**Model  
ISMS Internal Audit Procedure**

|  |  |
| --- | --- |
| **Release Date:** | October 4th 2024 |
| **Document Owner:** | C.D.Aluthge |
|  |  |

**Documentation Administration**

This work is copyright © 2012, **Richard O. Regalado and ISO27k Forum**, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum (www.ISO27001security.com), and (c) if shared, derivative works are shared under the same terms as this.

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

**Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Update Description** |
| 0 | August 2006 | Richard O. Regalado | Initial issue. |
| 1 | September 2007 | Richard O. Regalado and Gary Hinson | Updated Documentation Administration for incorporation into the ISO27k Toolkit |
| 2 | October 2012 | Gary Hinson | Reformatted using styles plus minor updates to the wording here and there |
| 3 | October 7, 2021 | A.D.Jaliya |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Purpose of this procedure

## To guarantee that the firm works in line with the defined policies, processes, and external regulations in order to achieve the organization's information security goals and objectives.

## Additionally, to guarantee that improvements to the Information Security Management System (ISMS) are identified, implemented, and appropriate for achieving goals.

# Scope

## This procedure applies to all departments and business units within the scope of the organization's ISMS and covers the planning, execution, reporting, and follow–up of ISMS internal audits.

# Rôles and responsibilities

## Information Security Management Representative (ISMR)

* The Lead Auditor and the Audit Team are appointed (note: the Lead Auditor and ISMR may be the same person).
* Reviews the remedial and preventive actions, as well as the follow-up audits, with the Lead Auditor, based on the internal audit report presented.
* Maintains the audit results' confidentiality.

## Lead Auditor

* Prepares an Audit Plan/Notification to serve as a foundation for planning the audit and disseminating audit information.
* Co-ordinates the audit schedule with appropriate department/section heads and leads the ISMS internal audit efforts.
* The audit is planned, the working materials are prepared, and the audit team is briefed.
* Organizes and writes an internal audit report based on all audit findings and observations.
* Critical non-conformities are immediately reported to the auditee.
* Report the audit results to the auditee in a transparent and timely manner.
* Organizes and leads the opening and closing meetings.

## Audit Team Member

* Supports the operations of the Lead Auditor.
* Using the consolidated audit checklist, conducts the audit.
* Reports nonconformities and makes recommendations for improvements.
* Maintains the privacy of audit findings.
* Acts in a morally upright manner at all times.

## Auditee

* Receives the audit report, evaluates it, and discusses it.
* As needed, determines, allocates, motivates, and completes remedial measures.
* Is and will continue to be responsible for the security of information assets.eceives, considers and discusses the audit report.
* Determines, resources, drives and completes corrective actions as necessary.
* Is and remains accountable for protecting information assets.

# Procedure

## General

### An ISMS audit program for the entire calendar year must be designed, which includes all scheduled and potential audits. This should include a schedule for internal audits, supplier audits, client audits, and third-party audits, as necessary.

### Internal audits will be performed twice a year or as needed.Only competent personnel who are truly independent of the subject area shall perform audits.

### The ISMR will appoint all members of the Internal Audit Team.

### The activity of the Audit Team will be overseen by the Lead Auditor..

### An Audit Notification Memo is sent to the department/section to be audited at least three working days in advance of the audit.

## Planning and Preparing the Audit

### The Lead Auditor must design an annual ISMS internal audit program that is approved by the President or CEO. It should be updated throughout the year to reflect any shifts in priorities or schedule.

### The Lead Auditor will draft the various audit plans based on the audit program..

### The Lead Auditor will prepare the Audit Plan/Notification, which will be reviewed and authorized by the ISMR. It must be shared with both the auditors and the auditees. It must be built to be adaptable so that adjustments can be made based on the information received during the audit. The strategy must incorporate the following elements::

* The purpose and scope of the audit
* In charge of the department/section and the responsible individuals.
* Members of the auditing team. The number of auditors is determined by the size of the audit area.
* The type of management system that will be examined
* Date, location, and time of the audit, as well as the date on which the audit report will be distributed

## Pre-audit meeting

### Not later than one day before the audit, the ISMR, Lead Auditor, and auditors will convene for one or more pre-audit meetings. The following are the goals::

* To guarantee that the necessary resources are available, as well as any additional logistics that the auditor may require.
* The Audit Plan confirms the scope of the audit.

