[Organization Name]

# INFORMATION SECURITY RISK MANAGEMENT PROCESS

Commented [AL1]: You can find more information on how to define the information classification policy in section "Step 5" of the ISO 27001 Lead Implementer course.

| | |
|---|---|
| Version | 1.0 |
| Document type | Process |
| Document owner | |
| Document location | |
| Effective from | |
| Status | |
| Approved by | |
| Classification | |

Commented [AL2]: Insert classification level according to classification scheme.

[organization's logo]

## APPROVAL HISTORY

| VERSION | DATE | APPROVED BY | DEPARTMENT |
|---|---|---|---|
| 1.0 | | | |
| | | | |
| | | | |

## REVISION HISTORY

| VERSION | DATE | CREATED BY | DESCRIPTION OF CHANGES |
|---|---|---|---|
| 1.0 | 01.01.2023 | Aron Lange | Initial release |
| | | | |
| | | | |

## Table of Contents

[organization's logo]

# 1 PURPOSE

The purpose of this document is to define and describe the standardized processes of risk assessment and risk treatment within [Organization Name]. It aims to provide a comprehensive guide to understanding, evaluating, and treating information security risks.

# 2 SCOPE

This document applies to all personnel within [Organization Name], who are involved in the management of risks.

# 3 TERMS AND DEFINITIONS

ISMS information security management system

# 4 RELATED DOCUMENTS

The following documents are related to this document:

- Information Classification Policy
- Information Security Policy

# 5 METHODOLOGY

## 5.1 Risk Evaluation Criteria

To quantitatively evaluate risks, we will use a matrix approach combining two dimensions: Impact and Likelihood.

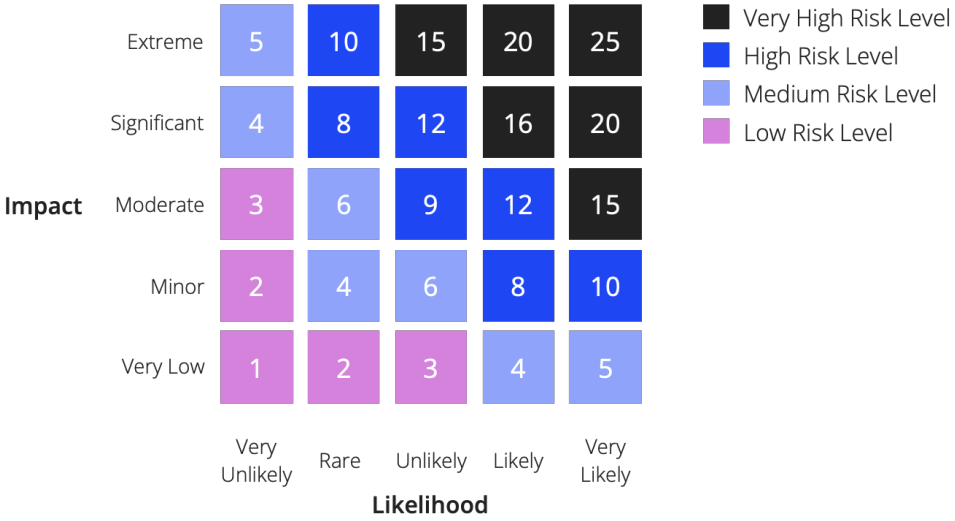
**Impact** refers to the potential consequences or damage that could occur if the risk materializes. We rate the impact on a scale from 1 to 5, with 1 being minor and 5 being catastrophic.

1. **Very Low** (1): No significant impact on operations, minor financial loss, minimal or no damage to the organization's reputation.
2. **Minor** (2): Some disruption to operations, moderate financial loss, minor damage to the organization's reputation.
3. **Moderate** (3): Disruption to operations that can be recovered in the medium term, significant financial loss, moderate damage to the organization's reputation.
4. **Significant** (4): Long-term disruption to operations, major financial loss, significant damage to the organization's reputation.
5. **Extreme** (5): Permanent disruption to operations, massive financial loss, irreparable damage to the organization's reputation.

**Likelihood** refers to the probability of the risk occurring. We rate likelihood also on a scale from 1 to 5, with 1 being rare and 5 being almost certain.

1. **Very Unlikely** (1): The risk event may occur only in exceptional circumstances.
2. **Rare** (2): The risk event could occur at some time.
3. **Unlikely** (3): The risk event might occur.
4. **Likely** (4): The risk event will probably occur in most circumstances.
5. **Very Likely** (5): The risk event is expected to occur in most circumstances.

