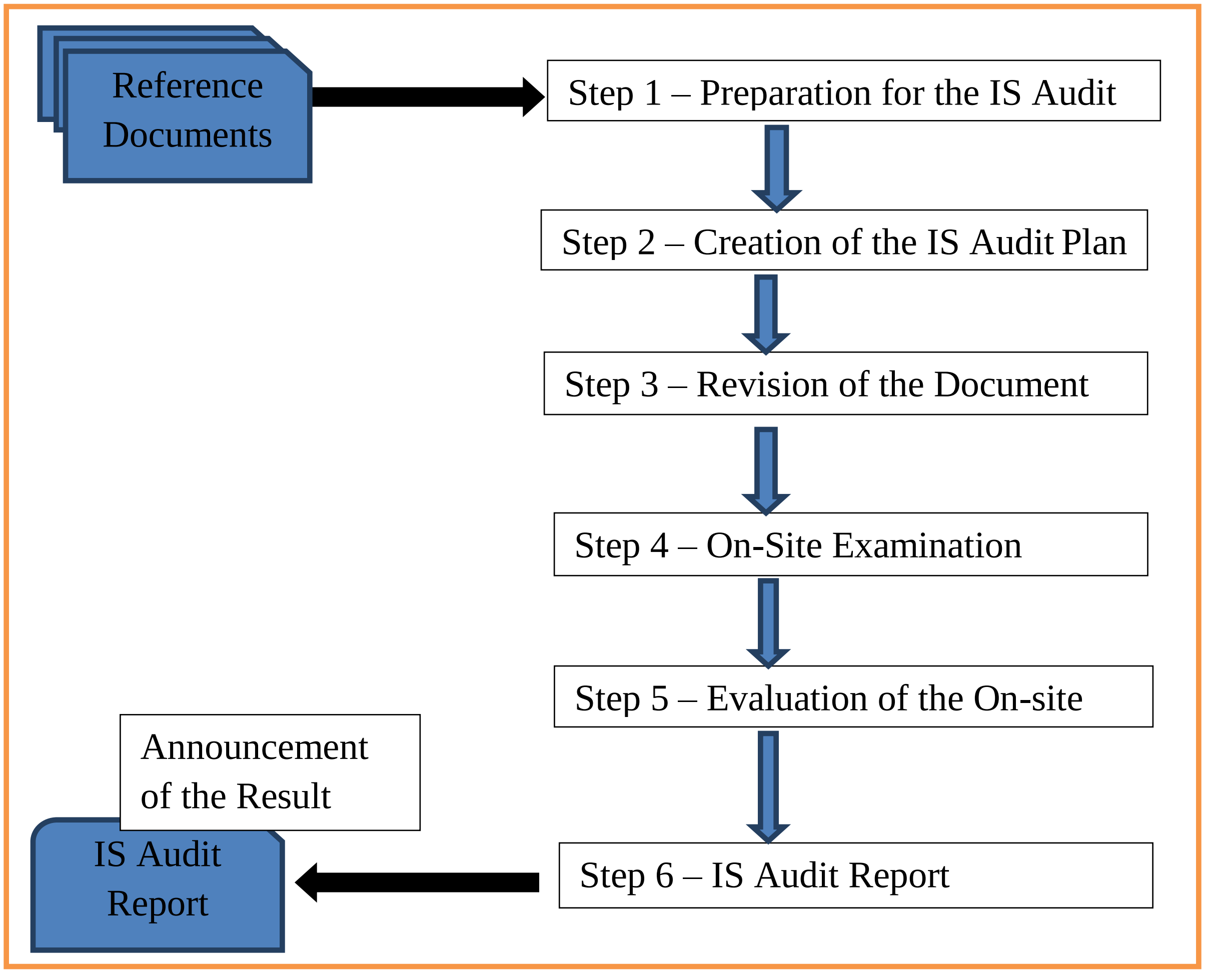
Reference Documents
Step 1 – Preparation for the IS Audit
Step 2 – Creation of the IS Audit Plan
Step 3 – Revision of the Document
Step 4 – On-Site Examination
Step 5 – Evaluation of the On-site
Announcement of the Result
IS Audit Report
Step 6 – IS Audit Report

Figure 3: Flow chart of Steps when performing an IS audit

The methodology includes:

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;
2. Based on the documents made available, the IS audit team gets a picture of the organisation to be examined and creates the IS audit plan;
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 coordinated together with the contact person at the organisation;

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;
5. The information obtained during the on-site examination is consolidated further and evaluated by the IS audit team;
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 schedule as seen from the table below:

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 %

6.1.1.1 Table 1: 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.

6.1 IS 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:

1. Observation (e.g. things observed incidentally in the context of the on-site examination);
2. Analysis of files (including electronic data);
3. Verbal questioning (interviews);
4. Visual inspection of the systems, locations, spaces, rooms, and objects;
5. Technical examination (e.g. testing of alarm systems, access control systems, applications);
6. Data analysis (for example of log files, database evaluations, etc.);
7. 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.

