ISO 27001 Audit Procedure

*Revision: rx.x*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Internal Audit 4

2.1 Internal Audit Objectives 4

2.2 ISO 27001 Internal Audit Planning 4

2.3 Audit Criteria 5

2.4 Selection and Appointment of the Auditors 5

2.5 Conducting Internal Audits 5

2.6 Internal Audit Method 5

2.7 Follow-Up Activities 6

2.8 Managing Records of Internal Audits 6

2.9 Validity and Document Management 6

3. Procedure Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 7

4. Glossary / Acronyms 8

4.1 Glossary / Acronyms 8

5. Document Management 9

5.1 Document Revision Log 9

5.2 Document Ownership 9

5.3 Document Coordinator 9

5.4 Document Approvers 9

5.5 Distribution 9

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The purpose of this document is to define all Internal Information Security Audit related activities, including establishment of the Audit Plan, selection of an auditor, audits execution and reporting.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Internal Audit

## Internal Audit Objectives

The objective of the internal audit is to determine whether procedures, controls, processes, arrangements and other activities within the ISMS are:

* Comply with ISO 27001:2013 standard, applicable regulations, legal and contractual obligations.
* Comply with organizational policies, procedures, and other internal documents.
* Effectively implemented and maintained by responsible organizational functions.

1. **Managing Records of Internal Audits**

|  |  |  |  |
| --- | --- | --- | --- |
| **Record Name** | **Storage Location** | **Person Responsible for Storage** | **Retention Time** |
| Annual Internal Audit Plan (in electronic form) | Network file server | Senior GRC Security Manager | As per GRC Security team retention schedule |
| Internal Audit Report (in electronic form) | Network file server | Senior GRC Security Manager | As per GRC Security team retention schedule |

## ISO 27001 Internal Audit Planning

* Senior GRC Security Manager will approve the annual plan for ISO 27001 internal audits.
* Annual ISO 27001 internal audit shall be conducted over the course of the year, ensuring:
* Cumulative coverage of the entire ISMS scope when first-time certification or a re-certification of a site/office is planned following the internal audit.
* Partial coverage of the ISMS scope during the annual internal audit and cumulative coverage of the entire ISMS scope over two successive years of surveillance audits.
* ISO 27001 Internal Audits shall be preferably conducted prior to the management review.
* The Annual Internal Audit Plan should contain the following information about each internal audit:
* Period of the audit (specifying dates, or month in which the audit is planned);
* Scope of the audit (departments, processes, clauses of the standards, etc.);
* Audit criteria (standards, legislation, regulations, internal documentation, corporate standards, and/or contractual obligations where applicable);
* Auditing methods (review of documentation, interviews with employees, review of records, review of information systems, etc.);
* Who will be conducting the audit (if there is more than one auditor, specify the audit team leader).
* Conducted audits should be recorded in the Annual Internal Audit Plan.

## Audit Criteria

* ISO 27001:2013 Standard Requirements.
* Internal global and local Policies, Procedures and other applicable documents.
* Risk Assessment Process.
* Applicable Regulatory and legal Requirements.
* Contractual Obligations.

## Selection and Appointment of the Auditors

* The Internal Audit will be performed by objective, internal/external, competent and qualified auditors.
* Senior GRC Security Manager shall appoint the external auditors in their capacity as internal auditors.
* Criteria for appointing external auditors are:
* Proven knowledge of ISO 27001:2013 standard;
* Proven experience of management system auditing techniques;
* Understanding of wide range of networks, information systems, communication technologies and information security tools.
* Understanding of business, regulatory and technological environments and their impact on security processes and/or on business continuity.
* ISO 27001:2013 Lead Auditor or equivalent certification is a prerequisite.
* External Auditors should be selection and appointment shall be done in a way that ensures objectivity, impartiality and avoidance of conflict of interest.

## Conducting Internal Audits

* The senior GRC Manager will supervise the Internal Audit activity or delegate the supervision of the activity to a GRC Security team member.
* Parties responsible for internal audits shall be identified in the Annual Internal Audit Plan.
* If an audit is conducted by a team consisting of several auditors, the person responsible for the audit is the one identified as Audit Team Leader.
* The following should be taken into consideration during an internal audit:
* Audit Criteria as determined in clause 1.3 of this document;
* Results of previous internal and/or external audits;
* Results of risk assessment, control implementation, business impact analysis, etc.

## Internal Audit Method

* Review of global and local Documentation (Policies, Procedures, Standards, Reports, etc.).
* Review of internal records.
* Review of ISMS activities.
* Review of existing controls’ effectiveness.
* Review of working processes.
* Interview with key stakeholders or relevant employees.
* On-site physical assessment (including Clear Desk and Clear Screen policy enforcement).

## Follow-Up Activities

* The person leading the audit shall monitor the implementation of corrective actions, identified during the internal audit, verify that corrective actions have been implemented appropriately and within the specified deadlines, report the results to the Senior GRC Security Manager or escalate to appropriate authority in case the corrective actions were not implemented as required.
* Employees, assigned with the execution of corrective actions and remediation activities, bare full responsibility for their implementation as well as for the reporting/escalation in cases the defined objectives are not met.

## Managing Records of Internal Audits

|  |  |  |  |
| --- | --- | --- | --- |
| **Record Name** | **Storage Location** | **Person Responsible for Storage** | **Retention Time** |
| Annual Internal Audit Plan (in electronic form) | Network file server | CISO | As per Data Retention Policy |
| Internal Audit Report (in electronic form) | Network file server | CISO | As per Data Retention Policy |

## Validity and Document Management

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered.

* The number of corrective actions identified during the audit;
* The number of corrective actions that have been closed as scheduled;
* The number of corrective actions identified during the certification/surveillance audit conducted after the Internal Audit;
* Whether the Internal Audit frequency is in line with the Annual Internal Audit Plan.

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
|  |  |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Distribution