Designing, implementing and evaluating your controls

To achieve your objectives, you need to be willing to take and create a risk. How much and what type of risk will depend on your appetite for risk.

If a risk seems too high, but you don't want to give up the objective, you can take steps to reduce the likelihood of the event or the severity of its potential impact. By *controlling* a risk in this way, you can take the risk confidently.

If you can demonstrate that you can control the risk effectively, you may even be able to take on more risks to achieve your objective and deliver further benefits to the community.

You'll also be able to demonstrate the value you're creating and protecting for the organisation and the Victorian public, by managing risk effectively.

The Control Effectiveness Guide [PDF, 1.41MB] will give you an overview of controls. In this topic, we'll focus on

- recognising when you need to control a risk
- investigating your options for control
- monitoring changes in the risk you're controlling
- weighing up the costs of control.

Recognising when you need to control a risk

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

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

Your executive team will also have analysed your organisation's tolerance for these risks. The tolerances are useful because they give material, and often quantitative, indications of the boundaries in which you can operate.

You may also need to consult your organisation's risk appetite. 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.

Even if the statement of risk appetite doesn't speak specifically to this risk, we recommend that you discuss it as a team. 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 [DOCX, 4.59MB] to help you analyse your external context.

The bow-tie brings it all together

This information is accurate as at 07/01/2022

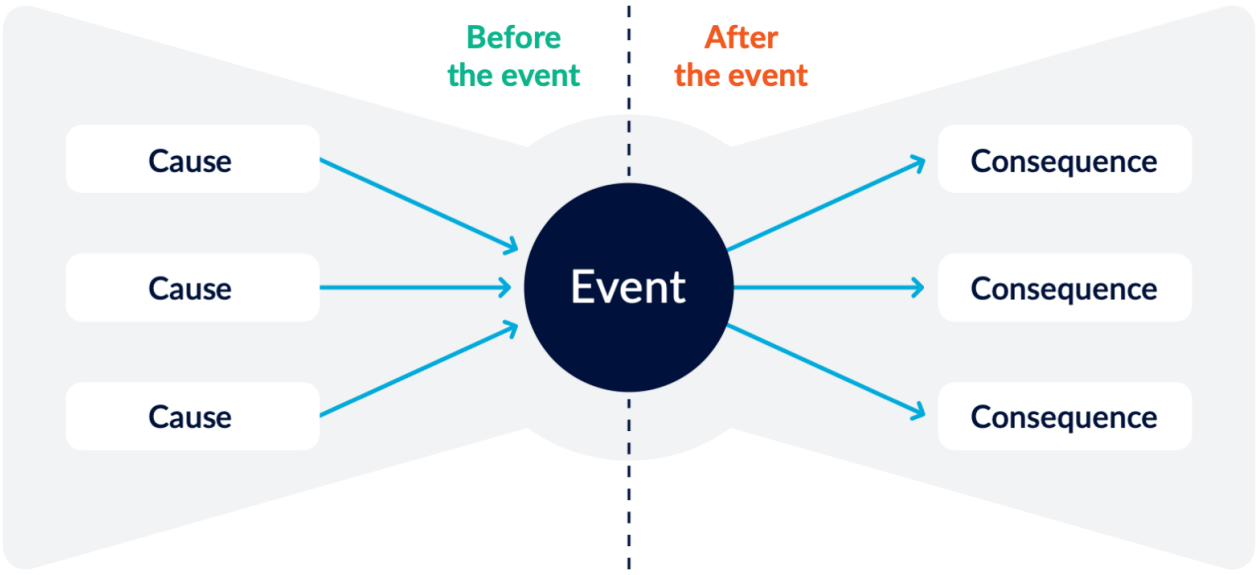
VMIA is the Victorian Government's insurer and risk adviser

Level 10 South,
161 Collins Street
Melbourne VIC 3000

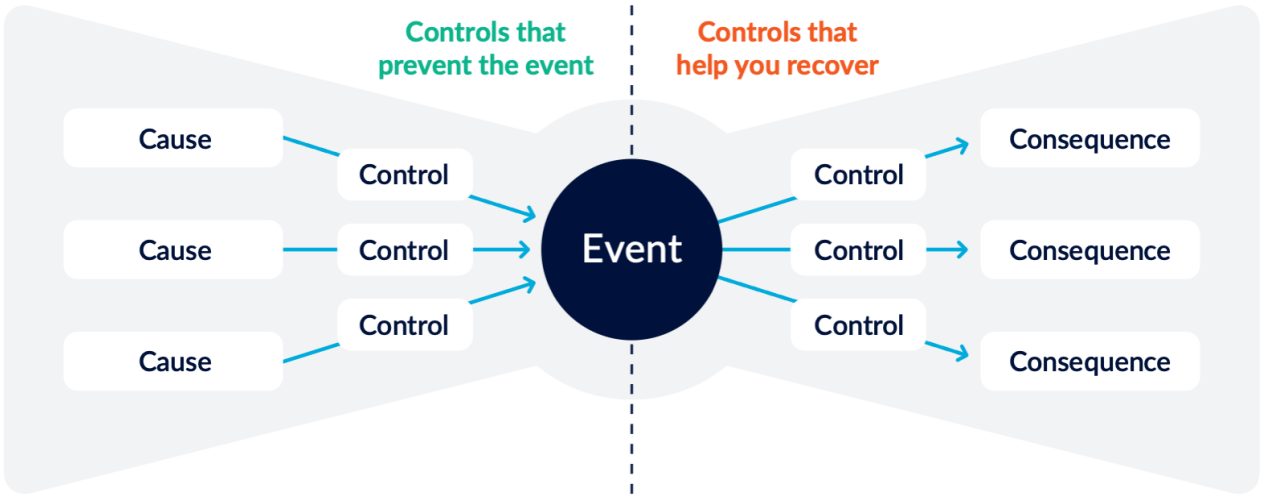
P (03) 9270 6900
F (03) 9270 6949
contact@vmia.vic.gov.au

vmia.vic.gov.au

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.



Don't stop with the assessment though. 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?
- transfer part of a risk with insurance or a contract with another party?
- make it less likely for the event to happen?
- change the consequences if the event did happen?

The guidelines for the international standard on risk management, AS ISO 31000, refer to these as your options for *risk treatment*.

When you're analysing your event, try to step back so that 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 even 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's 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 into 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 it was 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	
Possible event	A hacker invades your network and gets access to sensitive documents on your network drive and inserts a worm virus into files.
Causes	The firewall hasn't been updated with the latest defences.
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.
Options for controlling 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.
Transfer 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. Make sure your organisation operates according to better practice in procurement and managing third-party risk. Consult with VMIA about optimal risk transfer.
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. Build a risk management framework that takes risks relating to IT management into consideration. 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.
Change 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. You can find many 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 is an example 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.
- Corrective controls reduce the *severity of the consequences* if the event does happen.
- Detective controls pick up the signs that a *risk is changing* or an event has happened.

You can find more about these different types in our Controls Effectiveness Guide [PDF, 1.41MB]. We also encourage you to use the bow tie to help you identify the most effective way to control a risk.

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.

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.

Testing your controls

Our Control Effectiveness Guide [PDF, 1.41MB] has more information about how you can test the effectiveness of your controls.

Note this is about whether you're controlling the risk appropriately, not whether the control's functioning the way it should. For example, a *detective* control like your fire alarm might be functioning exactly as it should, but without *preventative* controls in place—such as proper waste disposal—you aren't controlling the risk appropriately.

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, we recommend that you 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.