6.1.1 Evaluation Scheme

The results obtained for each safeguard tested are to be included in the IS audit plan 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:

1. Safeguard implemented: All recommendations in the safeguard are completely, effectively, and adequately implemented;
2. Safeguard not implemented: The recommendations in the safeguard are not implemented for the most part;
3. Safeguard partially implemented**:** Some of the recommendations are implemented, others are only partially implemented or not implemented at all;
4. 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.

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 a 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 implemented	No security deficiency or security recommendation
Safeguard is not implemented	Security deficiency or serious security deficiency
Safeguard is partially implemented	Security deficiency or serious security deficiency
Safeguard is unnecessary	No security deficiency

6.1.1.2 Table 2: 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. 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.

6.2 Preparation of an IS Audit

Below are the required steps to be followed in the preparation of an effective IS Audit of an organisation.

6.2.1 Step 1 - Preparing the IS Audit

When initiating an IS audit,

1. 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);
2. The management of the organisation should inform NITDA of the planned IS audit;
3. The person responsible for IS audits in the organisation 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 coordinated (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.

6.2.1.1 Organisation's Documents

1. IT framework concept;
2. Schedule of responsibilities; and,
3. Organogram.

6.2.1.2 Technical Documents

1. Export of the information security management database;
2. The IS audit reports from the previous three (3) years (if available);
3. The security policy: The management is responsible for the efficient and proper functioning of the 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;

4. 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;
5. Security concept: The security concept is the main document in the security process and contains, at a minimum, network plan, the structure analysis, basic security check, defining protection requirements, and the supplementary security analysis. Likewise, the supplementary risk analyses and the implementation plans for the safeguards should be included.

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

6.2.2 Step 2 - Creating the IS Audit Plan and Screening Documents

1. When evaluating the up-to-datedness 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;
2. 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 logical for the IS audit team. In particular, decisions made should be justified intelligibly;

3. 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.

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.

6.2.2.1 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 objects for information security management including all associated safeguards that must always be tested completely. From the number of remaining module target objects, another 40% 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:

1. Which module target objects are particularly prone to error according to experience?
2. Which module target objects have a high or very high protection requirement according to the protection requirements determination in the security concept?
3. What are the main or critical business processes in the organisation? Which procedures support these business processes? Which module target objects affect these procedures?
4. 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?

The safeguards, like the module target objects, should be selected according to the risk-based audit approach.

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.

6.2.2.2 IS Partial Audit Procedure

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

6.2.3 Step 3 - Examining Documents and Updating the IS Audit Plan

1. 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;

2. 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;
3. 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;
   a. Is the safeguard applicable, easy to understand, and not prone to errors?
   b. What is the residual risk taken by the organisation? Is this level of residual risk bearable for the organisation according to the current documents?
   c. Which threats should be reduced by implementing the safeguard?
   d. Is the safeguard suitable and can it actually be implemented in practice?
4. 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 onsite examination. The IS audit plan is to be complemented by safeguards result from the discrepancies found while examining the documents;
5. 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;
6. For each safeguard in the IS audit plan, the main questions to be answered are collected with specifications of the intended audit techniques and of the

interview partners in the organisation (if these can be derived from the documents available) for the on-site examination.

7. 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 coordinating the schedules and possibly for reserving the necessary rooms.

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

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

6.3 Step 4 - On-Site Examination

This involves the following:

6.3.1 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;

1. Additional persons, such as the head of the personnel department, administrators, and additional interview partners may also participate in the opening meeting, if required;
2. In addition to the basic procedure for an IS audit, the audit objects and audit procedures are also explained;
3. 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. telephone, Intranet) available for the duration of the audit;
4. 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.

6.3.2 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.

1. 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?);
2. 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; and,
3. 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.

