Cyber Security Audit and Evaluation Guideline

Version 1.0

May 2015 E.C.

Contents

Acronyms

CC Common Criteria

CSMS Cyber Security Management System

CMCSRS Critical Mass Cyber Security Requirement Standard

INSA Information Network Security Administration

Terms and Definitions

Terms	Definitions
Audit	Systematic, independent, and documented processes for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
Audit Checklist	A structured questionnaire or work plan to guide the auditors in testing the audit subject.
Audit Client	Organization or person requesting an audit, In the case of an internal audit, the audit client can also be the auditee or the individual(s) managing the audit program. Requests for external audits can come from sources such as regulators, contracting parties, or potential or existing clients.
Audit Criteria	Set of requirements used as a reference against which objective evidence. Criteria can be legal (including statutory or regulatory, and contractual obligations) requirements. It can be policies, standards, procedures, work instructions, legal requirements, and so on.
Audit Findings	The results of the evaluation of the collected audit evidence (3.9) against audit criteria,
Audit Plan	A project plan for an audit lays out the main audit activities and their timing. description of the activities and arrangements for an audit
Audit Program	A step-by-step set of audit procedures and instructions should be performed to complete an audit.
Audit Recommendation	A corrective action is proposed to address one or more identified audit findings that must be addressed before certification or recertification of the CSMS.
Audit Scope or Subject	The organizations or parts of the organizations, which are being audited, i.e., the extent and boundaries of an audit,
Audit Team	One or more persons conducting an audit, and if needed, supported by technical experts.
Audit Work Papers	Information written and gathered by the auditor recording their examination, findings, and analysis of the CSMS, such as completed audit checklists.
Auditee	An auditee is a governmental, private, and nongovernmental organization as a whole or parts thereof being CSMS audited and evaluated.

Auditor	An auditor is an organization who has an authorized duty to conduct, monitor, control, and prove audit compliance with the CSMS.
Conformity	Fulfillment of a requirement
CSMS	a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving cyber security to achieve the organization's objectives. It consists of a framework, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its assets.
CSMS Audit	An audit centered on a Cyber Security Management System.
Cyber Security Audit	Security audit includes conducting penetration testing to computer-based critical infrastructures to identify vulnerabilities or assessing the organization`s CSMS under the national cyber security framework and adopted international cyber security frameworks. If necessary, corrective measures should be taken.
Cyber Security Test and Evaluation	Development, procurement, or deployment testing and evaluating information technology products, services, systems, and processes according to national cyber security frameworks and criteria.
Evaluation Scorecard	Evaluation Scorecard is a tool used to show the organization's cyber security audit results and its current security posture at a national level.
Follow-Up Activity	An activity determines whether management has taken appropriate corrective actions to resolve deficiencies.
Joint Audit	An audit carried out at a single auditee by two or more auditing organizations
Nonconformity	Nonfulfillment of a requirement,
Requirement	Need or expectation that is stated, generally implied, or obligatory.
Risk-Based Audit	An audit is planned and conducted based on an assessment of risks, specifically cyber security risks in the CSMCSRS, ISO27k, and organizational context, plus audit and other risks such as health and safety;

1. Introduction

A Cyber security audit and evaluation guideline outlines the ways to audit and evaluate an organization's overall compliance with CSMS regulatory requirements and cyber security stance. This guideline creates a common language and sets a standard for conducting cybersecurity audits and evaluations. It helps the auditor monitor and evaluates the security posture of organizations. Organizations conduct audits and evaluations to validate the effectiveness and efficiency of CSMS implementation, particularly cyber security vulnerabilities, and evaluate the information technology products and systems before being set into operation to ensure that they meet the national cyber security framework and criteria.

CSMS audit addresses the core security objectives such as confidentiality, integrity, availability, and other cyber security principles. It focuses on all aspects of organizational cybersecurity processes, people, and technology. The audit results help the target audience to determine whether they fulfill their security needs and what should be measured, properly implement the security measure, and hold themselves accountable for any violations of the framework.

The audit is mainly intended to check compliance and evaluate the implementation of controls taken by organizations to ensure cyber security based on the national and international frameworks accepted by INSA, to identify gaps and indicate corrective measures, and to hold organizations that do not comply with mandatory cyber security frameworks accountable by law based on the audit results. INSA will conduct an audit and evaluation of the human, process, and structural issues through the mandatory national cyber security frameworks developed according to the latest version of CMCSRS. The information technology and security products will be audited and evaluated based on the international Common Criteria for Information Technology Security Evaluation (CC) and other international frameworks accepted by INSA.

This guideline contains three focus areas. The first one presents the benefit of CSMS audit and the principle of conducting an audit. This part helps to understand the concept and principles of the guideline and the issues that auditors should consider while conducting audits. The second focus area addresses the fundamental audit requirement to understand and manage the audit target area, the context of the CSMS audit, and the active entity involving the audit process. The auditee and auditor should properly understand and implement the requirements. The third part focuses on the audit conducting process, which defines the life cycle of the audit process.

Furthermore, it addresses the competence of the CSMS auditors. Applying this guideline plays a vital role in validating the compliance of the CSMS.

2. Objective

The objective of this guideline is to provide guidance to conduct internal or external audits, evaluate a CSMS, and manage a CSMS audit program against the requirements specified in national and international cyber security frameworks.

3. Scope

This guideline provides guidance on conducting a CSMS audit, including the audit program, process, auditing, and competence of the CSMS auditor. It applies to governmental, private, and other organizations to conduct and manage internal and external audits of the CSMS.

4. Normative References

The following documents are normatively referenced in this guideline in such a way as to assure the compliance of the organization's CSMS.

1. Critical Mass Cyber Security Requirement Standard
2. Common Criteria (CC) for Information Technology Security Evaluation

5. Cyber Security Audit Principle

A security audit principle helps to make the audit an effective and reliable tool in support of management policies and controls by providing information on which an organization can act to improve its performance. Adherence to these principles is a prerequisite for providing audit conclusions that are relevant and necessary for enabling auditors to work independently from one another to reach similar conclusions in similar circumstances.

