



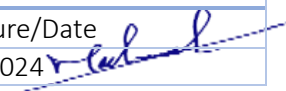
# Risk Assessment Process

Doc. Control Number	Version
SNL-68	0.2



## Document Reference

Item	Description
Title	Risk Assessment Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	10 March 2024
Revision-Date	10 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	10/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	10/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	10/3/2024 

## Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	10 March 2024	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The document has been reviewed



## Contents

1. Risk Assessment Process.....	4
3. Policy Compliance .....	6

## 1. Risk Assessment Process

### 1.1 Risk Identification

#### a) Asset Discovery

- The IT Team must identify and document all information assets within the Company, including data, systems, networks, applications, and devices.
- Conduct regular asset discovery scans and assessments to ensure the comprehensive coverage of all assets.
- Classify assets based on their criticality, sensitivity, and importance to the Company's operations and objectives.

#### b) Risk Register Maintenance

- GRC must maintain a centralized Risk Register to record and track identified risks.
- Document relevant details for each identified risk, including its source, description, potential impact, likelihood, existing controls, and mitigation strategies.
- Ensure that the Risk Register is regularly updated with new risks and changes to existing risks.

### 1.2 Risk Analysis

#### a) Probability Assessment

- GRC Team must Evaluate the likelihood of each identified risk occurring based on historical data, threat intelligence.
- Use a qualitative or quantitative approach to assign a probability rating to each risk, such as low, medium, or high.

#### b) Impact Analysis

- Assess the potential impact of each identified risk on the Company's objectives, operations, reputation, financials, and regulatory compliance.
- Consider both the immediate and long-term consequences of each risk event.
- Use a qualitative or quantitative approach to assign an impact rating to each risk, such as low, medium, or high.

### 1.3 Risk Evaluation

#### a) Identification of Treatable Risks

- Identify risks that exceed the Company's risk appetite or tolerance levels and require treatment or mitigation.
- Prioritize treatable risks based on their probability and impact ratings, focusing on those with the highest likelihood and potential impact.

#### b) Risk Treatment Options

- Develop and evaluate risk treatment options and mitigation strategies for each treatable risk.
- Consider a range of risk treatment options, including risk avoidance, risk reduction, risk transfer, and risk acceptance.

- Select the most appropriate risk treatment option based on cost-effectiveness, feasibility, and alignment with organizational objectives.
- c) Approval by Top Management
  - Present the results of the risk evaluation process, including the identified treatable risks, risk treatment options, and recommended courses of action, to top management for official approval.
  - Obtain explicit approval from top management for the implementation of selected risk treatment measures.
  - Document the outcomes of the risk evaluation process and management's decisions in the Risk Register and other relevant documentation.

#### 1.4 Monitoring and Review

- a) Implementation of Risk Treatment Measures
  - Implement the approved risk treatment measures and mitigation strategies in a timely manner.
  - Monitor the effectiveness of implemented controls and measures in reducing the likelihood and impact of identified risks.
- b) Ongoing Risk Monitoring
  - Continuously monitor the Company's risk environment for new threats, vulnerabilities, and changes that may impact previously identified risks.
  - Update the Risk Register and risk assessments as necessary to reflect changes in the risk landscape.
- c) Periodic Review and Reporting
  - Conduct periodic reviews of the Risk Register and risk assessments to ensure their accuracy, completeness, and relevance.
  - Provide regular reports on the status of risk management activities, including progress on implementing risk treatment measures and any emerging risks or trends, to senior management and relevant stakeholders.
  - Report the top cybersecurity risks within the Risk Register along with the remediation plans to the CST, and Aramco.

#### 1.5 Continuous Improvement

- a) Lessons Learned
  - Capture lessons learned from past risk management experiences, including successes, failures, and near misses.
  - Use lessons learned to inform future risk assessments, risk treatment decisions, and overall risk management practices.
- b) Feedback Mechanisms
  - Solicit feedback from stakeholders, including employees, customers, and partners, on the effectiveness of risk management processes and controls.
  - Use feedback to identify areas for improvement and enhance the organization's overall risk management capabilities.
- c) Adaptation to Changes

- Stay abreast of emerging threats, technologies, regulations, and industry best practices related to cybersecurity risk management.
- Continuously adapt and refine the risk assessment process and risk management practices to address evolving threats and organizational needs.

## 2. Policy Review

2.1 This document will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this document shall be communicated to all relevant employees and stakeholders.

## 3. Policy Compliance

### 3.1 Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### 3.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

### 3.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.