



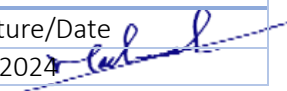
# Internal Audit Process


Doc. Control Number	Version
SNL-50	0.2



## Document Reference

Item	Description
Title	Internal Audit Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	16 July 2024
Revision-Date	16 July 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	7/16/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	7/16/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	7/16/2024 

## Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	16 July 2023	Muhaned Ali	First Release
0.2	16 July 2024	Muhaned Ali	The document has been reviewed



## Contents

1. Process Objective.....	4
2. Process Guidelines .....	4
3. Compliance .....	5
4. Review and Revision .....	5

## 1. Process Objective

The objective of this process is to verify compliance with the identified requirements for cybersecurity compliance within the company. It involves conducting independent audits, documenting findings and recommendations, presenting them to top management, protecting audit records, and continuously measuring, reviewing, and optimizing the requirements for cybersecurity audit and the effectiveness of the process and review activities.

## 2. Process Guidelines

### 2.1 Conduct Independent Audits

- a) Determine the planned intervals for conducting cybersecurity compliance audits based on the company's risk assessment, regulatory requirements, and significant changes to systems or processes.
- b) Develop an audit plan that outlines the scope, objectives, and criteria for the audit, including the identified requirements for cybersecurity compliance.
- c) Conduct independent audits by competent people or GRC team to review the implementation of the requirements for cybersecurity compliance within the company, ensuring that the audits are thorough and objective.
- d) Evaluate the effectiveness of controls, policies, and procedures related to cybersecurity compliance and identify any non-compliance or areas for improvement.
- e) GRC team conduct internal audit annually.

### 2.2 Document Findings and Recommendations

- a) Document the findings of the cybersecurity compliance audits, including identified non-compliance, areas of improvement, and noteworthy observations.
- b) Analyze the findings to understand the root causes and potential impact on the company's cybersecurity posture.
- c) Develop clear and actionable recommendations for addressing the identified non-compliance or improving cybersecurity controls.
- d) Ensure that the documentation is accurate, complete, and maintained in a standardized format for easy reference and future audits.

### 2.3 Present Findings and Recommendations to Top Management

- a) GRC team prepare a comprehensive report that includes a summary of the audit findings, key recommendations, and suggested remediation plans.
- b) GRC team present the audit report to top management, highlighting the significance of the findings and the potential risks to the organization's cybersecurity.
- c) Seek top management's approval for the recommended remediation plans and ensure their understanding of the urgency and importance of addressing identified non-compliance.

### 2.4 Protect Audit Records

- a) Establish strict access controls to protect audit records from unauthorized access, modification, or destruction.
- b) Store audit records in secure and tamper-proof systems or repositories, ensuring their confidentiality, integrity, and availability.
- c) Implement appropriate backup and disaster recovery measures to prevent data loss and ensure the continuity of audit records.

### 2.5 Retain Audit Records

- a) Define a retention period for audit records that aligns with legislative, regulatory, and contractual requirements.
- b) Ensure that audit records are retained for the specified duration and securely archived to serve as evidence of compliance with cybersecurity requirements.
- c) Regularly review and update the retention policy to accommodate changes in applicable laws and regulations.

#### 2.6 Continuously Measure, Review, and Optimize

- a) Continuously measure and evaluate the effectiveness of the requirements for cybersecurity audit, including the audit process and review activities.
- b) Review and update the requirements for cybersecurity audit to reflect changes in technology, regulations, or emerging threats.
- c) Identify opportunities for improvement, such as streamlining audit procedures, enhancing data analysis techniques, or implementing automation tools.
- d) Regularly communicate and collaborate with stakeholders to gather feedback and insights for further optimization.

### 3. Compliance

3.1 All employees involved in the internal audit process for cybersecurity compliance must adhere to this process.

3.2 Non-compliance may result in disciplinary action as per the company's policies.

### 4. Review and Revision

4.1 This process shall be reviewed periodically, at least annually or as necessary, to ensure its effectiveness, relevance, and alignment with changing cybersecurity requirements. Any proposed revisions shall be subject to appropriate approval and documentation.