Rose Lee

[Email address]

Risk management procedure

Template for a risk management procedure

## 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, which are 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.

## What we have covered in our procedure

Our procedure details

* Roles and responsibilities
* A model of governance that facilitates 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 the effectiveness of controls and other actions to manage risk
* How we’ll escalate action when risk cross tolerance thresholds
* How we’ll continuously improve.

## 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.

## 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*

## Roles and responsibilities

### What we all should do

* *What are the responsibilities of everyone in the organisation 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?*

### Specific roles

Describe the responsibilities for each of these roles

* *Responsible body*
* *Risk and Audit Committee*
* *Risk management sub-committee*
* *Internal audit team*
* *External audit consultants*
* *Chief executive officer*
* *Members of the executive team and senior management*
* *Risk manager*
* *Non-managerial members of staff*

## Governance

*What model of governance will you put in place to ensure that significant decisions are approved in the appropriate forums and that decisions are captured and made available to decision makers?*

* *What types of decisions need to be considered in by a specialist group before being implemented in the organisation? For example, clinical risks, environmental risks, state-significant risks, shared risks?*
* *What decisions do they have the authority to make and are accountable for?*
* *Who are these specialist decision-making groups themselves 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.*

## Embedding risk managing in all decision making

* *Use the diagram below to show the overall structure of risk management*
* *Unpack the three-step process of risk assessment: identify, analyse and evaluate*
* *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 the effectiveness of controls*
* *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 is dynamic, which means that they need to be ready to assess and re-assess risk and adjust controls in response to changes in risk indicators and performance indicators.*

*Other points*

* *Advocate a plain language approach to risk*
* *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 shift to a formal approach, carried out through the governance model defined in the previous section*



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

## Communication

*Describe how you will communicate to:*

* *share vital information for decision making with colleagues and external stakeholders*
* *facilitate collaboration and shared deliberation about risk*
* *manage change across the organization*

*You may like to:*

* *return to the roles listed above and draw attention to their responsibilities when it comes to communication*
* *describe special communication functions and channels in the organisation*
* *provide a template for a communications plan.*

## Training

*Describe what you will do to make sure decision makers across the organisation at all levels*

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

## Information management

* *How will you manage, share and use information in the risk register?*
* *How will you manage, share and use information about insurable risk?*
* *How will you manage, share and use information about claims?*
* *How will you provide information to VMIA and other external stakeholders?*

## Monitoring risk indicators and performance

* *What key risk indicators do you need to monitor to make sure you stay within the organisation’s risk appetite?*
* *What performance indicators will you monitor so that you have the information you need for continuous improvement of your risk management practices?*
* *How will you stay alert to potential changes in your internal and external context?*
* *How will you monitor these indicators and signs of change?*
* *How will you report to the appropriate decision-making group?*

## Escalation

* *Formalise your position on when a risk should be escalated to a decision maker for action.*
* *Feel free to adapt the table below so that it is specific to your organization.*

|  |
| --- |
| ESCALATION CONDITIONS AND RESPONSE |
| 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
 |

## Continuous improvement

* *How will you use the Risk Maturity Benchmark (RMB) to improve your frameworks, processes and culture?*
* *How will you demonstrate that risk management practices are improving the quality of decisions and the performance of the organisation?*

## Reviewing the effectiveness of the 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 |