Risk Management Procedure

Template

vmia

VICTORIA
State Government

1. Purpose of this procedure

Our procedure shows how we'll embed our risk framework and processes in the organisation so that they shape the way we make decisions every day across the organisation.

In developing this procedure, we've aimed to apply the risk management principles to make sure risk management:

- is integrated into organisational processes and decision making
- is systematic, structured, and comprehensive
- is based on the best available information
- is customised to our operating environment
- takes people and cultural factors into account
- is dynamic, iterative and responsive to change
- is transparent and inclusive
- facilitates continuous improvement.

2. What we've covered in our procedure

Our procedure details:

- Roles and responsibilities
- A governance model to facilitate decision making within the organisation and with other organisations, and makes sure decision makers are accountable
- How risk assessment is part of decision making
- Communication and training
- Information management
- How we'll monitor and report on control effectiveness of controls
- How we'll escalate action when risk crosses tolerance thresholds
- How we'll continuously improve.

3. Scope

This procedure should be followed by all decision makers in the organisation whether they work on the executive team or in frontline roles. It also applies to our volunteers, suppliers and to businesses contracted to provide services to our clients and public.

4. Other elements of our risk management framework

List the other elements of your framework. A foundation-level framework will have a:

- risk management policy
- risk management strategy
- risk appetite statement
- risk register.

5. Roles and responsibilities

Define what we all should do:

- What are everyone's responsibilities when it comes to managing risk?
- What are the legal obligations of people in various roles in the organisation?
- What does the code of conduct say about how we should manage risk?

Describe the responsibilities for each of specific roles:

- Responsible body
- Audit and Risk Management Committee
- Chief Executive Officer
- Executive team and management
- Chief Risk Officer or Risk Manager
- Non-managerial members of staff.
- Internal and external audit
- Other related bodies such as risk management sub-committee, clinical risk management committees, etc.

6. Governance

Describe the model of governance you'll put in place

This is to ensure that significant decisions are approved in the appropriate forums and there's space allowed to consider risk. This needs to include external forums where shared risks might be discussed:

- What types of decisions need to be considered in by a specialist group before being executed? E.g. those involving clinical, environmental, cyber, shared risks?
- What decisions do they have the authority to make and are accountable for?
- Who these specialist decision-making groups themselves are accountable to?
- How will they monitor key risk and performance indicators?

Use a diagram to show:

- the specialist decision-making groups you need in your organisation
- relations between decision making groups; for example, when a clinical risk needs to be communicated or escalated to the responsible body
- the flow of information: requests for decision, communications of decisions, reporting.

7. Embedding risk managing in all decision making

Use the risk process diagram below to visualise how you'll embed risk management in your own decision-making processes.

- Unpack what decision makers in organisation should do with the results of that risk assessment:
  - > Assign risk owners
  - > Design controls and assign control owners
  - > Record the assessment in the organisation's risk register
  - > Monitor controls effectiveness.

- Unpack the escalation procedure if a risk becomes more likely or the potential consequences more severe
- Link to tools that decision makers can use to identify, analyse and evaluate risk
- Remind readers that risk's dynamic, which means that they need to be ready to adjust controls in response to changes in risk indicators and performance indicators.

Other points

- Use plain language
- Describe the culture of decision making you want to see in the organisation, so that risk assessment is simply—and informally—part of decision making
- Describe when an informal approach to decision making needs to be more formal so that reporting and escalation happen through the governance model you defined earlier.

