Risk Treatment and Monitoring Process

Doc. Control Number	Version
SNL-70	0.2

Document Reference

Item	Description
Title	Risk Treatment and Monitoring Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	11 March 2024
Revision-Date	11 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	11/3/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	11/3/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	11/3/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	11 March 2024	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The document has been reviewed

Contents

1. Risk Treatment Process

1.1 Risk Assessment

a) The GRC team should conduct comprehensive risk assessments using standardized methodologies to identify and analyze cybersecurity risks.

b) Evaluate risks based on their likelihood of occurrence, potential impact, and severity.

1.2 Risk Prioritization

a) Prioritize identified risks based on their significance to the company, including potential impact on operations, reputation, and compliance requirements, and seek approval from top management.

1.3 Risk Mitigation Strategies

a) The GRC team should develop specific risk mitigation strategies and controls tailored to address the prioritized risks.

b) Consider a range of mitigation options, including risk avoidance, risk transfer, risk reduction, and risk acceptance.

1.4 Risk Treatment Plan Development

a) GRC team should develop a detailed Risk Treatment Plan (RTP) for each prioritized risk, outlining the selected mitigation strategies, responsible parties, timelines, and resource requirements.

b) Ensure alignment of the RTP with organizational objectives, risk tolerance levels, and regulatory requirements.

1.5 Implementation of Risk Treatment Measures

a) The GRC Team should Implement the identified risk treatment measures according to the timelines and milestones specified in the RTP.

b) Allocate necessary resources (financial, human, technology) to support the implementation process.

1.6 Monitoring and Evaluation

a) Monitor the progress and effectiveness of risk treatment measures throughout the implementation phase.

b) Regularly evaluate the outcomes of implemented measures and adjust strategies as needed to address emerging risks or changing organizational priorities.

1.7 Documentation and Reporting

a) Document all aspects of the risk treatment process, including risk assessments, mitigation strategies, and implementation activities.

b) Generate comprehensive reports on the status of risk treatment efforts, highlighting achievements, challenges, and areas for improvement.

2. Risk Monitoring Process

2.1 Identify and Review Risks

a) The GRC Team must continuously monitor, and review identified risks to ensure they remain relevant and up to date.

b) Regularly assess changes in the organizational environment, technology landscape, and threat landscape to identify new risks or changes in existing ones.

2.2 Monitoring Implementation of Risk Treatment Plan

a) Monitor the implementation of risk treatment measures outlined in the RTP to ensure they are executed according to plan.

b) Track progress against established timelines and milestones, identifying any deviations or delays for corrective action.

2.3 Assessment of Residual Risk

a) Assess the residual risk remaining after the implementation of risk treatment measures to determine whether it falls within acceptable tolerance levels.

b) Identify any gaps or areas where residual risk exceeds acceptable thresholds and develop strategies to address them.

2.4 Status of Accepted Risks

a) Monitor the status of accepted risks that have not been mitigated through treatment measures.

b) Regularly review the rationale for accepting these risks to ensure they remain acceptable within the context of organizational objectives and risk tolerance.

2.5 Reporting and Communication

a) Generate regular reports on the status of identified risks, the implementation of risk treatment measures, residual risk levels, and the status of accepted risks.

b) Communicate findings and recommendations to relevant stakeholders, including executive leadership, risk management committees, and relevant departments.