## Opening meeting

### On the day of the audit, but before the audit starts, the ISMR and Lead Auditor will hold an opening meeting, if they think it necessary. During the opening meeting, the following topics may be discussed:

* The audit's goal and scope.
* The audit plan is confirmed.
* Other issues need to be resolved before the audit may take place..

## Audit Execution

### The internal audit will be carried out by the auditors using the following checklists: Internal Audit Checklist/Observation Form - comprises items that are specific to the audited organizational unit. It is the responsibility of the designated auditors to generate questions using this form. Systemic Criteria Checklist – contains items pertaining to ISO/IEC 27001:2005 requirements. Control Requirements Checklist – contains elements relating to controls listed in Appendix A of ISO/IEC 27001:2005 and more completely described in ISO/IEC 27002:2005.

### Interviews, document examinations, and observation of activities and situations in the areas of concern are used to gather information, which is then recorded on the above-mentioned checklists.

### Other non-conformities should be documented if they appear to be important, even if they are not covered by the checklist. Other objective evidence and/or observations that may have a positive or negative impact on the information security management system should be noted on the above-mentioned checklists.

## Audit Reporting

### The auditors shall have a wash-up meeting after the audit. Agenda includes:

* Review and analysis of the information
* All findings are consolidated, including grouping and tabulation.
* Findings are categorized.
* Preparation of a suggestion and a report on the audit
* Findings are categorized (see section 4.6.4)
* Preparation of a suggestion and a report on the audit

### Whether they are to be reported as non-conformities or observations, the audit team must review all of their findings. Similarly, audit findings should be backed up by objective evidence.

### The Lead Auditor consolidates all the audit findings for the preparation of the audit report.

4.6.4 Classification of findings shall be:

* Major non-conformity — This refers to a significant flaw in the ISMS. A non-conformity occurs when one or more elements of ISO 27001 are not followed.
* Non-conformities have a direct impact on information security, particularly on the confidentiality, integrity, and availability of data assets.
* A minor shortcoming is referred to as a minor non-conformity. One or more ISMS parts are only partially completed. Minor noncompliance has an indirect impact on data security..

**Note: Both major and minor non-conformities require appropriate corrective actions to be documented on the NCPAR form.**

* Improvement potential – A hint for improvement which may or may not be implemented by the auditee.

**Note: Improvement potentials which pertain to an information security weakness shall require appropriate preventive actions to be documented on the NCPAR form.**

* Positive findings – Findings that pertain to processes and/or systems that go beyond what is required by the standard.

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

* Number assigned to the audit
* Department/Section Audited/Process Name Date of Audit
* Auditee and auditors' names
* Findings and conclusions (all non conformities found)
* The information security management system and standard are mentioned.
* Actions should be taken to correct and prevent problems, together with a completion date
* Actions must be taken in the event of non-compliance
* Checking for follow-up activities

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

* The report should be brief yet accurate, and it should be presented in a positive light.
* The findings should be within the scope of the audit and demonstrate the standard's relationship.
* Individual auditor bias should not be visible in the report.

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

### The internal audit report shall be maintained and controlled by the ISMR in accordance with the **Control of Records Procedure.**

## Closing Meeting

### The audit team and auditees will be present at the closing meeting, which will be presided over by the Lead Auditor..

### Before analyzing non-conformities backed by audit data, the auditors must report their findings, remarks, and suggestions, summarizing the positive points.

### All parties shall safeguard the confidentiality of the internal audit report.

# Audit Follow-up and Closure

### Auditees are responsible for resolving non-conformities, whereas auditors are responsible for identifying them.hereas the auditors are responsible for identifying non-conformities, auditees are responsible for resolving non-conformities.

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

### The Lead Auditor will examine to see if the corrective action listed on the Non-conformity/Corrective and Preventive Action Report, or NCPAR, has been implemented. In most cases, follow-ups will use a condensed version of this audit approach to check that the agreed-upon corrective or preventive activities were completed and were effective within the agreed-upon timeframes.