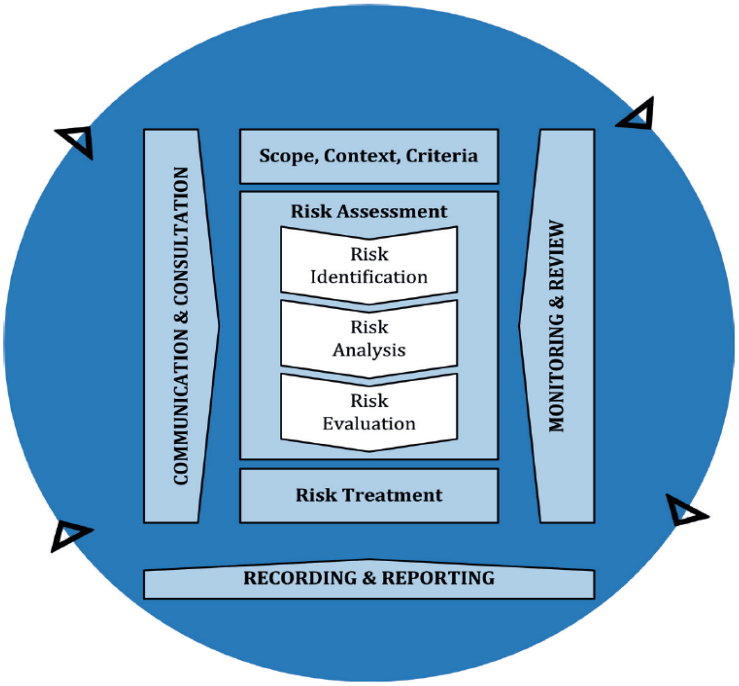

Figure 1: The risk management process *(AS 31000:2018 – Risk Management Guidelines)*

8. Communication

Describe how you'll communicate to:

- share vital information for decision making with colleagues and external stakeholders
- facilitate shared deliberation about risk
- manage change across the organisation.

You may like to:

- consider the roles listed above and decide what they need to know and do
- describe special communication functions and channels in the organisation
- provide a template for a communications plan.

9. Escalation

Formalise your position on when to escalate a risk to a decision maker for action.

Feel free to adapt the table below so that it's specific to your organisation:

ESCALATION CONDITIONS AND RESPONSE (sample)	
Extreme	• Requires immediate notification to the CEO (or delegate) • Commence treatment planning without delay • Escalate to chair of the responsible body (or delegate) • Ensure treatment plan is in place within 48 hours
High	• Requires immediate notification to the appropriate executive or senior manager • Ensure treatment plan is in place within 5 days
Medium	• Requires notification to line manager within 3 days • Ensure treatment plan in place by 10 business days
Low	• Discuss with line manager and agree treatment actions

10. Monitoring risk indicators and performance

Stay alert to potential changes in your internal and external context by defining:

- What key risk indicators you need to monitor to make sure you stay within the organisation's risk appetite
- What performance indicators you'll monitor so that you have the information you need for continuous improvement of your risk management practices
- How you'll monitor these indicators and signs of change
- How you'll report to the appropriate decision-making group.

11. Training

Describe what you'll do to ensure all decision makers across the organisation:

- understand their roles and risk management concepts
- have the skills to make decisions and manage risks.

VMIA is the Victorian Government's insurer and risk adviser

Level 10 South
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900
E contact@vmia.vic.gov.au
ABN 39 682 497 841

vmia.vic.gov.au

12. Information management

How will you manage, share and use information:

- in the risk register?
- about insurable risk, incidents and claims?
- to other external stakeholders to address shared risk?

13. Continuous improvement

How will you:

- assess and improve your maturity (e.g. using a diagnostic tool like VMIA's Risk Maturity Benchmark)?
- demonstrate that risk management practices are improving the quality of decisions and the performance of the organisation?

14. Reviewing this procedure

How will you make sure:

- risk management is contributing to your organisation's performance?
- risk is being managed according to the procedure?

Document number	Enter reference
Approver	Chief Executive Officer
Reviewer	
Owner	
Date of approval	Enter date
Date of effect	Enter date

VMIA is the Victorian Government's insurer and risk adviser

Level 10 South
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900
E contact@vmia.vic.gov.au
ABN 39 682 497 841

vmia.vic.gov.au