Office of the Victorian
Information Commissioner

PRACTITIONER GUIDE:

Information Security Risk Management

Version 2.0

Formerly Chapter 1 of the Assurance Collection

Freedom of Information | Privacy | Data Protection

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne Victoria 3001

First published July 2017
Amended April 2020

Also published on: https://ovic.vic.gov.au
ISBN 978-0-6486723-7-1

Information Security Risk Management

Version 2.0

Practitioner Guide Details

Practitioner Guide: Information Security Risk Management ***(formerly Chapter 1 of the Assurance Collection)***	
Protective Marking	N/A
Approved for unlimited public release	Yes – Authorised for release
Release Date	April 2020
Review Date	April 2021
Document Version	2.0
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit - OVIC

For further information, please contact the Information Security Unit on security@ovic.vic.gov.au

Information Security Risk Management

1. Background

The Office of the Victorian Information Commissioner (OVIC) issues security guides to support the Victorian Protective Data Security Standards (VPDSS).

This document forms part of a suite of supporting security guides of the VPDSS.

2. Purpose

This document provides organisations with guidance on security risk management fundamentals to enable them to undertake a Security Risk Profile Assessment (SRPA) as required under s89 of the *Privacy and Data Protection Act 2014* (PDP Act).

3. Audience

This document is intended for Victorian public sector organisations (including employees, contractors and external parties) that are subject to the protective data security provisions under Part 4 of the PDP Act.

This guide is designed to support practitioners and information security leads.

4. Use of specific terms in this document

Please refer to the VPDSS Glossary for an outline of terms and associated definitions. For a current copy of the glossary, please refer to the VPDSF Resources section of the OVIC website.

4.1. What is a Security Risk Profile Assessment?

A process that organisations undertake to assess and manage information security risks. Most SRPAs prepared under the VPDSS assess physical security risks and personnel security risks in addition to information technology risks as it relates to information assets[1].

5. Scope

The activities set out in this document help organisations identify, analyse and evaluate their information security risks more effectively, and then manage these with their existing risk management frameworks or by referencing established risk management material, such as:

- *AS ISO 31000:2018 Risk Management – Guidelines;*
- *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management;*
- *HB 167:2006 Security Risk Management*;
- *NIST SP 800-30 Guide for Conducting Risk Assessments;* and
- *Victorian Government Risk Management Framework (VGRMF).*

This document directly supports the VPDSS information security risk management standard, and also steps

[1] Although information assets are the focus under the VPDSS, organisations can use the same process for identifying security risks for other assets such as people and physical assets.

3 to 5 of the Five Step Action Plan[2] by identifying information risks, applying security controls and managing risks across the information lifecycle.

6. Assumptions

The activities set out in this document assume organisations have basic risk management practices in place and these are operating effectively[3].

Organisations deal with many categories of operational risk (financial, safety, people, operational, etc.). A risk category helps to classify a 'type' of risk and manage it more effectively.

Risk within the context of this document, is focused on the protection of public sector information assets. This is often referred to as security risk, information security risk or information risk and is a category of risk to be considered along with other risk categories within an organisational risk management framework. This makes it easier to understand the context of the risk and develop a profile of security risks of the organisation.

Organisations should continue to utilise these practices and refer to this guidance for information security risk advice to enable completion of the SRPA and Protective Data Security Plan (PDSP).

Organisations who have risk practitioners and/or security practitioners will be well placed to drive the actions set out in this document.

The way in which your organisation identifies information assets as the subject of the SRPA is flexible. Further guidance on information assets can be found in the *Practitioner Guide: Identifying and Managing Information Assets*.

7. Security Risk Profile Assessment Overview

There are a wide range of threats that if given the opportunity to interact with an organisation's information and supporting systems, could pose risks to an organisation. Organisations that identify and manage their risks will have greater confidence to minimise harm and damage, and recover from impacts faster and in a more cost effective manner than those that do not.

The VPDSS and Victorian Protective Data Security Framework (VPDSF) are built upon the foundation of risk management principles. It is imperative that organisations are aware of the application of those principles to allow for the identification and management of information security risks to Victorian government information.

A SRPA can be a powerful process for identifying and prioritising information security risks to provide efficient, effective and economic investment in security controls. This process does not need to be overly complicated or time consuming. The outcomes of the SRPA will allow organisations to provide a level of confidence to citizens, businesses and the community as a whole when interacting with government.

Prior to undertaking the SRPA, you should develop risk evaluation and acceptance criteria that aligns to, or uses, your organisation's existing risk evaluation processes. This may need to be revised as part of the risk evaluation process[4].

[2] Refer to the Five Step Action Plan for further guidance on each of the steps https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/.

[3] The Victorian Managed Insurance Agency (VMIA) provides guidance on implementing the Victorian Government Risk Management Framework (VGRMF). Organisations should refer to VMIA https://vmia.vic.gov.au for further guidance on risk management principles and practices.

[4] Further information is provided in section 10.4 – Risk evaluation.

This practitioner guide provides a simple-to-use methodology designed to assist you to undertake the SRPA to manage information security risks. The content in this guide is consistent with the principles detailed in local, national and international risk management standards and guidelines.

This walks you through the key stages of the standardised risk management process as visually represented by Diagram 1. Each stage of the process is represented by colour coded dots located throughout the document to keep track of where you are in the process.

