Developing a foundation-level framework for your organisation

One of the requirements of the Victorian Government Risk Management Framework (VGRMF) is that your organisation has a framework that is adequate for managing risks in its internal and external context.

For many organisations this will be what we call a foundation-level framework for managing risk. It consists of

- a risk management policy
- a risk management strategy
- a statement of risk appetite
- risk management procedure
- risk register.

In this topic we will concentrate on what you need to do to put in place these foundations.

For this foundation to be effective these references and tools should be *embedded* into the organisation's functions and activities.

Find out more about how to build a framework that is right for your organisation in our topic on *building* frameworks. Everything there applies to a foundation-level framework too and is worth reading, even if you intend just to deliver these basic elements.

In that topic we also answer questions such as

- What's a risk management framework?
- Who's responsible for building it?
- When does the work happen?
- What makes a framework adequate?
- Embedding risk management into the organisation's functions and activities

Risk management policy

In general, a policy states the organisation's intent and guides decisions. It defines the desired outcomes in definite and measurable terms. Importantly, a policy is something that can be implemented, whether that is through a strategy, or some sort of procedure or activity.

A risk management policy should state

- the spirit in which the organisation will approach uncertainty in its internal and external context

VMIA is the Victorian Government's insurer and risk adviser

Level 10 South,
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900
F (03) 9270 6949
contact@vmia.vic.gov.au

vmia.vic.gov.au

VICTORIA State Government

Victorian Managed Insurance Authority (VMIA) acknowledges the Traditional Custodians of the land on which we do business and we pay our respects to Elders past, present and emerging. We acknowledge the important contribution that Aboriginal and Torres Strait Islander peoples make in creating a thriving Victoria.

- the attitudes of its responsible body and executive team to the 'up-side' as well as the 'down-side' of uncertainty
- the commitments of its leadership to creating a culture that is alert to risk
- the responsibilities of all decision makers to manage risk and what exercising that responsibility looks like
- your commitment to managing shared and state-significant risk
- what success in managing risk looks like in a material sense—the difference it makes to the organisation's performance
- its approach to continuously improving how it responds to uncertainty
- how it intends to respond to critical risks, such as climate change for example, or other critical risks in its internal or external context
- how it will be transparent and accountable, disclosing its efforts to manage risk where that is appropriate or required by the VGRMF or by law.

Your organisation's risk policy should be specific to your organisation rather than a generic statement about risk. It should be time-bound and informed by your organisation's internal and external context. It should also connect transparently to the other reference documents in the foundation-level framework.

Tools

- A guide to writing your risk management policy [DOCX, 932KB]
- A template for a risk management policy [DOCX, 125KB]

Risk management strategy

A strategy defines how to get from where you are now to where you want to be at a definite point in the future. The connection between a strategy and a policy is that that strategy carries out the spirit and letter of the policy, showing how resources will be used to deliver the desired outcomes.

Note that not all paths from where you are now to where you want to be are equal. Your culture and other aspects of your framework set the parameters on whether a path is the right one or not.

A risk management strategy should set out

- the outcomes you want to achieve when it comes to management risk
- the frameworks and processes you'll put in place to achieve those outcomes
- the culture you want to create
- resources allocated to the work of change
- how you'll monitor the progress of the strategy
- how you'll measure success.

Tools

- A guide to writing your risk management strategy [DOCX, 949KB]

- A template for a risk management strategy [DOCX, 117KB]

A statement of risk appetite

A statement of risk appetite plays pervasive and crucial role in relation to reputation, developing strategy, but also day-to-day decision making across the organisation.

One of the mandatory requirements of the VGRMF is that your organisation defines its risk appetite. Your responsible body should do this with the support of the executive team and risk practitioners.

Find out more in our topic - Defining your organisation's risk appetite.

A risk management procedure

Your procedure describes how you will *embed* your risk framework and processes in the organisation so that they shape the way you make decisions in your organisational culture.

To effectively embed risk management frameworks and processes your procedure should cover the following:

- employees performing their roles and carrying out their responsibilities
- a model of governance that facilitates decision making within the organisation and with other organisations, and makes sure decision makers accountable
- risk assessment and its links to reporting
- communication and training
- systematic collection of information about what's going on in your internal and external context and what is likely to happen
- measuring, monitoring and reporting on the effectiveness of controls and other actions to manage risk
- escalating action when risk cross tolerance thresholds
- continuous improvement
- attestation.

Tools

- Template for a risk management procedure [DOCX, 340KB]
- Risk management roles and responsibilities [DOCX, 944KB]
- Role description for enterprise risk managers [DOCX, 938KB]
- Risk culture guide [PDF, 1.34MB]

A risk register

A risk register records the results of the risk assessments that decision makers across the organisation do for organisational, business and project objectives.

It also plays an important part in clarifying who's responsible for managing each risk, which is one of the requirements of the VGRMF.

-

As well as detailing the risk owner, your risk register should include:

  - a description of each risk
  - its evaluation
  - a description of how it'll be controlled and the degree to which that control is effective
  - the owner of the control
  - a summary of the treatment plan.

Risk is dynamic, which means that your register must be updated at least quarterly but also when there is a significant change in your organisation's internal and external context. All risks must show the dates they were registered and when they'll be reviewed.

Getting value from your risk register

A risk register captures a complete picture of the organisation's assessment of the risks emerging from its internal and external context—at a point in time—and what is being done to manage them.

It's an important reference for the executive team and the responsible body of your organisation as they steer the organisation towards its objectives. More important, it is a dataset from which you can draw insights for managing risk.

For example, reports on your risk register can home in on

  - highest rated risks
  - risks that have a financial impact, helping you make decisions about insurable risk
  - risks to objectives of interest to the responsible body, executive team or senior manager
  - the mitigation work that's been done so far to manage a particular risk or subset of risks
  - risk owners
  - dates of review of risks
  - target completion dates for treatment actions.

Governance

Getting that value depends on the quality of information in the register, of course. Understanding what a risk is —and is not—is also key.

Managing the information in a risk register so that it is relevant and correct can be difficult—we acknowledge that. Remember though, that the ultimate test of a risk register is how it informs management decisions such as,

- Where are we investing most in controlling risks to critical objectives?
- Does that investment match our risk appetite and evaluation of risks?
- Are we managing our exposure to insurable risk?
- Have we understood the risks associated with a critical objective or strategy?

So, start with the question: what information must we have so that we can effectively control the effects of uncertainty on our objectives? Design your governance model to deliver that information and your register to capture it.

Bear in mind too, that it is one of the documents that an auditor will always ask to see.

Tools

- Foundations risk register [XLSX, 189KB]

Continuous improvement

A foundation-level framework will be a solid basis on which to build a more detailed framework for managing the risks that your organisation faces.

This continuous improvement is exactly what the Risk Maturity Benchmark (RMB) is designed to help you with. Decide what your target is, create a plan and go from there.