**ISMS Internal Audit Procedure**

Version:

Date:

Classification

Document Control

|  |  |  |
| --- | --- | --- |
| 1. | Document Number: |  |
| 2. | Version History: |  |
| 3. | Created Date: |  |
| 4. | Created By: |  |
| 5. | Approved By: |  |
| 6. | Contact: |  |

Document Modify History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modified By | Modification |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Purpose of this Procedure 4](#_Toc179674309)

[Scope 4](#_Toc179674310)

[Roles and Responsibilities 4](#_Toc179674311)

[Procedure 5](#_Toc179674312)

[Audit Follow-up and Closure 8](#_Toc179674313)

[Records 9](#_Toc179674314)

# Purpose of this Procedure

* 1. To guarantee that the business consistently meets its information security goals and objectives by adhering to the prescribed policies, processes, and external requirements
  2. In order to guarantee that enhancements to the Information Security Management System (ISMS) are recognized, executed, and appropriate for accomplishing goals

# Scope

This procedure covers the planning, execution, reporting, and follow-up of internal audits for the ISMS. It is applicable to all departments and business units that fall within the scope of the organization’s ISMS.

# Roles and Responsibilities

1. **Information Security Management Representative (ISMR):**

* selects the Audit Team and Lead Auditor (note: ISMR and the Lead Auditor may be the same person).
* Review the preventative and corrective measures as well as the follow-up audits carried out in accordance with the internal audit report that was turned in with the lead auditor.
* preserves the privacy of the audit findings

1. **Lead Auditor:**

* creates an audit plan or notification that serves as a guide for organizing the audit and sharing information about it.
* oversees the ISMS internal auditing operations.
* coordinates the audit schedule with the leaders of the relevant departments or sections.
* Plan the audit, have the working papers ready, and give the audit team a briefing.
* assembles all audit observations and results, then creates an internal audit report.
* Immediately reports critical non-conformities to the auditee.
* Make sure to inform the auditee about the audit results clearly and promptly.
* leads the meetings for the opening and closing.

1. **Audit Team Member:**

* supports the actions of the Lead Auditor
* Employs the consolidated audit checklist to carry out the audit
* Identifies the non-conformities and offers suggestions for improvement.
* Keeps the audit findings confidential
* Always behaves ethically.

1. **Auditee:**

* accepts, evaluates, and talks about the audit report
* determines, gathers, organizes, and carries out the appropriate remedial action
* Is and continues to be responsible for safeguarding information assets.

# Procedure

1. **General:**

* A program for ISMS audits should be developed that includes all planned and possible audits for the entire calendar year. This will include a schedule for internal audits, audits of suppliers, audits to be conducted by clients, and third-party audits, as needed.
* Internal audits will be planned for twice a year or whenever necessary.
* Audits should only be conducted by personnel who are skilled and completely independent of the subject area.
* All members of the Internal Audit Team will be appointed by the ISMR.
* The Lead Auditor will oversee the work of the Audit Team.
* A Notification for an Audit A memo should be sent to the department or section that will be audited at least three working days before the audit takes place.

1. **Planning and Preparing the Audit:**

* The Lead Auditor will prepare an annual ISMS internal audit program, which needs to be approved by the President or CEO. It needs to be updated to show any changes in priorities or the schedule throughout the year.
* The Lead Auditor will create the necessary audit plans according to the audit program.
* The Lead Auditor will prepare the Audit Plan/Notification, which will then be reviewed and approved by the ISMR. The auditors and the auditees will be informed about it. It will be designed to be flexible so that it can adapt based on the information collected during the audit. The plan will include:
  + Audit Objective and Scope
  + Department/Section and responsible individual in charge
  + Audit Team members
  + Type of management system to be audited
  + Date, place, time of the audit and distribution date of the audit report

1. **Pre-audit meeting:**

* There should be one or more pre-audit meetings involving the ISMR, Lead Auditor, and auditors, scheduled no later than one day before the actual audit. The objectives are listed below:
  + To make sure that all the resources and other logistics needed by the auditor are available.
  + The scope of the audit is verified from the audit Plan

1. **Opening meeting:**

* A meeting will be held at the start of the audit, if the ISMR and Lead Auditor think it's necessary, but it will take place before the actual audit begins. We can talk about the following during the opening meeting:
  + The purpose and scope of the audit
  + Confirmation of the audit plan
  + Other matters need to be clarified and settled before the audit can happen.

