




Risk Assessment and Treatment Process


Doc. Control Number	Version
SNL-37	0.2



Document Reference

Item	Description
Title	Risk Assessment and Treatment Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	25 May 2024
Revision-Date	25 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/25/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/25/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/25/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	25 May 2023	Muhaned Ali	First Release
0.2	25 May 2024	Muhaned Ali	The document has been reviewed

Contents

1. Overview.....	4
2. Risk assessment and treatment process	4
2.1 Criteria for performing information security risk assessments	4
2.2 Risk acceptance criteria	4
2.3 Establish the context	5
2.4 Risk identification	5
2.4.1 Compile/Maintain Asset Inventory.....	6
2.4.2 Identify Potential Threats	6
2.4.3 Assess Existing Vulnerabilities	6
2.4.4 Identify Risk Scenarios	6
2.5 Risk analysis	6
2.5.1 Assess the likelihood.....	6
2.5.2 Assess the Impact	6
2.5.3 Risk classification	7
2.6 Risk evaluation.....	7
2.6.1 Risk Assessment Report.....	7
2.7 Risk treatment	8
2.7.1 Risk Treatment Options	8
2.7.2 Risk Treatment Plan.....	8
2.8 Management Approval.....	8
2.9 Risk Monitoring and Reporting.....	9
2.10 Regular review	9

1. Overview

The effective management of information security has always been a priority for SNLC to manage risk and safeguard its reputation in the marketplace. However, there is still much to be gained by SNLC in continuing to introduce industry-standard good practice processes.

It is important that SNLC has an effective risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them.

It is important also that the process is sufficiently clear so that successive assessments produce consistent, valid, and comparable results, even when carried out by different people.

2. Risk assessment and treatment process

The process described in this document is aligned with the following international standards:

- ISO/IEC 27001 - Information Security Management Systems
- ISO 31000 - Risk Management Guidelines

It is recommended that these documents be reviewed for a full understanding of the environment within which this risk assessment process operates.

The process of risk assessment and treatment is shown in figure 1 and described in more detail in the following sections. The process used is qualitative in nature in that it uses the terms high, medium, and low to describe the relative classification level for each specific risk. In some circumstances it may be appropriate to also use quantitative techniques i.e., using numbers such as financial values within the process to provide a higher degree of detail in assessing risks. In all cases where quantitative techniques are used the criteria should be clearly stated so that the risk assessment is understandable and repeatable

2.1 Criteria for performing information security risk assessments

In general, the criteria are that a risk assessment will be performed in the following circumstances:

- A comprehensive risk assessment covering all information assets as part of the initial implementation of the Information Security Management System (ISMS).
- Updates to the comprehensive risk assessment as part of the management review process – this should identify changes to assets, threats and vulnerabilities and possibly risk levels.
- As part of projects that involve significant change to the organization, the ISMS, or its information assets.
- As part of the IT change management process when assessing whether proposed changes should be approved and implemented.
- On major external change affecting the company which may invalidate the conclusions from previous risk assessments e.g., changes to relevant legislation, mergers, and acquisitions.
- When evaluating and selecting suppliers, particularly those that will play a part in the delivery of cloud services to customers.

If there is uncertainty regarding whether it is appropriate to carry out a risk assessment, the company should err on the side of caution and ensure that one is performed.

2.2 Risk acceptance criteria

One of the options when evaluating risks is to do nothing, i.e., to accept the risk. This is a valid approach but must be used with caution. The circumstances under which risks may be accepted must be fully agreed and understood.

Criteria for accepting risks will vary according to several factors which may change over time. These include the company's general or cultural attitude to risk, the prevailing financial climate, legal and regulatory requirements, the current view of top management and the sensitivity of the specific assets or business areas within scope.

Before carrying out a risk assessment the criteria for accepting risks must be discussed by appropriate people with knowledge of the subject area and, if necessary, top management. This discussion should establish guidelines for the circumstances in which risks will be accepted i.e., not subjected to further treatment.

These criteria may be expressed in several different ways, depending on the scope of the risk assessment and may include situations where:

- The cost of appropriate control is judged to be more than the potential loss.
- Known changes will soon mean that the risk is reduced or disappears completely.
- The risk is at or lower than a defined threshold, expressed either as a level e.g., low or as a quantified amount e.g., a financial sum.
- An area is known to be high risk but also high potential reward i.e., it is a calculated risk.

These acceptance criteria must be documented and used as input to the risk evaluation stage of the assessment process.

2.3 Establish the context

The overall environment in which the risk assessment is carried out must be described and the reasons for it explained. This should include a description of the internal and external context and any recent changes that affect the likelihood and impact of risks in general.

