# Risk Assessment and Treatment Policy Template

## Document Control Information

- **Document Title:** Risk Assessment and Treatment Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

## 1. Introduction

### 1.1 Purpose

This Risk Assessment and Treatment Policy establishes [ORGANIZATION NAME]'s approach to information security risk management in accordance with ISO 27001:2022 requirements. It provides a structured framework for identifying, analyzing, evaluating, and treating information security risks.

### 1.2 Scope

This policy applies to all information assets, systems, and processes within the defined scope of [ORGANIZATION NAME]'s Information Security Management System (ISMS). It covers: - All information in electronic or physical form - All information systems and networks - All business processes and activities - All employees, contractors, and third parties with access to information assets

### 1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing a systematic approach to information security risk management - Identifying and addressing risks to the confidentiality, integrity, and availability of information - Ensuring risk assessments are conducted at planned intervals and when significant changes occur - Applying appropriate risk treatment options based on organizational risk appetite - Continuously improving the risk management process

# 2. Risk Management Framework

## 2.1 Risk Management Process

[ORGANIZATION NAME] shall follow a structured risk management process consisting of: 1. Context establishment 2. Risk identification 3. Risk analysis 4. Risk evaluation 5. Risk treatment 6. Risk monitoring and review 7. Risk communication and consultation

## 2.2 Risk Management Roles and Responsibilities

### 2.2.1 Senior Management

- Approve the Risk Assessment and Treatment Policy
- Define risk acceptance criteria
- Approve risk treatment plans
- Accept residual risks

### 2.2.2 Risk Management Committee

- Oversee the risk management process
- Review and validate risk assessments
- Prioritize risks for treatment
- Monitor implementation of risk treatment plans

### 2.2.3 Information Security Manager/Officer

- Coordinate risk assessment activities
- Facilitate risk identification and analysis
- Develop risk treatment plans
- Report on risk status to senior management

### 2.2.4 Risk Owners

- Identify risks within their area of responsibility
- Contribute to risk analysis and evaluation
- Implement risk treatment measures
- Monitor and report on risk status

### 2.2.5 All Staff

- Report potential risks and security incidents
- Participate in risk assessment activities when required

- Implement risk controls as directed

# 3. Risk Assessment

## 3.1 Risk Assessment Methodology

[ORGANIZATION NAME] shall use a consistent methodology for risk assessment that includes:

### 3.1.1 Asset Identification and Valuation

- Identify information assets within the scope of the ISMS
- Categorize assets by type (information, software, physical, services, people)
- Assign value to assets based on confidentiality, integrity, and availability requirements

### 3.1.2 Threat Identification

- Identify potential threats to information assets
- Consider both internal and external threats
- Include natural, human, and technical threats

### 3.1.3 Vulnerability Identification

- Identify vulnerabilities that could be exploited by threats
- Consider technical, operational, and management vulnerabilities
- Use vulnerability assessments, penetration testing, and other methods as appropriate

### 3.1.4 Risk Analysis

- Determine likelihood of threat exploiting vulnerability
- Determine potential impact on confidentiality, integrity, and availability
- Calculate risk level using defined risk calculation method

### 3.1.5 Risk Evaluation

- Compare risk levels against risk acceptance criteria
- Prioritize risks for treatment
- Document risk assessment results

### 3.2 Risk Calculation Method

[ORGANIZATION NAME] shall calculate risk levels using the following formula:

**Risk Level = Likelihood × Impact**

#### 3.2.1 Likelihood Scale

| Level | Description | Criteria | Score |
|---|---|---|---|
| 5 | Almost Certain | Expected to occur in most circumstances; may occur multiple times per year | 5 |
| 4 | Likely | Will probably occur in most circumstances; may occur once per year | 4 |
| 3 | Possible | Might occur at some time; may occur once every 1-2 years | 3 |
| 2 | Unlikely | Could occur at some time; may occur once every 2-5 years | 2 |
| 1 | Rare | May occur only in exceptional circumstances; may occur once every 5+ years | 1 |

#### 3.2.2 Impact Scale

| Level | Description | Criteria | Score |
|---|---|---|---|
| 5 | Severe | Catastrophic financial loss; severe reputational damage; significant regulatory penalties; | 5 |

| Level | Description | Criteria | Score |
|---|---|---|---|
| | | business continuity severely affected | |
| 4 | Major | Major financial loss; significant reputational damage; regulatory non-compliance; business continuity significantly affected | 4 |
| 3 | Moderate | Moderate financial loss; some reputational damage; potential regulatory issues; business continuity moderately affected | 3 |
| 2 | Minor | Minor financial loss; limited reputational damage; minor compliance issues; business continuity minimally affected | 2 |
| 1 | Negligible | Negligible financial loss; no reputational damage; no compliance issues; no effect on business continuity | 1 |