The core principles of auditing that govern the professional responsibilities of an auditor use the following pillars.

a) **Integrity:** Auditors and individuals managing an audit program should perform their work ethically, with honesty and responsibility. The auditors should only undertake audit activities if they are competent to do so. The auditors should perform their work impartially.

b) **Confidentiality:** Auditors should exercise discretion in the use and protection of information acquired in the course of their duties. Audit information should not be used

inappropriately for personal gain by the auditor or in a manner detrimental to the interests of the auditee.

c) **Independence:** Auditors should be independent of the activity being audited wherever practicable, and should in all cases act in a manner that is free from bias and conflict of interest. For internal audits, auditors should be independent of the function being audited if practicable. Auditors should maintain objectivity throughout the audit process to ensure that the audit findings and conclusions are based only on the audit evidence.

d) **Due Professional Care:** Auditors should exercise due care in accordance with the importance of the task they perform and the confidence placed in them by the audit client and other interested parties.

e) **Risk-Based Approach:** The target audience (auditors) should consider the risks and opportunities associated with the auditing and evaluation process. The risk-based approach should substantively influence the planning, conducting, and reporting of audits to ensure that the audits are focused on matters that are significant for the audit client to achieve the audit program objectives.

f) **Evidence-Based Approach:** The evidence-based approach principle is the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process. Audit evidence should be verifiable. It should, in general, be based on samples of the information available since an audit conducted during a finite period with finite resources. Appropriate use of sampling should be applied since it is closely related to the confidence that can be placed in the audit conclusions.

g) **Fair Presentation:** It is **t**he obligation to report truthfully and accurately. Audit findings, audit conclusions, and audit reports should reflect truthfully and accurately the audit activities. Significant obstacles encountered during the audit and unresolved diverging opinions between the audit team and the auditee should be reported. The communication should be truthful, accurate, objective, timely, clear, and complete.

h) **Accountability:** The auditee holds accountability due to noncompliance with the national and adopted international cyber security frameworks. The auditee should provide accurate and relevant information to the auditor. The auditee organization should accept the audit finding result and apply the stated recommendations.

6. Cyber Security Audit Context

Cyber security audits mainly consider the target of audit, the target audience, and the context of evaluation.

6.1. Target of Audit

Target of Audit is the focus area of targeting in the auditing process in a cyber-security management system with a set of cyber security pillars. Organizations should audit and evaluate their human (capability, activity, action, responsibility, and accountability), process, and technology for corrective cyber security measures.

a) **People**: People are the most vital pillar of cyber security strategy. Most cybersecurity breaches are caused or aided by human error or weakness. People are a very critical pillar in any organization. People are active entity that engages in cyber security; they act as owners, employees, users, managers, and regulators who involve in the CSMS of the organization. From the perspective of people, the security attributes should include but are not limited to career paths, security awareness, security culture, security education, capacity building, personnel clearance, privacy, intellectual property rights, role and responsibility, top-level commitment, and so forth.

b) **Process and Structure**: Processes are keys to the business process to achieve the organization's mission through implementing an effective CSMS. A process is a basic unit to continuously and effectively governs, manages, executes, and builds the capability of an organization. From the perspective of the process and structure, the security attributes, such as cyber security frameworks that are used to govern and manage the entire cyber security domain, include core business practices, organizational structure, communication, cyber security programs, incident management, risk management, asset management, supply chain management, vulnerability scanning, penetration testing, and so forth.

c) **Technology:** Technology enables an organization to achieve its mission. The organization should assure the security of technology during its development, deployment, use, procurement, handling, disposal, and so forth. From this perspective, the security attributes include but are not limited to network, hardware, software, firmware, database, operating system, web, application, Internet of Things (IoT), cloud

computing, tools and technologies used to manage incidents, network technologies, cryptographic technologies, and evolving technologies.

6.2. Target Audience

The target audience is groups that have a stake in the audit and evaluation of the CSMS of an organization. The target audience can also be a group and/or individuals that are responsible and accountable for audit and evaluation processes.

a) **Regulatory Auditor:** INSA is the regulatory body responsible for the management and oversight of cyber security audits and evaluations. Key critical infrastructures will be audited and evaluated only by INSA.
b) **Internal Auditor**: The organization's internal self-auditor team conducts an internal audit. The internal audit team must be certified by a regulatory body. The team should be responsible to ensure that the evaluation fulfills the needs of security requirements;
c) **External Auditor**: The external security audit should be done by a regulatory body or a registered auditor, i.e., an organization that is certified by the regulatory body;
d) **Auditee**: organization as a whole or parts thereof being audited;
e) **Groups of Experts:** These are a group of experts holding different responsibilities in CSMS. These include:
    1. **Cyber Security Officer**: responsible for determining and meeting organizational cyber security frameworks and requirements;
    2. **Cyber Security Framework Formulator:** responsible for designing and setting administrative, technical, and physical requirements of CSMS;
    3. **Cyber Security Auditor**: responsible for evaluating the adequacy of the security of the CSMS per the defined requirements;
    4. **Security Evaluator**: responsible for forming judgments about the conformance of CSMS to their security requirements;

6.3. Context of Evaluation

a) The audit process should consider the organization's size, business nature, security posture, and maturity level.
b) Auditors should understand the overall audit objectives as the nature, timing, and extent of audit procedures vary depending on the audit objective.

c) The auditor should develop a unified and integrated cyber security audit model that assists in assessing and measuring the level of cyber security maturity and cyber readiness in any type of organization, no matter what industry or sector the auditee organization is positioned.

d) The auditor should build a mind-mapping diagram that serves as a model for accomplishing standardized audits.

   1. First, cyber security should be identified;
   2. Next, the specific security aspects under the main target of audit and evaluation should be inclusively listed and justified;
   3. Then, the cyber security governance frameworks that are internationally accepted regionally adapted, and nationally developed across all business sectors and industries should be determined.

e) The target audience should map against a specific cyber security framework's regulatory requirement to satisfy the demands of industry regulators, comply with internal or external audits, and satisfy business purposes and customer requirements, or simply by improving the enterprise`s cyber security strategy.

7. Managing Audit Program

7.1. Managing the CSMS Audit Program

a) Managing a program of CSMS audit involves planning, controlling, and monitoring/overseeing through the following activities.