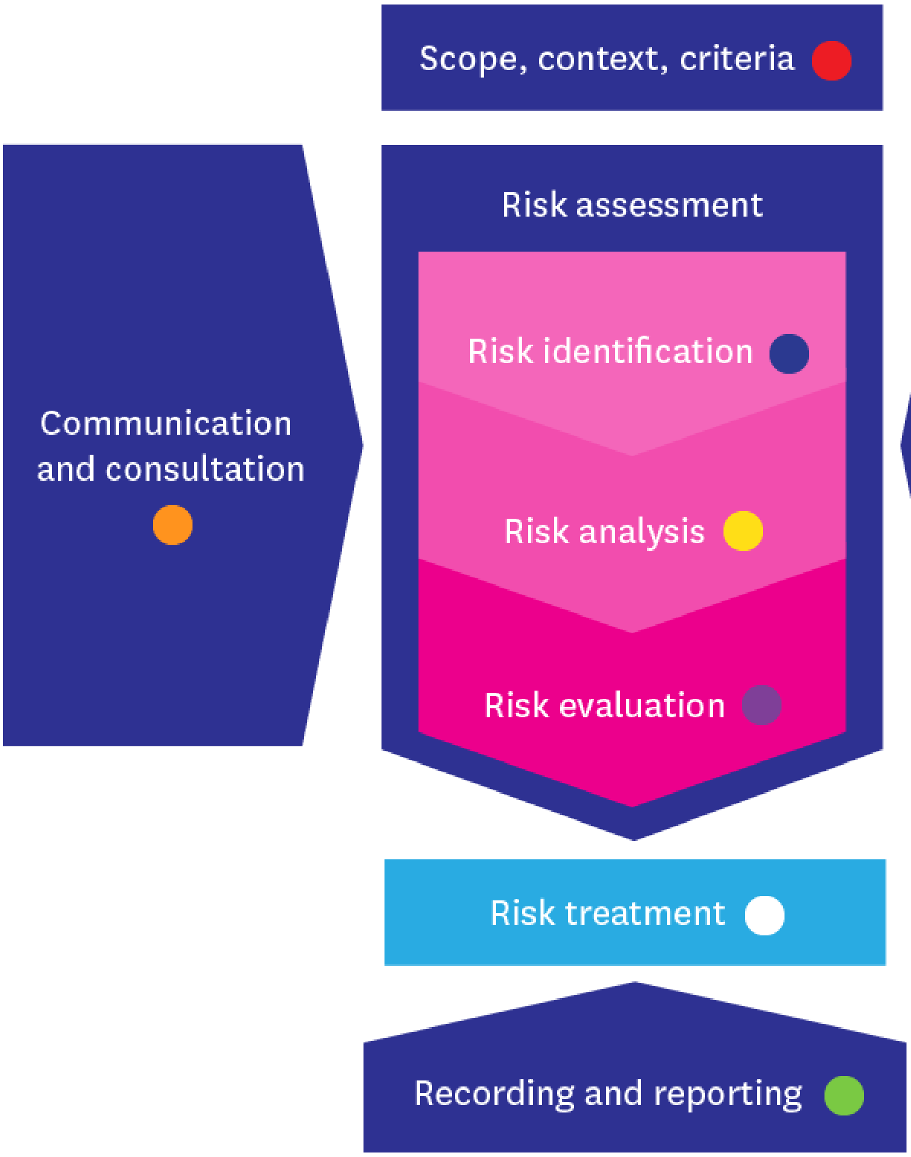


Diagram 1. Standardised risk management process

7.1. SRPA development

The SRPA process leverages existing organisational risk management decisions, such as:

- potential consequence levels; or
- accepted appetite for risks at certain levels.

Organisations assess operational risk categories (such as OH&S, finance, etc.) in variety of ways. For information security, you may consider developing a SRPA project plan that addresses the following:

- goals and objectives for information security;
- SRPA program/ project outline;
- SRPA stakeholder identification;
- SRPA resourcing, accountabilities and responsibilities;
- constraints on the SRPA (e.g. legislative requirements, available funding);
- assumptions;
- monitoring and review processes;
- information security incident history; and
- relationships with other security functions (e.g. personnel security, physical security, fraud control, anti-corruption.)

8. Consultation

Consultation across your organisation is important in order to identify all **probable** risks to information assets, and the impact of these to your organisation.

Formalising the consultation process for larger organisations ensures that it receives senior management support and includes all business areas and relevant third parties. This will also allow senior management to set priorities on functions they consider critical.

The consultation process will also allow you to identify the individual risk owners who have knowledge of risks and controls. These would normally be the information asset owners, although for critical risks the level of ownership may be escalated to a more senior person in your organisation. It is also important to understand the perspectives of each stakeholder as these will include natural biases.

8.1. Consultation with Information Owners, System Owners and Records Managers

Not all organisations will have the same information management (IM) roles and responsibilities, as these are largely informed by the size, structure and resourcing of the business. Regardless, consultation should start with information owners and supporting system owners (custodians), subsequently extending to records managers and other stakeholders with an interest in, or influence over these assets.

These stakeholders can add valuable input and an understanding of the criticality of these assets as well as probable threats to them. Stakeholders include internal and external parties.

A note on information owners: It is important to differentiate between an information custodian, versus information owner. Whilst someone may be the information custodian for a system they may not be best place to understand the information risks as the information owner may be.

8.2. Consultation with other areas of protective security

There may be overlap between the controls implemented to protect information and other assets, such as people, and physical assets (e.g. buildings and equipment). When undertaking the SRPA, it is important to identify any existing or planned implementation of security controls for other areas of protective security such as personnel security and physical security, that may have a material impact on, or assist in the mitigation of risks to information assets. Working with other security risk areas will also allow the use of single security controls that can mitigate multiple risks across the organisation and ensure that the risk management approach established within your organisation and the SRPA process work in unison.

The practitioners in these other security risk areas will be able to provide specialist advice and assistance throughout the SRPA by advising on the effectiveness of existing security controls and suitability of proposed new controls to mitigate risks to information assets.

Example 1. Protective security consultation

An organisation's human resources unit develops a personnel screening program as part of the recruitment and ongoing human resource management processes.

The security area (or equivalent) should engage with all business units so that all areas of the business are aware that any changes to systems, processes or people should include engagement with the security area. So in this example, this would be an opportunity for the human resources unit to consult with the security area to ensure the planned security controls will help mitigate identified risks (e.g. the risks of deliberate unauthorised disclosure of information, fraud, theft of assets and employing unsuitable personnel for roles).

8.3. Consultation with Third Parties

As part of the SRPA, it is important to consult with your third parties (e.g. contracted service providers), as these type of engagements may introduce additional risks. These third parties may be able to offer additional considerations that otherwise may not have been originally scoped.

You may also liaise with other Victorian government organisations such as the Victorian Managed Insurance Authority (VMIA) or the Cyber Safety Unit (CSU) in Department of Premier and Cabinet who may be able to provide insights and advice on the threats and risks in Victorian government.

9. Establishing the context

Prior to undertaking any form of risk assessment, you need to understand the context in which the assessment is being undertaken. By establishing the context you can properly understand, align, plan and prepare the most appropriate activities to support the SRPA process.

When gaining an understanding of the context, consider both internal business functions, as well as the broader environment in which your organisation is operating.

9.1. Organisational context

An essential foundation for the SRPA is having a thorough appreciation of your organisation's core functions and services, as well as the supporting information assets that are critical to meeting its business objectives.

By understanding your organisation's business you will be able to select security controls that:

- complement or enhance business operations; and
- meet any regulatory or operational requirements.

Prior to undertaking a risk assessment, your organisation will need to know the information assets across the business. Identifying information assets is Step 1 of the Five Step Action Plan. Guidance on identifying information assets is contained in the Practitioner Guide: Identifying and Managing Information Assets[5].

Organisations are also required to conduct a security value assessment of the information assets to understand the criticality of the information. Performing a security value assessment of your organisation's information assets is Step 2 of the Five Step Action Plan. Guidance on conducting a security value assessment is contained in the Practitioner Guide: Assessing the Security Value of Information[6].

Use the outcomes from Steps 1 and 2 of the Five Step Action Plan to enable you to prioritise which information assets to focus your risk assessment.

9.2. External context

It is important to have an understanding of the external environment in which your organisation is operating in, and consider any planned future activities. Understanding the risks arising from this environment will influence the selection of security controls to mitigate security risks.

Additionally, most organisations rely on contracted service providers for some of their services or functions. Organisations should consider all contracted service providers and their specific roles as part of undertaking a SRPA.

Environmental considerations may also impact the risks to your information. These could include natural and manmade environmental considerations (e.g. flood/ bushfire and local crime statistics).

[5] Refer to the Resources published on the OVIC website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/.