We calculate the risk score by multiplying the impact score by the likelihood score. The resulting score will be on a scale from 1 (lowest risk) to 25 (highest risk). This score will be used to evaluate and prioritize risks.




### 5.2 Risk Acceptance Criteria

The Risk Acceptance Criteria establish thresholds for deciding which risks are acceptable and which require treatment. This is based on the risk score calculated in the Risk Evaluation Criteria.

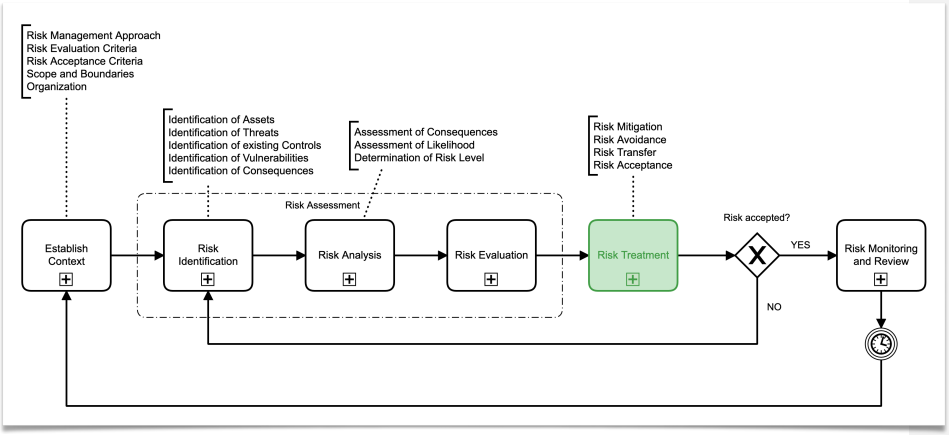
- **Low Risk** (1-3): Risks in this category are considered acceptable without an immediate need for mitigation. However, they should be monitored to ensure that they don't increase over time.
- **Medium Risk** (4-6): Risks in this category are considered acceptable without an immediate need for mitigation. However, they should be monitored to ensure that they don't increase over time.
- **High Risk** (8-12): Risks in this level are considered significant and require prioritized attention for mitigation. They pose a substantial threat and require proactive measures to reduce their potential impact or likelihood.
- **Very High Risk** (19-25): Risks in this level are unacceptable and require immediate and aggressive action for mitigation. They pose a severe threat to the organization's operations or objectives.

# 6 INFORMATION SECURITY MANAGEMENT PROCESS

This chapter provides an overview of the risk management process, which is a fundamental component of any robust information security management system (ISMS). As information security risks are continually evolving, the need for a systematic, repeatable, and consistent risk management process is critical for every organization.

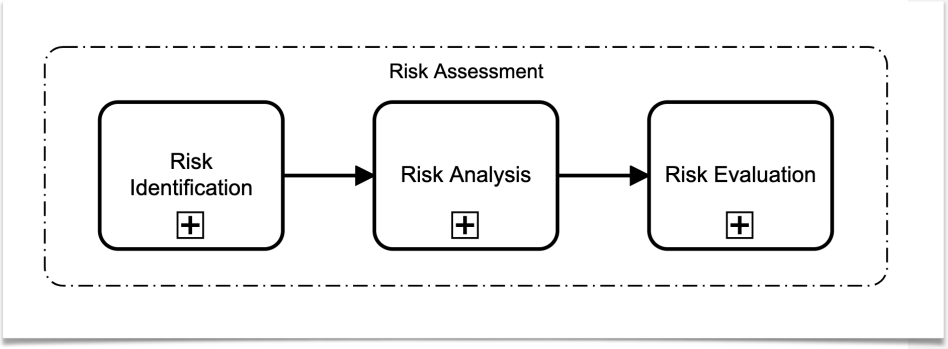
The risk management process is not a one-time activity, but rather a continuous cycle that involves identifying, assessing, and managing risks that could potentially impact the organization's information assets and operations. It spans several key stages, including context establishment, risk assessment, risk treatment, risk acceptance, and communication and consultation.

The ultimate goal of this process is to enable the organization to adequately manage potential threats and vulnerabilities, ensuring that risks are kept within acceptable levels. By understanding and applying the risk management process, we can make informed decisions about the allocation of resources, implementation of controls, and overall management of information security risk.



# 7 INFORMATION SECURITY RISK ASSESSMENT PROCESS

In this section, we will delve into the Risk Assessment process, a crucial component of risk management that involves the systematic identification, analysis, and evaluation of risks that could potentially impact the organization's information assets and operations.




