Risk Management Policy

For Australian Small & Medium Enterprises

Template Version 1.0 | December 2024

Important Notice

This template is provided as a general guide only and should be customised to your specific workplace and business context. The framework is based on AS/NZS ISO 31000:2018 Risk Management Guidelines. We recommend seeking professional advice for implementation.

1. Purpose

This policy establishes [Company Name]'s framework for identifying, assessing, treating, and monitoring risks. Effective risk management helps us protect our people, assets, reputation, and business continuity while enabling us to pursue opportunities.

2. Scope

This policy applies to:

- All business activities and operations
- All employees, contractors, and stakeholders
- All types of risk (strategic, operational, financial, compliance, WHS)

3. Policy Statement

[Company Name] is committed to:

- Integrating risk management into planning and decision-making
- Creating a culture where risk awareness is part of everyday activities
- Applying a systematic approach to risk management
- Allocating appropriate resources to manage risks
- Continuously improving our risk management practices
- Complying with legal and regulatory requirements

4. Risk Management Framework

[Company Name] follows the ISO 31000 risk management process:

- Establish context
- Identify risks
- Analyse risks

- Evaluate risks
- Treat risks
- Monitor and review
- Communicate and consult

5. Establishing Context

Before assessing risks, we consider:

- Our business objectives and strategy
- Internal factors (capabilities, culture, processes)
- External factors (economic, regulatory, competitive)
- Stakeholder expectations
- Risk appetite and tolerance

6. Risk Identification

Risks are identified through:

- Regular risk assessments and reviews
- Workplace inspections
- Incident analysis
- Stakeholder feedback
- Environmental scanning
- Project and change assessments
- Audits and reviews

All employees are encouraged to identify and report risks.

7. Risk Categories

[Company Name] considers risks across the following categories:

7.1 Strategic Risks

- Market and competitive changes
- Reputation and brand
- Strategic decisions and direction

7.2 Operational Risks

- Business processes and systems
- Technology and infrastructure
- Supply chain and suppliers
- Business continuity

7.3 Financial Risks

- Cash flow and liquidity
- Credit and debt
- Revenue and profitability

7.4 Compliance Risks

- Legal and regulatory requirements
- Contractual obligations
- Licences and permits

7.5 People Risks

- Work health and safety
- Workforce capability and capacity
- Employment relations

8. Risk Analysis

Identified risks are analysed by considering:

- Likelihood – how probable is the risk to occur?
- Consequence – what is the potential impact if it occurs?
- Existing controls – what is already in place?
- Control effectiveness – how well do controls work?

8.1 Likelihood Ratings

[Company Name] uses the following likelihood scale:

- Rare – May occur only in exceptional circumstances
- Unlikely – Could occur but not expected
- Possible – Might occur at some time
- Likely – Will probably occur
- Almost Certain – Expected to occur in most circumstances

8.2 Consequence Ratings

Consequences are assessed across multiple dimensions:

- Insignificant – Minimal impact
- Minor – Small impact, easily managed
- Moderate – Noticeable impact, requires management
- Major – Significant impact, serious consequences
- Catastrophic – Severe impact, threatens business viability

9. Risk Evaluation

The risk rating is determined by combining likelihood and consequence. This determines priority for treatment:

- Extreme risks – Require immediate action and senior management attention
- High risks – Require prompt action and management attention
- Medium risks – Require planned action
- Low risks – Managed through routine procedures

10. Risk Treatment

Risks are treated using one or more of the following strategies:

- Avoid – Eliminate the activity that creates the risk
- Reduce – Implement controls to reduce likelihood or consequence
- Transfer – Share the risk (insurance, contracts, outsourcing)
- Accept – Accept the risk if within tolerance

10.1 Control Selection

When selecting controls, consider:

- Effectiveness in reducing risk
- Costs versus benefits
- Practicability
- New risks introduced
- Legal and compliance requirements

10.2 Treatment Plans

For significant risks, treatment plans include:

- Specific actions to be taken
- Responsible person
- Timeframes
- Resources required
- Success measures

11. Risk Appetite and Tolerance

[Company Name] has a low appetite for risks that could:

- Cause harm to people
- Result in significant regulatory breach
- Cause major financial loss

- Damage reputation

We may accept higher levels of risk where there are significant opportunities aligned with our strategy.

12. Monitoring and Review

Risk management is an ongoing process. [Company Name] will:

- Review the risk register regularly (at least quarterly)
- Monitor key risk indicators
- Review control effectiveness
- Update risk assessments when circumstances change
- Conduct periodic audits of risk management processes
- Learn from incidents and near misses

13. Communication and Consultation

[Company Name] will:

- Communicate risk information to relevant stakeholders
- Consult with employees on workplace risks
- Report significant risks to management
- Maintain open channels for risk reporting
- Provide training on risk management

14. Risk Register

[Company Name] maintains a risk register that includes:

- Risk description and category
- Causes and consequences
- Existing controls
- Risk rating (before and after controls)
- Treatment actions
- Risk owner
- Review dates

The register is a living document, regularly updated and reviewed.

15. Responsibilities

15.1 Senior Management

- Set risk management direction and culture
- Approve risk appetite and tolerance
- Review significant risks

- Allocate resources
- Monitor risk management effectiveness

15.2 Managers

- Identify and assess risks in their area
- Implement and monitor controls
- Report significant risks
- Promote risk awareness

15.3 All Employees

- Identify and report risks
- Follow risk management procedures
- Participate in risk assessments
- Suggest improvements

16. Integration

Risk management is integrated with:

- Strategic planning
- Project management
- Change management
- Work health and safety
- Business continuity planning
- Compliance management

17. Documentation

[Company Name] maintains documentation including:

- This risk management policy
- Risk register
- Risk assessment templates
- Treatment plans
- Review and audit records

18. Review

This policy will be reviewed:

- At least annually
- Following significant incidents
- When business context changes significantly

- When legislation or standards change

Employee Acknowledgement

I acknowledge that I have read and understood [Company Name]'s Risk Management Policy. I understand my responsibility to identify and report risks and to follow risk management procedures.

Employee Name: _____

Signature: _____

Date: _____