Office of the Victorian Information Commissioner

PRACTITIONER GUIDE:
Control Analytics

Version 1.0 APRIL 2022

Freedom of Information | Privacy | Data Protection

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne Victoria 3001
First published April 2022
Also published on: https://ovic.vic.gov.au
ISBN

Practitioner Guide Details

Control Analytics	
Protective Marking	OFFICIAL
Approved for unlimited public release	*Yes – Authorised for release*
Release Date	April 2022
Review Date	April 2022
Document Version	1.0
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

Table of Contents

1 Introduction

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

This document is part of supporting security guides of the VPDSF and VPDSS and helps the organisation's approach to information security risk management. The guide complements existing activities within the organisation's enterprise risk management framework and assists completing Step 4 of the Five Step action plan[1].

Control analytics helps organisations validate the appropriateness and effectiveness of selected controls and manage security risks, providing a method for evaluating controls improvements aligned with the organisation's risk management framework.

2 Purpose

This document provides guidance on analysing the effectiveness of an organisation's existing controls as well as control improvements including uplifting existing controls and/ or analysing new treatments to mitigate information security risks. This document provides a quantitative way to assess controls to enable organisations to conduct a cost benefit analysis of control implementation aligned to the organisation's risk appetite.

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 Four of the Privacy and Data Protection Act (2014) (**PDP Act**).

This guide assumes a foundational level of security risk management knowledge and is designed to support practitioners, risk professionals and personnel responsible for testing and validating controls.

4 Use of specific terms in this document

Please refer to the *VPDSS Glossary*[2] for an outline of terms and associated definitions. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

In addition, the following terms are relevant and used throughout this document.

[1] Refer to the Five Step Action Plan - Office of the Victorian Information Commissioner (ovic.vic.gov.au)

[2] Refer to OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

Term	Description
Control analytics	An approach that analyses the appropriateness and effectiveness of existing controls, as well as the prioritisation of planned controls (treatments), to reduce risk to a target level.
Data point	Input that can be sourced either directly from the organisation and/ or externally that supports the analysis of risk and controls.
Likelihood	The rating, derived from the frequency of the risk event, multiplied by the susceptibility rating.
Primary impact	The business impact(s) directly incurred by the organisation when a risk is realised. These are referred to as primary because the organisation is the primary stakeholder.
Proxy data	When a data point cannot be obtained directly from the organisation, it is possible to use a substitute data point (proxy) that is either derived from industry peer research or other external bench marking sources. Also called reference data.
Resistance strength	The cumulative efficacy of a supporting asset's controls (expressed as percentages) to protect against a given threat. For example, if an organisation believes its controls are sufficient to successfully defend against the average cybercriminal but not a skilled cybercriminal, its resistance strength estimate may be around 40-70%.
Risk buy down	The amount of risk reduction achieved (expressed in dollar ($) terms), against a given spend in controls and capability uplift.
Risk event	Event that occurs as a result of a successful threat event/ cause on an information asset or supporting asset (information system).
Secondary impact	The flow on, or subsequent, business impact when a risk is realised. These impacts are referred to as secondary because they manifest due to the actions and reactions of secondary stakeholders such as citizens, clients, media, government/ regulatory bodies, contractual third parties. Depending on how a risk is managed, there may not always be a secondary impact.

Term	Description
Supporting asset(s)	The system(s) or other asset(s) that the information asset relies / depends on.
Susceptibility rating	Also called "vulnerability" under the FAIR model[3], a percentage-based ranking (typically derived by considering the threat capability and resistance strength) on how vulnerable an information asset or supporting assets may be to the risk event.
Impact	The sum (**+**) of both the primary and secondary impacts.
Threat capability	Represents the comparative place on the threat capability continuum (expressed as percentages) that the organisation believes the in-scope threat community resides. Each threat community (e.g., nation state sponsored hackers, script kiddies) falls in a range of values along the spectrum.
Threat event/ cause	An occurrence, activity, or situation where the threat source performs an act against an asset (typically via the supporting asset(s)) that could result in compromise or loss.
Threat source/ actor	A person, group of people, force of nature, piece of self-executing code etc that acts against an asset that causes compromise or loss. Threat sources are active entities and not passive control conditions.

5 Scope

The activities in this document are designed to help organisations decide the appropriateness and effectiveness of existing controls, as well as the prioritisation of future controls.

Suggested activities are not intended to replace existing control assurance activities (e.g., existing control maturity assessments, internal audit) but supplement and provide additional confidence on the suitability and effectiveness of a control, needed to appropriately reduce risk to a target level.

This document is not intended to explain the foundational concepts of information security risk management should be used with OVIC's *Practitioner Guide: Information Security Risk Management*[4] and VMIA's *High-level Control Effectiveness Guide*[5]. Additionally, the content in this document aligns to the *Victorian Government Risk Management Framework* (**VGRMF**)[6] and the supplemental VMIA *Risk Criteria*

[3] Refer to the FAIR Institute website https://www.fairinstitute.org/blog/fair-risk-terminology-vulnerability-is-susceptibility-the-open-group-says

[4] Refer to OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

[5] Refer to VMIA's website https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/control-effectiveness

[6] Refer to the Department of Treasury and Finance website https://www.dtf.vic.gov.au/planning-budgeting-and-financial-

Examples[7] document.

6 Assumptions

To use this guide the most effectively, your organisation has:

- Identified its information assets and recorded these in an Information Asset Register (**IAR**) (including assessing and recording the security value of the information, using the Business Impact Levels (**BILs**))[8];
- Identified the relevant risks to these information assets and recorded them in an appropriate register[9];
- Mapped the VPDSS Elements (or specific controls based on the VPDSS Elements) to these risks;
- Internal assurance processes relating to control testing; and
- Data points that can be used to determine the likelihood and impact of risk.

reporting-frameworks/victorian-risk-management-framework-and-insurance-management-policy

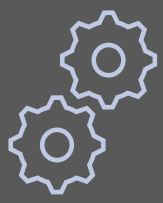
[7] Refer to VMIA's website https://www.vmia.vic.gov.au/tools-and-insights/risk-management-tools

[8] Refer to Steps 1 and 2 of the Five Step Action Plan on OVIC's website https://ovic.vic.gov.au/data-protection/information-security-resources/

[9] Refer to Steps 3 of the Five Step Action Plan on OVIC's website https://ovic.vic.gov.au/data-protection/information-security-resources/

7 Overview

This practitioner guide is organised into the following parts:



Part One - The fundamentals of control analytics

An explanation of control analytics and background information regarding this approach and how to use it.

Part Two - Template for the application of control analytics

A sample template that can be used to fast track the use of control analytics in your environment, to determine the suitability and effectiveness of controls.

Part Three - Control analytics examples

Three examples (based on the previously published OVIC Risk Scenarios[9]), using the template supplied in this guide.

Part Four - Appendix

The appendix includes a chart that maps the VPDSS Elements to their respective control type (this may also depend on how controls have been defined in your organisation) and provides links to further reading.

Footnote[10]

[10] Refer to the Risk Scenarios on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

8 Part One – The fundamentals of control analytics

8.1 Control analytics explained

Risk assessments are inherently subjective. They are shaped by the approach or methodology used, the data relied upon, and the skills and expertise of those involved in the assessment process. Under the VPDSS, organisations have autonomy and flexibility on how risk assessments are conducted, utilising their own risk management framework.

Despite the imprecise nature of risk assessments, organisations should strive for the consistent (reproducible and repeatable) assessment of risks. By adopting a structured approach, organisations can benefit from a holistic and balanced approach to the identification, estimation, and prioritisation of risk to their business operations, regardless of the methods used or individuals involved.

Control analytics is a data driven (quantitative) and structured method for risk analysis. It uses accepted organisational risk statements and structures them in a way that the risk factors (those that make up the likelihood and impact) are analysed from a financial perspective. By structuring risk assessments in this manner, those involved in the process gain a better understanding of how certain controls help manage risks, and , whether these controls are having the intended effect. Assessing and articulating impacts in financial terms adds benefit of being readily accessible to decision makers.

Most VPS organisations align their risk management practices with the VGRMF which refers to standard risk matrices (4 x 4, or 5 x 5) and guiding tables. Organisations using these risk management tools (matrices and tables) may encounter the following challenges:

- ambiguous or arbitrary criteria to determine likelihood and impact
- a limited data driven view of what makes up the likelihood and impact
- inadequate input from all relevant stakeholders when selecting the likelihood and impact, and
- limited understanding of the effect of controls (individually or collectively).

In this document, the process of framing and assessing a risk statement in an appropriate structure is referred to as a "risk story"[11].

Further information about structuring a risk statement into a risk story can be found in OVIC's *Practitioner Guide: Information Security Risk Management*[12].

The control analytics process in this guide establishes the risk story and determines the effect of existing and proposed controls, using a systematic approach. This approach involves four main steps, supported by supplementary actions -

[11] Also referred to as 'Risk Statement' in VMIA documentation

[12] Refer to the *Practitioner Guide: Information Security Risk Management* on the OVIC website https://ovic.vic.gov.au/data-protection/information-security-resources/

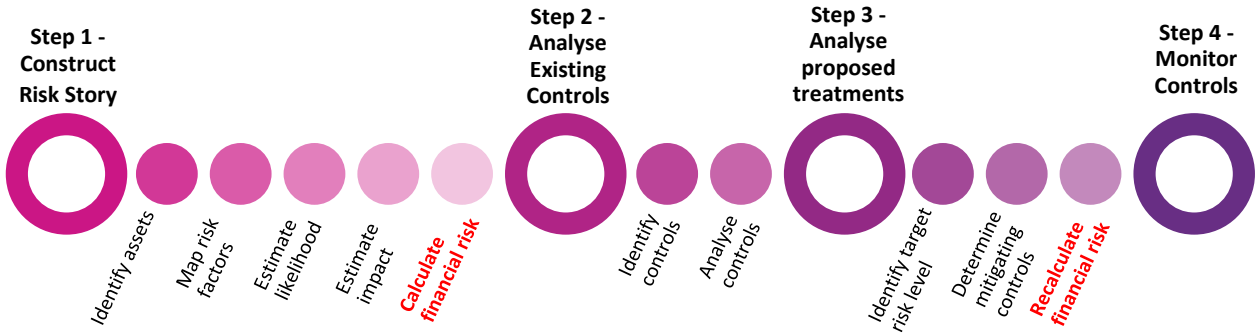


Figure 1 Control analytics process

***N.B**. A copy of this graphic is positioned in the top right-hand corner of each page header within Part One of this practitioner guide. The graphic will adjust, depending on which control analytics step or action it is referring to. Large circles represent the four major steps, and smaller circles represent the supplementary actions. Simply refer to the graphic in the page header, to determine where you are in the risk analysis journey.*

8.2 Step 1 – Constructing the risk story

A risk story takes an organisation's existing risk statement and structures to allow the critical analysis of its individual parts (risk factors). By doing so, an organisation will have further clarity of the actual risk in financial terms, as it:

- identifies the relationship between all the risk factors that make up "likelihood" and "impact", and
- sets out the data points (evidence based) that support the assessment.

There are five supplementary actions (Figure 2) to perform, when constructing a risk story.

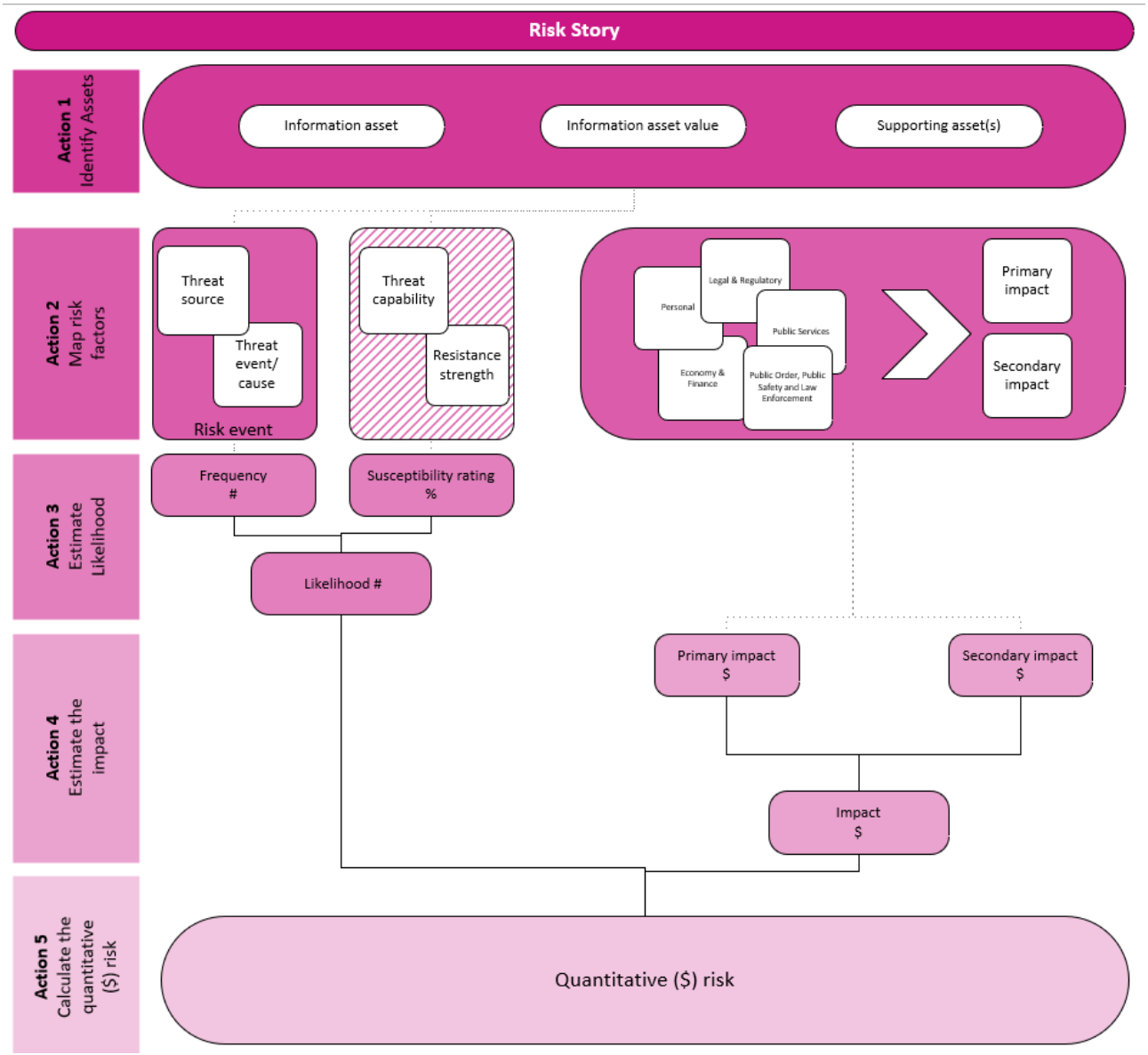


Figure 2 Constructing the risk story

8.2.1 Step 1: Action 1 – Identify the information asset components

Foundational activities need to be done to build a risk story. These activities are essential building blocks in developing a robust information security work program. OVIC's website has guidance material instructing organisations on how to complete the following activities.

