Model
ISMS Internal Audit Procedure

Document Number:	Xxxx
Version:	4
Release Date:	October 2022

NOTE: this is a generic model procedure, a template. It is unlikely to be entirely suitable for your specific purposes. Please amend and enhance it as necessary to suit your organization's requirements.

0 Document History

Version	Date	Author	Change
2022	October 2022	Gary Hinson	Further minor updates to the wording
2012	October 2012	Gary Hinson	Reformatted plus minor updates
2007	September 2007	Richard O. Regalado and Gary Hinson	Updated and licensed for incorporation into the ISO27k Toolkit
2006	August 2006	Richard O. Regalado	Initial release

1 Purpose of this procedure

1.1 This procedure is intended to ensure that:

- the organization continually operates in accordance with the specified policies, procedures and external requirements in meeting company goals and objectives in relation to information security.
- improvements to the Information Security Management System (ISMS) are identified, implemented and suitable to achieve objectives.

2 Scope

2.1 This procedure:

- includes planning, execution, reporting and follow–up of ISMS internal audits; and
- applies to all departments/business units within scope of the organization's ISMS.

3 Rôles and responsibilities

3.1 Information Security Management Representative (ISMR)

- Appoints the Lead Auditor and the Audit Team (note: the Lead Auditor and ISMR may be the same person).
- Together with the Lead Auditor, reviews the corrective and preventive actions and the follow-up.
- Maintains confidentiality of the audit evidence, analysis and findings/results.

3.2 Lead Auditor

- Prepares an Audit Plan/Notification as a basis for planning the audit and for disseminating information about the audit.
- Leads the ISMS internal audit activities.
- Co-ordinates the audit schedule with concerned department/section heads.
- Plans the audit, prepares the working documents and briefs the audit team.
- Consolidates all audit findings and observations and prepares internal audit report.
- Reports critical non-conformities to the auditee immediately.
- Report to the auditee the audit results clearly and without delay.
- Conducts the opening and closing meeting.

3.3 Audit Team Member

- Supports the Lead Auditor's activities (may be the same person).
- Performs the audit using the consolidated audit checklist.
- Reports any non-conformities and recommends suggestions for improvement.
- Retains the confidentiality of audit findings.
- Acts in an ethical manner at all times.

3.4 Auditee

- Receives, considers and discusses the audit report.
- Determines, resources, drives and completes corrective actions as necessary.
- Is and remains accountable for protecting information assets.

4 Procedure

4.1 General

4.1.1 An ISMS audit programme shall be created that contains all scheduled and potential audits for the whole calendar year. This shall include schedule of internal audits, audits of suppliers, audits to be performed by clients and third-party audits, as appropriate.

4.1.2 Internal audits shall be scheduled twice a year or as the need arises.

4.1.3 Only competent personnel who are truly independent of the subject area shall perform audits.

4.1.4 Members of the Internal Audit Team shall be appointed and supervised by the Lead Auditor.

4.1.5 Auditees are notified *at least* three working days in advance of the audit, ideally up to a month before giving them ample time to prepare.

4.2 Planning and Preparing the Audit

4.2.1 An annual ISMS internal audit programme shall be prepared by the Lead Auditor and approved by top management. It should be revised to reflect any changes in the priorities or schedule during the year.

4.2.2 Based on the audit programme, the Lead Auditor shall prepare the respective audit plans.

4.2.3 The Audit Plan/Notification shall be prepared by the Lead Auditor, reviewed and approved by the ISMR. It shall be communicated to the auditor/s and the auditees. It shall be designed to be flexible in order to permit changes based on the information gathered during the audit. The plan shall include:

- Audit objective and scope.
- Department/Section and responsible individuals in charge.
- Audit team members. The number of auditors depends on the audit area size.
- Management system/s to be audited (possibly more than one at once *i.e*. combined audits).
- Date, place and timescale for the audit fieldwork, planned distribution date of the audit report and some indication of the anticipated date of the clearance meeting.

4.3 Pre-audit meeting

4.3.1 One or more pre-audit meetings between the ISMR, Lead Auditor and auditors shall take place not later than one day prior to the audit proper. Objectives are as follows:

- To ensure the availability of all the resources needed and other logistics that may be required by the auditor.
- The scope of the audit is verified from the Audit Plan

4.4 Opening meeting

4.4.1 An opening meeting, where deemed appropriate by the ISMR and Lead Auditor, shall be held on the day of the audit but before the audit proper. The following may be discussed during the opening meeting:

- The purpose and scope of the audit.
- Confirmation of the audit plan
- Clarification of other matters must be settled before the audit takes place.

