Building your risk management framework

The Victorian Government Risk Management Framework (VGRMF) sets out the requirements for your organisation when it comes to managing risk. One of its requirements is that your organisation has a framework that's adequate for managing risks in its internal and external context.

The VGRMF also requires your responsible body to attest to the adequacy of your organisation's framework at the end of the financial year.

What's a risk management framework?

A risk management framework is a set of references and tools that decision-makers rely on to make decisions about how to manage risk. It could include, for example, policies, strategies, plans, processes and models, and statements of your organisation's position on risk.

What you have in your framework depends on two things:

- the risks, threats and challenges in your internal and external context
- your organisation's risk maturity.

Who's responsible for building it?

The executive team and board of your organisation need to decide what mix of references and tools are fit for this purpose.

They'll decide based on their agreed position on

- the governance they want to see in the organisation
- the culture of decision-making
- how dynamic or volatile they assess the risks to be in their internal and external context.

The person or team tasked with the organisation's risk services works with the executive team to

- analyse the internal and external environment which the organisation is operating in
- produce a framework of references and tools to guide decision-makers throughout the organisation—including themselves
- communicate to decision-makers about the framework and how it helps them to do their work.

The responsible body endorses that the framework is of the right quality and it's adequate for the organisation's activities and functions. At the end of the financial year, they'll need to publicly attest that their framework is adequate, or that they've put in place measures to improve it.

The framework's purpose is to give decision-makers the knowledge and the tools to manage their organisation's exposure to risk.

When does the work happen?

This information is accurate as at 07/01/2022

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.

This work on your framework needs to be done

- as soon as the organisation has defined its strategic objectives
- whenever the organisation takes on or puts aside any functions or activities
- annually as part of developing strategy and plans
- whenever changes in legislation and regulations affect strategy or operations
- as an outcome of audit and accreditation process
- with a change in leadership.

What makes a framework adequate?

Whatever it includes, your framework must be fit for purpose. It should

- equip decision makers to make good decisions in situations of uncertainty
- make it easy for them to be accountable for their decisions
- not encumber them with work that doesn't increase the quality of the decisions.

Managing risk and making decisions about objectives, strategies and projects are one and the same activity. The references and tools that make up your risk management framework should be embedded into the organisation's governance framework. See Embedding risk management below for more on that.

An auditor may also look for evidence that your framework is

- aligned with the eight principles in the Risk Management Standard 31000
- aligned with the VGRMF
- used by decision-makers across the organisation from the board to the frontline.

Examining your internal and external context

We recommend that you use an analytical tool like PESTLE [DOCX, 4.59MB] to understand the current events, plausible future scenarios, and risks to your organisation's objectives that are in your external context.

For your internal context, we recommend PPRACKIF tool [DOCX, 4.6MB].

We also encourage you to use the process of identifying, analysing and evaluating risks to understand how changes in these contexts could affect the people, places and systems in your care. Look at the topics on Making decisions in situations of uncertainty, and What is risk? for more information.

Don't restrict yourselves to these though. You may, for instance, need to carry out desktop or observational research to inform your analysis. The point is to thoroughly assess what's going on in and outside the organisation in enough detail to make decisions about the framework you need.

Building your framework

Having examined your internal and external context, you are now able to build your framework.

Begin by establishing your foundation-level risk management framework. Once you've developed your foundation-level framework, ask yourself two questions.

1. Do we need to develop any policies, strategies, plans or processes to deal with any specific risks that matter to our organisation?

For example, the risks associated with climate change, cyber threat or demographic changes across Victoria. Events and changes like these in your external context will almost certainly have implications for your organisation, which may call for specific risk management detailed in stand-alone documents.

You could also uncover a high number of insurance claims for certain types of incidents, which will require specific action. Again, addressing this might call for its own specific risk management, captured in dedicated strategy and procedures.

2. Do we need to develop any policies, strategies, plans or processes to lift our maturity when it comes to managing risk?

For example, do you want to take steps to cultivate a more positive risk culture? Do you want to get better at collaborating with other organisations on shared risk? Do you want to be more innovative in some area of your functions and activities?

The answer to each of those questions might be its own strategy, which would contribute to your overall risk management framework.

Important note

You're unlikely to need dedicated documents and tools for every risk. Take cyber threat, for example. Depending on your assessment of the risk and your risk appetite you could either

- Prepare stand-alone documents devoted specifically to the risks; for example, a policy or a strategy on cyber threat, or
- Add an explicit and well-considered section describing your policy on cyber threat to your organisation's IT policy, for example, and in other key IT strategies and plans.

Making sure you have the right tool for the task...policies, strategies, plans

We have more information here on how you can decide whether you need a policy or a strategy, a plan or a process.

Keep hold of your supply chains

Most public sector organisations rely on a commercial or not-for-profit organisation to help them deliver some of their services. Though they blur the boundary between external and internal context, they still need to be assessed as a source of risk to your organisation and have controls put in place. They do, after all, operate on different incentives to a public organisation—particularly commercial organisations.