Activity	Description	Examples of source material
Identify the information asset[13]	This is the information asset you are protecting.	• Risk statement[14] • Information Asset Register (IAR)[15]
Identify the protective marking of the information asset	The protective marking assigned to the information asset. Protective markings are linked to an assessment of the compromise of the confidentiality of the information asset.	• IAR • Information owner[16]
Identify the overall security value of the information asset[17]	This is sometimes referred to as the Business Impact Level (**BIL**) of the information asset. By understanding the security value of the information asset, an organisation is well placed to apply appropriate controls. The security value of the information asset considers the confidentiality, integrity, and availability impacts if the information asset was compromised. Note: This may be different from the protective marking assigned to an information asset.	• IAR • BIL table[18]

[13] Refer to the *Practitioner Guide: Identifying Information Assets* on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

[14] For help in constructing a risk statement, refer to the *Practitioner Guide – Information Security Risk Management* on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

[15] Refer to your organisation's Information Asset Register (**IAR**) or the IAR resources published on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

[16] For further guidance on information management roles, refer to the *Practitioner Guide: Identifying Information Assets* on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

[17] Refer to the *Practitioner Guide: Assessing the Security Value of Public Sector Information* on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

[18] Refer to your organisation's Business Impact Level (**BIL**) table or the *VPDSF BIL table* on OVIC's website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

Activity	Description	Examples of source material
Identify supporting asset(s)	Supporting assets provide another avenue for access to the information. Typically, these are identified as system(s) for the transmission, processing and/ or storage of the information asset).	• IAR • Asset register • Systems architecture

8.2.2 Step 1: Action 2 – Map the risk factors (threat source, threat event(s) / cause(s) and impact(s))

Activity	Description	Examples of source material
Identify threat source (actor)	By identifying a threat source, an organisation is best placed to implement appropriate controls. NIST characterises a threat source by: (i) the intent and method targeted at the exploitation of a vulnerability; or (ii) a situation and method that may accidentally exploit a vulnerability In general, a threat source[19] may be: • **adversarial** (e.g., individual, group, organisation, nation state) • **accidental** (e.g., user, administrator) • **structural** (e.g., environment controls, IT equipment, software) or • **natural** (e.g., environmental – fire, flood, earthquake)	• Existing risk statement • Internal risk group • Any historical information from incident registers • NIST Special Publication 800-30 Guide for conducting risk assessments (Appendix D Threat sources) • Public threat landscape reports • Associated professional bodies that an organisation may be subscribed to (e.g. AusCERT)

[19] As derived from NIST Special Publication 800-30 (Appendix D Threat sources). Equally valid are the sources outlined in the VPDSS *Practitioner Guide: Information Security Risk Management* (accidental, malicious or natural)

Activity	Description	Examples of source material
Identify cause(s) / threat event	A threat source initiates a threat event. A threat event is an occurrence, activity or situation that has the potential for causing undesirable consequences or adverse impacts. These events can be expressed as tactics, techniques and/or procedures (e.g., performing perimeter network reconnaissance/ scanning, conducting outsider-based social engineering to obtain information).	• Existing risk statement • Internal risk group • Any historical information from incident registers • NIST Special Publication 800-30 Guide for conducting risk assessments (Appendix E Threat events) • Public threat landscape reports • Associated professional bodies that an organization may be subscribed to (e.g. AusCERT)
Determine risk event	This is the result of a threat source successfully initiating a threat event on the information asset or supporting asset.	• Threat source • Threat event

Activity	Description	Examples of source material
Identify impact(s)	To conduct a risk assessment, organisations need to have a solid understanding of the impact(s) if there was a compromise to the asset or supporting asset(s). Following a risk event, organisations should reference the results from the information security value assessment, to help articulate the impact to operations, organisations, or individuals. The BIL table provides a standardised structure for understanding and articulating various impact categories, spanning topics such as legal and regulatory, personal, public services, etc. Impacts comprise of two types of loss, either primary or secondary: 1. **Primary impact**: The direct financial ($) impact incurred by the organisation at the time of the risk event. For example, a service delivery/ productivity impact. 2. **Secondary impact**: This impact typically occurs as a 'flow on' effect from the primary impact. For example, legal and regulatory/ fines/ reputation impacts that follow the primary impact of service delivery interruptions or cessation. Depending on how a risk is managed, there may not always be a secondary impact.	• Existing risk statement • Existing BIL assessments • Risk consequence table • BIL table • NIST Special Publication 800-30 Guide for conducting risk assessments (Appendix H Impact)

8.2.3 Step 1: Action 3 – Estimate the likelihood of the risk

Once actions 1 and 2 of the risk story have been done, a deeper analysis can be undertaken to decide the likelihood of the 'risk' (threat source, threat event, threat capability, resistance strength) occurring. A data informed approach should be used to support assumptions and understandings that make up the determining of likelihood.

Data points are often available to draw from in an organisation and can be obtained by engaging with relevant stakeholders for example information owners, incident managers, risk practitioners, IT. If these are not available, then "proxy data" (e.g., open-source research data based on organisations of similar size and complexity) can be used instead. Also, security intelligence reports that provide a view can be used. For example, for cyber risks, guidance or reference data may also be available from the Department of Premier and Cabinet's Cyber Safety Unit (**CSU**) based on the cyber incidents they have seen across the Victorian Government.

In a risk story, the likelihood assessment is made up of two measurements:

- the **frequency** of the defined risk event; and
- the **susceptibility** of the supporting asset(s).

By using these two primary measurements, a more data centric approach can be used to analyse the likelihood of a risk event exploiting a vulnerability.

Activity	Description	Examples of data points
Estimate the frequency (#) of the risk event	To estimate the frequency of the risk event, consider the likelihood of the threat event occurring. This can be measured in any time unit. For example, the threat of targeted phishing emails being clicked on by users can be measured monthly (by the number of users). For the benefit of consistency when calculating the frequency, it is typically helpful to derive a **per annum** expression of this frequency to enable comparison and prioritisation of risks. This frequency can also be expressed as a range (e.g., 2 - 4 times a year).	For the targeted phishing example, it is possible to obtain data from actual incident data collected by the organisation or through commonly used phishing simulation activities (as part of user awareness and training programs).

Activity	Description	Examples of data points
Estimate the susceptibility (%) of the supporting asset(s)	The susceptibility of the supporting asset(s) refers to how likely it would be for the threat event to be successful (i.e., achieving its objective against the targeted information asset or information system). In some risk literature[20], this concept may also be referred to as how "vulnerable" the supporting asset is e.g., 90% vulnerability rate (as distinct to what "vulnerabilities" the asset has). The level of susceptibility is expressed as a probability percentage range: • **Low** (1%-33%) • **Moderate** (34%-66%) or • **High** (67%-99%).	Susceptibility table (sample provided in Part One of this guide titled 8.6 Supporting Information.) Although not detailed in this document, some mature organisations may derive the susceptibility by considering the **threat capability** and **resistance strength**
Estimate the Likelihood	The likelihood represents a simplistic value of the overall likelihood of the risk eventuating. Frequency of the risk event (#) multiplied by the susceptibility of the supporting assets (%). **Likelihood = frequency x susceptibility** For example: A risk event occurs four (4) times per annum and is 90% likely to be effective (4 **x** 90% = 3.6). This would mean the likelihood would be 3.6 times per annum. The value can then be mapped back into the corresponding likelihood value according to the organisation's risk likelihood table.	Likelihood table (sample provided in 8.6 Supporting Information.)

[20] Refer to the FAIR Institute website https://www.fairinstitute.org/blog/fair-risk-terminology-vulnerability-is-susceptibility-the-open-group-says

8.2.4 Step 1: Action 4 – Estimate the impact of the risk

In action 2, the risk impacts were identified (e.g., primary impact of service delivery and secondary impact of legal and regulatory). To quantify these impacts, a financial indicator ($) can be used. By using a financial lens to describe the impact, non-risk educated stakeholders may be able to understand the impact of an adverse outcome and prompt the organisation to explore further questions like "what would this risk actually cost us?" In addition to this, quantifying the risk also provides more robust estimations to help determine the probable impact to the business.

In this action all the business impacts previously identified in action 2 are translated into a financial value ($).

The derived financial impact of the risk is on a "per event" basis. The impacts can also be expressed as ranges.

As described in action 2, the risk story structures the risk into two types of impacts:

- Primary impact; and
- Secondary impact.

Activity	Description	Examples of data points
Estimate the primary impact ($)	Calculate the primary impact ($) incurred by the organisation at the time of the risk event.	Incident response costs Productivity impact of people reliant on the information asset or information system Replacement costs associated with replacing or repairing lost or damaged assets
Estimate the secondary impact ($)	Calculate the secondary impact ($) ('flow on' effect) if any.	Costs associated with reputational impact (e.g., losing customers, insurance premium increases) Legal and regulatory recourse (e.g., legal action by citizens, fines).
Estimate the impact ($)	The impact refers to the sum of the primary impact and the secondary impact to arrive at a total financial impact value for a single risk event. **Impact ($) = primary impact + secondary impact**	Estimates taken from primary and secondary impacts (if any).

8.2.5 Step 1: Action 5 - Calculate the annualised financial risk

In action 4, the impact was calculated, using estimations of the primary and secondary financial impacts of a risk event. Using the impact figure, now calculate the annualised financial risk. By expressing this figure in a per annum format, organisations can better plan and budget accordingly.

Activity	Description	Examples of data points
Calculate annualised financial risk	The annualised financial risk is a multiplier of the likelihood (action 3) by the impact (action 4). **Annualised financial risk = likelihood x impact** For example, if the likelihood was estimated as 3.6 times per annum, and the total impact is $500,000, then the annualised financial risk would be calculated as $1.8M per annum (3.6 **x** $500,000 = $1.8M).	Outcome of actions 3 and 4

8.2.6 Mapping the outcomes of the risk story to an organisations' risk matrix

The outcomes of actions 1-5 of this guide help construct a risk story that can be effectively analysed, and easily mapped back to an organisation's risk matrix. As all the impacts have been translated into a financial value, the next step is to refer to the organisation's financial impact category ratings when mapping the outcomes of the risk story.

The following activities refer to the example data listed in section 8.2.5 of this guide.

Activity	Outcome	Mapping exercise	Result
Action 3 - Likelihood	3.6 times per year	Section 8.6 Supporting Information - Likelihood table (with added frequency guide)	Tier 3 - Possible
Action 5 – Annualised financial risk	$1,800,000	Section 8.6 Supporting Information - Consequence table	Tier 4 - Major
Determine organisation risk rating	-	The intersection of "Possible" and "Major" as shown in the table below	High

Based on outcomes from this risk calculation, a risk rating can then be assigned to the risk, in alignment with an organisational risk rating table. In the above example, the risk would be rated as **High** as the intersection of **Possible** and **Major** is **High**.

		Impact/ Consequence				
		1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Severe**
Likelihood	**5 Almost certain**	Medium	High	Extreme	Extreme	Extreme
	4 Likely	Medium	Medium	High	Extreme	Extreme
	3 Possible	Low	Low	Medium	High	Extreme
	2 Unlikely	Low	Low	Medium	Medium	High
	1 Rare	Low	Low	Low	Medium	High

8.3 Step 2 – Categorise and analyse existing controls

Once the risk story has been framed, the risk can now be assessed by categorising and analysing existing controls across specific areas of the risk story. This assessment assists in determining:

- the specific risk management function of the control (i.e., preventive, detective, or corrective control type), and
- whether the control is appropriate and operating effectively.

