Design, implement and evaluate your controls

This guide will help you understand:

Control fundamentals:

- what is a control
- the differences between:
    - a risk owner and a control owner
    - controls and treatments
- designing, implementing and evaluating controls.

Evaluation of controls and treatments:

- what control effectiveness means and why it's important
- how to determine if controls are effective and tips on how to strengthen controls
- the guidance on control effectiveness testing provided in the Victorian Government Risk Management Framework (VGRMF) 2020
- how to complete the control effectiveness section of your risk register.

Example

Throughout this guide, we'll be using examples from a fictional organisation, *Welcome Health,* to illustrate best practice.

Welcome Health is a 175-bed rural public health service. They employ around 800 staff and service an area covering approximately 120 km radius from the hospital, with an estimated population of 50,000 people.

We'll introduce two staff members: Anika, Building Manager and Kim, Insurance Manager to bring the theory of control effectiveness testing to life.

Control

What is a control?

A control is something an organisation is **currently** doing to 'modify' a risk. Modify usually means you're trying to reduce or manage a risk. The purpose of a control is to reduce one or both of the:

- likelihood of a risk occurring
- impact of the risk.

Controls take many forms, including policies, procedures, practices, processes, technology, techniques, methods or devices that reduce a risk. They may be manual (requiring human intervention) or automated (technology based).

Controls typically work in one of three ways:

- **Preventative** – reduces the likelihood of a situation occurring, such as policies and procedures, approvals, technical security solutions built into a system, authorisations, police checks and training
- **Detective** – identifies failures in the control environment, such as reviews of performance, reconciliations, audits and investigations (internal or via a third party)
- **Corrective** – implemented after an event, addresses the root cause or reduce the consequence. They can ***remediate*** (e.g patching a system vulnerability), ***recover*** (e.g restoring a process or system following a business continuity plan), or ***respond*** (e.g coordinated crisis communications with people affected by an incident.)

We learn more about the impacts of these types of risks in *Options for Controlling Risks*.

Example

Welcome Health's risk register includes a risk related to service operations:

Risk event

Disruption to critical services and operations

Causes

The inability to access our building due to inadequate fire prevention measures

Direct cyber-attack on our system

Consequences

Damage or loss of building

Financial loss due to costs of managing a cyber incident

IT system outage

There are three controls in place aiming to modify this risk:

Preventative: % of staff who have completed the mandatory fire safety training

Detective: % of smoke alarms that detect the occurrence of fire that have been tested and are fully effective

Corrective: Property insurance provides funds to recover from damage caused by fire;

Business continuity plan that has been reviewed and exercised in the past 3 months.

Where do controls fit in the risk management process?

The first steps in any risk management process are to establish the scope, context and criteria you're operating in and to identify risks.

The next step is risk analysis. It's rare that a risk, even a new one, doesn't already have some controls in place, so it's at this point that you want to test the effectiveness of those controls.

If the controls aren't meeting or don't adequately modify the risk, your next step is to develop a treatment plan if required (e.g. the risk rating after considering your controls and their effectiveness is not acceptable). These actions when completed become a new, or improved, control.

Ongoing testing of the control effectiveness then becomes an important part of the monitoring and review cycle.

Your controls and their effectiveness will be documented in your risk register.

Check out these resources if you need more information on the risk process:

- VGRMF Guidance Material: vmia.vic.gov.au/VGRMF
- Risk management tools: Risk Criteria Examples

