

# Giving your responsible body assurance



Assurance is about giving your responsible body confidence that decision-makers are exercising delegated power effectively, efficiently and ethically.

This concept of delegation goes to the heart of the responsible body's role, which is to make sure the reputation and assets of the organisation are managed and protected and the organisation can function in the long term.

The responsible body of a public sector organisation needs to look more *widely* though and make sure the organisation contributes to the management of state-significant risk and collaborates effectively with other public sector organisations.

It must also look more *deeply* at the value that the organisation creates and protects for Victorians.

The responsible body is the steward of this value. They need to delegate specified powers to individuals in the organisation who'll pursue the organisation's objectives in a way that secures it.

## Not just an audit

Assuring your responsible body that decision-makers are using powers as they should isn't just about auditing documents for evidence of controls and compliance with accounting standards.

For example, an organisation could engage an 'ethical hacker' to test their cyber-security systems. Inspections and other quality assurance activities also give assurance that products and services are being produced and delivered as they should. Regular and genuinely informative reporting is also a form of assurance.

## A coordinated activity

Assurance relies on a deliberately governed process of examination and assessment by

- the organisation's management
- its internal audit, quality assurance and testing functions
- independent external audit, quality assurance and testing specialists.

These people examine and assess the governance of the organisation, its frameworks, and its control processes. Who provides the assurance depends on the degree of objectivity or independence needed.

Talk to the assurance specialists in your organisation about coordinating all these activities so that the responsible body gets a coherent, true and timely picture of what's going on in the organisation.

Who these people are will depend on the size and functions of your organisation. Large organisations will have individuals and teams who specialise in organisational performance, quality assurance, compliance, financial reporting, health and safety, or supporting the sub-committees of the responsible body.

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



In this topic, we'll focus on assuring your responsible body that *risks* to the organisation's objectives are being managed well. This work of assurance should be embedded in a larger program of assurance about all aspects of the organisation's operations.

## The Audit and Risk Committee

Most organisations will also have an Audit and Risk Committee which has been delegated by the responsible body to oversee the organisation's risk management policies and processes.

As the Victorian Auditor-General's Office pointed out, public-sector organisations need to make sure "their committee maintains the required mix of skills, and for agencies to regularly and comprehensively assess the performance of individual members and effectiveness of their audit committee as a whole"

## Who needs assurance?

Your responsible body is the immediate beneficiary of assurance processes.

This assurance helps your responsible body to attest that it's meeting the requirements of the Victorian Government Risk Management Framework (VGRMF) . In doing this, assurance is also given to the Victorian Government and the Victorian public.

People who use your services also benefit from this assurance, so do other organisations in the public, non-government and private sectors which are part of your supply chain.

VMIA itself, as the state's insurer, benefits from the assurance that insurable risks are being managed well so that it can continue to get a good price in the global market for the government's risks.

## How do you give assurance?

Assurance is given according to an annual audit plan or as part of the regular cycle of reports through the financial year. If you have an internal audit function, it should

- survey the organisation's risk controls and compliance frameworks and processes, and the nature of its risks
- decide priorities for audit
- finalise an audit plan in consultation with stakeholders—such as you and your colleagues responsible for enterprise risk management
- consider end-to-end functions rather than discrete tasks or controls
- monitor and report on the progress of the plan.

Assurance can also be given through a special project to examine and assess what's going on in the organisation. You'd do this if there was an indication that the organisation was at risk of not complying with laws, policies or codes of conduct, or if performance objectives were threatened.

## What does the assurance process need to find?

Evidence comes in the form of

- documents that set policies, standards and procedures for managing risk, which should form your framework
- documents that show controls are tested to ensure they're effective
- documents that capture the results of your work to manage risk
- performance indicators.

## Your risk management framework

Your framework includes documents which show the responsible body that your organisation understands the work to be done to manage risk and how the work will be delegated.

A foundation-level framework includes a

- policy that clearly states the organisation's intentions when it comes to risk and opportunity and guides people's decisions
- risk management strategy and plan
- statement of risk appetite
- risk management procedure that specifies the processes and models of governance for assessing risk, escalating risk, collaborating on its management and reporting
- risk register.

## The results of work being done

An audit team, whether an internal or external service provider, examines documents and other evidence to find out if the processes specified in the framework *fulfil* the organisation's policy and remit.

They also determine if these processes would be *effective*; that is, if decision-makers follow them, will risks be identified, analysed and evaluated? If an individual reads these documents, would they know how to take responsibility for risks? Would risks be adequately controlled?

The auditors will also look for evidence of whether the processes have actually been *followed*.

Perhaps the most important evidence that risks are being assessed is the risk register. An auditor will examine the register and assess the quality of the information in there.

They'll look for

- an accurate list of the risks that have been identified, including the objectives they're a risk to
- a thorough analysis of the risks
- the organisation's evaluation of the risks in light of its risk appetite and tolerance
- a description of how the risk will be controlled.

Auditors will pay close attention to those systems of control referred to in the register.

- Are the controls effective?
- Do they control the risk efficiently?
- Is there evidence that the benefits of controlling the risk were weighed up against the costs?
- Do the risks which have been evaluated as intolerable and made a priority for action have treatment plans in place?
- Are the treatment plans being carried out?
- Are controls tweaked and modified in the light of information about changes in the risk?

Auditors will also review corporate documents, such as enterprise business plans, strategic plans, yearly reports, minutes of meetings and outside reports, external audit reports.

## Indicators of performance

Reporting on the performance of your risk management is one of the ways to assure your responsible body that risk is being managed well.

## Continuous improvement

How you manage risk—and how your organisation performs overall—is closely tied to your risk maturity. VMIA's Risk Maturity Benchmark (RMB) is designed to help you set targets and put in place action plans to improve the way you manage risk.

These improvement plans should be presented to your responsible body as evidence of your efforts to carry out delegated responsibilities effectively, efficiently and ethically.



## Assurance that helps the responsible body make decisions confidently

These formal processes of assurance provide objective information about the organisation's frameworks and processes and *reassure* the responsible body that the organisation is functioning as it should.

They also play an essential role in supporting the responsible body to make its own decisions and show leadership.

Through these formal processes, you have an opportunity to show how risk thinking and techniques can help them think productively about potential scenarios and define worthwhile objectives.

Use these same techniques to keep your responsible body informed about change in the internal and external context that's relevant to the organisation's objectives and their decision-making role. Show how their statement of risk appetite is helping people in the organisation to make decisions.

You can show how risk management helps the organisation to create and protect value, minimise insurable risk, and contribute to identifying and managing state-significant risks.

These are all big-picture issues that the responsible body needs to be alert to. They also show the value of risk management