



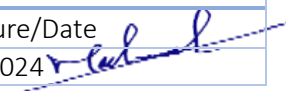
# Risk Assessment Policy

Doc. Control Number	Version
SNL-12	0.3



## Document Reference

Item	Description
Title	Risk Assessment Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	10 March 2024
Revision-Date	24 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	13 Jan 2022	Muhaned Ali	First Release
0.2	24 May 2023	Muhaned Ali	The policy has been reviewed and improved.
0.3	10 March 2024	Muhaned Ali	The policy has been reviewed and updated



## Contents

1. Purpose .....	4
2. Scope .....	4
3. Policy .....	4
5. Policy Compliance .....	6

## 1. Purpose

This policy outlines the principles and procedures for conducting comprehensive risk assessments within SNLC. Risk assessment is a critical component of our cybersecurity strategy, aiming to identify, evaluate, and manage potential risks that could impact the confidentiality, integrity, and availability of our information assets. The purpose of this policy is to establish a systematic and consistent approach to risk assessment, fostering informed decision-making and proactive risk management.

## 2. Scope

Risk assessments will be conducted for all information assets, business processes, and systems within the SNLC.

## 3. Policy

### 3.1 Frequency and Circumstances

Risk assessments should be conducted on a regular basis and whenever there are significant changes to the Company's IT infrastructure, processes, or threats landscape. The frequency of risk assessments should be determined based on the Company's risk appetite. At a minimum, risk assessments should be conducted annually, or more frequently if deemed necessary by the Company's cybersecurity team or management.

Risk assessments should also be conducted under the following circumstances:

- a) Prior to the implementation of new IT systems, applications, or technologies.
- b) Following significant changes to existing IT systems, applications, or technologies.
- c) After any cybersecurity incident or breach to identify gaps and vulnerabilities.
- d) In response to changes in the Company's business objectives, strategies, or regulatory requirements.

### 3.2 Requirements for Cybersecurity Risk Assessment

The cybersecurity risk assessment process should encompass the following requirements to ensure comprehensive coverage of risks to information assets, individuals, and other organizations:

- a) **Identification of Assets:** Identify and catalog all information assets, including but not limited to data, systems, networks, applications, and devices, along with their criticality and sensitivity levels.
- b) **Threat Assessment:** Assess the current threat landscape and identify potential threats and vulnerabilities that could exploit the Company's information assets.
- c) **Vulnerability Assessment:** Conduct regular vulnerability scans and penetration tests to identify weaknesses in the Company's IT infrastructure and applications.
- d) **Impact Analysis:** Evaluate the potential impact of identified risks on the confidentiality, integrity, and availability of information assets, as well as the potential financial, reputational, and regulatory consequences.
- e) **Risk Prioritization:** Prioritize risks based on their likelihood and potential impact, considering the Company's risk appetite and tolerance levels.
- f) **Mitigation Strategies:** Develop and implement appropriate risk mitigation strategies, controls, and countermeasures to reduce the likelihood and impact of identified risks to an acceptable level.

- g) **Monitoring and Review:** Continuously monitor and review the effectiveness of implemented controls and mitigation measures, and periodically reassess risks to ensure ongoing protection against evolving threats.
- h) **Documentation and Reporting:** Document the results of the risk assessment process, including identified risks, mitigation strategies, and residual risks, and report findings to relevant stakeholders, including senior management and regulatory authorities, as required.

### 3.3 Risk Assessment Methodology

- a) Utilize an established risk assessment methodology that considers industry best practices and regulatory requirements.
- b) The methodology shall involve identifying assets, assessing vulnerabilities, analyzing threats, determining likelihood, estimating impact, and calculating the risk level.
- c) The risk assessment methodology should be aligned with industry best practices and regulatory standards.

### 3.4 Risk Assessment Criteria

- a) Establish criteria for evaluating risks, considering factors such as potential impact, likelihood, vulnerabilities, and existing controls.
- b) Assign appropriate risk levels (e.g., low, moderate, high) based on the assessment criteria.
- c) SNLC must resolve or mitigate the identified security Vulnerabilities on a system, computer, network, or other computer equipment within the following timeframes:
  - Critical Risk: immediate correction up to fourteen (14) calendar days of critical vendor patch release, notification from Saudi Aramco, or discovered security breach whichever is earlier.
  - High Risk: within one (1) month of vendor patch release or discovered security breach whichever is earlier.
  - Medium and Low Risk: within three (3) months of discovery.

### 3.5 Risk Register

- a) Maintain a centralized risk register that document identified risks, their associated assets, risk levels, mitigating controls, and assigned ownership.
- b) Update the risk register regularly to reflect changes in the risk landscape.

### 3.6 Risk Assessment process integration

- a) During the early stages of major technical projects or significant changes to the organization or technical architecture.
- b) Before launching new products and services.

### 3.7 Reporting and Remediation

- a) Include the top cybersecurity risks, along with their prioritization and potential mitigations, in the Risk Register.
- b) Report the top cybersecurity risks within the Risk Register along with the remediation plans to the CITC, and Aramco.

## 4. Policy Review

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

## 5. Policy Compliance

### 5.1 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.

### 5.2 Exceptions

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

### 5.3 Non-Compliance

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