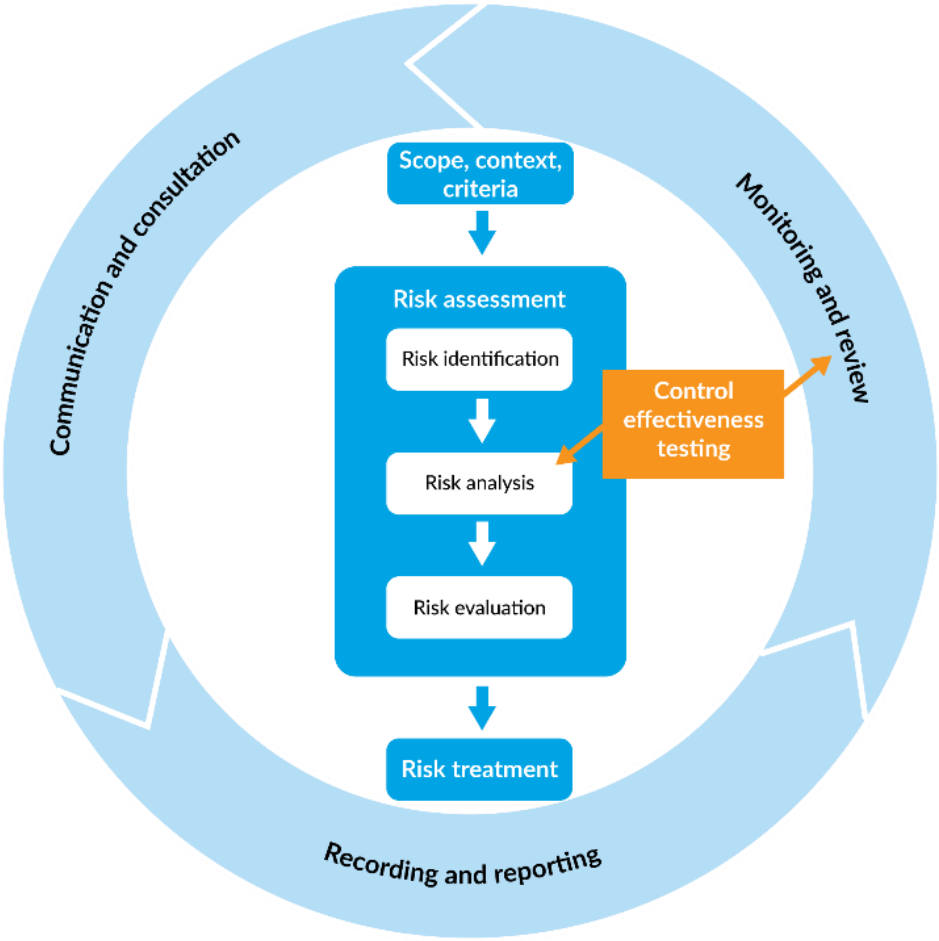
  You can find both tools at vmia.vic.gov.au/RMTs
- Risk Identification and Management Program.

What is the difference between controls and treatments?

A control is a measure that currently modifies a risk, usually with the aim of reducing or managing it. A risk treatment is a **future planned action** to address a risk.

The key difference is that treatments are new, and controls are existing. When a treatment is implemented, it becomes a control.

Figure 1 Risk Management process



Example

Welcome Health carried out a fire safety audit. The audit found smoke detectors were an older design and had a short battery life. The organisation decided to purchase and install new smoke detectors with lithium batteries. These actions were added as a treatment on the risk register.

Once the actions were completed, having operational and tested smoke detectors was then recorded as a control.

What's the difference between a risk owner and a control owner?

A risk owner is the person with the accountability and authority to manage a risk, including understanding what the controls are and how effective they are at modifying the risk.

A control owner is accountable for implementing and maintaining specific controls. This accountability may be recorded in a risk register or documented in position descriptions, or in organisational policies and procedures. Control owners may also be responsible for improving controls to increase their effectiveness.

A person might be both a risk owner and a control owner for one or more control, but often the roles are filled by separate individuals.

Example

As building manager, Anika is the owner of the risk, but she doesn't manage all the controls for it.

One of the key controls for the risk statement is Property Insurance, and it's Anika's colleague Kim who manages *Welcome Health's* insurance. In this case, Kim is the 'control owner' because she is responsible for this particular control: Property Insurance.

Methods for identifying controls

The bow-tie: a method for identifying controls, or the 5-step method

1. Bowtie identifies causes and consequences

2. 5-step method

Your first act is always to assess the risks to achieving your objectives.