[6] Refer to the Resources published on the OVIC website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/.

9.3. Legislative and regulatory requirements

The PDP Act[7] requires organisations to:

- undertake a SRPA; and
- submit their revised PDSP to OVIC every two years, or where there is a significant change.

To support these requirements, organisations should undertake the SRPA regularly (e.g. at least annually) to assist with completing their PDSP and align with other risk management activities across the organisation.

In addition, your organisation will have its own legislative and regulatory requirements relating to the management of public sector information. You should confirm these prior to undertaking the SRPA, as they may impact on how the risks to your organisation's information are managed.

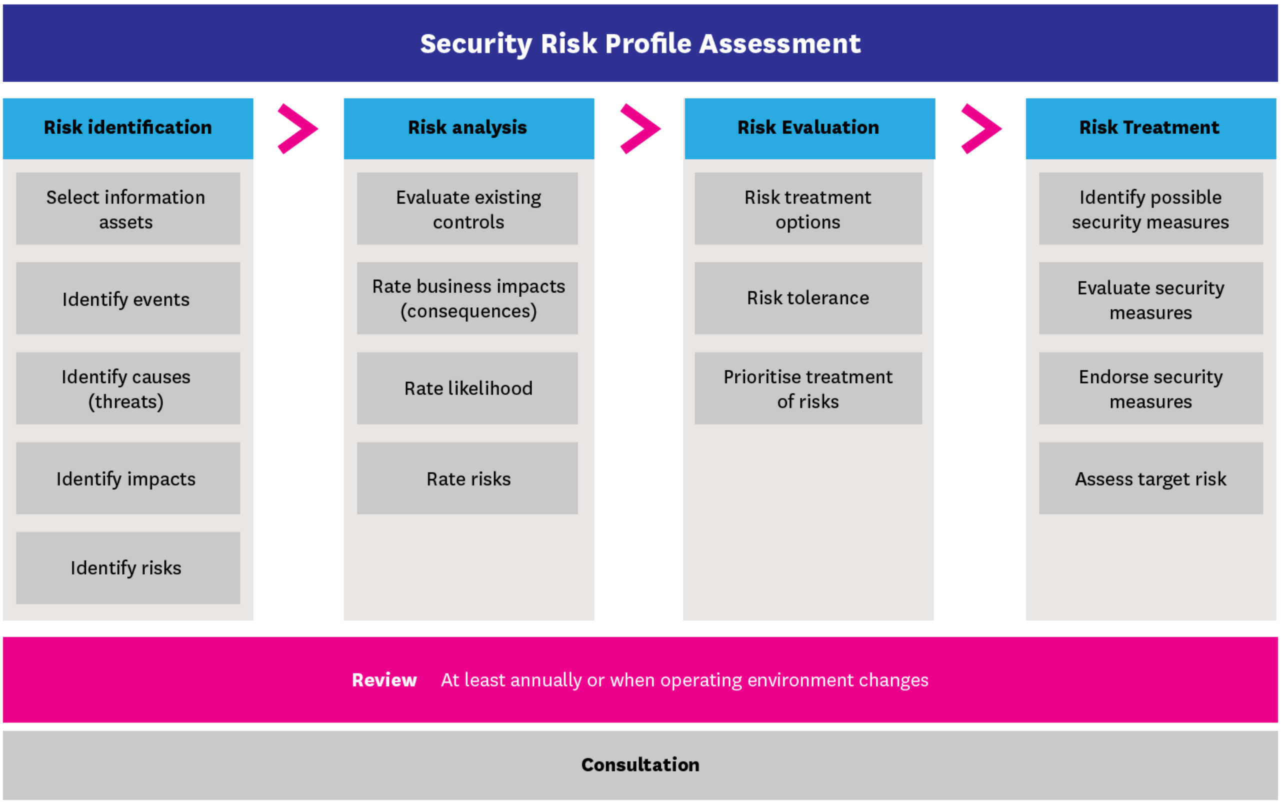
10. SRPA phases

The SRPA consists of four steps:

- risk identification;
- risk analysis;
- risk evaluation; and
- risk treatment.

These steps are detailed in Diagram 2. SRPA phases. It is important that the person undertaking the SRPA consult with all affected stakeholders at each step in the process.

[7] Refer to section 89 of the Privacy and Data Protection Act.



Security Risk Profile Assessment

Risk identification
- Select information assets
- Identify events
- Identify causes (threats)
- Identify impacts
- Identify risks

Risk analysis
- Evaluate existing controls
- Rate business impacts (consequences)
- Rate likelihood
- Rate risks

Risk Evaluation
- Risk treatment options
- Risk tolerance
- Prioritise treatment of risks

Risk Treatment
- Identify possible security measures
- Evaluate security measures
- Endorse security measures
- Assess target risk

Review At least annually or when operating environment changes

Consultation

Diagram 2. SRPA Phases

10.1. Recording risks ●

The SRPA will help you identify information security risks which should be recorded in your risk register. In order to manage security risks, some organisation have a separate register for security risks – whichever process you choose it should reflect your organisation's approach to managing categories of risk. A generic risk register template is available on the VMIA website[8]. The template should outline the minimum details to record each information security risk and should be tailored to fit your organisation's current risk management practices. The risk references in the register will also feed into your organisation's PDSP. Guidance on filling in the PDSP is contained in the PDSP form[9].

10.2. Risk identification ●

AS ISO 31000:2018 – Risk management – Guidelines defines risk as:

> *"the effect of uncertainty on objectives."*

In the context of conducting a security risk assessment (as described in this document), the objective is for organisations to ensure the confidentiality, integrity and availability of Victorian Government information.

Identifying risks, prior to implementing security controls, enables the efficient, effective and economic investment in information security. To perform this risk identification, organisations should utilise their existing processes where available.

[8] Refer to https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/risk-management-tools.

[9] Refer to the Resources published on the OVIC website https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/pdsp-submission/.

Risk identification defines the 'risk' problem and provides insight into 'uncertainty' and the probable effect on achieving the business objectives. A well-described risk will:

- provide context and meaning of the event, cause and impact for management;
- assist to direct assessments of security controls and treatment planning;
- provide meaningful information for reporting and oversight;
- reduce over or under investment in unnecessary security controls; and
- align the uncertainty to the business objective.

Recent incidents and security trends, along with results from audits, will also help to identify risks and inform your selection of security controls to best address these risks.

10.2.1. Selecting information assets

As part of undertaking a risk assessment, your organisation will need to select the information assets that become the focus of the SRPA.

Given the large number of information assets that some organisations may have, initially prioritise the security risk assessment process to critical information assets (i.e. by prioritising protecting the most valuable assets, which Step 2 of the Five Step Action Plan will identify for you). The outcomes of the security value assessment[10], will not only inform which assets to focus on but will also be used during the consequence rating activity of the risk assessment process.

Once these have been completed, it is expected that all other information assets (i.e. assessed as non-critical) are subsequently considered.