4.5 Audit Execution

4.5.1 The auditor/s will perform the ISMS internal audit using several checklists:

- **ISMS Internal Audit Checklist/Observation Form**: contains specific items that are particular to the organizational unit to be audited. The assigned auditors are responsible for generating the questions and checks on this form.
- **Mandatory Requirements Checklist**: describes checks relating to the mandatory requirements from the main body of the applicable version of ISO/IEC 27001.
- **Discretionary Requirements Checklist**: describes checks pertaining to the information security controls outlined in Annex A of ISO/IEC 27001. The organization chooses which – if any – of the Annex A controls are applicable *i.e*. are necessary to mitigate its unacceptable information risks.

4.5.2 Audit findings are collected through interviews, examination of documents and observation of activities and conditions in the areas of concern and noted on the checklists, referencing the supporting audit evidence (*e.g.* interview notes and ISMS documents reviewed).

4.5.3 Evidence suggesting other non-conformities should be noted if they seem significant, even though not covered by the checklist, along with other objective evidence and/or observations reflecting positively or negatively on the information security management system.

4.6 Audit Reporting

4.6.1 The auditor/s shall allow time for analysing, drafting and discussing the audit findings *e.g.*:

- Review and analysis of evidence leading to reportable findings.
- Consolidation of findings including grouping of related issues and tabulation.
- Classification/prioritisation of findings according to their significance and/or urgency (see section 4.6.4).
- Drafting of audit report including recommendations.

4.6.2 The audit team shall review all of their findings whether they are to be reported as non-conformities or as observations. Essentially:

- Everything significant enough to be 'reportable' should indeed be reported; and
- Everything reported should be supported by sufficient objective evidence to withstand reasonable scrutiny.

4.6.3 The Lead Auditor typically consolidates everything into the audit report, or at least checks and challenges the content of a report drafted by the team.

4.6.4 Classification of findings shall be:

- **Major non-conformity** – a significant deficiency in the ISMS, typically a point of absolute non-conformity with one of the *mandatory* requirements in the main body of ISO/IEC 27001 (*e.g.* a missing required document or one that substantially fails to address the specified content) or a serious error in the identification, assessment or treatment of information risks (such as missing or ineffective 'necessary' controls). These are show-stoppers, preventing certification unless/until resolved.
- **Minor non-conformity** – a minor deficiency or technical non-conformity with a limited or indirect effect on information risk and security.
- **Improvement potential** – a *suggested* ISMS improvement which may or may not be adopted by the organization, perhaps with modifications, drawing on the auditor's independent perspective and experience.
- **Positive findings** – something that goes beyond what is required by the standard, included for the sake of presenting a fair and balanced opinion that acknowledges good practice.

4.6.5 Both major and minor non-conformities require appropriate corrective actions to be documented using the corrective action policy/procedure within the ISMS (or, if absent, an equivalent process).

4.6.6 Improvement potentials concerning information security weaknesses require appropriate preventive actions to be documented, ideally entering the organization's continual improvement process.

4.6.7 The Lead Auditor shall prepare a standard internal audit Report containing the following information:

- Audit Reference Number
- Date of Audit
- Department/Section Audited/Process Name
- Name of Auditee and auditors
- Statement of findings (all non-conformities found)
- Reference to the information security management system and standard
- Corrective and Preventive Actions with completion date
- Follow-up actions for non-conformities
- Verification of follow-up actions

4.6.8 Auditors shall follow a code of conduct in the manner of reporting as stated in this document:

- The report should be concise but factual and presented in a constructive manner.
- The findings should be within the scope of audit and shows the relationship of the standard used.
- The report should not show bias by the individual auditor.

4.6.9 The Lead Auditor shall issue a formal Audit Report to the ISMR (if the ISMR is not the Lead Auditor).

4.6.10 The internal audit report shall be maintained and controlled by the ISMR**.**

4.7 Clearance Meeting

4.7.1 The Lead Auditor shall preside over the clearance meeting attended by the audit team and auditees.

4.7.2 The auditor/s shall report the findings and observations, summarising the good points before discussing non-conformities supported by the audit evidence and (if applicable) recommendations and improvement opportunities to be considered.

4.7.3 All parties shall safeguard the confidentiality of the ISMS internal audit report.

5 Audit Follow-up and Closure

5.1.1 Whereas the auditors are responsible for identifying non-conformities, auditees are responsible for resolving non-conformities.

5.1.2 Approved corrective actions shall be based on time scales agreed with the auditors.

5.1.3 The Lead Auditor shall follow-up to check the implementation of corrective action as stated on the Non-conformity/Corrective and Preventive Action report or NCPAR. Normally, follow-ups will use an abbreviated form of this audit procedure to verify the completion and effectiveness of the agreed corrective or preventive actions according to the agreed timescales.

5.1.4 The lead auditor shall issue a new NCPAR if corrective actions are not fully implemented by the committed date, and/or are not effective.