Controls can be broadly categorised into the following three control types:

1. ***Preventive***: Within a risk story, preventive controls have a direct effect on the reduction of likelihood. There are distinct types of preventive controls. Those that:
    - deter or avoid a threat event from occurring (referred to as *avoidance* controls), or
    - enhance the protection of systems (referred to as *protection* controls).

    For example, in a phishing scenario, user awareness and training would be referred to as an avoidance control as it educates the user to not "click the link" and therefore, avoids the threat event from occurring.

    If a user happens to click on the link, then an advanced malware protection control that prevents the end user device from being infected would be an example of a protective control.

2. ***Detective***: Within a risk story, detective controls can, in many instances, provide a reduction in both likelihood and impact. Impact reduction is achieved through timely detection and ability to respond to a threat event occurring. This minimises the primary impact of a risk, and if addressed swiftly enough, may reduce the likelihood of a secondary impact occurring. At the same time, a detective control can also function in a preventive mode.

    For example, a security camera that is clearly visible not only captures a potential threat, but it can also deter a potential threat source from taking action (*avoidance* control).

3. ***Corrective***: Corrective controls have a direct effect in reducing the primary and secondary impact of a risk. Some corrective controls focus on specific areas of impact.

    For example, crisis management (which may include public relations) generally reduce secondary impacts on a risk, while controls such as IT disaster recovery and restoring from backups may provide a stronger reduction in primary impact (e.g., minimising system downtime and productivity loss).

Part Four - Appendix provides a table categorising the current VPDSS 2.0 Elements to their associated control types.

It is important to note that not all controls are equally effective for different risk stories. The effectiveness of a control depends on several factors including:

- the type of control,
- the maturity of the control,
- how it has been designed, and
- whether it is operating as intended.

When analysing the effectiveness of a control, all measures need to be considered collectively, with respect to the risk story.

For example, even if a control is rated at a high level of maturity (e.g., Level 4 – *Managed*[21]), it may not necessarily reduce the risk.

A case in point – A Security Information and Event Management (**SIEM**) solution which alerts when events are detected, is rated as *Managed*. This rating is based on the understanding that the SIEM solution is outsourced to a service provider who provides 24 x 7 monitoring and rapid response, based on their standard library of use cases.

However, if the control (the SIEM) was implemented to mitigate a risk related to an internal threat source and it did not include a predefined use case which identifies inappropriate usage of data by a privileged internal threat source, then even at a high level of maturity (such as Level 4 - *Managed*), the control would not be deemed to be as effective, as it was unable to adequately address the risk.

To effectively categorise and analyse existing controls, complete the following two actions.

8.3.1 Step 2: Action 1 – Conduct an inventory of existing controls

Identify and categorise the controls that relate to the risk story.

Activity	Description	Examples of source material
Create a list of all existing controls	Compile a list of controls (e.g., VPDSS Element Reference ID) that have been implemented to manage the risk including a description, and the relevant control type category (preventive, detective, corrective).	Supporting material to the risk statement. Workshops with information and system owners to identify and inventory controls. VPDSS elements Organisation's control library

8.3.2 Step 2: Action 2 – Conduct an analysis of existing controls

When existing controls have been categorised and included into the risk story, assess the effectiveness of the control. Organisations can build a profile of these controls by assessing them in terms of maturity and assurance validation to understand how much reduction the control has had on the risk.

There may be instances where a control is:

- not designed correctly
- not operating effectively
- not offering as much of a reduction to the likelihood and/ or impact as first assumed

Now organisations should undertake more detailed testing to assess the maturity, design, and operating effectiveness of the existing controls (aligned with the risk story). During this testing think about what

[21] Example maturity table provided in 8.6 Supporting Information

measures can be used to determine if the control is functioning as expected by the original assessment, and in context of the risk story.

In some instances, this analysis will conclude that there are only a small number of controls that contribute to the greatest reduction in likelihood and/ or impact of the risk. These controls can now be formally defined as 'key controls.'

Alternatively, the analysis may determine that the effect a particular control has on the risk story may be negligible (ineffective). In these instances, it may be worth considering the appropriateness of the control for this particular risk (unless it has also been used in other risk stories for other purposes).

Activity	Description	Examples of source material
Analysis of existing controls	For each control assess the: • design effectiveness • operating effectiveness, and • the effect of the control on the reduction of likelihood and/ or impact.	VPDSS Element Maturity criteria Control effectiveness table Supporting material to the risk statement. Workshops with information and system owners to identify and inventory controls.

For example, consider the use of 'encryption at rest' controls. In a risk story where the risk event is unauthorised access and disclosure of data by an internal threat source – this control would have no effect if the internal threat source accessed the system as any normal legitimate user would. That is because the information the user accesses would always be unencrypted at the time of accessing it. In this instance, the control would not be relevant/appropriate for the risk story and have negligible impact.

In contrast, if the risk event of the risk story focused more on unauthorised access of data by physical theft of the system, then the control may be highly effective (assuming encryption strength etc). In that particular risk story, the control could be regarded as a 'key control'. It is this type of insight that control analytics aims to provide improved visibility of.

8.4 Step 3 - Analyse proposed treatments

Where a target risk rating has not been met, a risk may be managed through control improvements. These control improvements may include the uplift of existing controls and/ or analysing what new treatments could be introduced. This provides the ability for the practitioner to determine the best control improvement, based on the level of investment (cost, effort etc.) to achieve the target risk rating.

8.4.1 Step 3: Action 1 – Identify the target risk rating

At this point there should be a clear view of the risk story and the effect existing controls have to the likelihood and impact of the risk. Therefore, risk owners and associated stakeholders should question what a tolerable financial impact for the risk is and work back to agree on a target risk rating. Knowing what the financial impact of the target risk rating is would make decision making easier and more informed, with an understanding of which components of the risk story should be focused on to achieve that outcome.

Activity	Description	Examples of source material
Determine target risk rating	The risk owner (with relevant stakeholder input) determines the appropriate target risk rating	Workshops with system owners and relevant stakeholders

8.4.2 Step 3: Action 2 – Determine the treatments and control type(s) to reduce risk to the target risk rating

As with most forms of risk reduction, controls can be applied which either reduce the likelihood and/or impact (either primary or secondary impact).

Based on the structure of the risk story, it will become evident whether it is more sensible to try for a:

- reduction in likelihood (where the frequency and/ or susceptibility is high)
- reduction in impact (whether the primary and specifically the secondary impacts are high), or
- combination of both.

Existing controls may be enhanced to achieve the desired target risk rating, or it may be necessary to add new controls.

Activity	Description	Examples of source material
List proposed treatments	A list of proposed treatments (e.g., VPDSS Element Reference ID) with a description, cost to enable cost-benefit analysis, and corresponding control type (preventive, detective, corrective). These may be an uplift of existing controls or new treatments.	Workshops with system owners and relevant stakeholders

8.4.3 Action 3 – Analyse the effect of proposed treatments

Various controls based on their investment (effort and cost) can be analysed in the risk story, to determine the best option to achieve the target risk rating with the most appropriate amount of control investment. This provides a meaningful indicator demonstrating a potential 'return on investment' to management.

Activity	Description
Revise likelihood	Following the application of the proposed treatments, work through Step 1, action 3 to determine a revised likelihood
Revise calculated annualised financial risk	Following the application of the proposed treatments, work through, • Step 1, action 4 to determine a revised impact; and • Step 1, action 5 to recalculate an annualised financial risk **Revised annualised financial risk = revised impact x revised likelihood**
Revise organisational risk rating	Mapping the outcome of the revised likelihood and revised annualised financial risk to determine the revised organisational risk rating

8.5 Step 4 - Monitor control effectiveness

Once a selection of controls is analysed and becomes an agreed approach for the management of risk, control analytics doesn't need to end here. In fact, in some ways, it is just the beginning of the journey.

As the organisation begins to design and implement controls, control analytics can be continuously used to report on the gradual reduction of risk (based on the captured likelihood and impact data points), providing risk status reporting of controls against target risk reduction.

This feedback provides ongoing confidence to management that the control selection modelled was correct, or if circumstances change (or controls turn out to be less effective than anticipated), they can be refined/ changed/ remodelled to steer the outcome back into the appropriate direction.

8.6 Supporting Information

8.6.1 Sample risk criteria tables

The following risk tables are used throughout the examples in section 9 Part Two –Template for the application of control analytics. They are aligned to the *Risk Criteria Examples* available on the VMIA website[22].

An organisation should use its own risk criteria tables – typically set out within the organisation's enterprise risk management framework. The control analytics template and examples in this document should be adjusted to align with the organisation's own approach for assessing likelihood and impact / consequence of risk.

8.6.2 Likelihood table (with added frequency guide)

The likelihood table provides guidance on the possible likelihood rating assigned to a risk.

Frequency Guide	Likelihood		Description
> 100 times per year	Tier 5	Almost certain	The event is expected to occur as there is a history of regular occurrence at the organisation and/or similar institutions, or new conditions make it very likely to occur.
Between 11 & 100 times per year	Tier 4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at the organisation or similar institutions, or new conditions make it likely to occur.
Between 1 & 10 times per year	Tier 3	Possible	The event might occur at some time as there is a history of casual occurrence at the organisation or similar institutions, or new conditions make it possible to occur.
Between 0.1 & 0.9 times per year (less than once a year	Tier 2	Unlikely	The event is not expected and has not casually occurred before, but there is a small possibility it may occur at some time in certain circumstances.
<0.1 times per year (less than once every 10 years)	Tier 1	Rare	The event is highly unlikely. It may occur in exceptional circumstances but has never occurred before. It could happen, but probably never will.

[22] Refer to the VMIA website https://www.vmia.vic.gov.au/tools-and-insights/risk-management-tools

8.6.3 Susceptibility table

The susceptibility table provides guidance as to which rating should be assigned to the risk based on current controls/ proposed treatments for the purpose of control analytics.

Susceptibility Rating	Probability Range
Low	1%-33%
Moderate	34%-66%
High	67%-99%

8.6.4 Consequence (Impact) table

The consequence table assists in determining the level and type of consequence for a given risk. Given the quantitative nature of control analytics which provides a resulting financial figure, organisations can refer to the financial category under their existing risk consequence table to determine the resulting consequence rating e.g., minor, moderate, major.

Consequence		Financial	People	Reputation	Operational disruption	Legal and Compliance	Natural environment
Tier 5	Severe	Direct loss or opportunity cost of more than $5M Increase in budget more than 20%	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	Greater than 50% of media stories are negative for a period of up to 30 days or more; Significant impact on funding for several years; long-term loss of clients	Full service or business performance disruption > 1 weeks, partial disruption (months)	Major litigation costing $>5m; Investigation by regulatory body resulting in long term interruption of operations	Major release of toxic waste resulting in long term damage to the environment; Significant damage to natural areas and ecosystem health; Extensive decline in support to community for living sustainably
Tier 4	Major	Direct loss or opportunity cost of $1M to $5M Increase in budget of 15% to 20%	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	Greater than 50% of media stories are negative for a period of up to 30 days ; CEO departs affecting funding or causing loss of clients for many months	Full service or business performance disruption 2–7 days, sustained partial disruption (weeks)	Major breach of regulation with punitive fine, and significant litigation involving many weeks of senior management time and up to $3m legal costs	Major release of toxins/water resulting in high compensation or reconstruction costs; Decline in support to community for living sustainably
Tier 3	Moderate	Direct loss or opportunity $250K to $1M Increase in budget of 5% to 15%	Short term disability to one or more persons Some turnover of key staff and loss of key skills, knowledge and expertise	20-50% of media stories are negative for a period of up to 14 days ; senior managers depart; noticeable loss of clients for many months	Full service or business performance disruption <2 days, consistent partial disruption (weeks)	Breach of regulation with investigation by authority and possible moderate fine, and litigation and legal costs up to $999k	Significant release of pollutants; Residual pollution requiring clean-up work
Tier 2	Minor	Direct loss or opportunity $100K to $250K Increase in budget of 2% to 5%	Significant medical treatment; lost injury time <2 weeks Some staff turnover with minor loss of skills, knowledge and expertise	10-20% of media stories are negative for a period of up to 7 day; complaint to management	Part service or business performance disruption 1 day, limited partial disruption (days)	Breach of regulations; major fine or legal costs; minor litigation	Required to inform EPA; Contained temporary pollution
Tier 1	Insignificant	Direct loss or opportunity cost of less than $100K Increase in budget by less than 2%.	First aid or minor medical treatment No staff turnover	Less than 10% of media stories are negative for a period of up to 7 days; complaint to employee	Intermittent part service or business performance disruption, isolated partial disruption (days/hours)	Minor legal issues or breach of regulations	Brief, non-hazardous temporary pollution; No environmental damage

8.6.5 Risk matrix

The risk matrix provides a structure for the risk based on likelihood and consequence inputs.

		Impact/Consequence				
		1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Severe**
Likelihood	**5 Almost certain**	Medium	High	Extreme	Extreme	Extreme
	4 Likely	Medium	Medium	High	Extreme	Extreme
	3 Possible	Low	Low	Medium	High	Extreme
	2 Unlikely	Low	Low	Medium	Medium	High
	1 Rare	Low	Low	Low	Medium	High

8.6.6 Control effectiveness table

The control effectiveness table provides definitions when assessing controls for their design and/or operating effectiveness.

Control effectiveness	Description
Effective	• Controls eliminate or remove the source/root cause of the risk; • Controls are well documented, consistently implemented, and reliable in addressing the source/root cause of risk; and • 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; and • 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 are not documented or communicated or consistently implemented in practice; • The controls are not operating as intended and risk is not being managed; and • Controls are not in place to address root cause/source of risk.