10.2.2. Identify risk events

For the purposes of the risk statement, there is only one 'risk event'. While there may be a number of 'contributing events' as a result of the way in which causes (threats) interact with your organisation's information, the 'risk event' will typically be the most significant event. This one event is likened to a 'headline' (e.g. how would it be presented if it were to be reported in the press).

Example 3. Identification of risk events

A natural weather occurrence may be the initiating cause of 'data loss' (risk event) but as a result of the weather occurrence, a lightning strike can damage power lines (event), a plant room can flood (event) and a backup generator can be submerged in water (event). All of these events can contribute to the data loss.

[10] Refer to the BIL table published on the OVIC website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/.

10.2.3. Identify risk causes (threats)

The ‘cause’ of a risk can be described as the threats or sources of risk.

Understanding the composition of causes can be useful in gaining a deeper understanding of the overall threat environment in which you operate. This knowledge will be of benefit in the later stages of a risk assessment process, particularly in establishing the likelihood of risks eventuating, security controls required, and prioritising risk treatment.

The causes of risks to information assets can come from a variety of areas and may be accidental, deliberate or natural (environmental). Broadly they fall into two categories:

- **external causes** – vectors (people, organisations, governments, etc.) outside of the organisation’s control; and
- **internal causes** – actions/ failures of people, processes or systems within the organisation.

It is helpful to identify all of the probable (not possible) risk causes to your information in each category, including the identification of the root cause (i.e. the initiator – what started it all).

A list of typical threats to information are available from *AS/NZS ISO/IEC 27005:2012 Information Technology – Security techniques – Information security risk management, Annex C.*

Possible versus Probable

It is important that during the process, organisations work on probable events, causes and impacts rather than possible. It is unrealistic to cover off all situations (possible). Organisations are far better placed to work on situations that are more likely (probable) to ensure the most effective, efficient and economic use of resources.

Perhaps an extreme example to illustrate: You could plan for a meteorite hitting your data centre, and whilst this is possible, it is not probable and you should focus on more realistic scenarios like a cyber threat (for instance).

10.2.4. Identify potential impacts

‘Impacts’ are described as the effects of the event on your organisation, government operations or individuals, if the risk event occurred.

To help your organisation identify potential impacts, refer to the impact categories from the VPDSF Business Impact Level (BIL) table[11]. Use the BIL table categories to describe the resulting impacts to government operations, organisations or individuals if there were a compromise of the confidentiality, integrity and availability of public sector information.

10.2.5. Drafting the risk statement

Once you have established the three principal elements of risk (risk event, cause and impact) you now combine them to identify the final risk statement. The process contained in example 4, provides guidance on how to construct a risk statement using the three elements.

[11] Refer to the BIL table published on the OVIC website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/.

A well-formulated risk statement is fundamental to the assessment and evaluation of risks as it documents and sets the scope of an identified risk. If you leave any aspects of the risk statement out, analysis of the risks you get back will be influenced by assumptions and may not meet the initial intent or scope you desired.

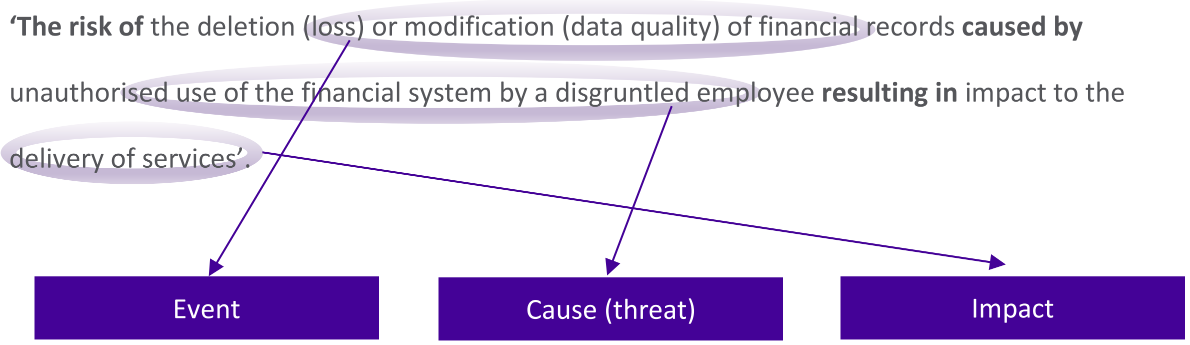
For the purposes of this document, risk will be described as:

> ‘**The risk of** ….event…. **caused by** ….how…. **resulting in** ….impact(s)…’.

Your organisation may, and can, describe risks differently – whatever form the risk statement takes, consistency is key to ensure ALL risks are understood and assessed equally.

Example 4. Risk statement

Event(s)	Deletion of financial records (availability); or Modification (integrity) of financial records
Cause (threat)	Disgruntled employee misusing resources / unauthorised use / abuse of rights
Impact	Loss of integrity and availability of information impacting on service delivery (degradation of business operations)
Risk statement	**The risk of** the deletion (loss) or modification (data quality) of financial records (events) **caused by** unauthorised use of the financial system by a disgruntled employee (cause) **resulting in** impact to the delivery of services (impacts).



‘**The risk of** the deletion (loss) or modification (data quality) of financial records **caused by** unauthorised use of the financial system by a disgruntled employee **resulting in** impact to the delivery of services’.

As a threat may have multiple probable events or vice versa, you could combine these as a single risk as above. However, it may be more beneficial to break them down into separate statements to allow each risk to be treated in its own right (as below).

Example 4 (Cont.)

Outcome: Sample risk statement(s)

1. The risk of the modification (data quality) of financial records caused by a disgruntled employee resulting in impact to service delivery.
2. The risk of the deletion (loss) of financial records caused by a disgruntled employee resulting in impact to service delivery.

Thinking of your organisation, would you treat the two sample risk statements differently or the same? This will differ organisation to organisation. The important outcome of the statement is that you treat the risk in a manner that provides you with the most assurance and is consistent with your risk management framework.

10.2.6. Introduction and overview of the 'Bowtie method' to determine risks

Organisations may gain further assistance to identify the risk elements and links between event, causes (threat) and impacts by undertaking a bowtie analysis of each risk. Diagram 3 is a sample of the bowtie method.