Check the Buyer's guide to procurement on the website of the Victorian Government Purchasing Board, for an excellent overview from planning procurement to closing and reviewing a contract.

Embedding risk management into the organisation's functions and activities

As noted earlier: managing risk and making decisions about objectives, strategies and projects are one and the same activity.

That means that the references and tools that make up your risk management framework shouldn't be a siloed or parallel system, but instead be part of strategic and operational planning and reporting.

Your corporate strategy and business plans could refer explicitly to risk and show evidence that a thorough risk assessment has informed their content and that the actions described in the strategy and plans will manage those risks.

Other techniques for embedding risk management are making sure

- all decision-making forums deliberate about risk
- all risk management tools earn their keep by helping decision-makers think and share the results of their deliberation in the organisation or with other stakeholders
- decision-makers have the time to identify, analyse and evaluate risks and do more research and analysis if necessary
- decisions made in any forum are communicated to stakeholders who have a stake in the decision or will need to take action, whether that's in or outside the organisation
- new processes and governance aren't put in place without checking whether there's something that can do the work already
- the leadership model risk thinking.

Policies, strategies, statements, and governance

Those of you looking to embed and optimise your risk management framework may be interested in building it out with policies or strategies that deal with specific risks, or which lift your organisation's maturity.

The language of management and governance can be vague, so it can be unclear sometimes if you need a policy or strategy, for example. Being precise about the differences will help ensure your framework is fit for purpose.

The following section set out definitions and examples of different types of references and tools that you might put in place.

Policy

A policy states the organisation's intent and guides decisions. It defines outcomes in definite and measurable terms. It can also have the imperative of an internal law for the organisation, including sanctions.

Importantly, a policy is something that can be implemented, whether that's through a strategy, or some sort of procedure or activity.

Example of a policy

Example of a policy	Why you might choose to make it
A policy on managing shared risk	If your organisation wants to make sure decision-makers are clear about the mandate on shared risk and the need to take the initiative.
A policy on innovation	If your organisation wants to take a positive stance to uncertainty, turning it into an opportunity for new services, technologies, modes of delivery that create value for people.
A policy on how the organisation will manage the risks produced for it by the events of climate change	If you want to make sure all the functions and activities deliver on the organisation's obligations in relation to the State Government's Climate Change Act.

Strategy

A strategy defines how to get from where you currently are to where you want to be. For example, you might put together a strategy to carry out a policy.

Note that not all paths from where you are now to a future state are equal. Your policy, culture, risk appetite and other aspects of your framework set the parameters on whether a path is good or not.

Example of a strategy

Example of a strategy	Why you might choose to make it
A strategy to continuously improve how the organisation manages risk	If you want to improve aspects of your framework, processes and culture, especially in the light of your Risk Maturity Benchmark (RMB) results.
A strategy to manage physical and transition risks for the agriculture sector	If your assessment of your internal and external context shows that your organisation must take an active role in protecting and creating value for the sector.

Plan

A plan defines actions, when they are going to be done, and who'll do them.

Example of a plan

Example of a plan	Why you might choose to make it
An improvement plan	To identify and assign resources and implement a continuous improvement strategy.
A plan to manage physical and transition risks in the agriculture sector	To identify and assign resources and implement a strategy to manage physical and transition risks of climate change in the agriculture sector.
A training plan	To ensure that your staff have knowledge and skills that'll make a material difference to one of your risks; for example, risk of cyber attack, or misdiagnosis of a patient's symptoms.

Processes and models

Processes, models and so on help make the decision-making activities that are going on at desks and in meeting rooms to be consistent, thorough and accountable.

Processes map sequences of actions, where one action depends on the success of the one before.

Models show the relationships between the entities in a system. For example, an organisation chart is a model of the positions in an organisation and how they're related to each other.

Example of processes and models

Example of a processes and models	You might choose to do it to make sure:
A process for assessing risks	decision-makers are assessing risks thoroughly for them to manage it effectively.
A process for escalating risk	risks are acted on with the appropriate urgency and resources.
A model of governance	vital information's shared and acted on in the appropriate forums, and those with responsibilities for managing risk are accountable.
A model for collaboration	your people understand how to efficiently and effectively manage shared risk.

Position statements

A statement of the organisation's position doesn't describe actions or purpose but gives an unambiguous signal of its appetite and tolerance in relation to a specific matter.

Example of a statement

Example of a statement	You might choose to make it if you want to control the risk of:
A statement on the desired culture of decision-making in the organisation	unwanted decision-making behaviour and poor relationships with other organisations and the public.
A statement on how it'll manage public information to protect and create value	confidential information being misused and make the most of opportunities to create value by sharing public data.

Continuous improvement

Building a framework specific to your needs is a sign that your risk maturity's growing. Stay alert to what's going on in your internal and external context and look for opportunities to refine it in response to change.

The RMB will help you steer a course through that change by helping you stay focussed on your goals and the requirements of the VGRMF.


Decide your target risk management maturity
Create plan to reach target maturity
Implement enhancements
Assess your current risk management maturity
Create and protect value