8.6.7 Maturity rating

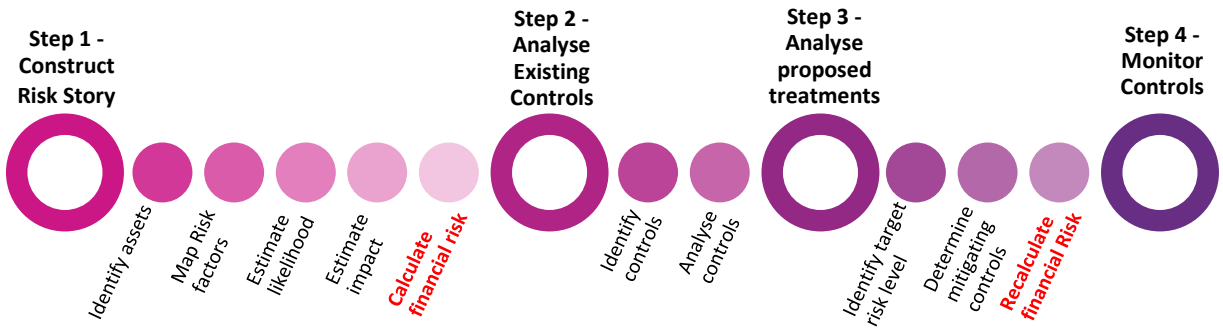
This table provides ratings for control elements/standards in alignment to the VPDSF/S definitions including in the Protective Data Security Plan (**PDSP**).

Rating	Description
Informal	Processes are usually ad-hoc and undocumented. Some base practices may be performed within the organisation, however there is a lack of consistent planning and tracking. Most improvement activity occurs in reaction to incidents rather than proactively. Where practice is good it reflects the expertise and effort of individuals rather than institutional knowledge. There may be some confidence security-related activities are performed adequately, however this performance is variable and the loss of key staff may significantly impact capability and practice.
Basic	The importance of security is recognised, and key responsibilities are explicitly assigned to positions. At least a base set of protective security measures are planned and tracked. Activities are more repeatable and results more consistent compared to the 'informal' level, at least within individual business units. Policies are probably well documented, but processes and procedures may not be. Security risks and requirements are occasionally reviewed. Corrective action is usually taken when significant problems are found.
Core	Policies, processes, and standards are well defined and are actively and consistently followed across the organisation. Governance and management structures are in place. Risk assessment and management activities are regularly scheduled and completed. Historic performance information is periodically assessed and used to determine where improvements should be made.
Managed	Day-to-day activity adapts dynamically and automatically in response to situational changes. Quantitative performance measures are defined, baselined, and applied to ensure security performance is analysed objectively and can be accurately predicted in advance. In addition to meeting VPDSS requirements, the organisation also implements many optional 'better practice' requirements in response to its risk assessment.
Optimised	Security is a strategic issue for the organisation. Long-term planning is in place and integrated with business planning to predict and prepare for protective security challenges. Effective continuous process improvement is operating, supported by real- time, metrics-based performance data. Mechanisms are also in place to encourage, develop and test innovations.

9 Part Two –Template for the application of control analytics

9.1 Introduction

The following diagram identifies the practical steps to follow, and a control analytics template to use, for the application of control analytics to a given risk story. Organisations may wish to add or remove activities when conducting their own analysis, depending on their business requirements.



Note. Guidance text for completing the template is written in italics in the appropriate section. To use this template, remove this guidance text and replace it with your own risk story.

The examples in section 10 Part Three – Control analytics examples of this guide may also assist you when using this template.

Detailed information about the approach to control analytics, including step by step guidance and further reference materials including sample risk rating criteria (likelihood, consequence, control effectiveness and risk tables), can be found in section 8.6 Supporting Information and section 11 Part Four - Appendix. Use relevant data points available from the organisation or proxy data where necessary to assist with completing the template.

Navigation within Part Two

Within Part Two of this document, the following graphic will highlight which stage and action you are in. If you are not sure where you are within the control analytics process, simply refer to graphic at the top right of each page. The large circles represent the stages and the small circles the actions within the stage. For instance, the graphic below represents actions 1 and 2 of step 2.

9.2 Step 1 – Constructing the risk story

Action 1 – Identify the information asset components	☐ Check the box once the action is finalised

Identify the information asset(s) for this risk story and their associated components.

Asset details	Input
Asset name/ description	*Identify the information asset and provide a description*
Protective marking	*Identify the protective marking (confidentiality)*
Security value / Business Impact Level (BIL)	*Identify the overall security value with additional consideration to integrity and availability*
Supporting asset(s)	*Identify the supporting asset(s) relevant to the information asset*

Action 2 – Map the risk factors (threat source, threat event(s)/ cause(s) and impact(s))	☐ Check the box once the action is finalised

Identify the risk factors of the risk story.

Risk factors	Input
Threat source	*Identify the internal/ external threat source(s)*
Cause/ Threat event	*Identify the action taken by the threat source(s)*
Risk event	*Describe the risk event (generally a compromise to the confidentiality, integrity and/ or availability of information)*
Impact	*List all impact(s) of the risk event expressed as primary and (if applicable) secondary impact*

Action 3 – Estimate the likelihood of the risk	☐ Check the box once the action is finalised

Estimate the likelihood.

Measures of likelihood	Input[23]
Frequency of the risk event	*Insert frequency rating (expressed in frequency (#) per annum)*
Susceptibility of supporting asset(s)	*Insert susceptibility rating (based on a % rate of susceptibility)*
Likelihood	*Calculate frequency **x** susceptibility (multiplied) expressed as a number (#) per annum* **Likelihood = *frequency x susceptibility***

Action 4 – Estimate the impact of the risk	☐ Check the box once the action is finalised

Estimate the impact.

Measures of impact	Input (in financial terms)
Primary impact	*Insert BIL value (description of impact)* *Explain $ value per incident*
Secondary impact (if applicable)	*Insert BIL value (description of impact)* *Explain $ value per incident*
Impact	*Calculate impact ($) = Primary impact **+** Secondary impact (addition)* **Impact ($) = *Primary impact + Secondary impact***

[23] Refer to the sample risk criteria tables provided in section 8.6 Supporting Information

Action 5 – Calculate the annualised financial risk	☐ Check the box once the action is finalised

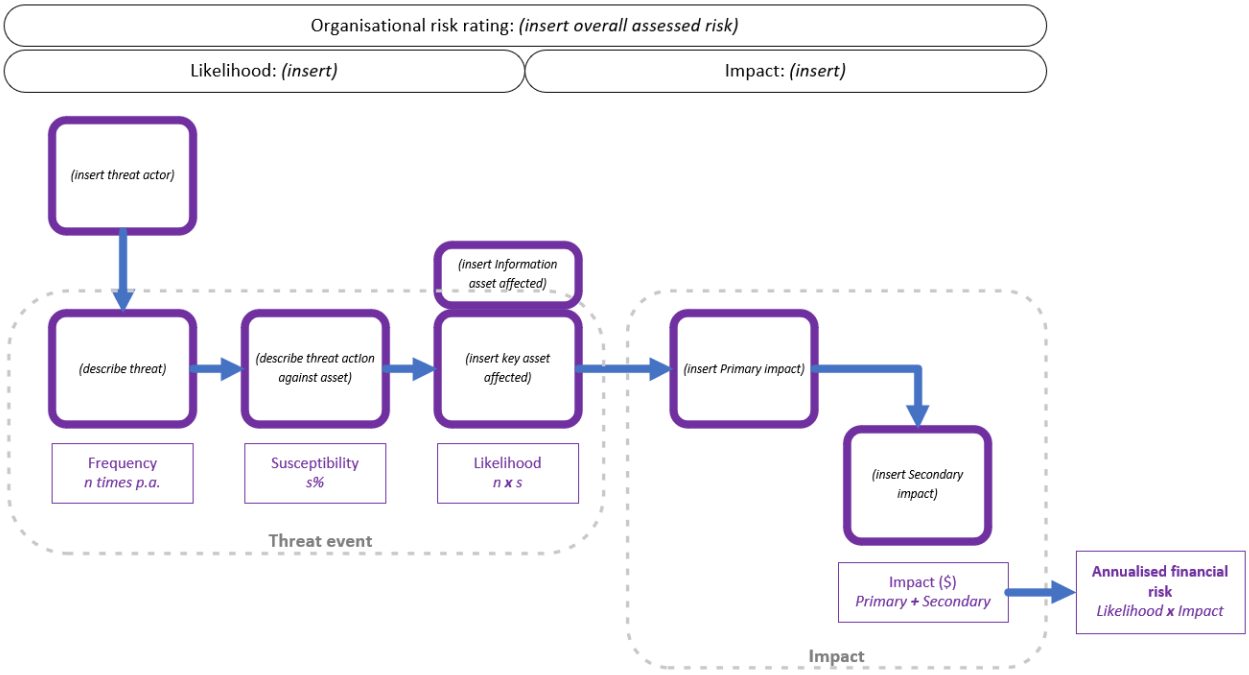
Calculate the annualised financial risk.

Risk	Input (in financial terms)
Annualised financial risk	*Calculate likelihood **x** impact (multiplied)* **Annualised financial risk = *likelihood x impact***

The organisational risk rating is determined by mapping the outcomes of the risk story to the organisation's risk matrix as follows:

Likelihood	Consequence / Impact	Organisation risk rating
***Likelihood** converted to organisational likelihood rating using sample table*	*Annualised financial risk converted to organisational **consequence**/ impact rating (financial category) using sample table*	*Organisation risk rating derived from the intersection of the organisational **consequence**/ impact against the organisational **likelihood** using sample table*

The risk story can then be illustrated as follows:



9.3 Step 2 – Categorise and analyse existing controls

Action 1 – Conduct an inventory of existing controls	☐ Check the box once the action is finalised

Identify existing controls.

Element(s) [24]	Control
VPDSS Element Reference ID *Element description*	***Control type*** *(preventive, detective, corrective)* *List of controls/ activities under the element*

Action 2 – Conduct an analysis of existing controls	☐ Check the box once the action is finalised

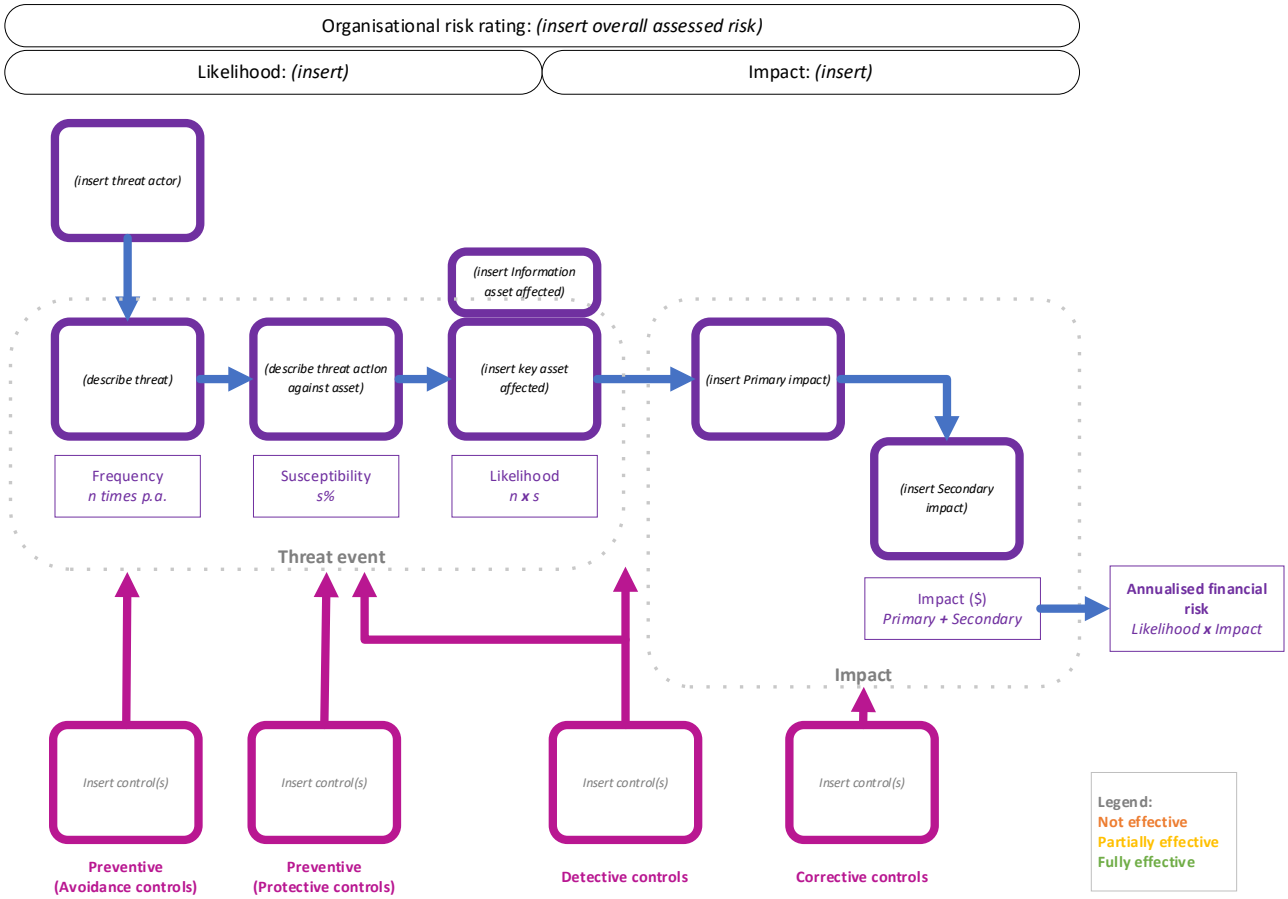
Review existing controls.