1. **Audit Execution:**

* The auditors are going to carry out the internal audit with the help of various checklists:
  + The Internal Audit Checklist/Observation Form includes specific items that relate to the organizational unit being audited. The auditors who have been assigned need to come up with questions using this form.
  + Systemic Requirements Checklist – includes items that pertain to the requirements of ISO/IEC 27001:2005
  + Requirements for Control Checklist – includes items related to the controls specified in Appendix A of ISO/IEC 27001:2022 and explained in detail in ISO/IEC 27002:2022.
* Audit findings are gathered by conducting interviews, reviewing documents, and observing activities and conditions in the areas of concern, and they will be recorded on the checklists mentioned above.
* It's important to point out any other non-conformities that appear to be significant, even if they aren't included in the checklist. Any additional objective evidence or observations that could have a positive or negative impact on the information security management system should also be noted in the space provided on the checklists mentioned above.

1. **Audit Reporting:**

* The auditors will hold a wrap-up meeting after the audit. The agenda consists of:
  + Review and Analysis of Findings
  + Consolidation of all findings including grouping and tabulation
  + Classification of findings
  + Preparation of recommendation and audit report
  + Classification of findings
  + Preparation of recommendation and audit report
* The audit team will look over all their findings, deciding if they should be reported as non-conformities or just observations. Audit findings should also be backed by objective evidence.
* The Lead Auditor gathers all the audit findings to prepare the audit report.
* The Lead Auditor is responsible for putting together a standard internal audit report that includes the following information:
  + Audit Reference Number
  + Date of Audit
  + Department/Section Audited/Process name
  + Name of Auditee and auditors
  + Statement of findings
  + Reference to the ISMS and standard
  + Corrective and Preventive actions with completion date
  + Follow-up actions for non-conformities
  + Verification of follow-up actions
* The Lead Auditor will provide a formal Audit Report to the ISMR, assuming the ISMR is not the Lead Auditor.
* The ISMR will keep and manage the internal audit report following the Control of Records Procedure.

1. **Closing Meeting:**

* The Lead Auditor will lead the closing meeting with the audit team and the auditees present.
* The auditors will share their findings, observations, and recommendations, highlighting the positive aspects before going over any non-conformities backed by the audit evidence.
* Everyone needs to keep the internal audit report confidential.

# Audit Follow-up and Closure

* The auditors have the job of finding non-conformities, while the auditees need to take care of fixing them.
* Corrective actions that get approved will depend on the timelines that we agree upon with the auditors.
* The Lead Auditor will check to see if the corrective actions mentioned in the Non-conformity/Corrective and Preventive Action report, or NCPAR, have been implemented. Usually, follow-ups will use a shorter version of this audit procedure to check if the agreed corrective or preventive actions have been completed and are effective, based on the timelines we agreed on.
* The lead auditor must issue a new NCPAR if the corrective actions are not completely implemented by the agreed date, and/or if they are not effective.
* “Re-issue” should be written in the remark’s column of the NCPAR log if any of the situations mentioned here occur.

# Records

* In addition to various types of audit evidence like document copies, audit notes, interview records, and system printouts, ISMS internal audits produce the following official records:
  + Audit Program
  + Audit plan
  + Audit checklist
  + Systematic requirement checklist
  + Control requirement checklist
  + Internal audit report
* All information should be properly secured because it is often confidential.