

# How well are you managing risk?



Your responsible body must be satisfied that the organisation has adequate frameworks, processes and culture for managing risk.

Adequate frameworks, processes and culture make it easier for people in your organisation to make decisions about setting objectives, assessing risks and controlling them effectively.

It's also how you meet the mandatory requirements of the Victorian Government Risk Management Framework (VGRMF).

If they're adequate, you should see evidence of that in a number of ways.

- the quality of the frameworks and processes themselves
- how they're used to make decisions
- how productively and efficiently the work of risk management is done
- the quality of what's produced
- how effectively risks are controlled.

## Continuous improvement and accountability

Frameworks, processes and culture need to be adequate, but the responsible body will also need to see signs of *improvement*.

Decision-makers also need to be *accountable* for the work they do.

Your model of governance is how you make sure people exercise the powers and responsibilities delegated to them in a way that's effective, efficient and ethical.

Your risk management strategy and plans put your commitments to the responsible body in writing. The strategy defines the future state of the organisation. The plans specify how the organisation will get there.

The Risk Maturity Benchmark (RMB) helps you to see where you are compared to other organisations in the Victorian Public Sector, set risk management targets and develop action plans.

Finally, your assurance processes present evidence of how your frameworks, processes and culture are performing to the responsible body. The evidence is in the form of documents and performance indicators and assesses their quality as well as how much is produced.

## How would you know how well you're managing risk?

Your best insight into how well you're managing risk is qualitative. This qualitative assessment comes from examining what's captured in the documents produced as part of managing risk.

Performance indicators and other quantitative measures are also valuable because they tell you that something is being produced, by when and at what cost.

This following guidance focusses on qualitative assessment of how well you're managing risk.

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](http://vmia.vic.gov.au)  
© Victorian Managed  
Insurance Authority



## What effective risk management doesn't mean

If you're managing risk well, it doesn't mean that nothing goes wrong.

When you're managing risk, you're making decisions in situations of uncertainty. Sometimes you have to make the decision, even when the risk is still high. Something might go wrong. Your situation might change in a way that you couldn't reasonably predict.

It doesn't follow that the risk management frameworks and processes have failed.

This is where the culture of the organisation matters. The organisation, as a whole, needs to *take* a risk to reach your objectives. Sometimes you need to *create* a risk—it will need to *increase* the uncertainty on the path to your objective to reach it.

Allow people—the individuals managing risks for the organisation—to do that. Give them space to seek out information, test propositions, make mistakes and *learn*.

## The quality of the frameworks and processes themselves

When you're looking at the policies, strategies, processes and other documents that make up your framework, ask yourself

- Do these documents refer specifically to your organisation's remit, objectives, risks, stakeholders and relationships, and contexts?
- In the past year, did you change any of these policies, statements or processes in light of new information or because of a change in context?
- Will you need to make the above changes in the coming year?
- Is the language precise, definite and goal-oriented?
- Is it clear who does the work of managing risk?
- Is it plausible that, if someone followed the processes you've defined, it would lead to a good decision about managing risk?
- Are these processes clear and easy to follow?
- Is it clear what outputs and outcomes we're asking of people in the organisation?

These questions all speak to the quality of the policies, strategies, processes and other documents that guide decision-makers in your organisation.

An effective framework starts with a thorough analysis of your internal and external context. It's specific to your organisation, not generic.

A foundation-level framework will include what we think are the essential elements for decision-makers.

Your processes need to make it easier for people to make decisions. They need to make sure people don't forget to do critical actions or waste time on unproductive ones.

Your framework must also be responsive to change—you update it if there's a change in the responsible body's appetite for risk or the organisation's risk tolerances. You add more if you're faced with risks that need concerted attention and effort, like cyber threats or climate change. You finetune processes so they produce the outputs and outcomes you need.

## How they're used to make decisions

Risk thinking and techniques help you define worthwhile objectives as well as deliver them.

Do you see evidence that they're being used to do that—formally or informally—in business planning and strategy development? Are there minutes, analyses or other documents which show the decision-makers, over the performance period,

- referred to the organisation's risk appetite?

- reviewed the organisation's tolerances?
- considered analysis of its internal and external context?
- looked at a range of potential scenarios?
- weighed up the costs and benefits of various options?
- considered opportunities to share risk?
- discussed state-significant risks?

## The role of culture

In a positive risk culture, people understand their responsibilities and work cooperatively with others to manage risk. They respond creatively to risk and with a strong sense of accountability. Managers listen to what people delivering services and carrying out the work of the organisation have to say.

- What do culture surveys tell you about attitudes to risk and the work of managing it?
- Are the people who've been delegated with powers to manage risk using it as they should?

## How productive and efficient is the work of risk management?

Your risk management policy and strategy specify what will be done over a business cycle. This is where performance indicators come into their own. They indicate that outputs are being delivered, or not, by agreed times.

Some examples of indicators you could use are the

- proportion of tasks to control high risks completed this month
- proportion of the actions in the annual risk management plan completed
- number of people trained in risk management this quarter against target
- number of contracts that've been assessed for risks this month against target
- number of root cause analyses conducted in a project this quarter to learn lessons from successes and failures
- number of assessments of controls conducted this month against target.

Performance indicators are useful because they show that agreed products are being delivered and the costs of delivering them. They don't indicate the quality of the work being done though.

For example, did decision-makers analyse root causes with enough detail to be able to adjust their approach next time?

This is also where the quality of your frameworks, processes and culture play out as *efficiency*. Make sure they are useful guides to action, easy to access and use.

The next section looks at how you evaluate the quality as well as the quantity of what's produced in carrying out the actions in the risk management plan.

## The quality of what's produced

The work of managing risk produces reports on research and analysis, assessments, options papers, treatment plans, reports and risk registers.

When you look at these products

- Do the research and analysis directly inform risk assessment and management decisions?
- Is there an appropriate cost-benefit analysis?
- Are risks well described?

- Is the risk register up to date?
- Do treatment plans present plausible risk controls?
- Do the decisions of the responsible body and executive team directly inform operations?

We recommend you pay special attention to the quality of documents produced as part of identifying, analysing and evaluating risks. The process should generate rich information about the risks your organisation faces.

Do you see evidence of that?

- Are there any documents presenting analysis and options?
- Was the organisation's risk appetite and tolerance considered when evaluating the risk?
- Did decision-makers consider potential risk indicators?
- Are risks well described?
- Do you use the information in your risk register to monitor, report and analyse your risk profile?

### **How effectively are risks controlled?**

Risk indicators tell you how a risk is changing. Is the potential event becoming more or less likely? Are the consequences becoming more or less severe?

Performance indicators, on the other hand, tell you whether or not someone or something is doing what it ought to do.

They're quite different. Risk indicators give you important information about how risks are being controlled, so they need to be considered when you're evaluating your risk management performance.

We recommend you look for evidence that

- risk owners have identified risk indicators for important risks
- risk and control owners are monitoring those indicators for signs that the risk is changing
- decision-makers have considered the organisation's risk appetite and tolerances.

### **The link between risk maturity and performance**

The Risk Maturity Benchmark (RMB) was developed to help you put in place frameworks, processes and culture to manage risk effectively.

We encourage you to use it to

- assess the elements of your risk framework, processes and culture objectively
- determine the level of maturity that is right for your organisation
- identify improvement opportunities that will help you reach that level of maturity.