   1. Prioritizing, planning, and outlining the scope of individual CSMS audits within the overall audit work program, perhaps combining wide-scope CSMS audits with more tightly-focused audits going to be more depth on areas of particular concern (e.g., Longstanding issues or significant risks);
   2. Allocating suitable resources to undertake planned and approved audits (e.g., Ensuring that CSMS auditors are trained, competent, and motivated to do the work to a required level of quality);
   3. Arranging or coordinating CSMS audits at multi-site organizations, including multinationals and 'group' structures, where comparisons between the CSMSs in operation within individual business units can help share and promote good practices;

4. Auditing the CSMSs of second parties, such as suppliers and business partners;

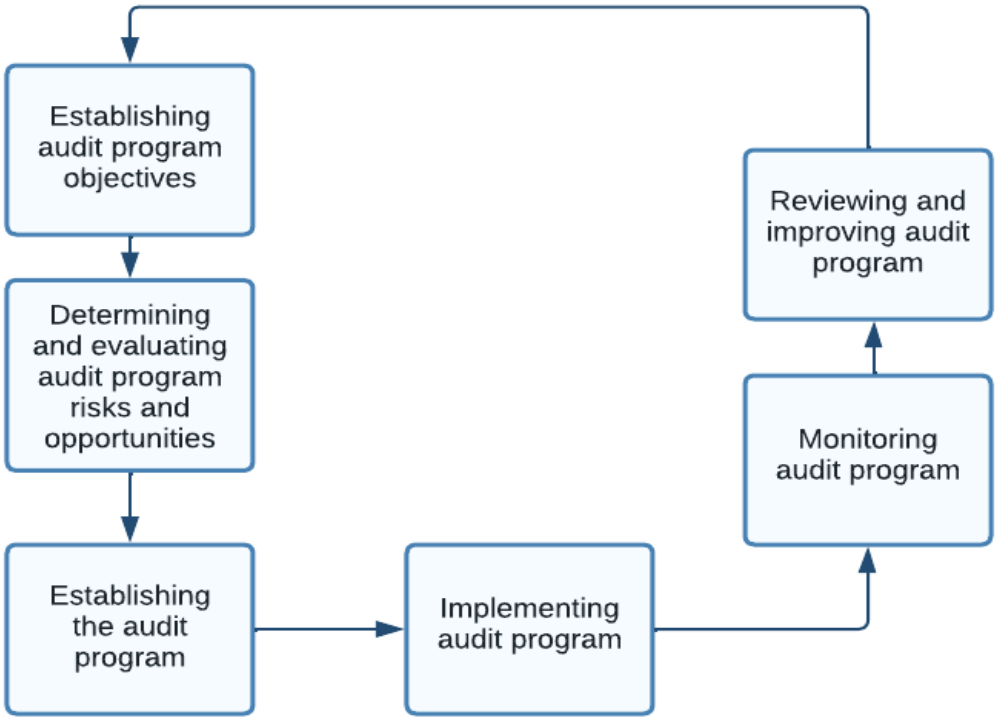

Figure 1: Process of Audit Management Program

7.1.1. Establishing the Audit Program Objectives

a) The audit client should ensure that the audit program objectives are established to direct the planning and conducting of audits and the implementation of the audit program effectively. Audit program objectives should be consistent with the audit client's strategic direction and support management system policy and objectives.

b) An organization should create an audit program to conduct audits, taking into account the risks and opportunities determined when planning the CSMS. Determining audit program objectives can include:

1. identification of cyber security requirements;
2. requirements of Ethiopian cyber security framework;
3. auditee's level of performance, as reflected in the occurrence of information security events and incidents and effectiveness of the CSMS;

4. information security risks to the relevant parties, i.e., the auditee include the following:
    i. verifying conformity with the relevant legal and contractual requirements and other requirements and their security implications;
    ii. obtaining and maintaining confidence in the risk management capability of the auditee;
    iii. evaluating the effectiveness of the actions to address information security risks and opportunities;

7.1.2. Determining and Evaluating Audit Program Risks and Opportunities

a) Measures to ensure cyber security should be determined considering auditee and other relevant party requirements. Other requirements can include relevant legal and contractual requirements.

b) There are risks and opportunities related to the context of the auditee that should be associated with an audit program and can affect the achievement of its objectives. The individual(s) managing the audit program should identify and present to the audit client the risks and opportunities considered when developing the audit program and resource requirements. There can be risks associated with the following:

1. Planning: failure to set relevant audit objectives and determine the extent, number, duration, locations, and schedule of the audits;
2. Resources: allowing insufficient time, equipment, and/or training for developing the audit program or conducting an audit;
3. selection of the audit team: insufficient overall competence to conduct audits effectively;
4. communication: ineffective external/internal communication processes/channels;
5. implementation: ineffective coordination of the audits within the audit program, or not considering information security and confidentiality;
6. control of documented information: ineffective determination of the necessary documented information required by auditors and relevant interested parties, failure to adequately protect audit records to demonstrate audit program effectiveness;

7. monitoring, reviewing, and improving the audit program: ineffective monitoring of audit program outcomes;
8. availability and cooperation of the auditee and availability of evidence to be sampled.

7.1.3. Establishing Audit Program

a) The roles and responsibilities of the individual(s) participating in the audit program should be declared.
b) Determine and ensure the provision of all necessary resources.
c) The individual(s) managing the audit program should have the necessary competence to manage the program.
d) The development of the audit program considers the following factors:
    1. the size of the organizational CSMS;
    2. the complexity of the CSMS (including the number and criticality of processes and activities) taking into account differences between sites within the CSMS scope;
    3. the significance of the information security risks identified for the CSMS to an organization;
e) The audit program should be developed based on the scope and objectives of the audit that include procedures to obtain sufficient, relevant, and reliable evidence to draw and support audit conclusions and opinions.
f) A best practice requires an audit program that contains the following:
    1. description of the audit area;
    2. audit objectives;
    3. criteria and resources for each audit step;
    4. work paper reference;
    5. auditor that performs the audit;
    6. audit performing dates;
    7. comments (e.g. If not applicable and why);
    8. conclusion;
    9. time and extent of auditing;

g) Procedures established for the audit program should address communication among participants, and resource identification in the audit program management.
h) When determining resources for the audit program, the individual(s) managing the audit program should consider:
    1. the financial and time resources necessary to develop, implement, manage, and improve audit activities;
    2. audit methods;
    3. the individual auditors and technical experts having competence appropriate to the particular audit program objectives;
    4. the extent of the audit program and audit program risks and opportunities;
i) In particular, for the significant risk applicable to the auditee and relevant to the audit program objective, CSMS auditors should allocate sufficient time to review the effectiveness of the actions to address cyber security risks and CSMS risks and opportunities.

