Identifying, analysing & evaluating risks

The Victorian Government Risk Management Framework (VGRMF) requires all decision-makers to assess risks to their strategies, business plans and projects.

The quality of your risk assessment will make a critical difference to how you manage risk, and the success of your strategy or project.

In a positive risk culture, decision-makers are always ready to *reassess* the situation and their decisions. You can find out more about risk here.

When do you need to do it?

You need to assess the risks to your objectives when:

- you're working out your objectives
- you're developing strategies and setting up projects that will achieve those objectives
- the environment you operate in changes
- your organisation changes.

These are situations of uncertainty. In the first two examples, you'd be uncertain about the best course of action. In the last two, you'd be uncertain about how change will affect your plans.

Uncertainty is a source of opportunity

As risk managers, we tend to focus on what could go wrong when we're pursuing our objectives: the obstacles, the issues, and the failures.

But uncertainty isn't all bad. When looking at a situation of uncertainty, after all, you're looking at an opportunity to *create* certainty through your actions. That creative potential has led to world-changing research and inventive solutions in the public sector, as well as the private.

You also need to take, and create, a risk to achieve anything. In other words, nothing is accomplished without taking a risk. The whole point of risk management is you do that with insight and knowledge about your environment, your capability and your appetite for change.

The Australian and International Standard for risk management AS ISO 31000:2018 treats risk in this way.

Think positively about uncertainty and see it as a way to create and protect value rather than something to avoid.

Three steps to assessing risks

The following text unpacks the steps to take for a thorough and transparent assessment of risk.

1. Identify your risk

What's the *event* that, if it happened, could affect your objectives?

This information is accurate as at 15/12/2023

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

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.

Once you've identified the event at the heart of your risk, you'll be in a good position to analyse its causes and consequences. You can also understand what type of risk it would pose to your objectives.

We also recommend that you examine your internal and external context and map out the sources of uncertainty associated with this event. For example,

- What cyber threats are there in our environment?
- What demographic changes are likely in the next 20 years in regional Victoria?
- How will transition to a net-zero emissions society affect the way we deliver services and operate as a public sector?
- Do we have the skills and organisational capability to anticipate and respond to the opportunities, risks and uncertainty we see ahead over the next five years?

By identifying sources of uncertainty, you'll develop a more nuanced understanding of the events and what they mean for your objectives.

Here are some tips for identifying the event.

Set time limits

A risk is a risk of something happening in the future. That something is an event which happens at a time and a place.

When you're trying to identify the event at the heart of your risk, we recommend that you think about a particular period of time—whatever is relevant to the scenario you're interested in. For example, the

- current financial year
- period of a three-year strategy
- six months leading up to the launch of a program
- duration of the pandemic
- end of the useful life of a piece of infrastructure
- first term of the school year.

It's helpful to think about the *lifespan of key decisions*. The effects of the decisions made today might not be felt by those making them. Knowing this will help you choose the right period.

Setting time limits like this will not only help you home in on the events that are a risk to your objectives, it'll also help you in the next step when you analyse its likelihood.

Use the bow tie

The bow-tie technique puts the event at the centre, making it easier to focus on the occurrence or change that's a risk to you. It'll also help you separate out the causes of that event and its consequences—something you'll need to do in the next step when you're analysing your risk.

Check your objectives

As the bow tie shows, events have causes and consequences. These causes and consequences are themselves events—they happen at a particular time and place. This means there's nothing essentially different between them. They're all events causally connected to each other.

So how can you identify the event you should focus on in your risk assessment?

The answer is to focus on your objectives. What are the events that pose a risk to your objectives? Those are the ones that you need to home in on when you are assessing and describing risks.

Think about potential scenarios

Scenario planning is a useful way to analyse the events that *may* happen—especially those that emerge from complex or complicated systems—rather than focussing on the one that *will* happen. By identifying a range of plausible scenarios, you can make better decisions about how your organisation can act now to be more resilient. You can watch this video about scenario planning.

You might also like to follow a practice used in insurable risk, which is to look at both the most likely scenario and the worst-case scenario.

Think about non-events

We've put the focus on events, but it's also true that something *not* happening can have consequences. For example, not acting to put out a fire at its earliest stages will mean assets are destroyed.

Scan your context

Your internal and external context are sources of uncertainty for you in pursuing your objectives. These tools will help you to comprehensively scan your organisation and its environment to identify sources of risk.

- The PESTLE [DOCX, 4.59MB] analysis tool for your external context
- The PPRACKIF [DOCX, 4.6MB] analysis tool for your internal context

2. Analyse your risk

Now that you've identified the event that's a risk to your objectives, you need to analyse its causes, consequences and likelihood.

- What are the causes of the event or the factors in its occurrence?
- What exactly would happen if this event occurred?
- How likely is this event to happen?

Understanding the causes and factors of an event and how likely it is will help you decide how to control the risk. Understanding how severe the damage could be if it happened will help you decide what you need to do to build resilience, if the event occurred.

At this point, you need to assess how much to invest in analysing your risk. How much depends on what you need to know in order to work out how to control it.