Element(s)	Control attributes[25]
VPDSS Element Reference ID	**Design effectiveness:** *Control effectiveness rating* **Operating effectiveness:** *Control effectiveness rating* *Details relating to effectiveness rating.* **Effect:** *The effect of the control in the reduction of likelihood and/ or impact.*

[24] This document uses the VPDSS Element descriptions extracted in Part Four - Appendix – however, an organisation can specify its own control descriptions.

[25] Refer to the sample risk criteria tables provided in section 8.6 Supporting Information

The risk story with application of controls can be illustrated as follows:



9.4 Step 3 – Analyse proposed treatments

Action 1 – Identify the target risk rating	☐ Check the box once the action is finalised

The risk owner (with relevant stakeholder input) determines the appropriate target risk rating.

Risk rating	Input
Target risk rating	*Document the target risk rating*

Action 2 – Determine the treatments and control type(s) to reduce risk to the target risk rating	☐ Check the box once the action is finalised

Based on the risk story and existing controls, determine which treatments will further reduce the risk.

Proposed treatment(s)	Control
VPDSS Element Reference ID *Proposed uplift or new control* *Element description*	*Control type (preventive, detective, corrective)* *List of controls/ activities under the element*

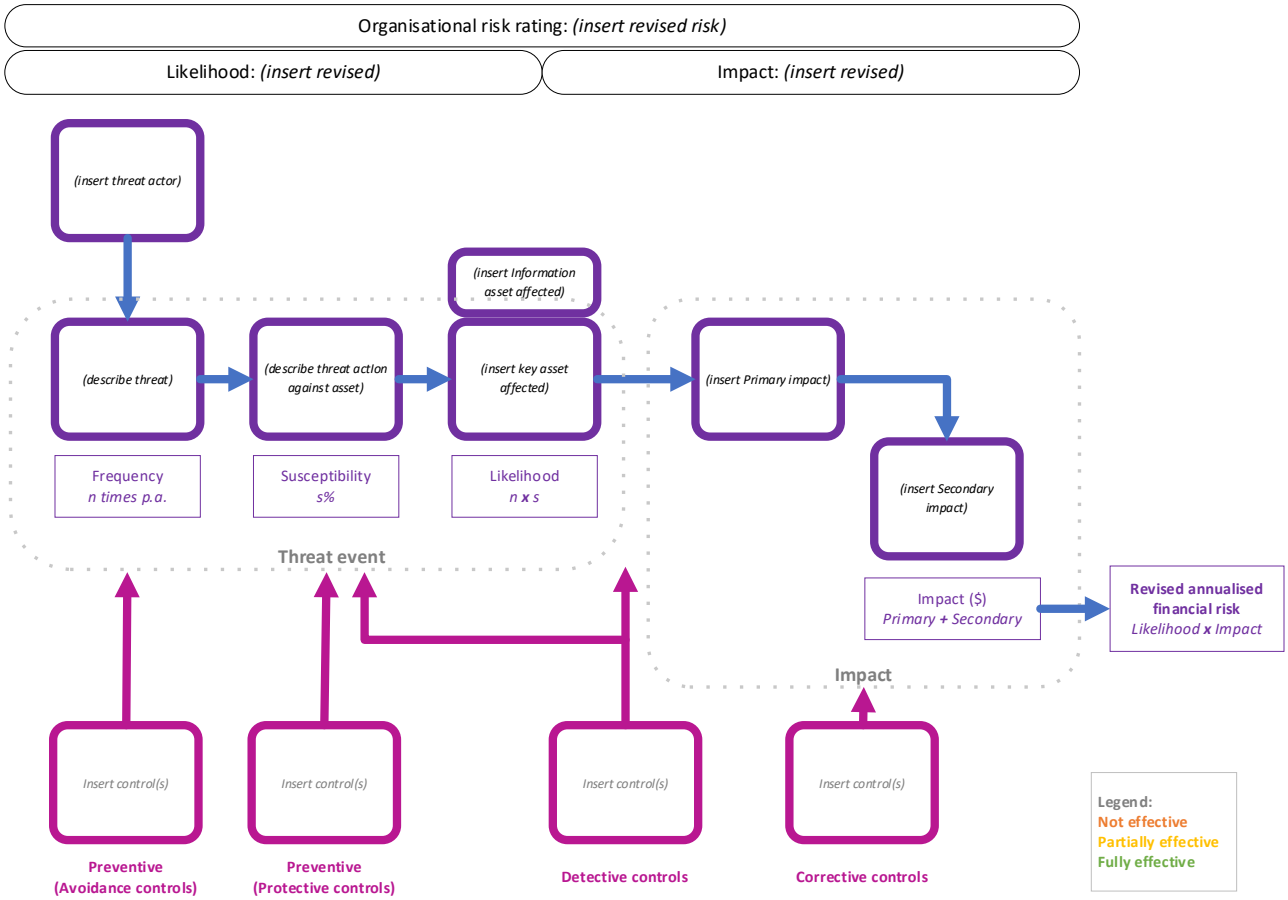
Action 3 – Analyse the effect of proposed treatments	☐ Check the box once the action is finalised

Analyse proposed treatments and their costs.

Risk attribute	Measure
Revised likelihood	*New likelihood rating* *Explanation of reduction considering cost analysis*

Risk attribute	Measure
Revised annualised financial risk	*Annualised financial ($) risk* Primary impact = *BIL value* inc. $ per incident Secondary impact = *BIL value* inc. $ per incident Revised impact = (Primary impact + Secondary impact) **Revised annualised financial risk = *revised impact x revised likelihood*** *Explanation of reduction considering cost analysis*
Revised organisational risk rating	*Map the revised likelihood with the revised annualised financial risk to arrive at a revised organisational risk rating*

The risk story with proposed treatments can be illustrated as follows:



9.5 Step 4 – Monitor control effectiveness

It is important to utilise the organisation's risk management tools to manage the risk. This can typically be found in the organisation's Risk Management Framework.

10 Part Three – Control analytics examples

This section provides an explanation of the 'risk story' by stepping through the template, using examples that transpose an existing risk statement into a risk story, and subsequently performing control analytics.

10.1 Example One – Disclosure of personnel information by third party service provider

Scenario.

The risk of the unauthorised access and disclosure (confidentiality) of sensitive personnel data stored in a third party provided service, caused by cybercriminal targeting vulnerabilities in the application, resulting in an impact to service delivery.

Step 1 – Constructing the risk story

Action 1 – Identify the information asset components	☑ Check the box once the action is finalised

In this example the asset type is human resources (**HR**) information (sensitive personnel data). The BIL value for the data as listed in the IAR is 2 (two) – Limited, with a protective marking of **OFFICIAL: Sensitive**.

Asset details	**Input**
Asset name/description	*HR Information*
Protective marking	*OFFICIAL: Sensitive*
Security value / Business Impact Level	*Limited*
Supporting asset(s)	*Third party service (a cloud/ hosted service)*

Action 2 – Map the risk factors (threat source, threat event(s)/ cause(s) and impact(s))	☑ Check the box once the action is finalised

Risk factors	Input
Threat source	*Cybercriminal (external threat source)*
Cause/ Threat event	*Targeting/ exploiting vulnerabilities in an application*
Risk event	*Unauthorised disclosure of information (loss of confidentiality)*
Impact	*Primary impact –* *Service delivery: Loss of productivity at the time of the incident.* *Secondary impact –* *Service delivery: As a result of the incident, key Human Resource processes have a significant productivity impact by reverting to manual methods.*

Action 3 – Estimate the likelihood of the risk	☑ Check the box once the action is finalised

In this example, information to assist with measuring likelihood was provided by the third-party service provider via monthly service reports.

Determining the likelihood of the risk requires us to understand more about the threat source, the threat event, and the supporting asset. This assists in identifying where relevant data can be gathered to assist with measuring the likelihood.

Let us assume that the service provider shares the following information during regular monthly service reviews. They:

- identify approximately five (5) targeted attempts per month to compromise their main system from cybercriminal threat source.
- identify only a small number of these attempts (10%) are successful.
- notify clients within seven (7) days if they suspect there has been a breach (after they have performed their preliminary incident investigation).

Based on this information, the likelihood of the risk can be measured as follows:

Measures of likelihood	Input
Frequency of the risk event	***Likely***[26] *(5 times a month or 60 times a year)*
Susceptibility of supporting asset(s)	***Low***[27] *(based on a 10% rate of susceptibility)*
Likelihood	***Possible*** *(60 times a year* ***x*** *10% = 6, or according to the sample Likelihood table, between 1 to 10 times a year)*

Action 4 – Estimate the impact ☑ Check the box once the action is finalised

The data points that assist with measuring impact are provided via interviews with business stakeholders to provide their perspective regarding each of the relevant impact categories to determine the primary and secondary impacts of the risk.

Measures of impact	Input (in financial terms)
Primary impact	• *BIL 2 (Public services: Service delivery – cessation of non-essential business service (HR))* • *$50,000 per incident* • *Loss of productivity*
Secondary impact (if applicable)	• *BIL 2 (Public services: Service delivery – cessation of non-essential business service (HR))* • *$200,000 per incident* • *Delays in recruiting new staff meaning delays to key projects and deliverables which incur wastage/ cost $ value per incident explanation*
Impact	*$50,000* ***+*** *$200,000 = $250,000*

[26] As derived from the sample Likelihood table in 8.6 Supporting Information

[27] As derived from the sample Susceptibility table in 8.6 Supporting Information

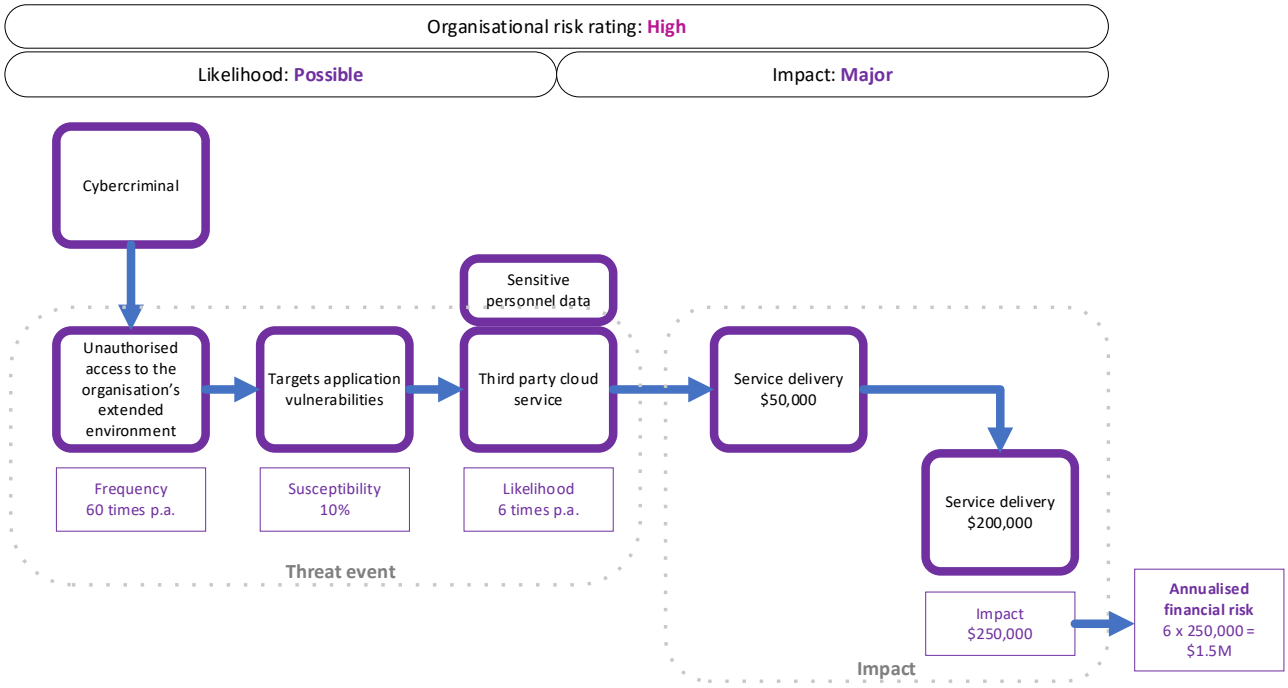
Action 5 – Calculate the annualised financial risk	☑ Check the box once the action is finalised

Risk	Input (in financial terms)
Annualised financial risk	*6 **x** $250,000 = $1,500,000*

The organisation *risk rating [according to organisational risk matrix].*

Likelihood	Consequence / Impact	Organisation risk rating
*6 times per year maps to **'3 - Possible'*** *(using sample likelihood table)*	*$1,500,000 maps to **'4 - Major'*** *(using sample consequence table)*	***High*** *(intersection of 'Possible' and 'Major' using sample risk table)*

The risk story can now be illustrated as follows:



Step 2 – Categorise and analyse existing controls

Action 1 – Conduct an inventory of existing controls	☑ Check the box once the action is finalised

In this example, the controls described are those that can be managed by the organisation itself (which is distinct to the controls that the service provider owns and operates). The organisation may have the ability to request certain controls of the service provider, and this should have been done during the initial risk assessment and contract establishment.