## 7.1 Risk Identification

1. **Identify Assets**: Begin by identifying and documenting all assets that fall within the defined scope of the ISMS.
2. **Identify Threats**: For each identified asset, document all potential threats. These could be human (like errors or fraud), natural (like fire or flood), or environmental (like power failure).
3. **Identify Existing Controls**: For each threat, identify and document the existing controls in place designed to prevent or mitigate these threats.
4. **Identify Vulnerabilities**: Document all vulnerabilities in the existing controls that could be exploited by these threats. This could include weak passwords, outdated software, or inadequate physical security.

## 7.2 Risk Analysis

1. **Determine Likelihood**: For each threat-vulnerability pair, estimate the likelihood of the threat exploiting the vulnerability, using the predefined scale.
2. **Determine Impact**: For each threat-vulnerability pair, estimate the potential impact if the threat were to exploit the vulnerability, using the predefined scale.
3. **Calculate Risk Levels**: Multiply the likelihood and impact for each threat-vulnerability pair to calculate the risk level.

## 7.3 Risk Evaluation

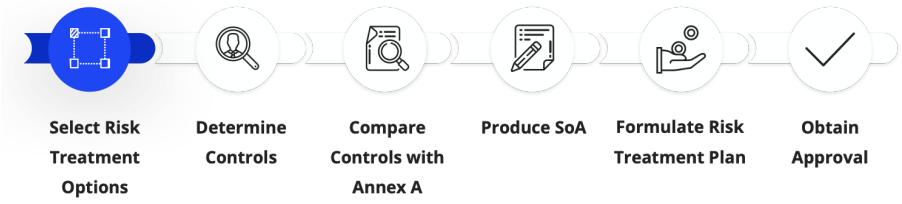
After risks have been identified and analyzed, they should be compared against the organization's predefined risk acceptance criteria. This involves the following steps:

1. **List Analyzed Risks**: Start with a list of all identified and analyzed risks, along with their calculated risk scores.
2. **Apply Risk Acceptance Criteria**: For each risk, compare its risk score with the predefined risk acceptance thresholds for Low, Medium, High, and Very High risks.
3. **Categorize Risks**: Based on the comparison, categorize each risk into one of the four categories (Low, Medium, High, Very High). Risks that are within the organisations risk acceptance criteria can be accepted and do not require further treatment. Risks that are not within them, need to undergo the following steps

Once the risks are categorized, they need to be prioritized to decide which risks should be addressed first.

1. **Rank Risks**: Within each category, rank the risks based on their risk scores. Higher risk scores should be given higher priority.
2. **Document Prioritized Risks**: Document the prioritized list of risks, along with their categories and risk scores. This list will serve as a guide for the risk treatment process.

# 8 INFORMATION SECURITY RISK TREATMENT PROCESS




## 8.1 Determine Risk Treatment Options

The first step in risk treatment is to determine the possible options for treating each risk. There are typically four options:

- **Risk Avoidance**: Completely avoid the activities giving rise to the risk.
- **Risk Reduction**: Implement controls to reduce the likelihood or impact of the risk.
- **Risk Transfer**: Shift the risk to another party, such as through insurance.
- **Risk Acceptance**: Accept the risk and monitor it continuously.

For each risk, consider all these options and determine the most appropriate one based on the organization's risk tolerance and business objectives.

## 8.2 Determine Controls

For risks that are to be reduced, specific controls should be determined. These controls could be technical, organizational, legal, or a combination thereof. The objective of these controls is to reduce the risk to an acceptable level.

### 8.3 Compare Controls with Annex A

The controls identified should be compared with the controls listed in Annex A of ISO 27001. This ensures that all relevant controls are considered and nothing is overlooked. If any controls from Annex A are not applied, justification for their exclusion should be documented.

### 8.4 Produce Statement of Applicability (SoA)

The Statement of Applicability (SoA) is a key document that lists all the controls from Annex A and describes whether they are applicable and implemented or not. For each control, provide a justification for inclusion or exclusion and describe how the control is implemented.

### 8.5 Formulate Risk Treatment Plan

The Risk Treatment Plan (RTP) outlines how the identified risks are to be treated. It includes information about the risk, the chosen treatment option, the controls to be implemented (if any), the expected outcomes, the resources required, and the timeline for implementation.

### 8.6 Obtain Approval

The final step in the risk treatment process is to obtain approval for the SoA and the RTP. This typically involves presenting the documents to the top management or a designated authority for review and approval. Once approved, the SoA and RTP guide the implementation of the risk treatment process.

Remember, risk treatment is a continuous process. The effectiveness of the risk treatment measures should be monitored and reviewed regularly, and the SoA and RTP should be updated as necessary.