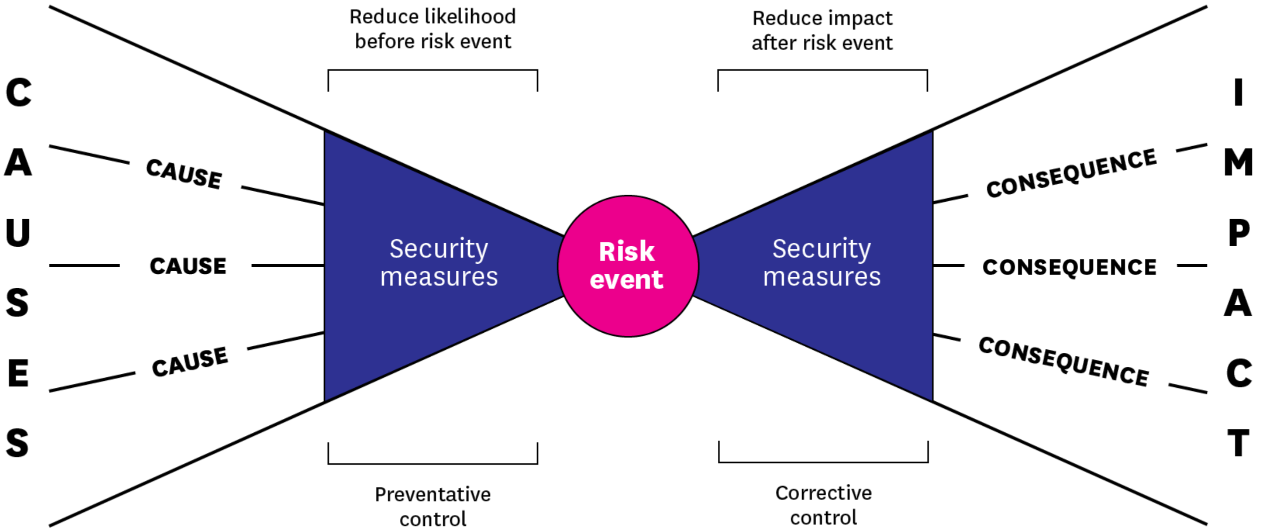


Diagram 3. Bowtie method

The first step in a bowtie analysis is understanding the 'risk event' (centre) followed by identifying the causes (threats) and impacts. A bowtie analysis will also help you identify possible root causes for risks and where in the activity any corresponding controls are needed to mitigate the risk.

The discovery of risk elements using a bowtie analysis gives great insight into selection of security controls that target all the factors contributing to the risk (i.e. preventative, detective and corrective security controls). The financial information risk in example 4 is represented using the bowtie model in Diagram 4 to enable you to visually see the risk statement.

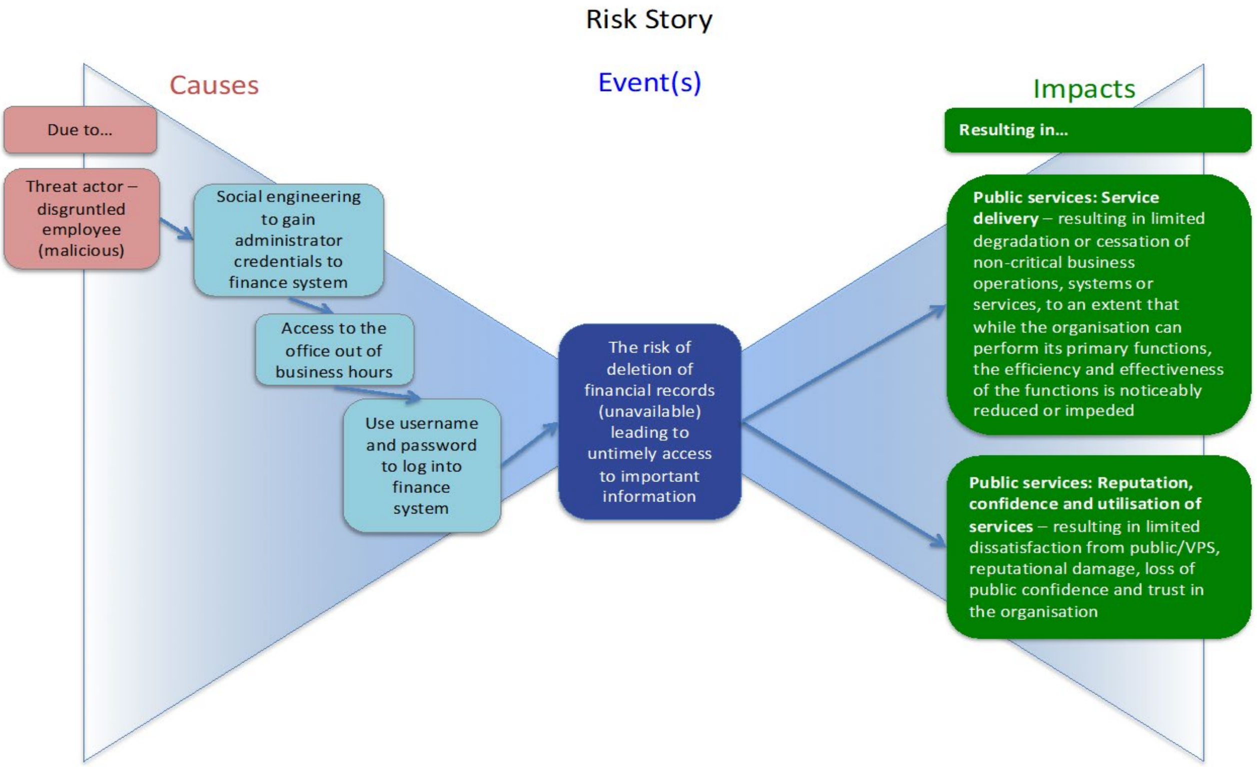

Risk Story
Causes
Event(s)
Impacts
Due to...
Threat actor – disgruntled employee (malicious)
Social engineering to gain administrator credentials to finance system
Access to the office out of business hours
Use username and password to log into finance system
The risk of deletion of financial records (unavailable) leading to untimely access to important information
Resulting in...
Public services: Service delivery – resulting in limited degradation or cessation of non-critical business operations, systems or services, to an extent that while the organisation can perform its primary functions, the efficiency and effectiveness of the functions is noticeably reduced or impeded
Public services: Reputation, confidence and utilisation of services – resulting in limited dissatisfaction from public/VPS, reputational damage, loss of public confidence and trust in the organisation

Diagram 4. Example risk using bowtie

10.3. Risk analysis ●

Risk analysis is the process of determining a rating for the level of each risk, also known as the 'risk rating'.

The analysis process is completed in four stages:

1. identification of current controls and their effectiveness;
2. assessing the business impacts (consequences);
3. considering the probability of the risk occurring (likelihood); and
4. determining the risk rating (likelihood *x* consequence).

10.3.1. Identification and effectiveness of existing security controls

The first level of risk analysis conducted during the SRPA process will identify the 'current risk rating' (i.e. consideration given to how existing security controls are operating to effectively reduce risk).

Identification of security controls currently implemented at this stage of risk analysis is imperative to rating the likelihood of a risk event occurring and the business impacts associated as a result.

Evaluation of the effectiveness of existing security controls should also be conducted prior to determining the rating of the business impacts or likelihood. Evaluation of effectiveness should be supported by audit activities and information that can be tested to confirm the effectiveness of security controls. Organisations should have their own evaluation of control effectiveness to guide the process.