Element(s)	Control type	Control
E6.030 *The organisation has an incident management process and plan consisting of the five (5) phases*	***Detective***	*The organisation has a process/ system to detect an incident that enables them to respond in a timely manner. This is based on notification provided from the service provider.*
E8.030 *The organisation includes requirements from all security areas in third party arrangements.*	***Preventive***	*The security requirements were identified by the organisation as part of the initial risk assessment and stipulated in subsequent service agreements and contracts with the service provider.*

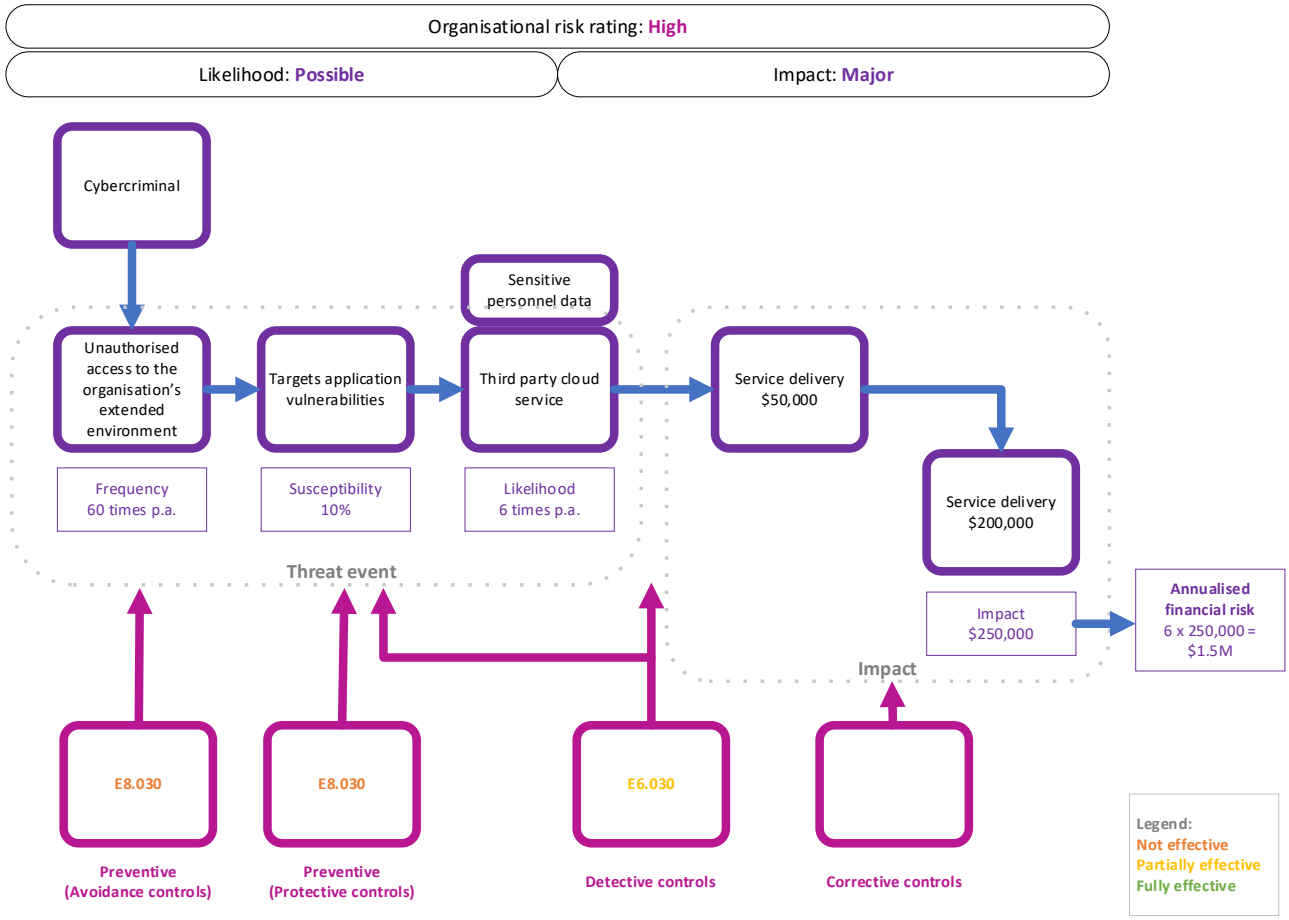
Action 2 – Conduct an analysis of existing controls	☑ Check the box once the action is finalised

Once all the controls have been identified and recorded, they can be analysed for their effect on the reduction of risk. This includes analysing the effect of the controls based on their profile (the design effectiveness, operating effectiveness, and maturity at which the control is implemented and operating).

Element(s)	Control attributes
E6.030	***Design effectiveness:*** *Partially effective* ***Operating effectiveness:*** *Partially effective* *Through both self-assessment and internal audit, the control was assessed to be partially effective in how the organisation identifies and manages a potential incident. It is noted that the notification period from the service provider is currently seven (7) days.* ***Effect:*** *Based on the assessment of the control, and the 7-day notification from the third party, the reduction to the probable risk impact is minimal.*

Element(s)	Control attributes
E8.030	***Design effectiveness:*** *Fully effective* ***Operating effectiveness:*** *Not effective* *Through both self-assessment and internal audit, the control was assessed to not be operating effectively. This was due to the control not always being put in place and management's ability to easily "override" the control.* ***Effect:*** *This has minimal reduction to the probable likelihood of the risk as the organisation couldn't validate what controls the third party had in place and whether these were appropriately aligned to the organisation's risk.*

Taking these controls into consideration, the overall risk position is at **High**. Our risk story including controls can be illustrated as follows:



Step 3 – Analyse proposed treatments

Action 1 – Identify the target risk rating	☑ Check the box once the action is finalised

In this example, assuming that the current risk rating of **High** is not acceptable, it is important for management to agree on a target risk rating commensurate to the risk appetite of the organisation. In this instance, management has chosen the target risk rating to be **Low**.

Based on the current risk story, possible ways of reducing the risk level to **Low** includes reducing the:

- likelihood from **Possible** to **Unlikely**[28], and
- impact from **Major** to **Insignificant**.

Risk Rating	Input
Target risk rating	*Low*

Action 2 – Determine the treatments and control type(s) to reduce risk to the target risk rating	☑ Check the box once the action is finalised

Based on the risk story, the impacts (specifically the secondary impact) contribute significantly to the assessment of the risk and to some extent, can be managed by the organisation through appropriate uplift of controls.

While reduction of likelihood is possible, in the context of a service provider, the organisation has little in the way of influence, apart from improved governance of the third party (which is important to ensure that the third party uplifts their respective controls and therefore, reduces the likelihood).

Using the risk story, and knowledge of the third party's response, consider what approach could be used to reduce the risk. Some considerations could include:

- Uplift the incident response process so the organisation is better prepared to respond to the incident and manage the impact of the incident;
- Receive more timely notification if the third party has an incident (reducing from 7 days);
- Prepare the business to operate with less impact should an incident occur that disrupts one of the key systems it relies on; and
- Improve existing third-party approaches to risk assessment including the introduction of ongoing validation which may lead to control improvements by the third party and therefore further reduce likelihood (although not in the direct control of the organisation).

Risk reduction may not necessarily involve the introduction of new controls as there may be benefit in

[28] As derived from the sample tables in 8.6 Supporting Information

uplifting existing controls. Risk treatments that may be considered in this example include:

Proposed treatment	Control type	Control
E8.030 – Proposed uplift *The organisation includes requirements from all security areas in third party arrangements.*	***Preventive***	*The organisation improves the application and governance of the initial risk assessment of third-party services ensuring that control obligations are articulated and appropriately assessed prior to initiation of service. Examples include adding/ appending a clause(s) in the contract for annual assurance/ right to audit.*
E7.010 – New treatment *The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.*	***Corrective***	*The organisation looks to put in place appropriate policies and plans to allow for suitable recovery from the incident whilst keeping business operating with minimal impact.*
E8.060 – New treatment *The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.*	***Preventive*** ***Detective***	*The organisation introduces and undertakes a periodic revalidation of the third party's security requirements where identified gaps are committed to be addressed by the third party.*

Action 3 – Analyse the effect of proposed treatments ☑ Check the box once the action is finalised

Analyse the treatments and estimate the risk buy-down value (the level of investment in the control for the level of risk reduction).

The probable effect of the proposed treatments (assuming the controls are designed and operating effectively) are as follows:

Risk attribute	Measure
Revised likelihood	***Unlikely*** *Improved third party governance leads to a reduction in third party susceptibility to the risk event (from 10% to 1%) and therefore, the revised likelihood is 0.6 events per annum (60 x 1%).*
Revised annualised financial risk	***Insignificant*** *Primary impact = $10,000 per incident*[29] *Secondary impact = $50,000 per incident* *Revised impact: $10,000 **+** $50,000 = $60,000 per incident* *Revised annualised financial risk = $36,000 per annum (60,000 **x** 0.6)* *With both an uplift in incident response processes as well as shortening the notification time from seven (7) days to 24 hours, the organisation is better able to detect and respond to the incident and therefore minimises the initial impact of the incident.* *Further, because of the introduction of appropriate business recovery processes, the organisation has appropriate processes in place to allow critical services to operate efficiently despite not having the third-party system fully operational.*
Revised organisational risk rating	*By using the organisational risk matrix and mapping the revised likelihood with the revised annualised financial risk, the risk rating has now been reduced to **Low***

[29] Impact figures based on data points provided by business stakeholders

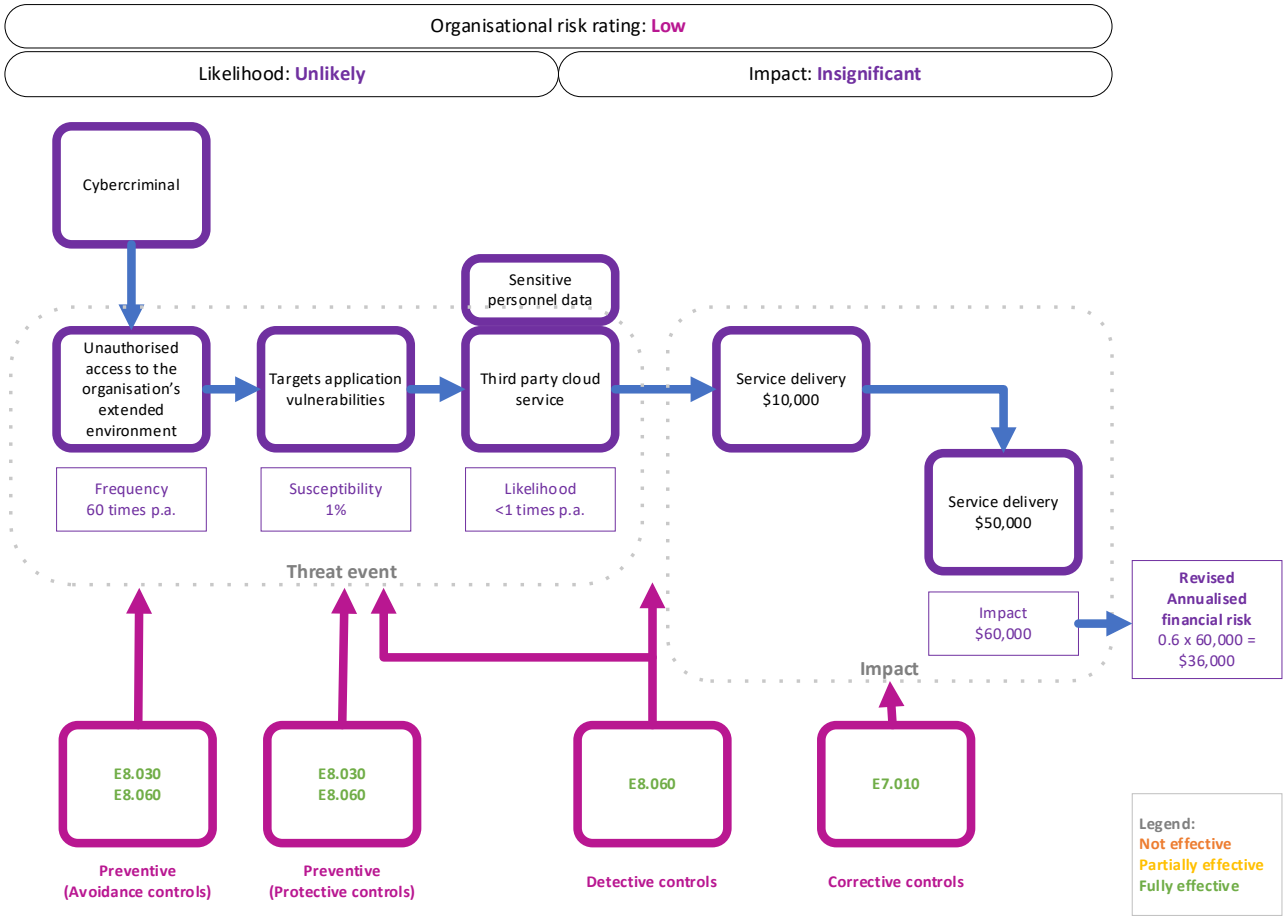
Risk attribute	Measure

Revised financial risk

The example demonstrates that if investment is placed in suitable controls, there is an opportunity for the organisation to achieve a considerable reduction of risk. This results in the probable risk moving from **High** to **Low** or a reduction in financial terms of $1.5M to **$36K** (more than a 95% impact reduction).