5.1.5 “Re-issue” shall be noted on the remarks column of the NCPAR log if any of the situations noted here become apparent.

5.1.6 An audit will not be considered complete and closed until all corrective actions or measures have been successfully implemented to the satisfaction of the Lead Auditor.

6 Auditors’ Qualifications

6.1 Personal attributes

6.1.1 Auditors shall possess the personal attributes, skills and competencies necessary to uphold the principles of auditing. An auditor should be:

- Ethical*:* fair, truthful, sincere, honest and discreet;

- Open-minded: willing to consider alternative ideas or points of view;
- Diplomatic: tactful in dealing with people, particularly those who are senior or over-committed;
- Observant and perceptive: actively aware of physical surroundings, activities, body-language, instinctively aware of and able to understand complex situations;
- Versatile: able to adjust readily to different situations;
- Tenacious: persistent, focused on achieving objectives;
- Decisive: reaches timely conclusions based on logical reasoning and analysis; and
- Self-reliant and self-motivated*:* acts and functions independently while interacting effectively with others.

6.2 General knowledge and skills of an ISMS auditor

6.2.1 Auditors should have knowledge and skills in the following areas …

6.2.2 **Audit principles, procedures and techniques**: to enable the auditor to apply those appropriate to different audits and ensure that audits are conducted consistently and systematically. An auditor should be able to:

- Apply audit principles, procedures and techniques;
- Plan and organize the work effectively;
- Conduct the audit within the agreed time schedule;
- Prioritize and focus on matters of significance;
- Collect information through effective interviewing, listening, observing and reviewing documents, records and data;
- Understand the appropriateness and consequences of using sampling techniques for auditing;
- Verify the accuracy of collected information;
- Confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- Assess those factors that can affect the reliability of the audit findings and conclusions;
- Use work documents to record audit activities;
- Prepare audit reports of suitable quality and professionalism;
- Maintain the confidentiality and security of information, and
- Communicate effectively, either through personal linguistic skills or through an interpreter.

6.2.3 **Management system and reference documents**: to enable the auditor to comprehend the scope of the audit and apply audit criteria. Knowledge and skills in this area should cover:

- Interaction between the parts of the management system;
- ISMS standards, applicable procedures or other documents used as audit criteria;
- Recognizing differences between and priority of the reference documents;
- Application of the reference documents to different audit situations, and

- Information systems and technology for, authorization, security, distribution and control of documents, data and records.

6.2.4 **Organization/business context**: to enable the auditor to comprehend the organization's operational context. Knowledge and skills in this area should cover aspects such as:

- Organization size, structure, functions and relationships,
- General business processes and related terminology, and
- Cultural and social customs of the auditee.

6.2.5 **Applicable laws, regulations and other obligations:** to enable the auditor to work within, and be aware of, various obligations towards information security, privacy, governance and other requirements that apply to the organization being audited. Knowledge and skills in this area should cover relevant:

- Local, regional and national codes, laws and regulations;
- Contracts and agreements;
- International treaties and conventions; and
- Other compliance requirements such as applicable standards.

6.3 Lead Auditors' Qualifications

6.3.1 Audit team leaders should have additional knowledge and skills in audit leadership to facilitate the efficient and effective conduct of the audit. An audit team leader should be able to:

- Plan the audit and make effective use of resources during the audit;
- Represent the audit team in communications with the audit client and auditee;
- Organize, direct and motive audit team members;
- Mentor and provide guidance to auditor team members;
- Lead the audit team to reach the audit conclusions;
- Prevent or resolve conflicts; and
- Prepare and complete the audit report.

6.4 Specific Knowledge and Skills of ISMS Auditors.

6.4.1 Information security management system auditors should have knowledge and skills in Information security-related methods and techniques. To enable the auditor to examine information security management systems and to generate appropriate audit findings and conclusions. Knowledge and skills in this area should cover

- Information security terminology and concepts;
- Information security management principles and their application; and
- Information security management tools and their application.

6.4.2 Processes and products, including services: to enable the auditor to comprehend the technological context in which the audit is being conducted. Knowledge and skills in this area should cover:

- Industry-specific terminology;

- Technical characteristics of processes and products, including services, and industry-specific processes and practices.

7 Records

7.1.1 As well as miscellaneous audit evidence (such as copies of documents, audit notes, records of interviews, system printouts *etc*.), ISMS internal audits generate the following formal records:

- Audit programme
- Audit plan/Notification
- Audit checklist/Observation sheet
- Mandatory requirements checklist
- Discretionary requirements checklist
- Internal audit report
- Nonconformity and corrective reports (if required)
- ISMS improvement suggestions (if appropriate)

7.1.2 All information shall be appropriately secured given its often confidential nature.

7.1.3 All information shall be properly filed and indexed, providing a starting point or background context for the *next* ISMS audit.