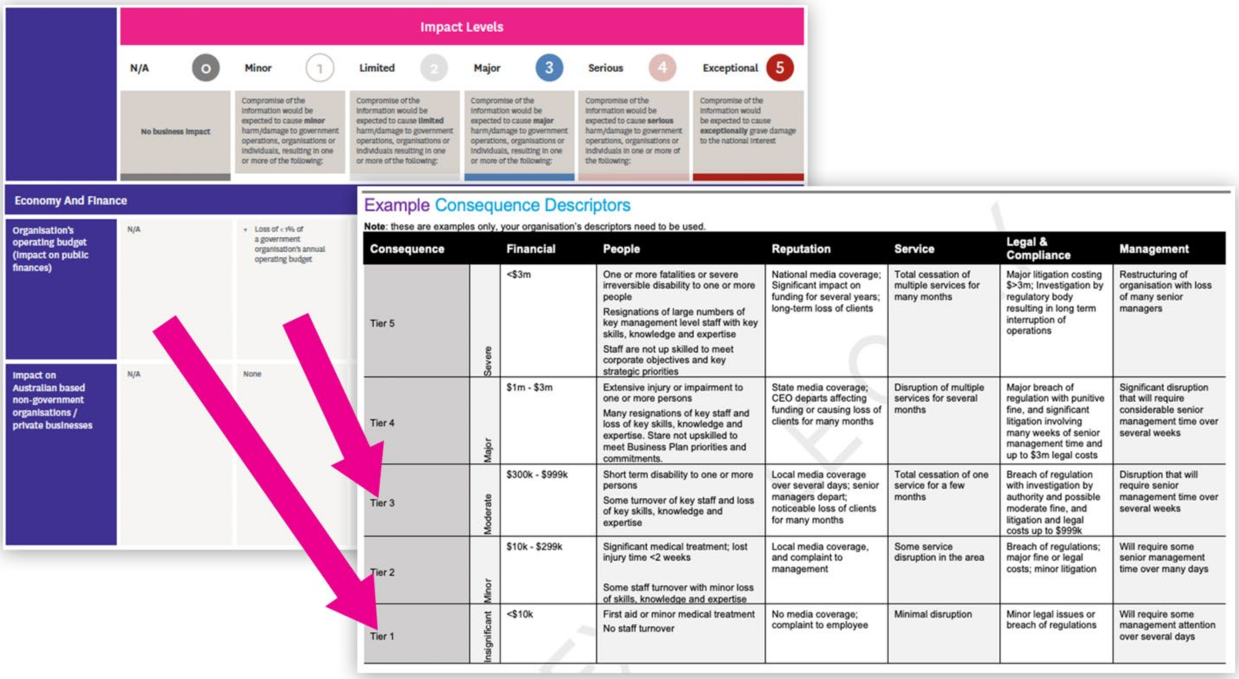
Additional advice on evaluating effectiveness of existing security controls is available from the *VGRMF Practice Guide*[12].

10.3.2. Rating business impacts (consequences)

Prior to conducting a risk assessment, organisations are required to perform a security value assessment of their information assets as per step 2 of the Five Step Action Plan. The outcome of this assessment informs the base level of protection required for this information asset and provides one part of a risk rating (i.e. likelihood x **impact (consequence)** = risk).

Assigning a security value to information assets is equivalent to rating the 'impact' (consequence) identified in a risk event. That is, once a risk event has been identified, an organisation is well positioned to understand the impact from a compromise to the information asset, as the assessment has already been conducted as part of the information security value assessment.

The organisation's BIL table can be aligned with your risk consequence ratings table. An 'indicative only' mapping is shown in Diagram 5. Alignment of BIL table and risk consequence ratings table.



Impact Levels

	N/A 0	Minor 1	Limited 2	Major 3	Serious 4	Exceptional 5
	No business impact	Compromise of the information would be expected to cause **minor** harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Compromise of the information would be expected to cause **limited** harm/damage to government operations, organisations or individuals resulting in one or more of the following:	Compromise of the information would be expected to cause **major** harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Compromise of the information would be expected to cause **serious** harm/damage to government operations, organisations or individuals in one or more of the following:	Compromise of the information would be expected to cause **exceptionally** grave damage to the national interest
Economy And Finance						
Organisation's operating budget (impact on public finances)	N/A	• Loss of < 1% of a government organisation's annual operating budget				
Impact on Australian based non-government organisations / private businesses	N/A	None				

Example Consequence Descriptors

Note: these are examples only, your organisation's descriptors need to be used.

Consequence		Financial	People	Reputation	Service	Legal & Compliance	Management
Tier 5	Severe	<$3m	One or more fatalities or severe irreversible disability to one or more people Resignations of large numbers of key management level staff with key skills, knowledge and expertise Staff are not up skilled to meet corporate objectives and key strategic priorities	National media coverage; Significant impact on funding for several years; long-term loss of clients	Total cessation of multiple services for many months	Major litigation costing $>3m; Investigation by regulatory body resulting in long term interruption of operations	Restructuring of organisation with loss of many senior managers
Tier 4	Major	$1m - $3m	Extensive injury or impairment to one or more persons Many resignations of key staff and loss of key skills, knowledge and expertise. Stare not upskilled to meet Business Plan priorities and commitments.	State media coverage; CEO departs affecting funding or causing loss of clients for many months	Disruption of multiple services for several months	Major breach of regulation with punitive fine, and significant litigation involving many weeks of senior management time and up to $3m legal costs	Significant disruption that will require considerable senior management time over several weeks
Tier 3	Moderate	$300k - $999k	Short term disability to one or more persons Some turnover of key staff and loss of key skills, knowledge and expertise	Local media coverage over several days; senior managers depart; noticeable loss of clients for many months	Total cessation of one service for a few months	Breach of regulation with investigation by authority and possible moderate fine, and litigation and legal costs up to $999k	Disruption that will require senior management time over several weeks
Tier 2	Minor	$10k - $299k	Significant medical treatment; lost injury time <2 weeks Some staff turnover with minor loss of skills, knowledge and expertise	Local media coverage, and complaint to management	Some service disruption in the area	Breach of regulations; major fine or legal costs; minor litigation	Will require some senior management time over many days
Tier 1	Insignificant	<$10k	First aid or minor medical treatment No staff turnover	No media coverage; complaint to employee	Minimal disruption	Minor legal issues or breach of regulations	Will require some management attention over several days

Diagram 5. Alignment of BIL table and risk consequence ratings table

The 'security value' of the information as derived from the BIL table will directly correspond to your risk consequence ratings table once mapping has occurred (i.e. negates the requirement to 'rate business impacts' as a stand-alone exercise).

By aligning your organisation's BIL table with the risk consequence ratings, this will not only strengthen the alignment with your internal risk management framework but will ensure the security controls used for the protection of information assets are selected in a consistent manner across your organisation and enable alignment with other internal control frameworks your organisation may be required to implement.

[12] Refer to the VGRMF Practice Guide published on the VMIA website https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/victorian-government-risk-management-framework.

10.3.3. Rating probability of the risk occurring (likelihood)

The next step is to determine the likelihood of the risk occurring. Primarily this will be achieved by reviewing the cause of the risk. You should use the likelihood rating criteria in your organisation's risk management framework.

It is worth noting that the effectiveness of any existing security controls in place may directly influence the likelihood of the risk occurring and should also be considered when determining the actual likelihood.

When determining likelihood, you should consider both previous occurrences and future considerations (e.g. the intent, motivation or the capability of human or adversarial threats)[13].