7.1.4. Implementing Audit Program

a) The auditor should define audit objectives, scope, and criteria. These should be consistent with the overall audit program objectives.
b) The audit objectives include the following:
    1. evaluation of whether the CSMS adequately identifies and addresses cyber security requirements;
    2. determination of the extent of conformity of cyber security control with the requirements of CSMS;
c) The audit scope should take into account the following cyber security risks and opportunities affecting the CSMS of relevant parties:
    1. boundaries of the CSMS of the auditee are clearly defined based on internal and external issues;
    2. addresses the needs and expectations of interested parties;
    3. addresses the requirements stated in CMCSRS, Ethiopian cyber security frameworks, and adopted international standards based on the scope;
d) The audit criteria should consider the conformity determined as follows:
    1. national cyber security frameworks;

2. cyber security framework, cyber security objectives adopted by the auditee;
3. legal and contractual requirements and other requirements relevant to the auditee;
4. the auditee cyber security risk criteria, cyber security risk assessment process, and risk treatment process;
5. the methods and criteria for monitoring, measurement, analysis, and evaluation of the cyber security performance and the effectiveness of the CSMS;

e) The individual(s) managing the audit program should select and determine methods to conduct an audit effectively and efficiently depending on the defined audit objectives, scope, and criteria.

f) If a joint audit is conducted, particular attention should be paid to the non-disclosure of information between the relevant parties. Agreement should be reached with all interested parties before the task of audit is commenced.

g) Selecting internationally qualified audit team members and cyber security auditor who have competence in cyber security audit, including adequate knowledge, skill, and ethics.

h) Assigning responsibility for an individual audit to the audit team leader,

i) Managing and maintaining the audit program`s records and outcomes.

j) The individual(s) managing the audit program should ensure that the following activities are performed:

1. evaluation of the achievement of the objectives for each audit within the audit program;
2. review and approval of audit reports regarding the fulfillment of the audit scope and objectives;
3. review of the effectiveness of actions taken to address audit findings;
4. distribution of audit reports to relevant interested parties;
5. determination of the necessity for any follow-up audit;

k) The individual(s) managing the audit program should ensure that audit records are generated, managed, and maintained to demonstrate the implementation of the audit program. The audit records can include the following:

1. records related to audit programs, such as schedule of audits, audit program objectives and extent, those addressing audit program risks, and opportunities, and relevant external and internal issues;

2. records related to each audit, such as audit plans and audit reports, objective audit evidence and findings, nonconformity reports, corrections, and corrective action reports, and audit follow-up reports;
3. records related to the audit team covering topics, such as competence and performance evaluation of the audit team members and criteria for the selection of audit teams;

7.1.5. Monitoring Audit Program

a) The individual(s) managing the audit program should ensure the evaluation of:
    1. whether schedules are being met and audit program objectives are being achieved;
    2. the performance of the audit team members, including the audit team leader and the technical experts;
    3. the ability of the audit teams to implement the audit plan;
    4. feedback from auditees, auditors, technical experts, and other relevant parties;
    5. sufficiency and adequacy of documented information in the whole audit process;
b) The individual(s) managing the audit program and the auditee should review the audit program to assess whether its objectives have been achieved. Lessons learned from the audit program`s review should be used as inputs for the improvement of the program.

7.1.6. Reviewing and Improving Audit Program

a) The individual(s) managing the audit program and the audit client should review the audit program to assess whether its objectives have been achieved. Lessons learned from the audit program`s review should be used as inputs for the improvement of the program.

7.2. Managing CSMS Audit Conducting

a) Each CSMS audit is managed throughout the cyber security process shown in section 8. Audit management activities include the following:
    1. gaining support from management to conduct the CSMS audit as proposed in the outline, with their agreement in principle and authority to proceed with the detailed scoping and planning (which may lead to a further authorization step once finalized);
    2. supervising, guiding, motivating, and supporting auditors, ensuring they follow accepted audit practices, conducting file reviews, and proofreading draft reports;

3. reviewing and challenging unsubstantiated or notable findings e.g., playing the devil's advocate to explore the evidence, depth of analysis, and nature of issues; proposing alternative explanations and potential recommendations; helping auditors evaluate the risks in the business context;
4. dealing with issues that jeopardize the audit assignment such as interpersonal problems, lack of engagement, delays, reluctance or refusal to supply essential information, etc. (issues may be raised or escalated by anyone involved in the process);
5. liaising with management, perhaps providing interim updates and setting expectations for the audit reporting phase;

b) Ensure the auditor has obtained security clearance to access asset that is required for audit activities.

c) The feasibility of the audit should be determined, taking into consideration such factors as the availability of:

1. sufficient and appropriate information for planning the audit,
2. adequate cooperation from the auditee, and
3. adequate time and resources;

8. Cyber Security Audit Process

The auditing process includes continuously monitoring the entire business network to detect and identify flaws that can be exploited for an attack. An audit process should comprise a step-by-step set of audit procedures and instructions such as audit scope, audit plan, audit fieldwork, audit analysis, audit report, and audit closure.

8.1. Audit Scope

a) During this phase, auditors should determine the focus areas for the audit, and any areas that are explicitly out-of-scope, based normally on an initial risk-based assessment and discussion with those who commissioned the security audit.

b) Auditors should ensure that the audit scope makes sense to the organization.

c) The audit scope should be mapped with the context of the auditee's business unit, process, and risk vulnerability. For example, large organizations with multiple divisions or business units, or separate cyber security departments, or an all-encompassing

enterprise-wide cyber security management, or some combination of local and centralized security management systems may have separate cyber security departments.

d) The auditors should pay particular attention to information risks and security controls associated with information conduits to other entities (organizations, business units, etc.) that fall outside the scope of the CSMS. For example, checking the adequacy of information security-related clauses in Service Level Agreements or contracts with IT service suppliers should be given due attention.
e) During the pre-audit survey, auditors should identify the main stakeholders, such as information risk and security managers and influential figures in the organization's cyber security department. In addition, other professionals, such as security architects, security administrators, IT and human resource facilitators, physical security professionals, CSMS framework formulators, and implementers perhaps take the opportunity to request pertinent documentation will be reviewed during the audit.
f) Management normally nominates one or more audit "escorts" - individuals who are responsible for ensuring that the auditors can move freely about the organization and rapidly find the people, information, and so on necessary to conduct their work.
g) Contact lists and other preliminary documents are also obtained and the audit files are opened to contain documentation (audit working papers, evidence, notes, feedback, draft, and final reports, etc.) arising from the audit.
h) The primary output of this phase is a security audit scope, charter, engagement letter, or similar agreed upon between the auditor organization and auditee organization.