One of the results of that assessment is an evaluation of the risk, which helps you assess what kind of investment you need to make to control the risk.

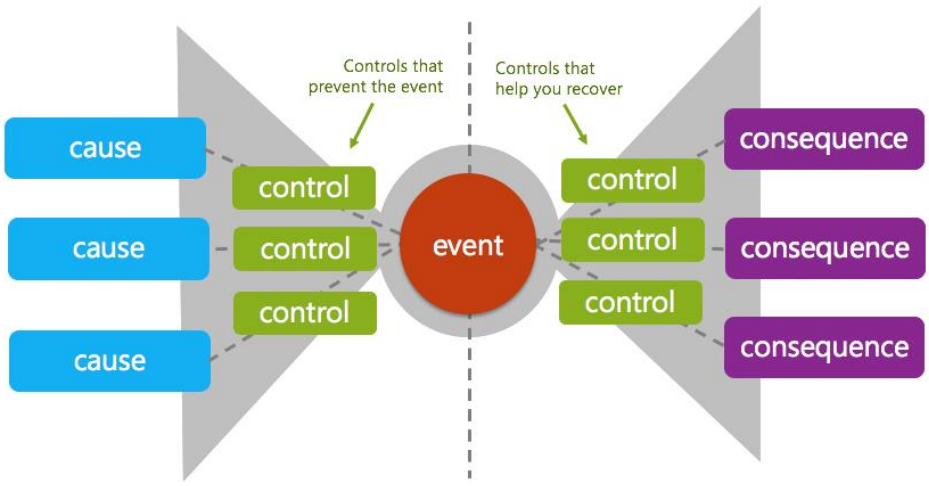
Your executive team will also have determined your organisation's risk criteria. The risk criteria is useful because it sets the boundaries in which you can operate (often quantitatively) and is based on your organisation's appetite for risk. One of the reasons the Victorian Government Risk Management Framework (VGRMF) requires your responsible body to define its risk appetite is precisely to help you make these decisions.

You may need to consult more widely or escalate decisions to the right decision-making body within your organisation, or even outside if it's a shared risk or a state-significant risk.

Finally, don't confine your attention to what's going on within your organisation. You're part of a supply chain, in contractual arrangements that expose you to risk. You need to look at those relationships, own the risks and control them. Use the PESTLE tool to help you analyse your external context.

The bow-tie brings it all together

We encourage you to use the bow tie to do your risk assessment. As you can see, it's a good way to lay out your event, together with its causes and consequences. Use it to identify how you can control the likelihood of the event happening and the severity of the consequences if it does.



Investigating your options

As part of assessing your risk, you also analyse the causes of a possible event, its consequences, and how likely it is.

This analysis will produce the information you need to work out what your options are for controlling the risk. For instance, could you

- avoid the risk entirely by taking another path to your goal?
- remove the source of the risk?
- share the risk with another agency?
- share part of a risk with insurance or a contract with another party?
- make it less likely for the event to happen?
- reduce the consequences if the event did happen?

The international standard on risk management, AS ISO 31000: Risk management - Guidelines, refer to these as your options for *risk treatment*.

When you're analysing your event, try to step back so you can get a full sense of the risks in your internal and external context. If it's a significant risk, spend some time working on the scenario. It may be worthwhile to explore a range of scenarios: probable and worst case, and even rare events that would still have consequences the organisation or the state doesn't want.

Here, we'll explore risks relating to a cyber threat. We'll first describe a risk and then set out the range of options for controlling the risk. The aim is to show you what an analysis could look like and how you would consider a wide range of options for controlling the risk. You can then decide what should go into your treatment plan.

A scenario

Say, for example, your organisation has entered a contract with a managed service provider (MSP) for IT services, including provision and maintenance of a firewall.

The vendor of the firewall has released updates for new vulnerabilities that have become apparent. Your MSP sends the IT operations manager a maintenance schedule and costs to do the updates in February.