Here are some tips for analysing the causes, consequences and likelihood at the heart of your risk.

Back to the bow tie

The bow tie is useful here too because it helps you to keep the event at the centre and the causes and consequences in their place. It's a good method for a thorough analysis as it allows people with different perspectives to visualise and contribute to the picture of risk you're creating.

Dig deep into causes

Human behaviour is a major source of causes and other factors in events. BehaviourWorks at Monash University has a method which will help you analyse behaviour so that you can identify behaviours that lead to certain outcomes, and so design controls and communications more effectively.

Their video on systems mapping will also help you to identify dependencies in a network of stakeholders and organisations in your context.

This page on using root-cause analysis may also be useful.

The work of identifying risk indicators may also help you single out causes because risk indicators are a sign that these causal events are becoming more likely.

Work on your scenarios

As well as the previous video, we recommend this technical supplement from the Taskforce on Climate-Related Financial Disclosures. It's a thorough description of the technique even though it's focussed on climate change, and it'll help you to do a deep analysis of your risks.

Don't forget likelihood

With risk, we're talking about events that *could* happen. It's one of the reasons why an analysis of likelihood is so important in describing a risk.

The likelihood of an event is the chance that something will happen in a given period of time, in a given place.

To illustrate this, think about the question "what's the likelihood of a bushfire?". In that form, the question really has no answer. The question would need to be something like "what is the likelihood of a bushfire causing catastrophic destruction in the East Gippsland Fire District in the period 2021-2030?"

With an event like bushfire, an objective analysis of the probability of an event is an essential part of your efforts to control it. You'll also find that your insurable risks are risks where likelihood can be quantified—it's part of what makes them insurable.

For some risks, it's not possible to calculate the probability. And for the kinds that most organisations face, an ordinal or relative evaluation will be enough. It'll serve the purpose of prioritising risks for action and tracking whether a risk's becoming more or less likely.

This webpage presents likelihood tables while also making an important point about how controls can (and should) affect the likelihood of an event. Always bear in mind your current controls when analysing your likelihood.

Look at your context

PESTLE[DOCX, 4.59MB] analysis will help you to analyse risk as well as identify it. PPRACKIF [DOCX, 4.6MB] will also help you to analyse your internal context.

3. Evaluate your risk

Look at your analysis and ask whether the risk is within your risk appetite and tolerance.

- Do you have the appetite to take or create this risk to achieve your objectives?
- How much risk could you tolerate if things change while pursuing those objectives?

Also look at how you currently control this risk.

- How effectively do you control the risk right now?
- What difference do they make to the likelihood of the event happening or the severity of the consequences?
- Would you be able to monitor signs of the risk changing?

Evaluation is the point in your assessment where you decide whether to take or create this risk.

- Is the benefit of achieving your objective worth the cost of controlling the risks?
- If you go ahead with this, then what *won't* you be able to do?
- Do you need to do further analysis to understand this risk?
- Do you need to reconsider your objectives?

Decisions that are defensible, transparent and accountable

Decisions need to be made known to others—they need to be *transparent*. Decision-makers should also be *accountable* for any commitments they make because of their risk assessment and *defend* their assessment of risks when weighing up options for action.

These are the ethical dimensions of decision-making in an organisation and they're vital for a positive risk culture.

This Ethics Centre decision-making guide for directors gives a good overview of the issue and is useful for anyone, whatever their role is in the organisation.

Formal or informal?

What do we mean by a formal or an informal approach?

A formal approach to risk assessment will deploy your frameworks and processes and document the outcomes of deliberation. It'll involve scheduling meetings specifically for the task, recording deliberations on timeframes and monitoring, requesting resources for analysis and consultation, and reporting the details of the assessment to other decision-makers in the organisation.

An informal approach will rely more on the implicit experience and know-how of relevant decision-makers and be resolved in discussions, whether face-to-face or over emails. This is where a positive risk culture matters.

All risk assessments start informally. Deciding to adopt a formal approach will depend on the risk and its impact on the people, places and systems in your care.

Risk assessment is about slowing down your decision-making. Make it a deliberate and conscious decision to remain informal in your approach. We also suggest that you have a variety of decision-makers involved in the assessment to pool knowledge, test assumptions and build the relationships needed to manage the risk further down the track.

Whether you adopt a formal or an informal approach, it's important to remember you'll be accountable for your decisions. Consider how the *results* of that informal assessment will be recorded, if not the whole assessment process, whether that's in emails, minutes or other meeting notes.

Capture the results of your assessment

Once you've assessed and described your risks, you need to capture that in a form that's usable and useful to others—that's what a risk register is for.

Here are two templates you can use, depending on whether you're at the Foundations level or Embedding and Optimising.

- Foundations risk register [XLSX, 189KB]
- Embedding and optimising risk register [XLSX, 185KB]

Next steps

Having assessed your risks, we recommend you check whether you need to:

- Update the risk register
- Escalate to the appropriate business unit, management level, committee or the Board
- Prepare documentation for action on shared or state-significant risk
- Communicate with those affected by the risk or the changes you've made in your strategy, plan or controls
- Put in place new treatments or adjust existing controls