8.2. Audit Plan

a) The determining audit scope should be broken down into detail, typically by generating a security audit checklist.
b) The audit checklist should be developed based on targeting, auditing, and evaluating the focus area`s assets and the purpose of validating compliance. It reflects and refers primarily to the national, adopted international and industrial standards mandatory security requirements.
c) Once the subject, objective, and scope are defined, the audit team can perform pre-audit planning and identify the resources needed to perform the audit work. Some of the resources to be defined are listed as follows:

1. technical skills and resources needed;
2. the budget and effort needed to complete the engagement;
3. locations or facilities to be audited;
4. roles and responsibilities among the audit team;
5. the time frame for the various stages of the audit;
6. sources of information for testing or reviewing, such as functional flowcharts, policies, standards, procedures, and prior audit work papers;
7. points of contact for administrative and logistics arrangements;
8. A communication plan that describes to whom to communicate, when, how often, and for what purposes;

d) To perform audit planning, an auditor should perform the following steps:
   1. gain an understanding of the organization's mission, objectives, purpose, and processes, which include information and processing requirements such as availability, integrity, security, business technology, and information confidentiality;
   2. gain an understanding of the organization's governance structure and practices related to the audit objectives;
   3. understand changes in the business environment of the auditee;
   4. review prior work papers;
   5. identify stated contents such as policies, standards, required guidelines, procedures, and organizational structure;
   6. perform a risk analysis to help the designing of the audit plan;
   7. set the audit scope and audit objectives;
   8. develop the audit approach or audit strategy;
   9. assign personnel resources to the audit;
   10. address engagement logistics,

e) The overall timing and resourcing of the audit should be determined by the management of both the auditee and the auditor in the form of an audit plan or schedule.

f) The Security Audit Plans should identify and put broad boundaries around the remaining phases of the audit.

g) The auditor should make preliminary bookings for the formal audit discussion meeting due at the end of the audit to allow senior participants to schedule their attendance.

h) Audit plans should include checkpoints and specific opportunities for the auditors to provide informal interim updates to their management contacts including preliminary notification of any observed inconsistencies or potential nonconformities, etc.

i) The audit plan should be an opportunity to raise any concerns over limited access to information or people, and for management to raise any concerns over the nature of the audit work.

j) The timing of important audit work elements may be determined, particularly to prioritize aspects that are believed to represent the greatest risks to the organization and if the specific target of auditing focus is found to be inadequate.

k) The output of this phase is the (customized) security audit checklist and an audit plan agreed upon with management.

8.3. Audit Fieldwork

a) During audit fieldwork, audit evidence is gathered by the auditors working methodically through the audit checklist; for example, interviewing staff, managers, and other stakeholders associated with the audit scope, audit target, document review, printouts, and data (including records of cyber security activities such as security log reviews), observing security processes in action and checking system security configurations, etc.

b) Auditors use possible methods to collect relevant information during the audit including:

   1. review of documented information (including computer logs and configuration data);
   2. visit information processing facilities;
   3. observation of CSMS processes and related controls;
   4. use of automated tools;

c) The auditor should review documents relating to and arising from the audit scope and objective.

d) The auditor generates audit documentation comprising audit evidence and notes in the form of completed audit checklists and working papers.

e) The auditor should verify that documented information as required by the audit criteria and relevant to the audit scope exists and conforms to the audit criteria requirement.

f) The auditor should confirm that the determined controls within the scope of the audit should be related to the results of the risk assessment and risk treatment process.

g) Findings from the documentation review often indicate the need for specific audit tests to determine how closely the target of auditing as currently implemented follows the documentation, as well as testing the general level of compliance and appropriateness of the documentation.

h) Technical compliance tests may be necessary to verify the configuration of the organization's information security policies, standards, and guidelines.

i) Automated configuration checking and vulnerability assessment tools may speed up the performance rate at which the technical compliance checks are performed, but they potentially introduce security issues that need to be taken into account.

j) Audit tests are performed to evaluate and validate the evidence as it is gathered.

k) The output of this phase should be an accumulation of audit working papers and evidence in the audit files. During this phase, audit works papers are prepared, documenting the tests are performed, evidence is gathered, and initial results are generated.

8.4. Audit Analysis

a) The accumulated audit evidence is sorted out, filed, reviewed, and examined with the cyber security risks, audit criteria, audit scope, and objectives.

b) Preliminary findings, conclusions, and recommendations should be developed at this stage, concerning any significant issues identified.

8.5. Audit Report

a) The auditor ensures that findings in the audit report are supported by sufficient and appropriate evidence.

b) A cyber security audit report should contain the following elements:

1. title and introduction, including naming the organization and clarifying the scope, objectives, period of coverage, the nature, timing, and extent of the audit work performed;
2. an executive summary indicating the key audit findings, a brief analysis and commentary, and an overall conclusion;

3. the intended report lists, specific recipients and appropriate document classification or instructions on circulation;
4. an outline of the credentials, audit methods, and so forth.
5. individual auditors` and team members' participation and their roles in the audit process;
6. detailed audit findings and analysis, sometimes with extracts from the supporting evidence in the audit files which aids comprehension;
7. the audit conclusions and recommendations, perhaps initially presented as tentative proposals to be discussed with management and eventually incorporated as agreed on action plans depending on adapted practices;
8. a formal statement by the auditors of any reservations, qualifications, scope limitations, or other warnings to the audit;
9. depending on normal audit practices, management may be invited to provide a short commentary or formal response, accepting the results of the audit and committing to any agreed actions;

c) The audit's quality assurance processes should ensure that everything reportable is reported and everything reported is reportable, normally based on a review of the audit file by an experienced senior auditor. These include the following:
    1. factual basis meaning sufficient and appropriate audit evidence to support the findings reported;
    2. the wording of the draft audit report is checked to ensure readability and avoidance of ambiguity and unsupported statements;
    3. when approved by audit management for circulation, the draft audit report is usually presented to and discussed with management;
    4. further cycles of review and revision of the report may take place until it is finalized;
    5. Finalization typically involves management committing to the action plan.
d) Audit finding result should outline their maturity level based on section 9 (evaluation scorecard) requirements (i).
e) The auditor’s assessment of the significance of any issues or shortcomings identified during the audit is the main determinant of a ‘pass’ or ‘fail’ result. The audit findings are

commonly categorized according to their significance or severity, and (at least in respect of certification audits) reported as follows:

1. **Major Non-Conformance Report:** It is a nonconformity that substantially affects the capability of cyber security to achieve its objectives. Nonconformities may be classified as major in the following circumstances:
    i. if there is significant doubt that effective process control is in place, that the confidentiality, integrity, and availability of assets meets specified requirements; or
    ii. Several minor nonconformities associated with the same requirement or issues are symptoms indicative of a deeper and more substantial failure in the management system (e.g. poor governance).
2. **Minor Non-Conformance Report:** It is a nonconformity that does not substantially affect the capability of cyber security to achieve its objectives. Substantiality is a subjective matter for the auditor to determine taking into account the following factors.
    i. the degree of departure from the recommendations in cyber security frameworks, or generally accepted good practices in this domain;
    ii. whether the nonconformity is deliberate/intentional, or merely an oversight;
    iii. the duration of the nonconformity is a complex issue since sometimes longstanding issues are worth escalating to management's attention, yet the organization may have coped quite successfully with the nonconformity for the intervening period;
    iv. The amount of information risk to the organization (by far the most important factor);
3. **Observation or Opportunity for Improvement:** a statement of fact substantiated by objective evidence, and identifying a weakness or potential deficiency in the cyber security that, if not resolved, the auditor belief may lead to nonconformity in the future.
    i. according to convention and circumstances, the auditor may offer formal or informal recommendations, guidance, and advice (e.g., promoting good

practices and other improvements) but no specific solution need necessarily be provided;

ii. if an audit finding is expressed effectively and the issue is discrete, the resolution will often be self-evident;

iii. audits are merely advisors, i.e. management must decide what to do and when to do it, if at all;

iv. The output of this phase is a completed cyber security audit report; signed, dated, and distributed according to the terms of the audit engagement letter;

8.6. Audit Follow-Up and Audit Closure

a) Responsibility for cyber security audit follow-up activities should be defined in the audit charter.

b) After the reporting of findings and recommendations, the auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management promptly.

c) Progress on the overall status of the implementation of audit findings should be regularly reported to the auditor.

d) The nature, timing, and extent of the follow-up activities should be taken into account the significance of the reported finding and the impact if corrective action is not taken.

e) The timing of cyber security audit follow-up activities about the original reporting should be a matter of professional judgment dependent on some considerations, such as the nature or magnitude of associated risks and costs to the entity.

f) A report on the status of follow-up activities, including agreed recommendations not implemented, may be presented to the audit committee if one has been established, or to the appropriate level of entity management.

g) As a part of the follow-up activities, the cyber security auditor should evaluate whether findings, if not implemented, are still relevant.

h) Where management provides information on actions taken to implement recommendations, the security auditor has doubts about the information provided, and appropriate testing or other procedures should be undertaken to ascertain the true position or status before concluding follow-up activities.

i) If management's proposed actions to implement reported recommendations have been discussed with or provided to the auditor, these actions should be recorded as a management response in the final report.

j) In addition to indexing, cross-referencing, and shutting the audit files, closure involves clean-up any loose ends, preparing notes for future cyber security audits, and perhaps following up to check that the agreed actions are completed more or less on time and as specified.

9. Evaluation Scorecard

a) When conducting a cyber security audit, both types of testing – compliance and substantive testing should be involved.

b) Compliance testing determines if controls are being applied in the manner described in the program documentation or as described by the auditee.

c) Compliance test determines if controls are being applied in a manner that complies with security governance frameworks.

d) Substantive audit substantiates the adequacy of existing controls in protecting the organization from fraudulent activity and encompasses substantiating the reported results of processing transactions or activities.

e) With the help of computer-assisted audit tools and techniques (CAATs), security auditors can plan for 100% substantive testing of the auditee's data.

f) The assessment of each security requirement/control can comply with a minor nonconformity or with a major nonconformity:

g) The specific security requirement evaluation is calculated after the audit has been completed. The evaluation consists in assigning scores and ratings for each specific security requirement.

h) The final cyber security maturity rating of each audit score should be calculated and summarized by using the following criteria.

i) The audit score can be mapped to a specific maturity level.

j) The auditee`s organization audit results should be classified under the following maturity level.

Score	Maturity	Justification

	Level	
0-35	**Immature**	Auditee organization`s security posture is poor in cyber security and cyberspace practices. Deployed security requirements/controls are inexistent or very weak.
36-75	**Developing**	Auditee organization`s security posture is in progress to protect its cyber landscape/climate. The organization is starting to focus on cybersecurity matters. If technologies are in place, the auditee organization's attention should be focused on processes and people to protect cyber assets.
76-90	**Mature**	Auditee organization`s security posture is matured. Improvements are required to the key security areas that have been identified with weaknesses.
91-100	**Advanced**	Auditee organization`s security posture is excellent. There is always room for improvement. The organization should become a national leader and help other governmental organizations with cyber security and cyberspace matters.

Table 1: Audit Maturity Evaluation Scorecard

10. Competence of Auditor

a) Professional competence denotes the possession of skills, knowledge, and expertise through an adequate level of education and experience, which enable the auditors appropriately perform an audit engagement.

b) Confidence in the audit process and the ability to achieve its objectives depends on the competence of those individuals who are involved in performing audits, including auditors and audit team leaders.

c) The auditor`s competence should be evaluated regularly through a process that considers personal behavior, and the ability to apply the knowledge and skills gained through education, work experience, auditor training, and audit experience.

d) Each auditor, in the audit team, does not need to have the same competence. However, the overall competence of the audit team needs to be sufficient to achieve the audit objectives.

e) The evaluation of the auditor`s competence should be planned, implemented, and documented to provide an outcome that is objective, consistent, fair, and reliable.

f) The evaluation process should include four main steps, as follows:
    1. determine the required competence to fulfill the needs of the audit program;
    2. establish the evaluation criteria;
    3. select the appropriate evaluation method;
    4. conduct the evaluation;

g) Auditors should develop, maintain, and improve their competence through continuing professional development and regular participation in audits.