Your organisation hasn't allocated budget for upgrades because when the budgets were drawn up it was assumed that these were covered by the service contract, which had a line referring to 'firewall maintenance'.

The IT operations manager, concerned about raising the issue, decides to defer the upgrade to July when funds become available in the new financial year, informing the director of their decision in the next management meeting. The director assumes that the operations manager has weighed up the risks appropriately.

In this table, we show the results of a risk assessment, which has been analysed as highly likely to happen, given current controls. We then look at the options for future treatment of the risk.

Description of the risk	
Risk event	Unauthorised access to confidential information
Causes	The firewall hasn't been updated with the latest defences. A hacker invades the network and inserts a worm virus into sensitive files. A disgruntled employee removes medical records and sells them to a 3rd party for profit.
Consequences	Documents containing sensitive and confidential information are stolen and the virus corrupts documents. Services and workflow are heavily disrupted. The organisation incurs a large bill for repair and recovery. The privacy and safety of your clients' information is compromised. Your organisation's reputation suffers. Money spent on repair and recovery is now not available for other planned projects and operations Previous work is lost in corrupted files.
Likelihood	The chances of this happening with current controls are high.
Current Controls and their effectiveness	IT System Firewall – ineffective Crisis Management Plan – Adequate IT Disaster Recovery Plan - Adequate
Options for treating the risk: what you can consider for your treatment plan	
Avoid the risk	Identify precisely, and independently of your service provider, what IT services you need to stay secure. Make sure the description of service is clear and explicit and understood by those with accountability for services and expenditure. Make sure you have budget for maintenance and other work not covered in the contract, so you can discuss variances with your manager. Meet regularly (once a month or quarterly for example) with your service provider to assess risks and opportunities and discuss controls.
Remove the source of the risk	Patch hardware in a timely manner and conduct regular updates. Meet once a month with your service provider to assess risks and discuss controls.
Share the risk with another public sector organisation	Set up and participate in a technical working group where you share tips about managing technical controls as well as accountabilities.
Share part of the risk	Make sure the contract's clear about what risks will be retained by you and what will be transferred to the service provider.

Description of the risk	
	Make sure your organisation operates according to better practice in procurement and managing third-party risk. Consult with VMIA about optimal risk transfer (insurance).
Make it less likely for the event to happen	Stick to the recommended maintenance schedule. Make sure you have the financial resources for maintenance not covered by the contract because of the rate of change in the environment. Make sure you have financial reserves for financial risks you've decided to retain. Build a positive risk culture in relation to decisions about IT management. Put frameworks, processes and a culture in place in which it's possible to escalate risks quickly in a fast-changing environment. Put in place performance management so that managers have the incentive to make sure their teams are capable, equipped and motivated to make the right decisions. Liaise with your legal and procurement team to interrogate contracts properly before they're signed.
Reduce the consequences if that event happened	Map your network and prepare an emergency containment plan so that you can isolate damage as far as possible. Put in place a back-up solution and procedures for getting essential information and services back online. Put in place a recovery plan that'll minimise the cost of getting operational again.

Options for controlling risk

So far we've looked at how you might assess your options for controlling risk, using the bow tie to analyse how you can control likelihood or the severity of the consequences.

You may not need to do that bespoke analysis though. Many regulatory and accreditation processes *build in controls* when they require you to demonstrate that you have certain procedures in place. There are examples of this in health care and education.

Procurement, privacy and prudential standards should all be understood as ways of controlling risk—if you comply with the standard, then the risk of financial waste or corruption, for example, is controlled. This is also true for compliance with legislation such as the Climate Change Act and the Modern Slavery Act.

Moving out of the compliance sphere, we can also find examples of voluntary codes and strategies, where someone's already done the work to validate their effectiveness in a wide range of situations. The Australian Cyber Security Centre's Essential Eight or AS/NZS ISO/IEC 27001- Information security, cybersecurity and privacy protection — Information security management systems — Requirements are examples of that.

Preventing, correcting and detecting

Another way to look at controls is to look at the structure of risk.