#### 3.2.3 Risk Level Matrix

| Likelihood/ Impact | Negligible (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|---|
| Almost Certain (5) | 5 | 10 | 15 | 20 | 25 |

| Likelihood/ Impact | Negligible (1) | Minor (2) | Moderate (3) | Major (4) | Severe (5) |
|---|---|---|---|---|---|
| Likely (4) | 4 | 8 | 12 | 16 | 20 |
| Possible (3) | 3 | 6 | 9 | 12 | 15 |
| Unlikely (2) | 2 | 4 | 6 | 8 | 10 |
| Rare (1) | 1 | 2 | 3 | 4 | 5 |

### 3.3 Risk Acceptance Criteria

[ORGANIZATION NAME] shall use the following risk acceptance criteria:

| Risk Level | Risk Rating | Action Required |
|---|---|---|
| 15-25 | Critical | Immediate action required; senior management attention needed |
| 9-14 | High | Specific management responsibility must be specified |
| 5-8 | Medium | Management responsibility must be specified |
| 1-4 | Low | Manage by routine procedures |

### 3.4 Risk Assessment Frequency

[ORGANIZATION NAME] shall conduct risk assessments: - At planned intervals, at least annually - When significant changes occur to the organization, technology, or business processes - When new threats or vulnerabilities are identified - Following major security incidents - When required by regulatory or contractual obligations

### 3.5 Risk Assessment Documentation

Risk assessment results shall be documented and include: - Scope and objectives of the assessment - Risk assessment methodology used - Identified assets, threats, and vulnerabilities - Risk analysis and evaluation results - Recommended risk treatment options

# 4. Risk Treatment

## 4.1 Risk Treatment Options

[ORGANIZATION NAME] shall consider the following risk treatment options:

### 4.1.1 Risk Modification (Mitigate)

- Implement controls to reduce the likelihood and/or impact of the risk
- Select controls from ISO 27001:2022 Annex A or other appropriate sources
- Document controls in the Statement of Applicability

### 4.1.2 Risk Retention (Accept)

- Accept the risk without further action
- Only applicable when risk level is within risk acceptance criteria
- Must be formally approved by risk owners and senior management

### 4.1.3 Risk Avoidance (Avoid)

- Eliminate the risk by removing the risk source
- Discontinue the activity that generates the risk
- Change the conditions under which the activity operates

### 4.1.4 Risk Sharing (Transfer)

- Share the risk with another party
- May include insurance, outsourcing, or contractual agreements
- Does not eliminate responsibility for the risk

## 4.2 Risk Treatment Plan

[ORGANIZATION NAME] shall develop and maintain a risk treatment plan that includes: - Selected risk treatment options for each risk - Required resources for implementation - Responsibilities and timelines - Metrics for measuring effectiveness - Residual risk after treatment

## 4.3 Statement of Applicability

[ORGANIZATION NAME] shall maintain a Statement of Applicability that: - Lists all controls from ISO 27001:2022 Annex A - Indicates whether each control is applicable or not - Provides justification for inclusion or exclusion of controls - Documents the implementation status of each applicable control

### 4.4 Residual Risk Acceptance

Residual risks remaining after risk treatment shall be: - Documented and communicated to relevant stakeholders - Formally accepted by risk owners and senior management - Monitored and reviewed at planned intervals

## 5. Risk Monitoring and Review

### 5.1 Monitoring Activities

[ORGANIZATION NAME] shall monitor: - Implementation and effectiveness of risk treatment plans - Changes to risks, threats, and vulnerabilities - Changes to risk acceptance criteria - Incidents and events that may affect risk levels

### 5.2 Review Frequency

Risk monitoring and review shall be conducted: - For critical risks: Monthly - For high risks: Quarterly - For medium risks: Semi-annually - For low risks: Annually

### 5.3 Risk Communication

Risk information shall be communicated to: - Senior management through regular reports - Risk owners and stakeholders as appropriate - External parties when required by contractual or regulatory obligations

## 6. Continuous Improvement

[ORGANIZATION NAME] shall continuously improve the risk management process by: - Learning from experience and incidents - Updating risk assessment methodology based on effectiveness - Incorporating new threat intelligence and vulnerability information - Adapting to changes in the organization and its context

## 7. Related Documents

- Information Security Policy
- Statement of Applicability
- Risk Assessment Methodology
- Risk Treatment Plan
- Risk Register
- [LIST OTHER RELEVANT DOCUMENTS]

## 8. Approval

This Risk Assessment and Treatment Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____