07-ISMS Internal Audit Policy and Procedure

Version	1.0
Effective Date	23 May 2024
Document Owner	[Document Owner Name]
Document Type	ISMS Document
Classification	Internal

Approval History

Version	Date	Created by	Approved by & Designation
1.0	22 May 2024	External Consultant	[Company CEO Name], CEO

Revision History

Version	Date	Created by	Description of Changes
0.1	-	Consultant	Initial Release
1.0	30-04-2024	External Consultant	Final Draft

Table of Contents

Purpose

The purpose of this procedure is to establish a framework for planning, conducting, and reporting on an internal audit of K15t Information Security Management System ("ISMS"). An internal audit is used to help determine whether the ISMS control objectives, controls, policies, and procedures:

- Conform to the applicable requirements of the ISO/IEC 27001 ("ISO 27001") standard.
- Conform to the identified information security requirements.
- Are effectively implemented, maintained, or have opportunities for improvement.

Scope

The intended audience for this document comprises the ISMS Management Team at K15t and the internal auditors. The audits will cover all elements of the ISMS for all in-scope information assets and the applicable controls identified within the Statement of Applicability.

Reference Documents

- ISO/IEC 27001:2022 Standard (Clause 9.2 and Annex A)
- K15t ISMS Policy

Internal Audit Planning (Clause 9.2)

Audit Objectives

An internal audit aims to assess the extent to which procedures, controls, processes, and arrangements for information security activities conform to applicable regulations, the organization's internal documentation, and whether they are effectively implemented, maintained, and aligned with policy requirements and set objectives.

Auditor Selection

The ISMS Team may engage third-party auditors with knowledge of ISO 27001 standards. Auditors must be objective, impartial, qualified, and approved by Company Leadership.

- The ISMS Manager appoints internal auditors.
- Internal auditors may be from within or outside the organization.
- Criteria for selection:
  - Knowledge of ISO/IEC 27001 Clauses and Annex A controls.
  - Familiarity with management system auditing techniques.
  - Understanding of information and communication technologies.

It is recommended that auditors complete ISO/IEC 27001 training and obtain relevant certifications.

Provision of Resources

The auditor(s) will work with the ISMS Manager and Team. Their responsibilities include:

- Planning internal audits as per the schedule.
- Conducting audits and sharing findings with the ISMS Manager for review.
- Ensuring audit data confidentiality and integrity.
- Providing audit records as needed.
- Identifying and reviewing corrective actions for audit observations/non-conformities.

Frequency & Schedule

The frequency of the internal audit is scheduled to be conducted annually at a minimum. The ISMS Management Team will determine if the frequency of the audit needs to be increased depending on the number of findings identified during the audit, the severity of the previous audit findings, and the operating efficiency of conducting the audit annually.

Audit Criteria

Internal audits are scheduled based on risk assessments and prior audit results. The internal audit encompasses all ISO/IEC 27001 standard requirements. Audit criteria consider ISMS policies and procedures, legal requirements, ISO 27001, and other relevant standards.

Evaluation Criteria

Audit findings are categorized as:

- **Major Non-Conformity (NC):** Immediate adverse impact on ISMS objectives.
- **Minor NC:** Impact over time without immediate adverse effects.
- **Conformity:** Effective controls in line with ISO 27001 requirements.
- **Opportunity for Improvement (OFI):** Suggestions for enhancement.

Alternative Labeling of Findings

Alternative audit methods for information security controls can also be used. These approaches may use terms like "Yes/No/Partial" or "In Place/Not in Place." When employing alternate methods for ISO 27001 requirements, a mapping process aligns controls with ISO 27001 standards and language, ensuring effective evaluation and alignment with recognized criteria.

Conducting an Audit

Audit Steps

All audits are based on the following steps:

Document Review	Compare the management system documentation against the requirements of any applicable standard.
Auditing	Compare actual practice against the management system's requirements and any applicable standard. Obtain objective evidence to support each requirement or indicate the nonconformities where such evidence is lacking. All findings are to be recorded in the Internal Audit Report.
Verification of Process Effectiveness	Pose general questions to establish that the audited process is effective and not prone to generating nonconformities.