The internal context may include:

- Governance, organizational structure, roles, and accountabilities
- Policies, objectives, and the strategies that are in place to achieve them.
- The capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies)
- Information systems, information flows and decision-making processes (both formal and informal)
- Relationships with, and perceptions and values of, internal stakeholders
- The company culture.
- Standards, guidelines, and models adopted by the company.
- Form and extent of contractual relationships

The external context may include:

The cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or local

- Key drivers and trends having an impact on the objectives of the company.
- Relationships with, and perceptions and values of, external stakeholders
- The prevailing market or industry view of the security of cloud service providers – this may be affected by any recent breaches involving the loss of personally identifiable information (PII)

The scope of the risk assessment must also be defined. This may be expressed in terms of factors such as:

- Geographical location e.g., countries, offices, data centers
- Organizational units e.g., specific departments
- Business process(es)
- IT services, systems, and networks
- Customers, products, or services

2.4 Risk identification

The process of identifying risks to be assessed will consist of the following steps in line with the requirements of ISO/IEC 27001. Risks are identified to the confidentiality, integrity, or availability of information within the scope of the ISMS.

Identify and document internal and external risks based on the information assets of the SNLC Asset Discovery and maintain the identified risks in a Risk Register

2.4.1 Compile/Maintain Asset Inventory

A full inventory of assets is compiled and maintained by SNLC.

The list of assets is held in the document Information Asset Inventory as part of the ISMS. Within the inventory every asset is assigned a value which should be considered as part of the impact assessment stage of this process. Each asset also has an owner who should be involved in the risk assessment for that asset. Where appropriate for the purposes of risk assessment.

2.4.2 Identify Potential Threats

For each asset (or asset group), the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft, or sabotage. Threats will apply to one or more of the confidentiality, integrity, and availability of the asset.

2.4.3 Assess Existing Vulnerabilities

Attributes of an asset (or asset group) which may be exploited by any specific threat are referred to as vulnerabilities and will be detailed as part of the risk assessment.

Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of malware) or the existence of paper files in a data center (which could be exploited by the threat of fire).

2.4.4 Identify Risk Scenarios

The identification of risks to the information security of the company will be performed by a combination of group discussion and interview with interested parties.

Identified risks will be recorded with as full a description as possible that allows the likelihood and impact of the risk to be assessed. Each risk must also be allocated to the owner.

2.5 Risk analysis

Risk analysis within this process involves assigning a numerical value to the a) likelihood and b) impact of a risk. These values are then multiplied to arrive at a classification level of high, medium, or low for the risk.

2.5.1 Assess the likelihood

An estimate of the likelihood of a risk occurring must be made. This should consider whether it has happened before either to this company or similar companies in the same industry or location and whether there exists sufficient motive, opportunity, and capability for a threat to be realized.

The likelihood of each risk will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 1. When assessing the likelihood of a risk, existing controls will be considered. This may require an assessment to be made as to the effectiveness of existing controls.

GRADE	DESCRIPTION	SUMMARY
1	Improbable	Has never happened before and there is no reason to think it is any more likely now
2	Unlikely	There is a possibility that it could happen, but it probably won't
3	Likely	On balance, the risk is more likely to happen than not
4	Very Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Almost certain	Either already happens regularly or there is some reason to believe it is virtually imminent

Table 1: Risk likelihood guidance

2.5.2 Assess the Impact

An estimate of the impact that the loss of confidentiality, integrity or availability could have on the company must be given. This should consider existing controls that lessen the impact if these controls are seen to be effective.

2.5.3 Risk classification

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers. This resulting score is then used to decide the classification of the risk based on the matrix shown in figure 1.

Each risk will be allocated a classification based on its score as follows:

