**GUIDE TO RISK MANAGEMENT POLICY TEMPLATE**

**ABOUT THIS POLICY AREA**

This policy guides how the organisation plans and manages its risks.

**Policy checklist**

The following checklist will help you check that an existing policy covers this area adequately.

The policy should:

* say who will be responsible for risk assessment and management
* say how risk management will be documented
* explain how risks will be identified, assessed and removed, minimised or managed
* explain how implementation of actions responding to risks are monitored and reviewed for effectiveness
* contain clear procedures and actions
* indicate the timing of any actions
* show when it was approved
* show when it was last reviewed.

**COMPLETING YOUR RISK MANAGEMENT POLICY**

**Using the policy template**

The template provides some example statements. You can adapt these statements and include them in your policy or write your own statements to better suit the operations and services of your organisation.

The policy templates include **red text** prompts to insert information that is specific to your organisation.

**Guidelines for each section of your policy**

***1. Purpose***

In thinking about the purpose of this policy, consider how it might apply to the range of risks your organisation might encounter.

***2. Scope***

To determine the scope of the policy, consider the following questions:

• Does this policy apply to all your organisation’s services, assets, personnel? The risk management process should apply to all aspects of your organisation, unless you have

 a separate policy dealing with specific aspects of risk, in which case make reference to those policies.

• Are there any specific areas of risk, such as Business Continuity and planning for disasters? This is also an aspect of risk management, probably best covered by a separate policy. Again, make reference to this policy in the scope.

***3. Policy statement***

If you are adopting the policy statement in the template, consider whether there are any additional

commitments your organisation wants to make.

In identifying the actions your organisation will take to implement this policy, you should include the following:

* Following an agreed process to identify, assess and manage risks appropriate to our organisation.
* Regular reviews of previously identified risks to improve the strategies to minimise the risk and plans for responding to the risk if it occurs and
* The continuous identification of new risks and strategies to control the risks.
* Maintenance of a Risk Management Plan or Register which records risks and agreed actions.
* Integrating risk management into the Continuous Improvement process, by including improvements to reduce or control risks in the improvement process and in the Continuous Improvement Plan.
* Reporting regularly to the Board or Management Committee on the Risk Management Plan and progress.

***4. Procedures***

The procedures describe how your organisation achieves the aims and goals you have outlined in your purpose, scope and policy statement.

*4.1 Risk Management Plan/Register*

Indicate who will be responsible for maintaining the Risk Management Plan or Register.

List the information that will be included in the Register. Consider including the following:

* A Risk Management Plan will be developed and maintained and has three sections:
	+ Risks to the **organisation** such as loss of funding, inability to deliver funded outcomes within budget, Board of Management dysfunction, embezzlement of funds, lack of suitably qualified staff, extended staff illness, loss of data due to natural disasters, etc.
	+ Risks relating to **staffing** such as a lack of suitably qualified staff, extended staff illness, staff injury ( physical or psychological) due to OHS risks or client contact risks, impacts of natural disasters and infection control risks, etc.
	+ Risks to s**ervice users** such as home environment risks, risks from confidentiality breaches, falls risks, transport risks, risks from staff in the home, interruptions to service delivery including from natural disasters. ( This will vary depending on your service types and is essentially about risks associated with the services you provide)
* The *Risk Management Plan* includes the following information:

*Date identified:* date the risk was identified

*The specific risk identified*: these are the risks identified by the organisation

*What can go wrong:* details of what can go wrong in relation to the risk

*Consequence*: the consequence of the risk, using the risk rating matrix (included in the policy template):

1= Insignificant

2= Minor

3= Moderate

4= Major

5= Catastrophic

*Likelihood*: the likelihood of the risk occurring, using the risk rating matrix (included in the policy template):

A: Almost Certain

B: Likely

C: Possible

D: Unlikely

E: Rare

*Risk Rating*: the rating for each identified risk, using the risk rating matrix:

L = Low

M = Moderate

H = High

E = Extreme

*Current controls to reduce risk*: the controls or strategies in place to control or reduce the risk

*Date reviewed:* Date the risk and controls were reviewed to identify improvements

*New controls:* Additional controls necessary to control or reduce risk or changes to existing controls.

*Persons Responsible for Identified Actions*

*Date actions are to be completed by.*

*4.2 Identifying and Assessing Risks*

Identify who is involved in identifying risks, and what sources of information and expertise are considered in identifying risks, such as:

* Staff and service user feedback
* Staff Accident/ Incident Reports
* Service user Complaints
* Hazards and maintenance information
* Review of policies and procedures and processes
* Management knowledge and understanding of service delivery and work processes.
* Results and advice from external audits and compliance processes.
* Information from peak, industry and funding bodies.

What processes are used to regularly identify risks? This could be a standing agenda item for staff and Committee meetings, and/or a part of annual organisation planning with all personnel. Or the Coordinator may consult with specific staff around various types of risk (eg. Financial, HR, client services).

Identify the process you use to assess each risk. We suggest using the matrix included in the template.

*4.3 Identifying and Implementing Controls*

Controls are strategies to manage risk balanced against the cost and inconvenience of the control. Common controls include:

* Staff training
* Provision of information
* The use of safe or safer equipment
* Maintaining adequate insurance
* Changes in procedures or practices
* Personal checks including referee checks, driver’s licences, motor vehicle registrations, professional registrations, criminal history checks
* The development of plans for dealing with risks that occur.

Decisions about controls are generally made following the identification and assessment of risks.

Simple controls may be determined by staff or the Coordinator. Controls which entail any significant cost or policy change may require Committee approval.

*4.4 Recording Improvements*

Improvements implemented as a result of risk management reviews and planning are recorded in the Continuous Improvement Plan (may just be noted and a reference made to the Risk Management Plan) as well as in the Risk Management Plan to ensure that they are implemented, monitored and evaluated.

Consider who will be responsible for keeping these Plans up to date, and how they will be monitored (eg: standing agenda item at staff/Committee meetings) to ensure actions are implemented.

Actions also need to be reviewed to ensure that they are having the intended effect and that there are not unintended consequences.

***5. Other related policies and documents***

List the other policies related to the risk management policy. The policy should be linked to:

* financial management and delegations policy
* asset management
* business continuity and disaster planning
* continuous improvement
* work health and safety policies

***6. Review processes***

Consider how often the policy should be reviewed and the process for doing this:

• **frequency of review:** Most policies benefit from an annual review. The experience of implementing the policy is used to decide which changes are necessary. Consider reviewing your risk management policy as part of an annual review of your organisation’s governance- and accountability-related policies or, if your organisation is small, perhaps over a three-year period. Critical incidents may prompt you to review the policy ahead of schedule.

• **responsibility for the review:** In most organisations, the senior staff and/or board or management committee would be responsible for reviewing this policy.

• **process for the review:** Decide which particular staff, volunteers, external people and organisations will provide input to the policy review.

• **decision-making process:** Who will review draft changes to the policy and approve changes? What will be the timeframe for the review process?

• **documentation and communication:** What records of the policy review process are needed? How will changes to the policy be communicated to staff implementing the policy? In a small organisation, this may be as simple as noting the changes at a staff meeting. In a larger organisation, an email memo may be needed.

• **key questions for the review:** Is the policy being implemented? Are procedures being followed? Is the policy clear? What has changed that may prompt a change to the policy? Have particular stakeholders had difficulty with any aspect of the policy? Can their concerns be resolved? How does the policy compare with that of similar organisations?