Additional guidance is available in the *VGRMF Practice Guide*[14].

Example 6. Likelihood

An organisation's threat intelligence data indicates that they could expect a malware attack against their firewall almost weekly and therefore attract an 'almost certain' rating.

When the organisation considers its existing security controls (e.g. a cloud 'Security as a Service' provider which filters and stops known malware attacks reaching the organisation's firewall), they assess the likelihood rating as 'unlikely'.

10.3.4. Rating the overall current risk

Once you have identified the business impact and likelihood rating for each risk (taking into account the existing security controls), you now need to assign an overall current risk rating.

You should use the risk ratings matrix developed in your organisation's risk management framework. If your organisation doesn't have one, you can refer to the *Risk Criteria Examples* published by VMIA under their *Risk management tools*[15].

10.4. Risk evaluation ●

After you have identified and analysed the risks to your organisation's information assets, you should evaluate which risks are rated at an acceptable level and which need to be prioritised for further action.

The evaluation of risk appetite and prioritisation is a key component in determining the next steps in implementing additional security controls in order to bring the risks to levels that are considered acceptable by your organisation.

[13] An indicative list of potential threats to information are available from *AS/NZS ISO/IEC 27005:2012 Information technology — Security techniques — Information security risk management, Annex C.*

[14] Refer to the VGRMF Practice Guide published on the VMIA website https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/victorian-government-risk-management-framework.

[15] Refer to the VMIA B2 Risk criteria examples published on the VMIA website https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/risk-management-tools.

Good governance of the identified risks becomes increasingly important at this stage and the use of your risk register is recommended to track your progress, allocate accountability and encourage a perpetual cycle of monitoring and review.

10.4.1. Risk treatment options

There are four potential options for treating each risk:

(1) **accept** – if the risk is within the risk appetite for your organisation then ongoing monitoring will be the primary requirement;

(2) **share** – parts of the risk can be shared with a third party, although overall ownership of the risk will remain with the information owner (i.e. your organisation). While this may reduce financial consequences to an organisation, it is unlikely to reduce other BIL categories;

(3) **reduce** – you can attempt to minimise the risk by introducing additional security controls to reduce the impact (consequence) and/ or likelihood of the risk; or

(4) **avoid** – if an activity produces a risk that is higher than your organisation is willing to accept and it cannot be treated by other means, you may cease that activity altogether in order to avoid the risk. However, if the function is mandated by government then this may not be possible.

You should determine which option is best for your organisation for each risk after considering your organisation’s risk appetite, tolerance and priorities.

Risk appetite is the amount and type of risk that your organisation is willing to take to achieve its business objectives. Risk appetite is set at the strategic level, it influences and guides decision-making, and will vary from organisation to organisation. Risk appetite may also vary within your organisation depending on criticality of information/ services that may be affected by the risk.

In an ideal world, the acceptable level of risk would be the lowest available rating. However, due to cost restrictions and other considerations, this may simply not be practical. When you consider what level would be acceptable for each risk, you should take into account what is reasonably practical to achieve.

If the identified risk is within your organisation’s risk appetite, the risk may be accepted.

10.4.2. Risk tolerance

The organisation’s readiness to endure the risk after risk treatment in order to achieve objectives. Risk tolerances are articulated at the operational level of an organisation because the business understands how much risk they can withstand are based on the maximum level of acceptable risk and may be expressed as a range.

The *Articulate risk appetite tolerance* document published by VMIA under their *Risk management tools*[16] includes example risk appetite and tolerance statements.

10.4.3. Prioritisation of risk treatment

To determine with what urgency you should address risks, they must first be prioritised. Risks with the highest risk rating are normally attended to first.

[16] Refer to the A6 Articulate risk appetite tolerance document published on the VMIA website https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/risk-management-tools.

Your organisation may choose to identify a default level at which risks rated above this level must be attended to more urgently and where increasingly more senior levels of management need to be kept up-to-date on progress. For example, internal standards may state that risks rated as ‘high’ or ‘very high’ must be addressed immediately with the organisation’s most senior person or body notified whereas risks rated at ‘medium’ require action at the local level.

With the risks grouped according to their risk rating, further criteria now needs to be considered in order to prioritise them further. Typically, additional considerations may include:

- safety – what are the implications if the risk is not addressed?
- cost – how much will it cost to reduce the risk (and will the benefits outweigh the expenditure)?
- reputation – what is the likely effect on reputation if the risk is not treated?
- legal obligations – is the organisation likely to be unable to meet its legal obligations if the risk is left in its current state?
- occurrence – which risks are more likely to occur?

Example 7. Prioritisation of risk

An organisation has rated three risks:

SECRISK01. The risk of disclosure of personal address information caused by disgruntled customer resulting in personal serious injury due to assault of personnel: ‘high’

SECRISK02. The risk of disclosure of critical asset location information leading to vandalism of assets caused by malicious contractor resulting in service delivery outage: ‘high’

SECRISK03. The risk of failure of the Client Relationship Management system database caused by natural event (power outage) resulting in personal stress related injuries due to verbal abuse of call centre staff from customers: ‘medium’

With risks first prioritised by rating, the organisation considers safety to be its priority so the assault related risk is ranked first, with the vandalism related risk ranked second and the call centre risk ranked third.

10.5. Risk treatment (security controls selection). ○

For risks identified as being beyond your organisation’s risk appetite, apply additional security controls in order to reduce risks.

A list of high-level security measures called the VPDSS Elements have been derived from the ‘primary sources’ listed within the VPDSS Implementation Guide[17]. Organisations should implement specific controls appropriate to their organisation considering:

[17] Refer to the VPDSS Implementation Guide https://ovic.vic.gov.au/data-protection/standards/.

- their internal and external context;
- the security value of the information; and
- associated risks.

The selection of these elements (or granular controls) will form your internal control library and will also enable you to fill in your PDSP.

10.5.1. Identifying possible security controls

When selecting security controls to mitigate risks, consider the most effective, efficient and economic use of your budget. The grouping of like risks, or risks from similar threats, even when they have different ratings, may allow you to achieve better value for money.

Identify a range of security controls that when used singularly or in combination will allow you to mitigate the risks to an acceptable level. Additionally, when selecting a range of security controls, not all controls should be of a technical nature, and may also relate to processes and people. Consider selecting controls across all the security areas (governance, information, personnel, Information Communications Technology (ICT), and physical).

Security controls should also provide ‘defence-in-depth’ (i.e. a number of controls may provide overlapping risk mitigation which can provide some surety if one control fails).

10.5.2. Evaluating security controls

Prior to selecting any security controls, you should develop outcome-focused selection criteria that clearly define what risk mitigation you are trying to achieve. In order to ensure that the security controls are fit for purpose the relevant stakeholders including information owners or business areas should be consulted in the development of the selection criteria. The risk mitigation may be a reduction in business impact, likelihood or perhaps both.

