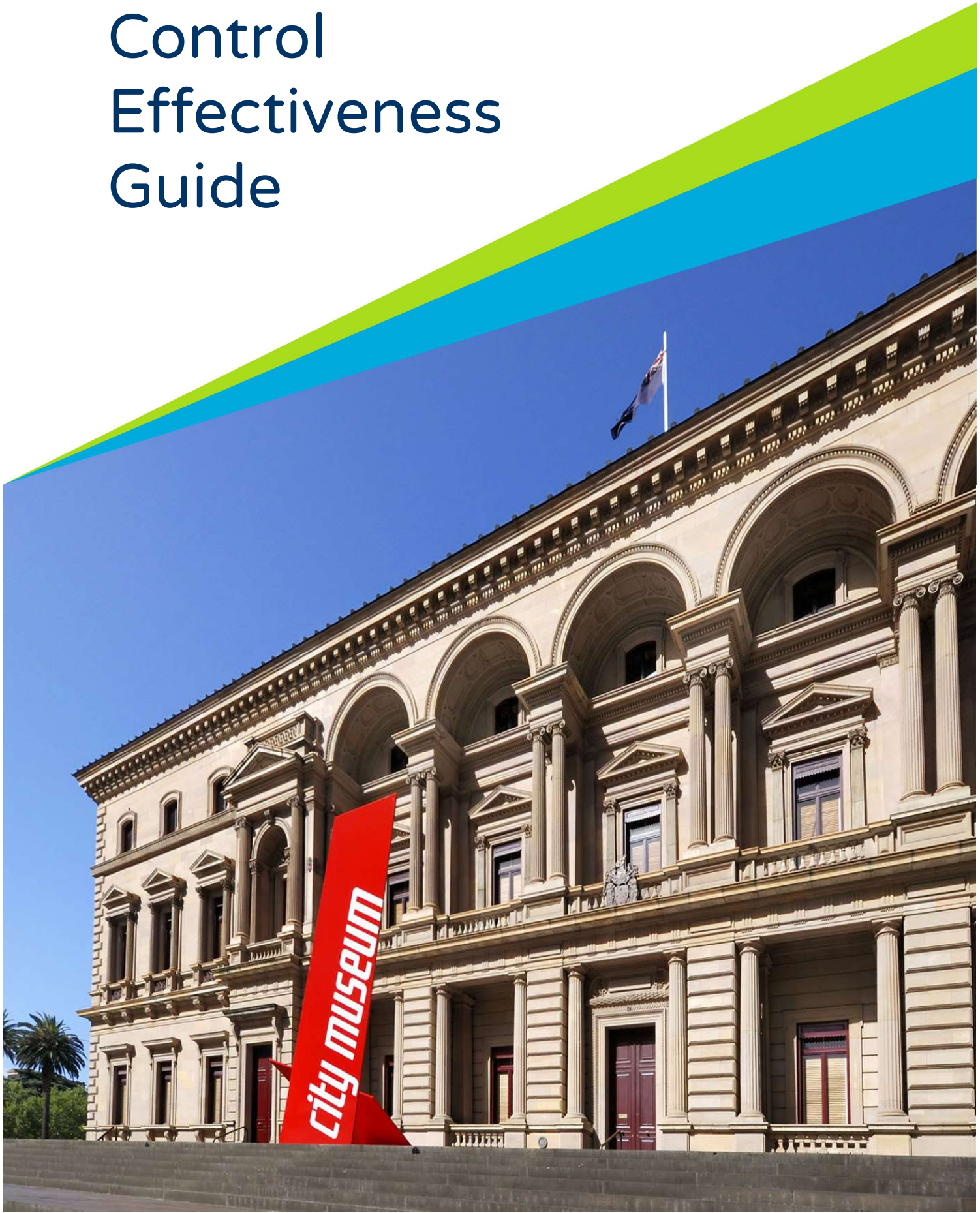
# Control Effectiveness Guide



# Contents






© Victorian Managed Insurance Authority

Level 10 South, 161 Collins Street Melbourne VIC 3000

PO Box 18409, Collins Street East Victoria 8003

ABN 39 682 497 841
P (03) 9270 6900
F (03) 9270 6949

contact@vmia.vic.gov.au
vmia.vic.gov.au


VMIA is the Victorian Government's insurer and risk adviser

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.

# Purpose

This guide will help you understand:

- what a control is
- the difference between a risk owner and a control owner
- 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.

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.

# What's 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).

A control typically works in one of three ways:

- Preventative – controls that reduce 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 – controls that identify failures in the control environment, such as reviews of performance, reconciliations, exception reporting, staff culture surveys, IT security event logs and investigations (internal or via a third party)
- Corrective – controls that reduce the consequence and/or rectify a failure after it has been discovered, such as continuous improvement actions, crisis management, business continuity and/or disaster recovery plans or insurance.

**Example**

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

> Risk Statement
>
> The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services.

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

Preventative: Fire safety training is mandated for all staff, so they know what could start a fire and what to do if there's a fire

Detective: Smoke alarms detect the occurrence of fire

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

# What's 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.

**Example**

Welcome Health undertook an essential fire safety audit. It found that some smoke detectors were an old style and no longer compliant with relevant codes. While Welcome Health commenced the process to purchase and install new smoke detectors, this action was recorded as a treatment on the risk register. Once the action was completed, having compliant smoke detectors was moved on the risk register to be noted 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 controls, but often the roles are filled by separate individuals.

**Example**

As building manager, Anika is the owner of the risk statement, 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's responsible for this control: Property Insurance.

