TECH THAT MATTERS

Elevaite365

Internal Audit, Continual Improvement And Non - Conformity and Corrective Action Policy

Version 1.0

PURPOSE

This policy defines responsibilities and requirements for planning and conducting audits, reporting results, and maintaining records of ISMS internal audits. It also defines processes for ensuring continuous ISMS improvement using best management practices, corrective actions, and preventive actions for identified non-conformities.

SCOPE

This policy covers ISMS internal and external audits conducted in the **Elevaite365** (herein referred to as Organization).

DEFINITION

1. **ISMS**: Information Security Management system
2. **CEO**: Chief Executive Officer
3. **ISG**: Information Security Group
4. **Audit**: Systematic, independent, and documented process for obtaining and evaluating audit evidence objectively to determine the extent to which the audit criteria are fulfilled.
5. **Audit evidence**: Records, statements of fact, or other information relevant to the audit criteria and verifiable. *Note: Audit evidence may be qualitative or quantitative*
6. **Audit criteria**: Set of policies, procedures, or requirements
7. *Note: Audit criteria are used as a reference against which audit evidence is compared*
8. **Auditor**: A person with the competence to conduct an audit.
9. **Auditee**: One or more auditors conducting an audit, supported if needed by technical experts.
10. **Continuous improvement -** the ongoing effort of a business to improve services, systems, processes, or products to maximize client benefits while maintaining ISMS.
11. **Non-Conformity**: Non-fulfilment of a requirement
12. *Note: a requirement may be stated in a standard, policy, procedure, contract, act, law, management decision, etc., which is mandatory. Guidelines are not to be considered requirements.*
13. **Correction**: action to eliminate a detected non-conformity.
14. **Corrective action**: action to eliminate the cause of a detected non-conformity or other undesirable situation.

RESPONSIBILITIES

The primary responsibility of implementing this procedure is with the ISG Team.

The ISMS internal auditors will implement this procedure in various departments, coordinating with the ISG team and department heads.

POLICY

1. ISMS Internal Audit shall be conducted at least annually.
2. The interval between two consecutive internal audits shall be maintained to be more than 6 (Six) months.
3. The ISMS internal auditors must know the ISO 27001 requirements and ISO 19011 auditing guidelines.
4. ISMS internal auditors are prohibited from auditing their work, process, procedure, or department. The audit team leader shall ensure this while planning audits and selecting auditors.
5. The auditees or audit representatives for each department/area being audited must extend full cooperation to auditors during the audits regarding the availability of personnel and information.

6. The internal auditors shall report audit findings in the following categories.

    a. **Non-Conformity** – for all findings that indicate a non-fulfillment of any requirement about either ISO 27001:2022 standard, legal, contractual, or process requirements. All nonconformities MUST be supported by objective evidence.

    b. **Opportunity for Improvement** – for all findings that indicate a potential non-fulfillment of either ISO 27001:2022 standard, legal requirements, contractual obligations, or process requirements. The scope for improvement may not be supported by objective evidence.

    c. **Good Practice—** any process or practice followed by the auditee identified to improve ISMS or departments' performance can be highlighted as good practice. However, good practice may not be supported by objective evidence.

    d. **Conformity** – for all findings indicating the fulfillment of any requirement about either ISO 27001:2022 standard, legal requirements, contractual obligations, or process requirements. All conformities must be supported by objective evidence.

7. The auditee shall ensure that the appropriate corrections and corrective actions, if applicable, are implemented promptly.

8. The audit team leader shall submit the audit reports to the top management within 15 working days of the audit.

9. The auditors shall maintain the confidentiality of the audit observations and information accessed during the audits. The information shall be shared only with the auditee, the audit team leader, and the top management.

10. The audit team leader shall ensure that the documented information control procedure is followed to control audit documents and records.

CONTINUAL IMPROVEMENT POLICY

The organization will continually improve the suitability, adequacy, or effectiveness of the ISMS on an ongoing basis by performing periodic reviews and making appropriate and timely decisions for effective implementation and maintenance of the ISMS.

Continual improvement will be ensured through the following methods:

1. Feedback/suggestions from interested parties and Process Heads/Program Managers as and when required
2. Any improvement suggestion received during Business as usual
3. Results from Internal audit and External audit

Improvements are shared in Management Review Meetings and logged and tracked in the risk register.

PRINCIPLES

1. **Risk-based Approach:** Improvement initiatives will be driven by a thorough understanding of information security risks. A risk management framework will be utilized to identify, assess, and prioritize risks, ensuring that improvement efforts focus on mitigating significant risks to an acceptable level.
2. **Compliance and Regulatory Requirements:** Improvements to the ISMS will consider changes in applicable laws, regulations, and contractual obligations. The organization will proactively monitor and assess compliance requirements and ensure that necessary enhancements are made to align with evolving legal and regulatory landscapes.
3. **Continual Learning and Innovation:** Continuous improvement efforts will embrace a culture of continual learning and innovation. Lessons learned from security incidents, near misses, internal and external audits, and industry developments will drive improvements. The organization will foster an environment that encourages employees to suggest innovative ideas for enhancing information security practices.
4. **Security Awareness and Training:** Continuous improvement efforts will include ongoing security awareness and training programs to enhance employees' knowledge and understanding of information security best practices. Regular training sessions, awareness campaigns, and communication channels will be utilized to promote a security-conscious culture throughout the organization.
5. **Lessons Learned:** Lessons learned from security incidents, near misses, and internal and external audits will drive improvements. Incidents will be thoroughly investigated, and corrective and preventive actions will be identified and implemented to address root causes and prevent reoccurrence.

NON - CONFORMITY AND CORRECTIVE ACTION POLICY

1. For each non-conformity, a correction has to be done without any delay. The consequences arising out of correction shall be dealt with.
2. The ISG team or the initiator of the non-conformity shall verify that the non-conformity has been closed and review the effectiveness of the correction.
3. The need for action to eliminate the causes shall be evaluated for each non-conformity. Each non-conformity's root cause(s) shall be identified and documented.
4. For each non-conformity, determine if the non-conformity could recur.
5. For each non-conformity, determine if the non-conformity exists or could potentially occur elsewhere.
6. Corrective action shall be planned for all such non-conformities where action to eliminate the cause is needed.
7. The corrective action must be based on the cause and shall be documented along with the time plan and responsibilities for implementation.
8. The respective department/auditee is accountable for non-implementation or delays in implementing the corrective action.
9. Any deviation in implementation shall be supported by a formal authorization or concession from top management for such deviation.
10. The ISG or the initiator of the non-conformity shall verify the completion of corrective action and review its effectiveness.
11. The status of correction and corrective action shall be presented to top management during the management review.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	-	Initial Release	Borhan	-	-