Preventative controls reduce the *likelihood* of an event happening.

The best way to control a risk is to prevent it from arising in the first place. You might be able to reduce the likelihood of loss or harm to, or close to, zero. Two examples of this, one from everyday life and the other from the workplace, are:

- the design of electric plugs and sockets which make it impossible for a person to touch a live current
- a protocol for releasing confidential information with approval steps designed to ensure that any release for any purpose is approved by the appropriate person in the organisation.

Detective controls pick up the signs that *a risk is changing,* or an event has happened.

Another way to control a risk is to attempt to detect and report undesirable events or conditions, enabling you to respond promptly and take corrective actions. Examples of detective controls are:

- Audit reviews: Regular audits by internal or external auditors to review financial and operational processes
- System logs and alerts: Using automated systems that log activities and flag unusual actions for review.

Corrective controls reduce the severity of the consequences if the event does happen.

These controls are activated after a risk event has been materialised, aiming to restore operations to their desired state and to prevent the recurrence of similar problems in the future. Examples of corrective controls include:

- A Business Continuity Plan that has been reviewed, exercised and updated in the past 3 months
- An IT Disaster Recovery Plan that has been reviewed, exercised and updated in the past 3 months.

Monitoring changes to your risks

Risk is dynamic. A risk may increase or decrease as a possible event becomes more or less likely. It can also increase or decrease according to a change in the potential consequences. You need to monitor signs of that change.

These signs are your risk indicators.

Your risk analysis will help you to work out what indicators you need to pay attention to, by giving you insight into the causes of events and the factors that make them more likely and their consequences more harmful.

By watching these indicators, you'll be able to see

- whether your efforts to control the risk are effective
- when you need to escalate a risk that's approaching a threshold of tolerance.

An evidence-based approach to controlling risk depends on risk and performance indicators. Not only will it help you achieve your objectives, it'll help you demonstrate, in economic terms, the value of managing risk effectively.

What is control effectiveness and why is it important?

Control effectiveness is the term used to describe how well a control is reducing or managing the risk it is meant to modify.

The more effective a control is, the more confidence you have the risk is being managed as you expect. A control is more effective when it is highly:

- relevant (it's designed to address the intended risk)
- complete (it addresses most/all the risk)
- reliable (it operates as expected)
- timely (it operates at the right time and reacts quickly enough).

Understanding how effective your controls are will assist you in planning and prioritising risk management actions and making informed decisions.

What is control effectiveness testing?

Control effectiveness testing involves regular review of your controls, to ensure they're designed correctly and are effectively reducing or managing risks as expected.

Note that you are evaluating whether the established controls (preventive, detective, and corrective) within your organisation are operating as intended and are effective in mitigating identified risks to acceptable levels.

Purpose of Control Effectiveness Testing

- **Assess adequacy and effectiveness:** To determine if controls are adequate to address specific risks and if they are effective in either reducing the likelihood of an event occurring or minimising its consequences should it occur
- **Identify weaknesses and gaps:** Testing helps identify weaknesses or gaps in the control environment, providing an opportunity to strengthen controls before failures occur
- **Compliance verification:** Your organisations must adhere to various regulatory requirements and standards. Control testing ensures compliance with these mandates by verifying that controls meet or exceed required standards
- **Support continual improvement:** By regularly testing controls, you can make informed decisions about where to make improvements or adjustments, supporting a continual improvement cycle in risk management.

Control effectiveness testing may be more suited for organisations that have stable control environments, mature risk management frameworks and resources available to do the testing. You may choose to test some controls more often than others, or to prioritise testing based on factors such as internal audit findings.

The VGRMF includes control effectiveness testing in its guidance on good practice risk management, however it's not a mandatory requirement.

Risk and/or control owners are usually responsible for testing control effectiveness and ensuring the control is working as intended.

Example

Kim is new to her role and wants to understand the effectiveness of the control: Property Insurance.