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

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

### After all corrective actions or measures have been successfully executed to the satisfaction of the Lead Auditor, the audit will be considered complete and closed.

# Auditors’ Qualifications

## Personal attributes

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

* Fair, true, sincere, honest, and discrete are examples of ethical behavior.
* open-minded, that is, prepared to examine other ideas or points of view;
* Diplomatic, i.e. tactful while dealing with others, especially those who are senior or overworked;
* Perceptive, i.e. instinctively aware of and able to understand situations; Observant, i.e. actively aware of physical surroundings and activities; Observant, i.e. actively aware of physical surroundings and activities; Observant, i.e. actively aware of physical surroundings and activities; Observant, i.e
* Versatile, in the sense of being able to adapt to a variety of conditions;
* tenacious, in the sense of being persistent and goal-oriented;
* Self-reliant i.e. acts and functions independently while communicating effectively with others; and Decisive i.e. draws timely judgments based on logical thinking and analysis.

## General knowledge and skills of an ISMS auditor. Auditors should have knowledge and skills in the following areas.

### **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:

* Use auditing concepts, procedures, and methods;
* Effectively plan and organize your job;
* Conduct the audit according to the agreed-upon timeline;
* Prioritize and concentrate on important issues;
* Gather data through conducting successful interviews, listening, observing, and evaluating papers, records, and data;
* Recognize when sampling strategies for auditing are suitable and what the repercussions are;
* Check the accuracy of the data you've gathered;
* Confirm that audit evidence is sufficient and appropriate to support audit findings and conclusions.
* Examine the aspects that may have an impact on the audit results and conclusions' reliability;
* To keep track of audit activities, use work papers.
* Prepare audit reports that are of appropriate quality and expertise;
* Maintain information security and confidentiality, and communicate effectively, either through own language abilities or through the use of an interpreter.

### To enable the auditor to comprehend the scope of the audit and apply audit standards, the management system and reference documentation must be in place. This area's knowledge and skills should include:

* ISMS standards, applicable procedures, or other documents used as audit criteria; interaction between aspects of the management system; ISMS standards, applicable processes, or other documents used as audit criteria;
* Recognizing the distinctions between the reference documents and the order in which they should be read;
* Application of reference documents to various audit circumstances, as well as information systems and technology for document, data, and record authorization, security, dissemination, and control..

### Organization/business context: to allow the auditor to grasp the operational context of the organization. This knowledge and skill set should include things like:

* Size, structure, functions, and relationships of the organization, general business procedures and related terminology, and the auditee's cultural and social customs.

### Applicable laws, regulations, and other obligations: to allow the auditor to operate within and be aware of different duties relating to information security, privacy, governance, and other requirements that apply to the examined company. This area's knowledge and abilities should include the following:

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

## Lead Auditors’ Qualifications

### Audit team leaders should have extra audit leadership knowledge and abilities to help with the audit's efficiency and effectiveness. A leader of an audit team should be able to:

* Plan the audit and make efficient use of resources while doing it.
* In contacts with the audit client and auditee, represent the audit team.
* Organize, direct, and motivate members of the audit team.
* Members of the auditing team are mentored and guided.
* Organize the audit team such that the audit conclusions may be reached;
* Preventing or resolving disputes is a good idea. and
* Complete and submit the audit report.

## Specific Knowledge and Skills of ISMS Auditors.

### Information security management system auditors should be knowledgeable about and skilled in procedures and techniques relevant to information security. To allow the auditor to conduct a thorough examination of information security management systems and come up with suitable audit findings and conclusions. This area's knowledge and abilities should include

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

### Processes and goods, including services: to give the auditor a better understanding of the technical framework in which the audit is taking place. This area's knowledge and abilities should include:rocesses 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.

# Records

## 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 plan/Notification/Audit program
* Systemic requirements checklist/audit checklist/observation sheet
* Checklist of control needs
* Non-conformity/Corrective and Preventive Action Report (internal audit report) (NCPAR)

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

## All information shall be properly filed and indexed.