Risk Assessment Template

Document Control Information

- **Document Title:** Information Security Risk Assessment
- **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 document provides a structured approach for conducting information security risk assessments in accordance with ISO 27001:2022 requirements. It outlines the methodology for identifying, analyzing, and evaluating information security risks to [ORGANIZATION NAME]'s assets.

1.2 Scope

This risk assessment covers all information assets within the defined scope of [ORGANIZATION NAME]'s Information Security Management System (ISMS).

2. Risk Assessment Methodology

2.1 Risk Assessment Process

[ORGANIZATION NAME] follows a systematic approach to risk assessment:

1. **Asset Identification**: Identify and value information assets
2. **Threat Identification**: Identify potential threats to those assets
3. **Vulnerability Assessment**: Identify vulnerabilities that could be exploited
4. **Risk Analysis**: Determine likelihood and impact of risk scenarios
5. **Risk Evaluation**: Compare risk levels against acceptance criteria
6. **Risk Treatment**: Determine appropriate risk treatment options

2.2 Risk Calculation

Risk is calculated using the following formula:

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

Risk Level = Likelihood × Impact

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

Impact Scale

Level	Description	Criteria	Score
5	Severe	Catastrophic financial loss; severe reputational damage; significant regulatory penalties; business continuity severely affected	5

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

Level	Description	Criteria	Score
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

Risk Level Matrix

Likelihood/ Impact	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20

iso27001kit.com

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

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

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. Risk Assessment Register

Risk ID	Asset	Threat	Vulnerability	Existing Controls	Likelihood (1-5)	Impact (1-5)	Risk Level	Risk Rating
R001	[Asset Name]	[Threat Description]	[Vulnerability Description]	[Existing Controls]	[1-5]	[1-5]	[L×I]	[Critical/ High/ Medium/ Low]
R002								
R003								
R004								

iso27001kit.com

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

Risk ID	Asset	Threat	Vulnerability	Existing Controls	Likelihood (1-5)	Impact (1-5)	Risk Level	Risk Rating
R005								

4. Risk Treatment Options

For each identified risk, one or more of the following treatment options will be selected:

1. **Risk Modification (Mitigate)**: Implement controls to reduce the likelihood and/or impact of the risk
2. **Risk Retention (Accept)**: Accept the risk without further action (typically for low risks or where cost of mitigation exceeds benefit)
3. **Risk Avoidance (Avoid)**: Eliminate the risk by removing the risk source or discontinuing the activity
4. **Risk Sharing (Transfer)**: Share the risk with another party (e.g., insurance, outsourcing)

5. Risk Treatment Plan

Risk ID	Risk Treatment Option	Control(s) to be Implemented	Responsible Person	Target Completion Date	Resources Required	Status	Ve Me
R001	[Option]	[Control Description]	[Role/Name]	[Date]	[Resources]	[Not Started/In Progress/ Completed]	[Ve Me
R002							
R003							
R004							
R005							

iso27001kit.com

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com

6. Risk Monitoring and Review

All identified risks will be monitored and reviewed according to the following schedule:

- **Critical Risks**: Monthly review
- **High Risks**: Quarterly review
- **Medium Risks**: Semi-annual review
- **Low Risks**: Annual review

Additionally, risk assessments will be reviewed: - When significant changes occur to the organization, technology, or business processes - Following security incidents - When new threats or vulnerabilities are identified - As part of the internal audit program - At least annually as part of the management review process

7. Approval

This Risk Assessment has been reviewed and approved by:

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

iso27001kit.com

ISO27001KIT — Personal use only. Need a customised version? Visit iso27001kit.com