10.1. Determining Auditor Competence

a) The general auditors should have knowledge and skills related to the following:
    1. the size, nature, complexity, products, services, and processes of auditees;
    2. the methods for auditing;
    3. the management system disciplines to be audited;
    4. the complexity and processes of the management system to be audited;
    5. the types and levels of risks and opportunities addressed by the management system;
    6. the objectives and extent of the audit program;
    7. the uncertainty in achieving audit objectives;
    8. Other requirements, such as those imposed by the audit client or other relevant interested parties, where appropriate;

b) The following requirements apply to the audit team as a whole, or the auditor if working alone. In each of the following areas of knowledge and expertise, at least one audit team member should take primary responsibility within the team.
    1. Managing the team, planning the audit, and assuring audit quality processes;
    2. Audit principles, methods, and processes;
    3. Management systems in general and CSMS in particular;
    4. Relevant legislative, regulatory, and contractual obligations applicable to the organization being audited;
    5. Information-related threats, vulnerabilities, and incidents, particularly concerning the organization being audited and comparable organizations;
    6. CSMS measurement techniques (information security metrics);

7. Relevant CSMS standards, industry best practices, security policies, and procedures;
8. Business continuity management, including business impact assessment, incident management, resilience, recovery, and contingency aspects;
9. The application of information technology to business and hence the relevance of and need for cyber security; and
10. Cyber security risk management principles, methods, and processes;

c) Auditors should be aware of the following**:**

1. **The field:** this is a dynamic area with frequent changes to the information risks (i.e., the threats, vulnerabilities, and/or impacts); security controls and the cyber environment; emerging and current threats; vulnerabilities being actively exploited, and the changing nature of incidents, and impacts within the organization's business context;
2. **Changes to national, international, and other sector-specific frameworks**: new and updated standards in Ethiopia cyber security standard - ISO/IEC 27000-series, and others if there are frequent changes in other potentially relevant standards;
3. **Legal and regulatory changes:** a significant forthcoming change to privacy laws and practices with global business implications;
4. **Business and organizational changes:** changing business activities, processes, priorities, and relationships;
5. **Technology changes:** new hardware, software, and firmware; new paradigms, such as IoT (Internet of Things), BYOD (Bring Your Own Device), cloud computing, and emerging technology;

10.2. Personal Behavior

Auditors should possess the necessary attributes to enable them to act under the principles of auditing. Auditors should exhibit professional behavior during the performance of audit activities. Desired professional behaviors include, being:

a) ethical, i.e. fair, truthful, sincere, honest, and discreet;
b) open-minded, i.e. willing to consider alternative ideas or points of view;
c) diplomatic, i.e. tactful in dealing with individuals;

d) observant, i.e. actively observing physical surroundings and activities;
e) perceptive, i.e. aware of and able to understand situations;
f) versatile, i.e. able to readily adapt to different situations;
g) tenacious, i.e. persistent and focused on achieving objectives;
h) decisive, i.e. able to reach timely conclusions based on logical reasoning and analysis;
i) self-reliant, i.e. able to act and function independently while interacting effectively with others;
j) able to act with fortitude, i.e. able to act responsibly and ethically, even though these actions may not always be popular and may sometimes result in disagreement or confrontation;
k) open to improvement, i.e. willing to learn from situations;
l) culturally sensitive, i.e. observant and respectful of the culture of the auditee;
m) Collaborative, i.e. effectively interacting with others, including audit team members and the auditee's personnel;

10.3. Generic Knowledge and Skills of Security Auditors

a) Auditors should possess the knowledge and skills necessary to achieve the intended results of the audits they are expected to perform.
b) Cybersecurity auditors should familiarize themselves with influential international auditing frameworks.
c) Audit team leaders should have additional knowledge and skills necessary to provide leadership to the audit team.
d) Auditors should have knowledge and skills of audit principles, processes, and methods in this area to enable the auditor to ensure audits are performed consistently and systematically. An auditor should be able to:
    1. understand the types of risks and opportunities associated with auditing and the principles of the risk-based approach to auditing;
    2. plan and organize the work effectively;
    3. perform the audit within the agreed schedule;
    4. prioritize and focus on matters of significance;

5. communicate effectively, orally and in writing (either personally, or through the use of interpreters);
6. collect information through effective interviewing, listening, observing, and reviewing documented information, including records and data;
7. understand the appropriateness and consequences of using sampling techniques for auditing;
8. understand and consider technical experts' opinions;
9. audit a process from start to finish, including the interrelations with other processes and different functions, where appropriate;
10. verify the relevance and accuracy of collected information;
11. confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
12. assess those factors that may affect the reliability of the audit findings and conclusions;
13. document audit activities and audit findings, and prepare reports;
14. Maintain the confidentiality and security of information.

e) Management system standards and other references: knowledge and skills in this area enable the auditor to understand the audit scope and apply audit criteria, and should cover the following:
   1. management system standards or other normative or guidance/supporting documents used to establish audit criteria or methods;
   2. the application of management system standards by the auditee and other organizations;
   3. relationships and interactions between the management system(s) processes;
   4. understanding the importance and priority of multiple standards or references;
   5. Application of standards or references to different audit situations;

f) The organization and its context: knowledge and skills in this area enable the auditor to understand the auditee's structure, purpose, and management practices, and should cover the following:
   1. needs and expectations of relevant interested parties that impact the management system;

2. type of organization, governance, size, structure, functions, and relationships;
3. general business and management concepts, processes, and related terminology, including planning, budgeting, and management of individuals;
4. cultural and social aspects of the auditee;

g) Applicable statutory and regulatory requirements and other requirements: knowledge and skills in this area enable the auditor to be aware of, and work within the organization's requirements. Knowledge and skills specific to the jurisdiction of the auditee's activities, processes, products, and services should cover the following:

1. statutory and regulatory requirements and their governing agencies;
2. basic legal terminology;
3. contracting and liability;

10.4. Discipline and Sector-Specific Competence of Auditors

a) Auditors should possess generic competence and a level of discipline and sector-specific knowledge and skills.

b) Audit teams should have the collective discipline and sector-specific competence appropriate for auditing the particular types of management systems and sectors. The discipline and sector-specific competence of auditors include the following:

1. management system requirements, principles, and their application;
2. fundamentals of the discipline(s) and sector(s) related to the management systems standards as applied by the auditee;
3. application of discipline and sector-specific methods, techniques, processes, and practices to enable the audit team to assess conformity within the defined audit scope and generate appropriate audit findings and conclusions;
4. principles, methods, and techniques relevant to the discipline and sector, such that the auditor can determine and evaluate the risks and opportunities associated with the audit objectives;

10.5. Generic Competence of Audit Team Leader

a) To facilitate the efficient and effective conduct of the audit, an audit team leader should have the competence to:

1. plan the audit and assign audit tasks according to the specific competence of individual audit team members;
2. discuss strategic issues with top management of the auditee to determine whether they have considered these issues when evaluating their risks and opportunities;
3. develop and maintain a collaborative working relationship among the audit team members;

b) Manage the audit process, including:
1. making effective use of resources during the audit;
2. managing the uncertainty of achieving audit objectives;
3. protecting the health and safety of the audit team members during the audit, including ensuring compliance of the auditors with the relevant health and safety, and security arrangements;
4. directing the audit team members;
5. providing direction and guidance to auditors-in-training;
6. preventing and resolving conflicts and problems that can occur during the audit, including those within the audit team, as necessary;

c) Represent the audit team in communications with the individual(s) managing the audit program, the audit client, and the auditee;

d) Lead the audit team to reach the audit conclusions;

e) Prepare and complete the audit report.

10.6. Knowledge and Skills for Auditing Multiple Disciplines

When auditing multiple discipline management systems, the audit team member should have an understanding of the interactions and synergy between the different management systems. Audit team leaders should understand the requirements of each of the management system standards being audited and recognized the limits of their competence in each of the disciplines.

10.7. Achieving Auditor Competence

a) Auditor competence can be acquired using a combination of the following:
1. completing training programs that cover generic auditor knowledge and skills;

2. experience in a relevant technical, managerial, or professional position involving the exercise of judgment, decision-making, problem-solving, and communication with managers, professionals, peers, customers, and other relevant interested parties;
3. education/training and experience in a specific management system discipline and sector that contribute to the development of overall competence;
4. Audit experience acquired under the supervision of an auditor competent in the same discipline.

b) Auditing is a highly privileged activity that depends on the auditees' trust and respect, which must be earned by consistently high standards of professionalism, competence, and personal integrity. Auditors must be able to demonstrate their knowledge and experience:

1. Cyber security auditors should be holder recognized and relevant qualifications certification such as Certified Information Security Auditor, CMCSRS leader implementer, ISO 27001 Leader Implementer, Certified Ethical Hacker, Certified in Risk and Information Systems Control, and other mandatory internationally recognized cyber security auditor certifications;
2. Registration as an auditor with a recognized professional body such as ISACA;
3. Completion of recognized CSMS training courses such as lead implementer and lead auditor;
4. Up-to-date and continuous professional development records;
5. Records confirming the audits in which they have participated (particularly CSMS and IT audits), and their roles;
6. Practical demonstration to more experienced auditors in the course of CSMS audits;
7. Earning the trust and respect of colleagues;

10.8. Achieving Audit Team Leader Competence

a) An audit team leader should have acquired additional audit experience to develop competence. This additional experience should have been gained by working under the direction and guidance of a different audit team leader.

b) Up-to-date and continuous professional development records; e.g. completion of recognized security training courses such as lead implementer and lead auditor;

c) Records confirming the audits in which they have participated and ……their roles

10.9. Establishing Auditor Evaluation Criteria

a) The criteria should be qualitative (such as having demonstrated desired behavior, knowledge, or the performance of the skills, in training or the workplace) and quantitative (such as the years of work experience and education, number of audits conducted, hours of audit training).

b) Cyber security audit and evaluation management should communicate the desired and/or expected level of professional competence, based on appropriate benchmarks, for the different roles in audit engagements, and ensure such benchmarks are periodically reviewed and updated.

c) The audit management should document the professional competence required for various job levels, e.g., by documenting job/position descriptions or by formulating a skills matrix that indicates the professional competence required for the various job levels.

10.10. Selecting Appropriate Auditor Evaluation Method

a) The evaluation should be conducted using the following audit methods.
   1. The methods outlined represent a range of options and may not apply in all situations.
   2. The various methods outlined may differ in their reliability.
   3. A combination of methods should be used to ensure an outcome that is objective, consistent, fair, and reliable.

b) During auditing, the auditor should apply the following evaluation methods.

Evaluation method	Objectives	Examples
Review of records	To verify the background of the auditor	Analysis of records of education, training, employment, professional credentials, and auditing experience
Feedback	To provide information about how the performance of the auditor is perceived	Surveys, questionnaires, personal references, testimonials, complaints, performance evaluation, peer review
Interview	To evaluate desired professional behavior	Personal interviews

	and communication skills, to verify information and test knowledge and to acquire additional information	
Observation	To evaluate desired professional behavior and the ability to apply knowledge and skills	Role-playing, witnessed audits, on-the-job performance
Testing	To evaluate desired behavior and knowledge and skills and their application	Oral and written exams, psychometric Testing
Post-audit review	To provide information on the auditor performance during the audit activities, identify strengths and opportunities for improvement	Review of the audit report, interviews with the audit team leader, the audit team, and, if appropriate, feedback from the auditee

Table 2: Audit Evolution Method

10.11. Conducting Auditor Evaluation

a) The information collected about the auditor under evaluation should be compared against the stated criteria. When an auditor under evaluation, who is expected to participate in the audit program, does not fulfill the criteria, then additional training, work, or audit experience, should be undertaken and a subsequent re-evaluation should be performed.

10.12. Maintaining and Improving Auditor Competence

a) Auditors and audit team leaders should continually improve their competence. Auditors should maintain their auditing competence through regular participation in management system audits and continual professional development. This may be achieved through means such as additional work experience, training, private study (self-development), coaching, attendance at meetings, seminars, and conferences, or other relevant activities.

b) The individual(s) managing the audit program should establish suitable mechanisms for the continual evaluation of the performance of the auditors and audit team leaders.

c) The continual professional development activities should take into account the following:

1. changes in the needs of the individual and the organization responsible for the conduct of the audit;
2. developments in the practice of auditing including the use of technology;

3. relevant standards including guidance/supporting documents and other requirements;
4. changes in sector or disciplines;

Reference

1. ISO/IEC 27007: 2020 Information technology — Security techniques — Guidelines for information security management systems auditing.
2. ISO 19011 Guidelines for auditing management systems