Therefore, even if the control investment required $300,000 for upfront cost, the return of the controls would still be considerable.

Our risk story, considering the control improvements, can now be illustrated as follows:



Step 4 – Monitor control effectiveness

The organisation utilises its risk management tools to manage the risk.

10.2 Example Two – Unavailability of critical financial information

Scenario

The risk of the unavailability of critical finance information caused by a cybercriminal originated ransomware attack resulting in the degradation of service delivery and reputational damage.

Step 1 – Constructing the risk story

Action 1 – Identify the information asset components ☑ Check the box once the action is finalised

In this example the asset type is critical finance information. The BIL value for the data as listed in the IAR has been assessed as 3 (three) – Major, with a protective marking of **PROTECTED.**

Asset details	Input
Asset name/ description	*Critical financial information*
Protective marking	*PROTECTED*
Security value/ Business Impact Level	*Major*
Supporting asset(s)	*Legacy system (Reporting system/ application)*

Action 2 – Map the risk factors (threat source, threat event(s)/ cause(s) and impact(s)) ☑ Check the box once the action is finalised

Risk factors	Input
Threat source	*Cybercriminal (external threat source)*
Cause/ Threat event	*Phishing email leading to ransomware attack that makes critical financial information unavailable*
Risk event	*Unavailability of critical information and reduced ability to operate the reporting system*
Impact	*Primary impact –* *Service delivery: Loss of productivity including the need to respond to the incident.*

Risk factors	Input
	Secondary impact – *Service delivery: Reduced ability to operate the reporting system and process the reporting information completely and accurately, impacting the organisation's ability to deliver core services.* *Reputation: When the incident is disclosed via media to the public, there is a cost in government time and finances to manage the public relations incident.*

Action 3 – Estimate the likelihood of the risk ☑ Check the box once the action is finalised

In this example, data to assist with measuring likelihood were provided by the organisation through monthly service/ operational reports.

Determining the likelihood of the risk requires us to understand more about the threat source, the threat event, and the supporting asset. This assists in determining where relevant data can be gathered to assist with measuring the likelihood.

Let us assume that the system administrator shares information about existing attempts to compromise the organisation's environment, including attempts that targeted the legacy reporting system. They identify:

- approximately 6 (six) instances per month where users have clicked on a phishing email and malware attempts to be installed on the end point, and
- a regular number of these attempts have been detected before the ransomware has been able to propagate.

Based on this information, the likelihood of the risk can be measured as follows:

Measures of likelihood	Input
Frequency of the risk event	***Likely***[30] *(6 times a month or 72 times a year)*
Susceptibility of supporting asset(s)	***Moderate***[31] *(based on a 50% rate of susceptibility given a 'regular' number of attempts have been detected)*
Likelihood	***Likely*** *(72 times a year* ***x*** *50% = 36, or according to the sample Likelihood table, between 11 and 100 times a year)*

[30] As derived from the sample Likelihood table in 8.6 Supporting Information

[31] As derived from the sample Susceptibility table in 8.6 Supporting Information

Action 4 – Estimate the impact	☑ Check the box once the action is finalised

The information to assist with measuring probable impact(s) is provided through interviews with business stakeholders (like when information assets were being valued).

Measures of impact	Input (in financial terms)
Primary impact	• *BIL 3 (Public services: Service delivery – cessation of essential business operations, systems, or services)* • *$50,000 per incident* • *Loss of availability of system access and associated productivity impact*
Secondary impact one	• *BIL 3 (Public services: Service delivery – cessation of essential business operations, systems, or services)* • *$200,000 per incident* • *Loss of productivity, efficiency, and costs of missed deadlines. This also includes the cost of paying the ransom if the organisation chose to do so.*
Secondary impact two	• *BIL 3 (Reputation – major dissatisfaction from public/VPS, reputational damage, and loss of confidence)* • *$100,000 per incident* • *Loss of confidence and distrust resulting in the need to spend time and effort on public relations as well as handle queries from relevant regulator(s).*
Impact	*$50,000 + $200,000 + $100,000 = $350,000*

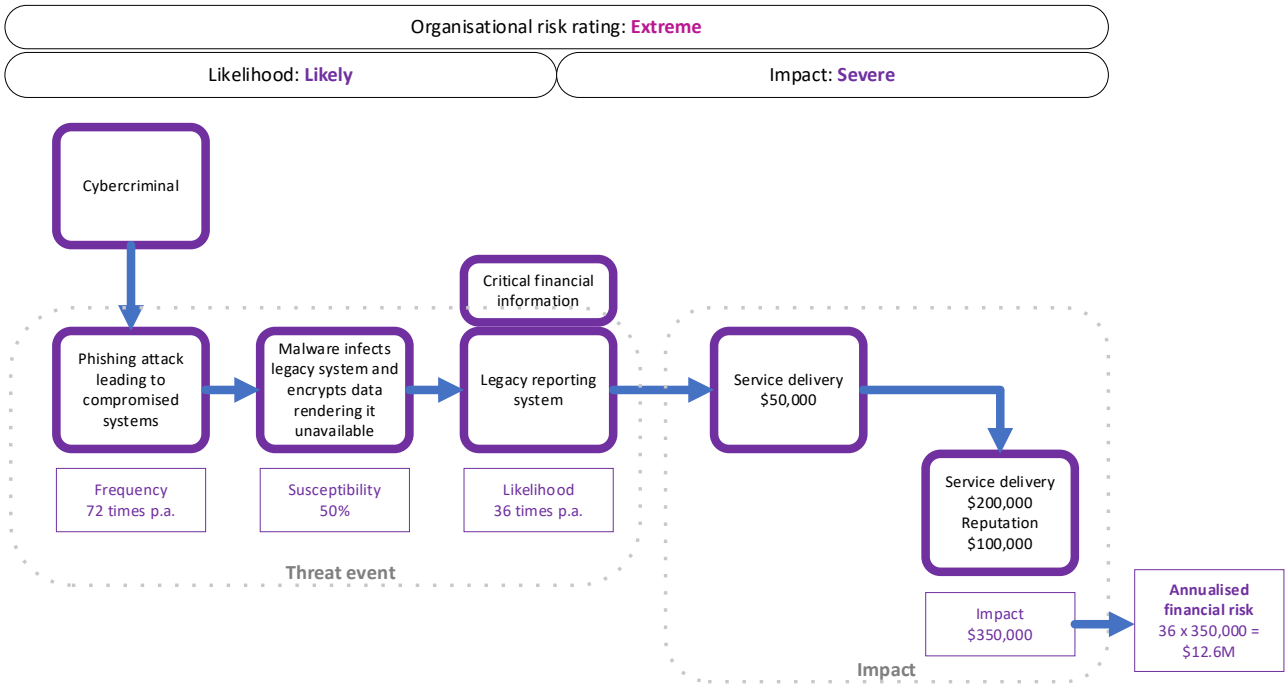
Action 5 – Calculate the annualised financial risk	☑ Check the box once the action is finalised

Risk	Input (in financial terms)
Annualised financial risk	*36 **x** $350,000 = $12,600,000*

The organisation *risk rating [according to organisational risk matrix].*

Likelihood	Consequence / Impact	Organisation risk rating
*36 times per year maps to **'4 - Likely'*** *(using sample likelihood table)*	*$12,600,000 maps to **'5 – Severe'*** *(using sample consequence table)*	***Extreme*** *(intersection of 'Likely' and 'Severe' using sample risk table)*

The risk story can now be illustrated as follows:



Step 2 – Categorise and analyse existing controls

Action 1 – Conduct an inventory of existing controls	☑ Check the box once the action is finalised

In this example, the organisation's current controls are below.

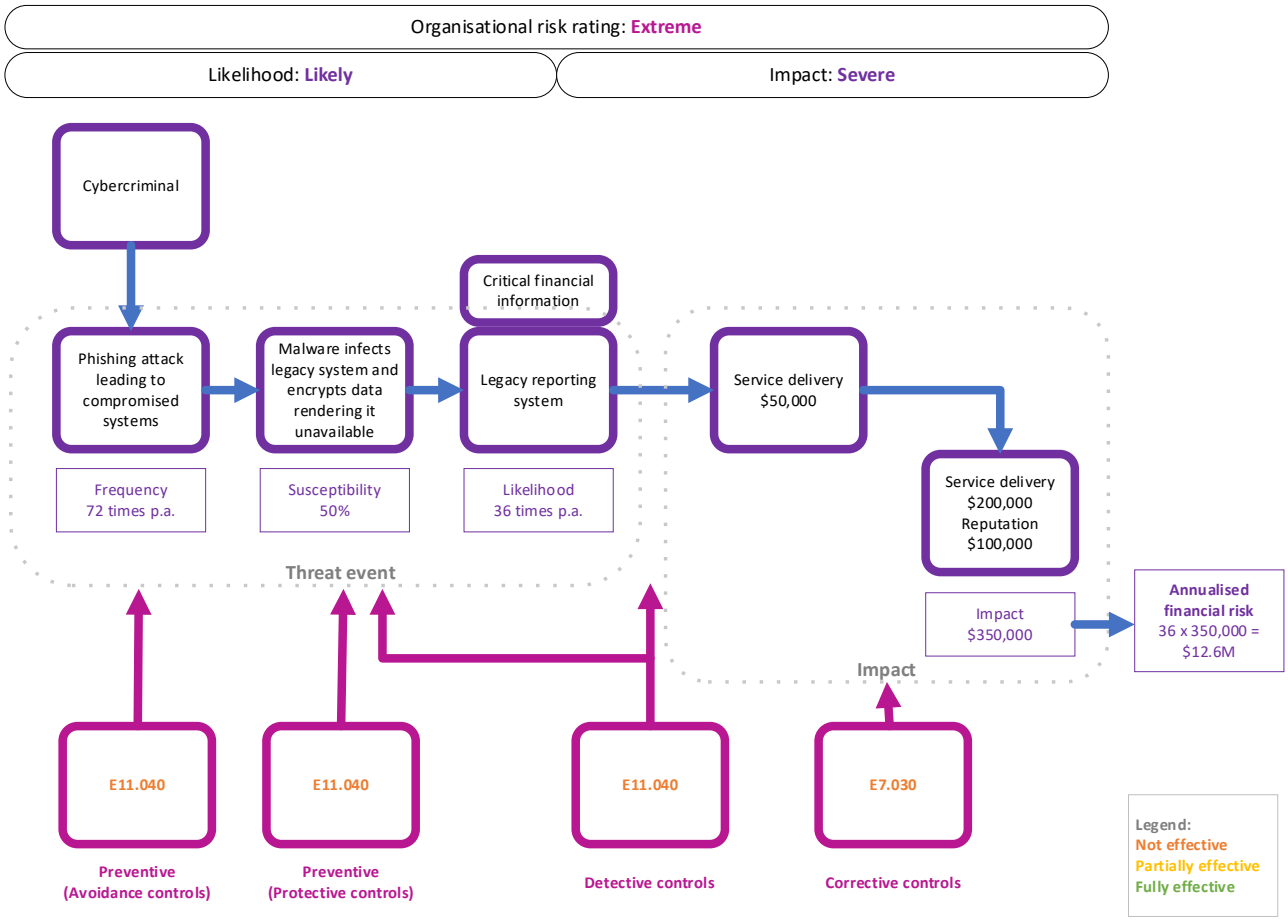
Element(s)	Control type	Control
E7.030 *The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas that are approved, tested and effective.*	***Corrective***	*The organisation undertakes regular testing of key information security aspects of business continuity and disaster recovery to help ensure that the impact of disruption can be better managed.*
E11.040 *Identification and management of vulnerabilities of key ICT assets.*	***Preventive*** ***Detective***	*The vulnerabilities of ICT assets, including those that are legacy, are identified and a remediation approach (which may include compensating controls) to limit the likelihood of vulnerabilities from being exploited is planned.*

Action 2 – Conduct an analysis of existing controls	☑ Check the box once the action is finalised

Once all the controls have been identified and recorded, they can be analysed for their effect on the reduction of risk. This includes analysing the effect of the controls based on their profile (the design and operating effectiveness at which the control is implemented and operating).

Element(s)	Control attributes
E7.030	***Design effectiveness:*** *Partially effective* ***Operating effectiveness:*** *Not effective* *Through both self-assessment and internal audit, the control was assessed as not effective in how the organisation utilises its disaster recovery and business continuity processes and plans regarding this legacy system. The attempts made to recover system backups were ineffective and should be tested further.* ***Effect:*** *Based on the assessment of the control, and the lack of tests performed to validate the effectiveness of the control, there is a minimal reduction to the probable risk impact.*
E11.040	***Design effectiveness:*** *Partially effective* ***Operating effectiveness:*** *Not effective* *Through both self-assessment and internal audit, the control was assessed as not effective. This was due to the organisation not having a robust method for the identification and management of system vulnerabilities.* ***Effect:*** *As the organisation lacks a well-defined plan or process for identifying vulnerabilities within ICT assets, this would have a minimal reduction to the probable risk impact.*

Taking these controls into consideration, the overall risk position is at **Extreme**. Our risk story including controls can be illustrated as follows:



Step 3 – Analyse proposed treatments

Action 1 – Identify the target risk rating	☑ Check the box once the action is finalised

In this example, with the current risk rating of **Extreme** not acceptable, it is important for management to agree on a target risk rating commensurate to the risk appetite of the organisation. In this instance, management has chosen the target risk rating to be **Low**.