6.4 Step 5 - Evaluating the On-Site Examination

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.

6.5 Step 6 - Producing the IS Audit Report

1. 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;
2. 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;
3. The organization being audited is responsible for ensuring that all affected 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;
4. 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.

6.5.1 Features of IS Audit Report

The IS audit report is made up of four different parts:

1. **Part 1:** 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;

2. **Part 2:** This 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;
3. **Part 3:** In addition to the management summary, it is also recommended to provide a graphical representation of the results of the audit. This part should contain, in particular, graphical overviews of the implementation status and security deficiencies;
4. **Part 4:** 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	**Visualization in the IS audit report**
Serious security deficiency	red
Security deficiency	yellow
Security recommendation	grey

6.5.1.1 Table 3: Visualization of security deficiencies

6.5.2 Formal Aspects

When creating the IS audit report, the following formal aspects must be considered:

1. All tests conducted, their results, and the evaluations of the results must be documented, reproducible and understandable;
2. 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;
3. All reference documents used must be listed;
4. Recorded data, for example notes from meetings or log file evaluations referred to in the report, must be included as an appendix;
5. 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);
6. 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;
7. Special terminology or abbreviations not commonly used that appear in the report must be collected in a glossary or an index of abbreviations.

6.5.3 Management Report

In order for the organisation's management to make the right decisions when managing the information security process, they need an overview of the current state of information security. Management should regularly receive reports on the following

1. The main results of the IS audit report;

2. The security status and the development of the security status determined in the IS audit reports;
3. The necessary follow-up activities.

6.5.4 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 five (5) 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 are:

1. Correctness;
2. Completeness;
3. Protection against changes and falsification;
4. Securing against loss;
5. Use by authorised persons only;
6. Maintenance of the archiving periods;
7. Documentation of the procedure;
8. Testability;
9. Reproducibility

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

References

National Information Technology Development Agency http://nitda.gov.ng/mandate/ (no date)(Accessed: 24 August 2018).

National Institute of Standards and Technology (NIST), http://www.nist.gov/ (no date) (Accessed: 28 August 2018).

Center for Internet Security (CIS), www.cisecurity.org/ (no date) (Accessed: 28 August 2018).

National Security Agency (NSA), www.nsa.gov/ (no date) (Accessed: 24 August 2018).

Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/ (no date) (Accessed: 27 August 2018).

Institute of Electrical and Electronic Engineers (IEEE), www.ieee.org/ (no date)(Accessed: 28 August 2018)

Payment Card Industry Security Standards Council (PCI SSC), www.pcisecuritystandards.org/ (no date) (Accessed: 28 August 2018).

The IT Infrastructure Library (ITIL), https://www.axelos.com/best-practice-solutions/itil/ (no date) (Accessed: 27 August 2018)

TechRepublic, http://www.techrepublic.com/ (no date) (Accessed: 28 August 2018).
National Vulnerability Database (NVD), https://nvd.nist.gov/ (no date) (Accessed: 27 August 2018).

Common Vulnerability and Exposures (CVE), https://cve.mitre.org/ (no date) (Accessed: 28 August 2018).

International Organization of Supreme Audit Institutions (INTOSAI), www.intosai.org/ (no date) (Accessed: 28 August 2018).

The Institute of Internal Auditors (IIA), https://theiia.org/ (no date) (Accessed: 27 August 2018).

The American Institute of CPAs (AICPA), www.aicpa.org/ (no date) (Accessed: 28 August 2018).

Computer Security Resource Center, http://csrc.nist.gov/ (no date) (Accessed: 28 August 2018).

Build Security In, https://buildsecurityin.us-cert.gov/ (no date) (Accessed: 25 August 2018).

Homeland Security Cybersecurity, http://www.dhs.gov/topic/cybersecurity/ (no date) (Accessed: 28 August 2018).

Open Web Application Security Project (OWASP), www.owasp.org/ (no date) (Accessed: 24 August 2018).

European Network and Information Security Agency (ENISA), www.enisa.europa.eu/ (no date) (Accessed: 28 August 2018).

Auditing standards and guides, https://www.irba.co.za/ (no date) (Accessed: 28 August 2018).

The framework for governance and management of enterprise IT, https://www.isaca.org/ (no date) (Accessed: 24 August 2018).

Certified Information Systems Auditor, https://www.cybersecurityeducation.org/ (no date) (Accessed: 24 August 2018).