# Risk Management Procedure

## 1. Introduction

This document outlines the Risk Management Procedure for [Organization Name], designed to ensure compliance with ISO 27001 standards. It provides a framework for identifying, assessing, treating, and monitoring risks to safeguard the confidentiality, integrity, and availability of information assets.

## 2. Purpose

The purpose of this procedure is to establish a systematic approach to risk management, ensuring that risks to organizational information and assets are effectively identified, assessed, and mitigated. This contributes to the organization's ability to meet business objectives and regulatory requirements.

## 3. Scope

This procedure applies to all employees, contractors, and third parties who manage or interact with [Organization Name]'s information assets. It covers all types of risks, including operational, strategic, compliance, and information security risks.

## 4. Policy Statement

1. Risk management activities will follow a defined process, including:  
 - Risk identification: Documenting potential risks to information assets.  
 - Risk assessment: Evaluating the likelihood and impact of identified risks.  
 - Risk treatment: Implementing measures to mitigate, transfer, accept, or avoid risks.  
 - Risk monitoring: Continuously reviewing and updating risk profiles.

2. A Risk Register will be maintained and updated regularly by the Risk Management Committee to document identified risks, assessment results, and treatment plans.

3. Risk assessments must be conducted:  
 - Annually as part of the organization’s risk management review cycle.  
 - Whenever significant changes occur in systems, processes, or regulatory requirements.

4. All risk management activities must be documented and retained for audit and compliance purposes.

5. The organization will provide adequate resources, training, and tools to support effective risk management.

## 5. Roles and Responsibilities

- Risk Owners: Responsible for managing specific risks and implementing treatment plans.

- Employees and Contractors: Identify and report risks and adhere to risk management practices.

- Risk Management Committee: Oversees risk management activities and ensures alignment with organizational objectives.

- Information Security Team: Provides guidance on information security risks and supports mitigation efforts.

- Compliance Officer: Ensures risk management aligns with regulatory and legal requirements.

## 6. Compliance and Monitoring

Compliance with this procedure will be ensured through:  
- Regular reviews of the Risk Register and treatment plans.  
- Periodic internal and external audits.  
- Monitoring key risk indicators (KRIs) and control effectiveness.  
Non-compliance will result in corrective actions, including retraining, process adjustments, or disciplinary measures.

## 7. Related Documentation

- [Information Security Policy]

- [Business Continuity Plan]

- [Incident Management Procedure]

- [Risk Assessment Template]

## 8. Review and Revision

This procedure will be reviewed annually or following any significant organizational, technological, or regulatory changes. The Risk Management Committee will initiate and document updates as required.

## Appendix A: Risk Assessment Process

- Step 1: Risk Identification: Document potential risks, their sources, and affected assets.  
- Step 2: Risk Analysis: Assess the likelihood and impact of risks using a risk matrix.  
- Step 3: Risk Evaluation: Prioritize risks based on their severity.  
- Step 4: Risk Treatment: Develop and implement measures to mitigate, transfer, accept, or avoid risks.  
- Step 5: Documentation: Record all findings, decisions, and actions in the Risk Register.  
- Step 6: Monitoring and Review: Regularly review and update the Risk Register and treatment plans.

## Appendix B: Risk Matrix Example

| Likelihood/Impact | Low | Medium | High |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Low | Low Risk | Low Risk | Medium Risk |
| Medium | Low Risk | Medium Risk | High Risk |
| High | Medium Risk | High Risk | Critical Risk |