Risk Management Plan

Instructions for using this template:

1. Replace all *[bracketed placeholders]* with your specific information.

2. Customize the risk categories and scoring scales to match your organization.

3. Complete the risk register with your identified risks.

4. Distribute to all stakeholders and begin implementation.

5. Schedule regular reviews and updates as specified.

Organization: *[Your organization's name]*	**Date:** *[Current date]*
Project/Department: *[If applicable]*	**Risk Manager:** *[Name and contact information]*
Plan Version: *[Version number]*	**Review Date:** *[Next scheduled review date]*

1. Risk Management Approach

Risk Management Objectives

- *[State your primary risk management goals, e.g., "Protect project timeline and budget while ensuring quality deliverables."]*
- *[Add 2-3 specific objectives relevant to your context.]*

Risk Appetite Statement

- Our organization's risk appetite is: *[Low/Medium/High]*
- We will accept risks with scores up to: *[Number, e.g., "8 on our 1-25 scale"]*
- Risks scoring above this threshold require: *[Escalation process, e.g., "Executive approval and dedicated mitigation resources."]*

2. Risk Assessment Framework

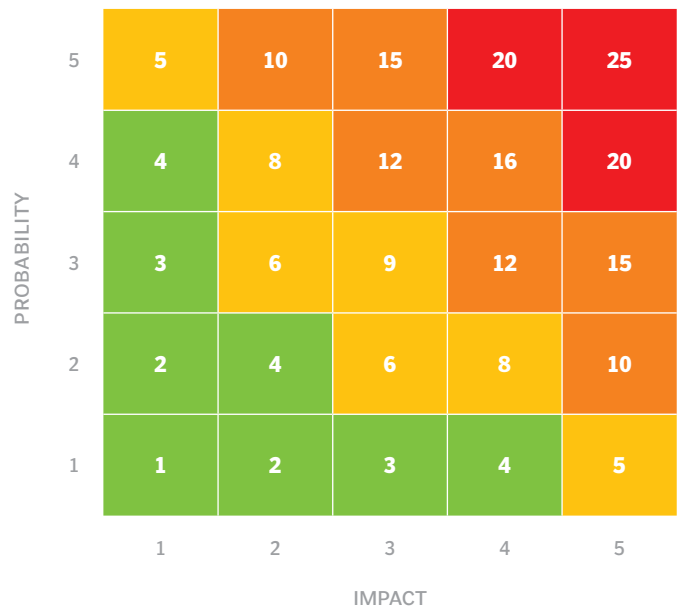
Risk Probability Scale (1-5)

SCORE	LIKELIHOOD	DESCRIPTION
1	Very low	Risk is unlikely to occur (less than 10% chance).
2	Low	Risk might occur but is uncommon (10-30% chance).
3	Medium	Risk has a moderate likelihood of occurring (30-60% chance).
4	High	Risk is likely to occur (60-80% chance).
5	Very high	Risk is almost certain to occur (over 80% chance).

Risk Impact Scale (1-5)

SCORE	IMPACT LEVEL	DESCRIPTION
1	Minimal	Minor disruption easily managed within normal operations.
2	Low	Some impact but manageable with existing resources.
3	Medium	Significant impact requiring management attention and additional resources.
4	High	Major impact that affects multiple business areas or key objectives.
5	Critical	Severe impact that could threaten business viability.

Risk Priority Matrix



Risk Priority Levels (Probability x Impact)

- **Critical priority** (Scores 20-25):
  Executive escalation and dedicated resources.
- **High priority** (Scores 10-16):
  Immediate mitigation required.
- **Medium priority** (Scores 5-9):
  Active management with an assigned risk owner.
- **Low priority** (Scores 1-4):
  Monitor only.

3. Roles and Responsibilities

ROLE	RESPONSIBLE PERSON	KEY RESPONSIBILITIES
Risk Manager	*[Name/title]*	Overall plan coordination, reporting, training
Senior Leadership	*[Names/titles]*	Risk appetite decisions, resource approval
Department Managers	*[Names/titles]*	Departmental risk identification and response
Risk Committee	*[Names/titles]*	Risk management plan review and policy decisions

Risk Ownership Assignments *[Complete for each major risk category]*

Operational Risks	Financial Risks	Technology Risks	Regulatory Risks	External Risks
[Department/ person]	*[Department/ person]*	*[Department/ person]*	*[Department/ person]*	*[Department/ person]*

4. Risk Response Strategies

Response Strategy Framework

STRATEGY	WHEN TO USE	EXAMPLE ACTIONS
Avoid	High-impact risks that can be eliminated.	Change project scope, alter processes.
Transfer/share	Risks others can manage more effectively.	Insurance, outsourcing, contracts.
Mitigate	Risks worth reducing but not eliminating.	Training, backup systems, controls.
Accept	Low-priority, unavoidable or tolerable risks.	Monitor only, with contingency planning.