Summarise Findings	Create a detailed list of the findings to be entered into the Corrective and Preventative Action Reporting (CPAR) system. The Auditor submits CPAR forms as necessary to address the non-conformities or propose preventative actions or improvements. Each nonconformity is characterized by: ▪ a statement-making clear requirement in question by reference to an internal document and/or the clause of the standard ▪ a summary of the traceable objective evidence found which supports the negative finding (e.g., documents found, replies to questions, product examined) – in all cases, sufficient detail must be supplied to allow a third party to find the evidence subsequently ▪ a statement setting out why the objective evidence leads to non-conformance against the requirement ▪ a rating of either 'Minor' or 'Major' taking into account any requirements set down by customers or regulators An identifier classifies the nonconformity as 'Corrective,' 'Preventative,' or 'Opportunity.'
Review of Report	The Auditor reviews all findings and evidence to ensure that the audit report is clear, complete, objective, and based on traceable objective evidence.
Communication of Findings	The Auditor reviews the report with the responsible manager(s) and agrees to take corrective actions to close out the non-conformities.
Finalizing the Report	Include the agreed actions and timetable in the report.

Management Review

The responsible manager ensures that the required actions are implemented and the nonconformities are closed out within the agreed timescale; minor areas of non-conformance are taken care of immediately, and the status of corrective actions and nonconformities are kept up to date.

Review of Audit Conclusions

The company places great importance on the review of all audit conclusions. This review process ensures that any findings or observations from internal audits are comprehensively examined, enhancing the effectiveness of the audit process.

The company ensures:

- A thorough review of all audit conclusions.
- Identification of emerging trends.
- Generation of recommendations for ISMS improvement.
- Issuing of the internal audit report to Company Leadership.
- Closure of the internal audit report in the Internal Audit Log upon action completion.
- Reporting of internal audit results and corrective actions at management review meetings.
- Designation of an Audit Team Leader for audits conducted by a team of auditors.

During internal audits, the following aspects are considered and assessed in comparison to the company's current situation:

- Compliance with the organization's security policies, procedures, and plans.
- Findings and lessons from previous internal or external audits.
- Results of risk assessments, control implementation, and data protection impact assessments.
- Adherence to applicable controls listed in ISO 27001 Annex A as outlined in the Internal audit checklist.

Identifying Trends

As part of the internal audit process, the company actively identifies emerging trends. These trends are carefully monitored and recognized during internal audits, allowing the organization to address potential issues proactively and continuously improve its ISMS.

Recommendations for Improvement

Recommendations for enhancing the ISMS are derived from audit findings. The internal audit report is submitted to Company Leadership. Upon completion of actions, the audit report is formally closed out in the Internal Audit Log. All internal audit results, along with corrective actions, are reported in management review meetings to assess their effectiveness and implementation.

Documentation and Reporting

Audit Documentation

Internal auditors record all findings in the Internal audit checklist. In the event of nonconformities, the Internal Auditor is responsible for notifying the ISMS Manager and the ISMS Management Team in written form.

Audit Reporting

The internal auditor documents results and observations, producing a final report. The ISMS Manager reviews the report, and key findings are shared with the ISMS Management Team. The complete report is available upon request and includes audit results, non-conformities, and observations, ensuring transparency and accountability.

Audit Records Retention

All collected evidence and documentation from internal audits will be safeguarded and retained in compliance with the guidelines outlined in the Procedure for the Control of Documented Information.

Annex A - Audit Program

The company will arrange an Internal Audit before the Stage 2 certification audit. The scope of this internal audit includes a comprehensive evaluation of the full ISMS implementation, covering Clauses 4 to Clauses 10 and the relevant Annex A controls as outlined in the current Statement of Applicability.

Audit	Time	Auditor	Status

Audit	Time	Auditor	Status