# What's 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's 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's highly:

- relevant (it's designed to address the intended risk)
- complete (it addresses most/all of 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 to plan and prioritise risk management actions and make informed decisions.

# What's control effectiveness testing?

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

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 2020 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 Welcome Health property. Kim contacted VMIA and clarified the extent of the cover, 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 Statement | Controls |
|---|---|
| The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services. | **Preventative:** Fire safety training is mandated for all staff so they know what could start a fire and what to do if there's a fire.<br>**Detective:** Smoke alarms detect the occurrence of fire.<br>**Corrective:** Property insurance provides funds to recover from damage caused by fire. |

## 2. Gather evidence to test the control

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

Use information or approaches such as:

- 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 some examples of different types of rating scales:

*Example of a three-level scale (simpler)*

| Control effectiveness | Description |
|---|---|
| Effective | Controls eliminate or remove the source/root cause of the risk.<br>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.<br>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 isn't being managed. Controls aren't in place to address the root cause/source of risk. |

*Example of a five-level scale (more complex)*

| 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 always believes they're 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 aren't currently very effective.<br>Or some of the controls don't seem correctly designed in that they don't treat root causes. Those that are correctly designed are operating effectively. |
| Largely ineffective | Significant control gaps. Either controls don't treat root causes, or they don't 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**

Welcome Health use 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 rating | Description | Evidence |
|---|---|---|
| Partially effective | Controls are in place but could be improved | • training attendance registers showed 10% of staff hadn't completed mandatory fire safety training<br>• the need to review insurance policies when leasing/buying property isn't 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 changes or new actions that'll 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 statement | Controls | Treatments |
|---|---|---|
| The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services | Preventative: Fire safety training is mandated for all staff so they know what could start a fire and what to do if there's a fire<br>Detective: Smoke alarms detect the occurrence of fire<br>Corrective: Property insurance provides funds to recover from damage caused by fire | • Develop a process for following up staff who haven't undertaken mandatory fire safety training<br>• 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. Consider the example in Appendix A taken from VMIA's sample risk register.

# What's a control library?

## A control library is a central list of all your organisation's controls. Control libraries are best suited to larger organisations and entities, 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. It helps you work out which controls should be checked, in what priority and how the checking can be done (eg by staff or an external specialist),

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 B.

## 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<br>• 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<br>• 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<br>• 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<br>• 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 |

# Where do controls fit in the risk management process?

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

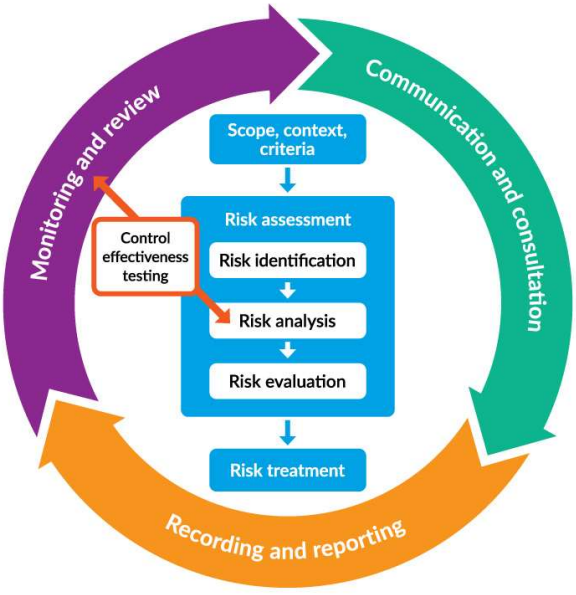
The next step is risk analysis. It's rare that a risk, even a new one, doesn't already have some controls in place, so it's at this point that you want to test the effectiveness of those controls.

If the controls aren't meeting your expectations to adequately modify the risk, you'll develop a treatment plan. As these actions are completed, they become a new control.

Ongoing testing of the effectiveness of your controls 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 VMIA's Practical guidance for managing risk if you need more information on the risk process.



# Appendix A – Example risk register

| Risk ID | Date registered | Date of review | Strategic objective | Risk category | Risk description | Control actions | Control effectiveness | Likelihood | Consequence | Risk rating | Treatment actions | Risk owner |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R23 | 7/2/20 | 3/4/20 | 3. A thriving and sustainable health service | Business continuity | The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services | 1. Preventative: Fire safety training is mandated for all staff so they know what could start a fire and what to do if there's a fire<br>2. Detective: Smoke alarms detect the occurrence of fire<br>3. Corrective: Property insurance provides funds to recover from damage caused by fire | 1. Partially effective<br>2. Fully effective<br>3. Partially effective | Unlikely | Major | Medium | • Develop a process for following up staff who haven't undertaken mandatory fire safety training<br>• Update procurement checklist to include the need to review insurance policies when leasing/buying property | Building Manager |

# Appendix B – Example control library

| ID | Control | Control description | Associated risk description/s | Effectiveness | Last tested date | Control owner | Preventative, detective, or corrective |
|---|---|---|---|---|---|---|---|
| C001 | Fire safety training | Mandated training for all staff so they know what could start a fire and know what to do if there's a fire | The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services | Partially effective | 3/4/20 | Building Manager | Preventative |
| C002 | Smoke alarms | 80 smoke detectors to detect the occurrence of fire. | The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services | Fully effective | 3/4/20 | Building Manager | Detective |
| C003 | Property insurance | Policy provides funds to recover from damage caused by fire.<br>Limit: $3.2b<br>Deductible: $100k | The inability to access our building caused by inadequate fire prevention measures resulting in an inability to deliver our services | Partially effective | 3/4/20 | Insurance Manager | Corrective |