She read the policy documents and found that she had some questions about coverage for fire safety equipment at a property that *Welcome Health* owns. Kim contacted VMIA for clarification about the extent of the coverage, which gave her confidence that the control was meeting *Welcome Health's* needs. Regularly reviewing policies to ensure they meet current/changing business needs is a way to test the effectiveness of a control.

How do I test control effectiveness?

1 – Understand the control's purpose

Understand what risk(s) the control is intended to reduce or manage, how the control works (preventative, corrective, detective), and the intended effect.

Example

Welcome Health's risk register has the following controls in place, aiming to reduce the likelihood and severity of fire impacting access to the building.

Example risk register:

Risk Event	Causes	Controls
Disruption to critical services and operations	The inability to access our building due to inadequate fire prevention measures Direct cyber-attack on our system	**Preventative**: % of staff who have completed the mandatory fire safety training **Detective**: % of smoke alarms that detect the occurrence of fire that have been tested and are fully effective **Preventative**: Implementation of the Essential 8
	Damage or loss of building Financial loss due to costs of managing a cyber incident IT system outage	**Corrective**: Business Continuity Plan that has been reviewed and exercised in the past 3 months **Corrective**: Property insurance provides funds to recover from damage caused by fire. **Corrective**: IT Disaster Recovery Plan that has been reviewed and exercised in the past 3 months

2 – Gather evidence to test the control

Gather quantitative and/or qualitative data that shows whether the control is having the intended effect.

Here are some examples of the information or approaches you can use:

- self-assessment
- feedback, such as complaints and survey findings
- review of errors and incidents
- specialist review by trained auditors and assessors
- root-cause analysis
- quality control
- loss event data
- insurance claims
- historical instances of identified risk being realised
- modelling
- user testing.

3 – Evaluation

When evaluating the effectiveness of your controls, it's helpful to use an agreed rating scale for all control testing to ensure consistency and common understanding.

Here are examples of different types of rating scales:

Example of a five-level scale

Control effectiveness	Description
Fully effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk and address the root causes. Management believes they are always effective and reliable.
Substantially effective	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness, or management has doubts about operational effectiveness and reliability.
Partially effective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. Or, some of the controls do not seem correctly designed in that they do not treat root causes. Those that are correctly designed are operating effectively.
Largely ineffective	Significant control gaps. Either controls do not treat root causes, or they do not operate at all effectively.
None or totally ineffective	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design or very limited operational effectiveness.

Example of a three-level scale

Control effectiveness	Description
Effective	Controls eliminate or remove the source/root cause of the risk. Or, controls are well documented, consistently implemented and reliable in addressing the source/root cause of risk. High degree of confidence from management in the protection provided by the controls.
Partially effective	Controls are in place but may be partially documented or communicated, or inconsistently applied or infrequently tested. Weaknesses in the controls are minor or moderate and tend to reflect opportunities for improvement, rather than serious deficiencies in systems or practices.
Ineffective	Controls aren’t documented or communicated or are inconsistently implemented in practice. The controls aren’t operating as intended and risk is not being managed. Controls aren’t in place to address the root cause/source of risk.

Example

Welcome Health uses the three-level rating scale to evaluate their controls. Anika gathered a range of information to determine that whilst the control was modifying the risk, there was room for improvement.

Control effectiveness	Description	Evidence
Partially effective	Controls are in place but could be improved	• training attendance registers showed 10% of staff had not completed mandatory fire safety training • the need to review insurance policies when leasing/buying property is not included on the procurement checklist

4 – Plan treatments and update the risk register

Where a control is rated in a way that suggests it's ineffective at reducing or managing the risk, or not in line with your expectations, you should decide if you need to make changes that will have the intended effect. This may include stopping or changing a control, or adding a treatment.

Example

Having reviewed the evidence and rated the effectiveness of the controls, Anika found opportunities to enhance the control effectiveness by taking further action/treatments. She added these to the risk register.