- High: 12 or more
- Medium: 5 to 10 inclusive
- Low: 1 to 4 inclusive

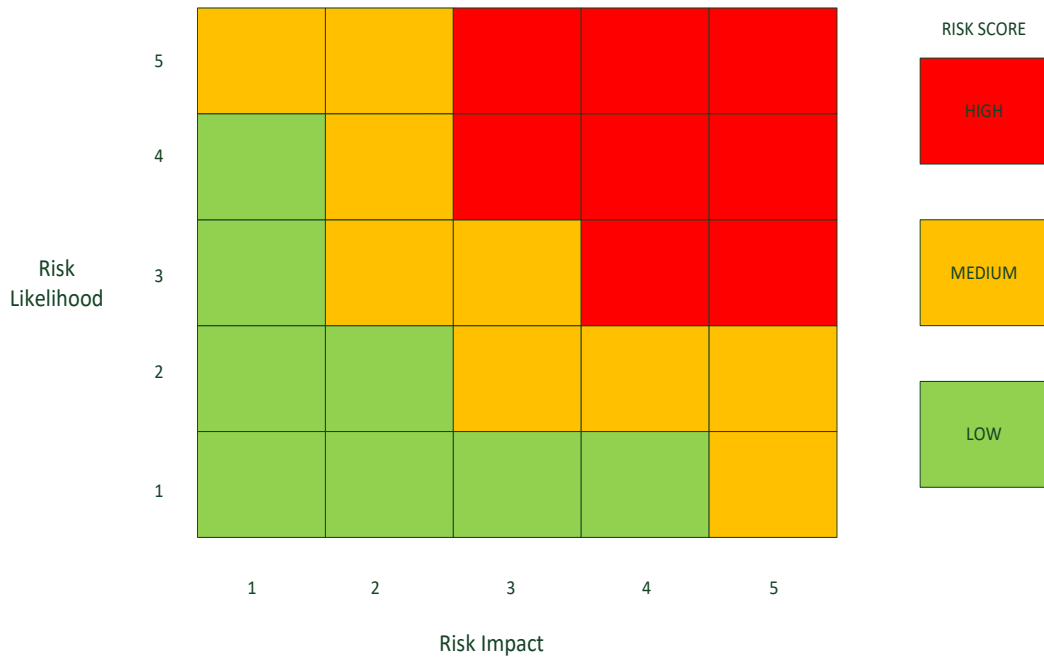


Figure 1: Risk matrix chart

The classification of each risk will be recorded as input to the risk evaluation stage of the process.

2.6 Risk evaluation

The purpose of risk evaluation is to decide which risks can be accepted and which ones need to be treated. This will consider the risk acceptance criteria established for this specific risk assessment (see Risk Acceptance Criteria, above).

The matrix in Figure 1 shows the classifications of risk, where green indicates that the risk is below the acceptable threshold. The orange and red areas generally indicate that a risk does not meet the acceptance criteria and so is a candidate for treatment.

Risks will be prioritized for treatment according to their score and classification so that very high scoring risks are recommended to be addressed before those with lower levels of exposure for the company.

Risk evaluation outcomes must be officially approved by the top management.

2.6.1 Risk Assessment Report

The output from the risk evaluation stage is the risk assessment report. This shows the following information:

- Assets [asset-based risk assessment only]
- Threats [asset-based risk assessment only]
- Vulnerabilities [asset-based risk assessment only]
- Risk scenario descriptions [scenario-based risk assessment only]

- Controls currently implemented.
- Likelihood (including rationale)
- Impact (including rationale)
- Risk Score
- Risk Classification
- Risk Owner
- Whether the risk is recommended for acceptance or treatment
- Priority of risks for treatment

This report is input to the risk treatment stage of the process and must be signed off by management before continuing, particularly in respect of those risks that are recommended for acceptance.

Report the top cybersecurity risks within the Risk Register along with the remediation plans to the CITC.

2.7 Risk treatment

For those risks that are agreed to be above the threshold for acceptance by SNLC, the options for treatment will then be explored.

The overall intention of risk treatment is to reduce the classification of a risk to an acceptable level. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g., reducing the score from 8 to 6 means it remains a medium level risk. The company may decide to accept these risks even though they remain at a medium rating. Such decisions must be recorded with a suitable explanation.

2.7.1 Risk Treatment Options

The following options may be applied to the treatment of the risks that have been agreed to be unacceptable:

- **Modify** the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk.
- **Avoid** the risk by taking action that means it no longer applies.
- **Share** the risk with another party e.g., insurer or supplier.

Judgement will be used in the decision as to which course of action to follow, based on a sound knowledge of the circumstances surrounding the risk e.g.

- Business strategy
- Regulatory and legislative considerations
- Technical issues
- Commercial and contractual issues

The Risk Manager will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted, including the risk owner.

2.7.2 Risk Treatment Plan

The evaluation of the treatment options will result in the production of the risk treatment plan which will detail:

- Risks requiring treatment.
- Risk owner
- Recommended treatment option
- Control(s) to be implemented.
- Responsibility for the identified actions
- Cost estimate for implementing the control(s)
- Timescales for actions
- Expected residual risk levels after the controls have been implemented.

2.8 Management Approval

At each stage of the risk assessment process management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the following documents:

- Risk Assessment Report
- Risk Treatment Plan
- Statement of Applicability

Signoff will be indicated according to SNLC documentation standards. In addition to overall management approval, the acceptance or treatment of each risk must be signed off by the relevant risk owner.

2.9 Risk Monitoring and Reporting

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exceptional situations can be identified and dealt with as part of the management review process of the ISMS.

2.10 Regular review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed regarding major changes to the business such as office moves, mergers and acquisitions or the introduction of new or changed IT services.