Contingency Planning Requirements

All risks with scores above *[threshold, e.g., "15"]* must have documented contingency plans including:

- Trigger events that activate the plan.
- Specific response actions and timelines.
- Required resources and authorization levels.
- Communication protocols and escalation paths.

5. Risk Register

Current Risk Inventory

	R001	R002	R003
RISK DESCRIPTION	*[Example: Cybersecurity breach]*	*[Expand the table to add all relevant risks.]*	
CATEGORY	Technology		
PROBABILITY	3		
IMPACT	5		
SCORE	15		
PRIORITY	High		
OWNER	IT manager		
RESPONSE STRATEGY	Mitigate		
STATUS	Active		
REVIEW DATE	*[Date]*		

Risk Identification Methods

- Stakeholder interviews conducted.
- Historical incident review completed.
- Industry benchmark analysis performed.
- Expert consultation sessions held.
- Process walkthrough assessments done.

6. Risk Monitoring and Reporting

KEY RISK INDICATORS (KRIS)	REVIEW SCHEDULE	REPORTING REQUIREMENTS
[Define 3-5 metrics that provide early warning of emerging risks.] *1. [Example: "Number of failed login attempts per day (cybersecurity risk indicator)."]* *2. [Example: "Budget variance percentage (financial risk indicator)."]* *3. [Add your organization's specific KRIs.]*	■ **Daily:** Risk owner monitoring of assigned risks. ■ **Weekly:** Department manager risk status updates. ■ **Monthly:** Risk committee formal review meeting. ■ **Quarterly:** Complete risk register review and update. ■ **Annually:** Full risk management plan review and revision.	■ **Risk status dashboard:** Updated weekly, accessible to all stakeholders. ■ **Monthly risk report:** Summary for senior leadership. ■ **Incident reports:** Within 24 hours of a risk event occurring. ■ **Annual risk assessment:** Comprehensive review for board presentation.

7. Communication Plan

Internal Communication

AUDIENCE	INFORMATION	FREQUENCY	METHOD
Executive Team	Risk summary, critical issues	Monthly	Dashboard and report
Department Managers	Departmental risks, action items	Weekly	Email and meetings
All Staff	Risk awareness, procedures	Quarterly	Newsletter and training
Board of Directors	Strategic risks, major incidents	Quarterly	Formal presentation

External Communication

- Regulatory bodies: *[As required by specific regulations.]*
- Insurance providers: *[Annual policy reviews and incident reports.]*
- Key stakeholders: *[Define communication triggers and protocols.]*

8. Training and Awareness

Required Training

- Risk identification workshop for all managers.
- Risk assessment methodology training for risk owners.
- Incident response procedure training for all staff.
- Annual risk management refresher training.

Training Schedule

- New employee orientation: Risk management overview.
- Annual all-staff training: Risk awareness and procedures.
- Specialized training: Role-specific risk management skills.

9. Plan Maintenance

Review Triggers

This plan will be reviewed when:

- Significant organizational changes occur.
- Major risk events happen.
- New regulations or standards are introduced.
- Annual review cycle is reached.
- Risk tolerance levels change.

Version Control

VERSION	DATE	CHANGES MADE	APPROVED BY
1.0	*[Date]*	Initial plan creation	*[Name/title]*

Plan Approval

RISK MANAGER	DEPARTMENT HEAD	SENIOR EXECUTIVE
[Name/Date]	*[Name/Date]*	*[Name/Date]*

10. Appendices

Appendix A: Risk Assessment Worksheets
[Attach blank forms for risk identification and assessment.]

Appendix B: Incident Response Procedures
[Link to or include detailed response procedures.]

Appendix C: Escalation Contact List
[Emergency contacts and escalation procedures.]

Appendix D: Regulatory Requirements
[Industry-specific compliance requirements.]