Example risk register:

Risk Event	Controls	Treatments
Disruption to critical services and operations	**Preventative**: % of staff who have completed the mandatory fire safety training **Corrective**: Property insurance provides funds to recover from damage caused by fire.	• Develop process for following up staff who have not undertaken mandatory fire safety training • Update procurement checklist to include the need to review insurance policies when leasing/buying property

Risk registers normally have a section for you to list controls and their level of effectiveness.

Check out VMIA risk tools for risk register templates.

Weighing up the costs of control

Controlling and monitoring risk, like all management activities, comes with a cost. There are two ways to look at this:

- weigh up the cost against the benefit of achieving your objective
- look at the opportunity cost of spending money on controlling the risk, rather than something else of value to the organisation.

Costs and benefits

The benefit you're seeking comes from achieving your objective. So, your question here is whether the cost of controlling the risk you need or want to take to achieve your objective is worth it.

For example, is it worthwhile to invest $500,000 on building upgrades when the whole organisation will be moving to another office within 12 months?

Opportunity costs

The other concept to bear in mind is opportunity cost. Your organisation's resources are finite. If you decide to spend money on controlling a risk so that you can achieve an objective, then that money isn't available for other work.

That needs to be a conscious decision. When you're making decisions about how to control your risks, you should always ask yourself whether that puts other objectives at risk.

For example, if you didn't spend that $500,000 on the building upgrade, that money would be available for an upgrade to the health and well-being program and other culture initiatives.

This is how you demonstrate, in economic terms, the value of managing risk effectively.

What is a control library?

A control library is a central list of all your organisation's controls. Control libraries are best suited to larger organisations, where there's a critical reliance on operational processes that need to be well documented and regularly monitored.

A control library may contain:

- a list of controls
- a description of each control
- the risk/s a control aims to modify
- the effectiveness of a control
- the control owner
- categorisation into preventative, detective, or corrective
- categorisation into key controls or non-key
- categorisation of general type (IT, manual, environment).

A control library allows you to see all controls operating within your organisation and their effectiveness in one place. It allows you to view controls that are in place for other business areas, so you can consider using or adapting them to address other risks.

For some organisations, control libraries exist as databases or modules within their governance, risk and compliance applications/systems, including safety, IT and finance. Control libraries are sometimes used by auditors to identify and test the key controls relating to an audit area.

Consider the Example Control Library in Appendix A.

Constructing your own control library

Building a control library involves considering the main activities of the business, and then identifying the critical points where a check is in place. For example:

Function	Example activity	Example key controls
People and culture	Payroll processing	Authorising payment is separated from adding new employees Performance and development processes are aligned to organisational objectives
Governance & compliance	Annual attestations in annual report	Executives provide sign-off for their business area based on documented evidence Key legislative compliance obligations are recorded and regularly tested
Marketing & communications	News release via social media	Head of communications reviews draft content prior to release Senior staff rehearse giving interviews in the event a future crisis occurs
Service delivery	Provision of frontline service to the community	New staff must complete induction training package before delivering service A business continuity plan is in place and regularly practiced
Public policy	Gathering community feedback on new policy	Evidence of stakeholder feedback is gathered against policy objectives

Appendix A – Example Control Library

ID	Control	Control description	Associated risk event	Effectiveness	Last tested date	Control owner	Preventative, detective or corrective
C001	Fire safety training	>80% of staff who have completed the mandatory fire safety training.	Disruption to critical services and operations	Ineffective	3/4/24	Building Manager	Preventative
C002	Smoke alarms	>90% of smoke alarms that detect the occurrence of fire that have been tested and are fully effective	Disruption to critical services and operations	Fully effective	3/4/24	Building Manager	Detective
C003	Property insurance	Policy provides funds to recover from damage caused by fire. Limit: $3.2b Deductible: $100k	Disruption to critical services and operations	Partially effective	3/4/24	Insurance Manager	Corrective

VMIA is the Victorian Government's insurer and risk adviser

Level 10 South,
161 Collins Street
Melbourne VIC 3000

P (03) 9270 6900

contact@vmia.vic.gov.au

vmia.vic.gov.au