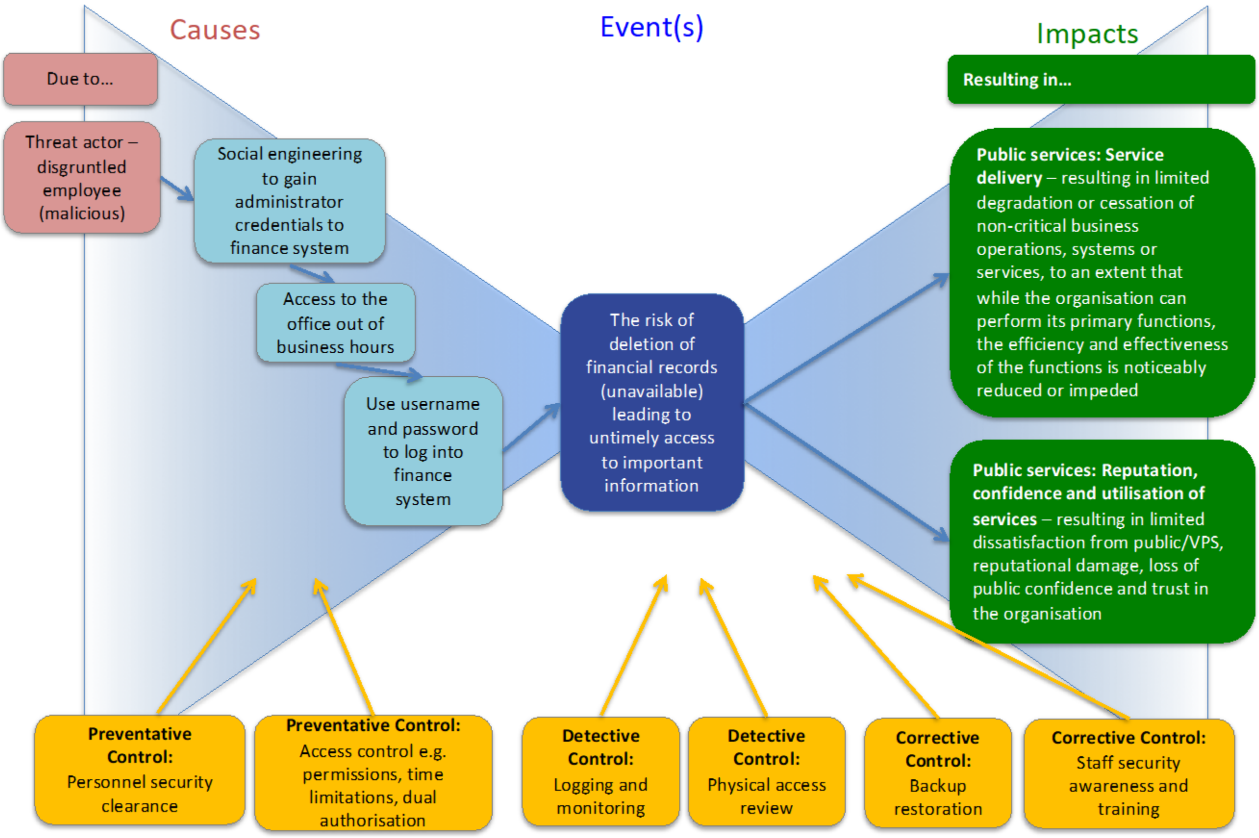
For instance, it may be possible for you to lower the business impact from a risk event by separating information into multiple repositories, thereby limiting the amount of information that can be compromised. This control could lower the overall impact of an information security incident if it were to occur.

It is more probable that you could select security controls that lower the likelihood of a compromise to your information assets.

Security controls, or groups of controls, that lower the likelihood of compromise of information are ideal, as they will give the greatest overall reduction to achieve the desired target risk.

Consider using the bowtie model to visualise the controls. Although applying controls will generally assist to modify the risk, you may find preventative controls are more effective as they prevent the risk event from occurring in the first place. Example controls to mitigate the financial information risk in Example 4 are represented using the bowtie model in Diagram 5 to enable you to visually see where the controls sit with respect to the risk statement. Some controls (e.g. staff training and awareness), may be both a preventative and corrective control.

Risk Story


Causes
Event(s)
Impacts
Due to…
Threat actor – disgruntled employee (malicious)
Social engineering to gain administrator credentials to finance system
Access to the office out of business hours
Use username and password to log into finance system
The risk of deletion of financial records (unavailable) leading to untimely access to important information
Resulting in…
Public services: Service delivery – resulting in limited degradation or cessation of non-critical business operations, systems or services, to an extent that while the organisation can perform its primary functions, the efficiency and effectiveness of the functions is noticeably reduced or impeded
Public services: Reputation, confidence and utilisation of services – resulting in limited dissatisfaction from public/VPS, reputational damage, loss of public confidence and trust in the organisation
Preventative Control: Personnel security clearance
Preventative Control: Access control e.g. permissions, time limitations, dual authorisation
Detective Control: Logging and monitoring
Detective Control: Physical access review
Corrective Control: Backup restoration
Corrective Control: Staff security awareness and training

10.5.3. Endorsing selection of controls

Seek senior management endorsement for the selected security controls, as they will have initial and ongoing management implications for your organisation.

It may be useful to undertake a cost benefit analysis of the selected security controls to support your submission to senior management.

The controls are more likely to receive endorsement if you can demonstrate that your selected security controls not only reduce the risk to an acceptable level (where possible) and meet the business needs of your organisation, but also provide other benefits to your organisation or improvements to business processes.

10.5.4. Determining target risk ratings

Once your organisation has determined its risk treatment(s) options, identified possible security controls, and selected the most appropriate security controls to treat the risk, they can now reassess the original risk rating by reconsidering the likelihood and impact (consequence) of the risk eventuating given the new security controls and record the target[18] risk rating.

[18] Term as used by VMIA. Some organisations may also use the term residual in their risk management framework or refer to 'resulting risk' as per AS ISO 31000.

11. Ongoing maintenance ●

11.1. Review of the register

All risks identified as part of the SRPA are subject to ongoing monitoring and review. The frequency and depth of attention you give each risk should reflect its rating and priority.

Review risks if there are any changes to your organisation's operating environment as these changes may impact the existing risks, introduce new risks or change the criticality of your assets.

11.2. Risk ownership

If your organisation has not already done so, allocate an owner to each identified security risk to ensure it is reviewed with an appropriate frequency and that any additional actions and controls identified are undertaken within a designated timeframe.

In most circumstances the information owner/ custodian could be the risk owner, as they are most likely to be aware of changes to the threat environment of the asset. However, for higher risks to critical information assets it may be more appropriate to assign a senior officer as the risk owner to ensure the risk receives the level of oversight commensurate with the risk to your organisation.

11.3. Review of the SRPA process

The overall owner of the SRPA is the public sector body Head. The Head may delegate the management of the SRPA to a senior officer who should be independent of the information owners to ensure all risks to information are given appropriate priority.

As part of continuous improvement, the SRPA process should be regularly reviewed (e.g. annually, upon significant change) to ensure it is fit for purpose and aligned with your organisation's risk management framework.