[organization's logo]

Document ID:	Owner:	Document Type:	Language:	Version:
00000005	OWNER	Procedure	EN	0.1

Title:

RISK ASSESSMENT PROCEDURE

Commented [AL1]: Edit according to your organisations document management system.

Status:	Name:	Function:	Date:	Signature:
Created	Aron Lange	The GRC Lab	2024-04-08	AL
Reviewed				
Approved				

REVISION HISTORY

VERSION	DATE	CREATED BY	DESCRIPTION OF CHANGES
0.1	2024-04-08	Aron Lange	Initial draft

Table of Contents

[organization's logo]

1 PURPOSE

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

2 SCOPE

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

Commented [AL2]: Refine scope according to your organisational structure and responsibilities.

3 TERMS AND DEFINITIONS

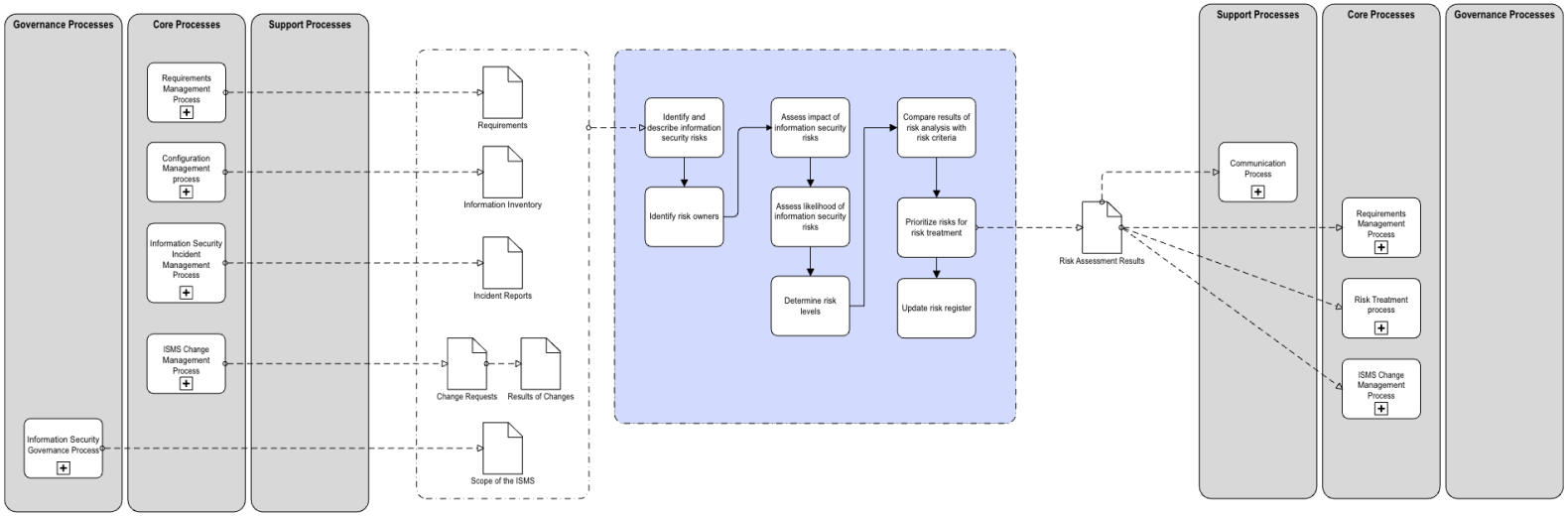
ISMS information security management system

4 RELATED DOCUMENTS

- ISO/IEC 27001:2022 – clause 6.1, 8.2
- Project Plan – Step 7, 8
- Risk Assessment Process
- Risk Treatment Process
- Risk Treatment Procedure

5 PROCEDURE

This procedure describes the activities of the Risk Assessment Process.



5.1 Identify and describe information security risks

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 This could include weak passwords, outdated software, or inadequate physical security.

Commented [AL3]: This step might be redundant to your asset management procedure. This step can be erased in case of an already existing asset inventory.

5.2 Identify risk owners

For each identified risk, assign a risk owner. The risk owner is typically someone with the authority and knowledge to manage the risk and implement necessary controls. Document the name or role of the risk owner alongside each risk.

5.3 Assess impact of information security risks

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

For each threat-vulnerability pair, estimate the potential impact if the threat were to exploit the vulnerability, using the predefined scale.

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.

5.4 Assess likelihood of information security risks

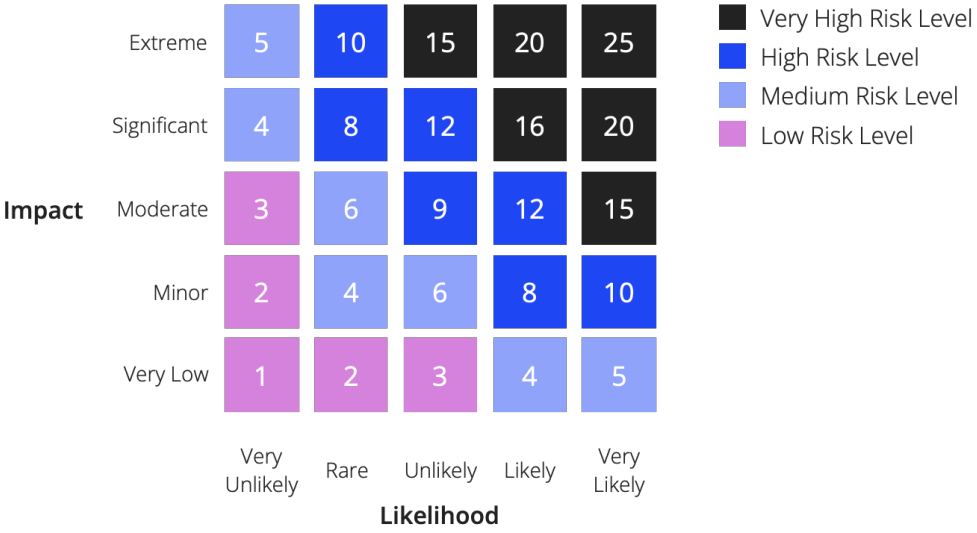
For each threat-vulnerability pair, estimate the likelihood of the threat exploiting the vulnerability, using the predefined scale.

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.

5.5 Determine risk levels

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.



5.6 Compare results of risk analysis with risk criteria

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 treatment as described in the Risk Treatment Procedure.

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.

Commented [AL4]: Adjust the described risk acceptance criteria accordingly, to align with your actual risk appetite.

- **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.

5.7 Prioritize risks for risk treatment

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.

5.8 Update risk register

The risk register should be updated regularly to reflect the current status of each risk, including newly identified risks, changes in existing risks, and the impact of implemented controls on risk levels. This document serves as a central repository for tracking and managing information security risks within the organization.