SOP Information Security Risk Assessment

ISO 27001:2023 Section	Document Section
6.1.1 Actions to address risks and opportunities - General	1., 2., 3.
6.1.2 Information security risk assessment	2.
6.1.3 Information security risk treatment	3.

Summary

This document describes the process for assessing and treating information security risks within the Information Security Management System (ISMS) at *<your company name>*. It outlines the procedures for risk identification, analysis, evaluation, and treatment to ensure that information security risks are managed effectively.

The purpose of the Information Security Risk Assessment Process is to identify, assess, and manage risks that could potentially affect the confidentiality, integrity, and availability of the information assets of *<your company name>*. This process is vital for maintaining robust security practices and ensuring compliance with ISO/IEC 27001:2023 standards.

This document shall be reviewed annually or upon significant changes to the ISMS or the risk landscape. All revisions must be approved by the Information Security Officer (ISO) and communicated to all relevant stakeholders.

Process Steps

1. Risk Identification

The company will:

- Identify the risks associated with the loss of confidentiality, integrity, and availability of information within the scope of the ISMS.
- Document the potential security threats and vulnerabilities that could affect the organization's information assets.

Participants
Management
ISO
Employees

Input	Output
	Identified risks Identified security threats Identified vulnerabilities

2. Risk Analysis

- Analyze the likelihood of each identified risk occurring, along with its potential impact on the organization.
- Utilize qualitative and quantitative methods to evaluate the severity of risks based on predefined criteria.

Participants
ISO

Input	Output
Identified risks Identified security threats Identified vulnerabilities	Information Security Risk Analysis Plan

3. Risk Assessment

- Prioritize the risks based on their likelihood and impact.
- Determine which risks are acceptable and which require further action or treatment based on the risk appetite of the organization.
- Identify appropriate risk treatment options such as risk avoidance, risk transfer, risk acceptance, or risk mitigation.
- Select specific security controls to implement from Annex A of ISO/IEC 27001:2023 or other relevant sources.

Participants
Management ISO

Input	Output
Information Security Risk Analysis Plan	Information Security Risk Table Information Security Risk Analysis Report

4. Monitoring and Review

- Regularly monitor and review the effectiveness of the risk treatment measures and controls.
- Update the Risk Plan, Table and Report appropriately.

Participants
ISO

Input	Output
Monitoring data	
Information Security Risk Analysis Plan	Information Security Risk Analysis Plan (updated)
Information Security Risk Table	Information Security Risk Table (updated)
Information Security Risk Analysis Report	Information Security Risk Analysis Report (updated)