Based on the current risk story, possible ways of reducing the risk level to **Low** includes reducing the:

- likelihood from **Likely** to **Unlikely**, and
- impact from **Extreme** to **Insignificant.**

Risk Rating	Input
Target risk rating	*Low*

Action 2 – Determine the treatments and control type(s) to reduce risk to the target risk rating	☑ Check the box once the action is finalised

Based on the risk story, the impacts (specifically the secondary impact) contribute significantly to the assessment of the risk and to some extent, can be managed by the organisation through appropriate uplift in detective and corrective controls.

While reduction of likelihood is possible, in the context of this organisation, controls can be more easily influenced or uplifted on a wider scale and therefore having a greater ability to reduce risk likelihood.

Using the risk story and the nature of the organisation, consider what approaches could be used to reduce the risk. Some considerations could include:

- Ensure that appropriate project plans are in place to migrate from legacy-based systems, especially those that are difficult to support, manage and secure;
- Ensure a greater level of preparedness through the identification of points of failure or weakness within the organisation's ICT assets so appropriate planning and management is in place;
- Improve incident management and ensure that suitable standard operating procedures are in place for the handling of information security related incidents so incidents can be managed as efficiently as possible;
- Create effective business continuity and disaster recover processes to manage business disruption and regularly test them so they can operate effectively when most needed including appropriate backup and restoration controls;
- Enhance the protection of ICT systems using a standard operating environment which limits the ability for systems to be compromised; and
- Provide appropriate security user awareness and training including how to identify phishing attempts and avoid clicking on malicious content.

Risk reduction may not necessarily involve the introduction of new controls as there may be benefit in uplifting existing controls. Risk treatments that may be considered in this example include:

Proposed treatment	Control type	Control
E7.030 – Proposed uplift *The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).*	***Corrective***	*The organisation invests in timely backups and a more rapid restoration process which is regularly tested that allows data to be restored in a smaller time window and therefore minimising the impact should data be lost.*

Proposed treatment	Control type	Control
E11.040 – Proposed uplift *Identification and management of vulnerabilities of key ICT assets.*	***Preventive*** ***Detective***	*While application of patches onto legacy systems are difficult, depending on the nature of the system it is possible to apply "virtual patching" solutions. In this instance, the organisation utilises a form of network intrusion prevention to identify targeted attacks that exploit vulnerabilities on the legacy system and block them.*
E5.030 – New treatment *The organisation delivers information security training and awareness to all persons with access to public sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.*	***Preventive***	*To further minimise the likelihood of phishing attempts being successful, the organisation implements a security user awareness program that includes a strong focus on phishing-based attacks and how to identify them.*
E6.030 – New treatment *The organisation has an incident management process and plan consisting of the 5 phases.*	***Detective***	*The organisation develops a formalised incident management process and introduces a "playbook" that specifically deals with ransomware attempts. The playbook provides clear guidance on how to capture appropriate log data, the procedures to follow should an attempt be detected, and should an incident occur, how the incident should be managed (and by whom).*
E11.090 – New treatment *The organisation manages standard operating environments (SOEs) for all ICT assets, including end user access devices (workstations, mobile phones, laptops), network infrastructure, servers, and Internet of Things (IoT) commensurate with security risk.*	***Preventive***	*The organisation introduces an SOE for all key systems including a strong focus on end user devices. This allows those systems to be less "exploitable" to known, and unknown attacks (such as the loading of malware should a user click on a phishing link that downloads and installs malware).*

Action 3 – Analyse the effect of proposed treatments ☑ Check the box once the action is finalised

Analyse the treatments and estimate the risk buy-down value (the level of investment in the control for the level of risk reduction).

The probable effect of the proposed treatments (assuming the controls are designed and operating effectively) are as follows:

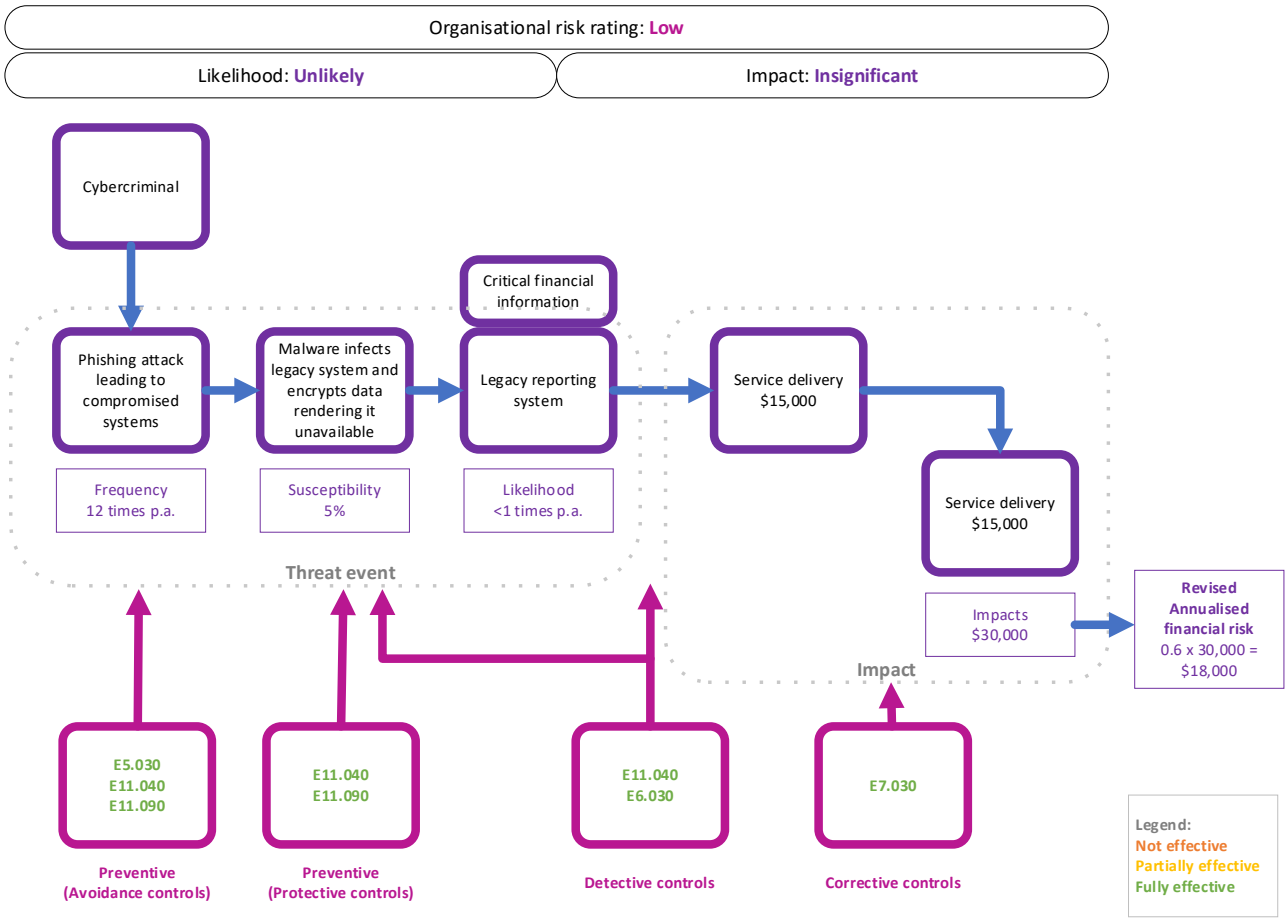
Risk attribute	Measure
Revised likelihood	***Unlikely*** *The investment in preventive controls sees a large reduction in the number of phishing emails that are clicked on and the SOEs in place minimise the ability for malware to be installed and executed. Improved vulnerability management ensures that vulnerabilities are identified and remediated in a timely manner for end user devices (a reduction from 6 per month to 1 per month).* *In addition, the introduction of the "virtual patching" capability for the legacy system reduces its susceptibility (from 50% to 5%) which provides a considerable overall reduction in likelihood (12 times a year x 5% = 0.6 events per annum).*
Revised annualised financial risk	***Insignificant*** *Primary impact = $15,000 per incident* *Secondary impact = $15,000 per incident* *Revised impact: $15,000 **+** $15,000 = $30,000* *Revised annualised financial risk = $18,000 per annum (30,000 **x** 0.6)* *With improved detection capability, an actual incident is detected and responded more rapidly. The ransomware playbook provides a coordinated approach across the organisation to minimise the impact of the incident. While there is still minimal impact at the time of the incident and effort involved in recovering data, this amount of manual effort is considerably reduced. There is also no longer a need to pay for the ransom as the data can be successfully recovered from backup. Further to this, as the ransom isn't required to be paid, there isn't a flow on secondary impact to reputation.*
Revised organisational risk rating	*By using the organisational risk matrix and mapping the revised likelihood with the revised annualised financial risk, the risk rating has now been reduced to **Low***

Risk attribute	Measure

Revised financial risk

The example demonstrates that if the investment is placed in the suitable controls, there is an opportunity for the organisation to achieve a considerable reduction of risk. This results in the probable risk moving from **Extreme** to **Low** or a reduction in financial impact terms of $12.6M to **$18K** (more than a 99% impact reduction). Therefore, even if the control investment required $400,000 for upfront cost, the return of the controls would still be considerable.

Our risk story, considering the control improvements, can now be illustrated as follows:



Step 4 – Monitor control effectiveness

The organisation utilises its risk management tools to manage the risk.

10.3 Example Three – Modification of sensitive personal information

Scenario

The risk of the unauthorised modification of sensitive personal information caused by privileged employees abusing their access to the Oracle database resulting in a negative impact to the organisation's operating budget.

Step 1 – Constructing the risk story

Action 1 – Identify the information asset components	☑ Check the box once the action is finalised

In this example the asset type is sensitive personal information. The BIL value for the data as listed in the IAR has been assessed as 2 (two) – Limited, with a protective marking of **OFFICIAL: Sensitive**

Asset details	Input
Asset name/ description	*Sensitive personal information*
Protective marking	*OFFICIAL: Sensitive*
Security value/ BIL	*Limited*
Supporting asset(s)	*Oracle database*

Action 2 – Map the risk factors (threat source, threat event(s)/ cause(s) and impact(s))	☑ Check the box once the action is finalised

Risk factors	Input
Threat source	*Privileged employee (internal threat source)*
Cause/ Threat event	*Abusing access privileges in a key application*
Risk event	*Unauthorised modification of information (loss of integrity)*

Risk factors	Input
Impact	*Primary impact –* *Impact to operating budget (public finances): Loss of operating budget in terms of unauthorised funds transferred at the time of the incident* *Secondary impact –* *Impact to operating budget (public finances): As a result of the incident, reconciliation and compensation needs to be provided for losses experienced.*

Action 3 – Estimate the likelihood of the risk

☑ Check the box once the action is finalised

In this example, data to assist with measuring likelihood were obtained from internal log sources.

Determining the likelihood of the risk requires us to understand more about the threat source, the threat event, and the supporting asset. This assists in determining where relevant data can be gathered to assist with measuring the likelihood.

Let us assume that internal system logs provide the following data points:

- privileged users access the internal database five (5) times per day, but typically never need to access sensitive personal data (depending on their role);
- where access to sensitive personal data is required by certain roles, it typically occurs once a day, on weekdays and during business hours (8am-6pm) so equates to 252 days;
- to date, there has only been two (2) prior recorded incidents of users abusing their privilege to access and disclose sensitive personal data. The period of these incidents is once a year. However, it was noted that the number could have been higher, as the only way these incidents were detected was based on notification by external parties that they had inappropriately seen this information being shared;
- all attempts to access data are successful (as it is provided as part of the user's role); and
- basic logging is performed (who accessed and when) but detailed activity logging (what users do once they are on) is not performed. Logs are checked on a weekly basis.

Based on this information, the likelihood of the risk can be measured as follows:

Measures of likelihood	Input
Frequency of the risk event	***Possible***[32] *(4 times a year)**

[32] As derived from the sample Likelihood Table in 8.6 Supporting Information

Measures of likelihood	Input
Susceptibility of supporting asset(s)	***High***[33] *(based on a 99% rate of susceptibility)*
Likelihood	***Possible*** *(4 times a year* ***x*** *99% = 3.96, or according to the sample Likelihood table, between 1 to 10 times a year).*

**Based on a minimum of once per year and maximum 252 times a year. Through discussion with the business, four (4) was estimated as a nominal realistic frequency rather than taking the average.*

Action 4 – Estimate the impact ☑ Check the box once the action is finalised

The information to assist with measuring probable impact(s) is provided from interviews with business stakeholders (similar to when information assets were being valued).

Measures of impacts	Input (in financial terms)
Primary impact	• *BIL 2 (Economy and Finance: Organisation's operating budget – 1%-10% of annual operating budget)* • *$50,000 per incident* • *Loss of finances due to inappropriate transfer of funds to modified HR records*
Secondary impact	• *BIL 2 (Economy and Finance: Organisation's operating budget – 1%-10% of annual operating budget)* • *$250,000 per incident* • *Cost of recovery and compensation for transferred funds*
Impact	*$50,000 + $250,000 = $300,000*

[33] As derived from the sample Susceptibility Table in 8.6 Supporting Information

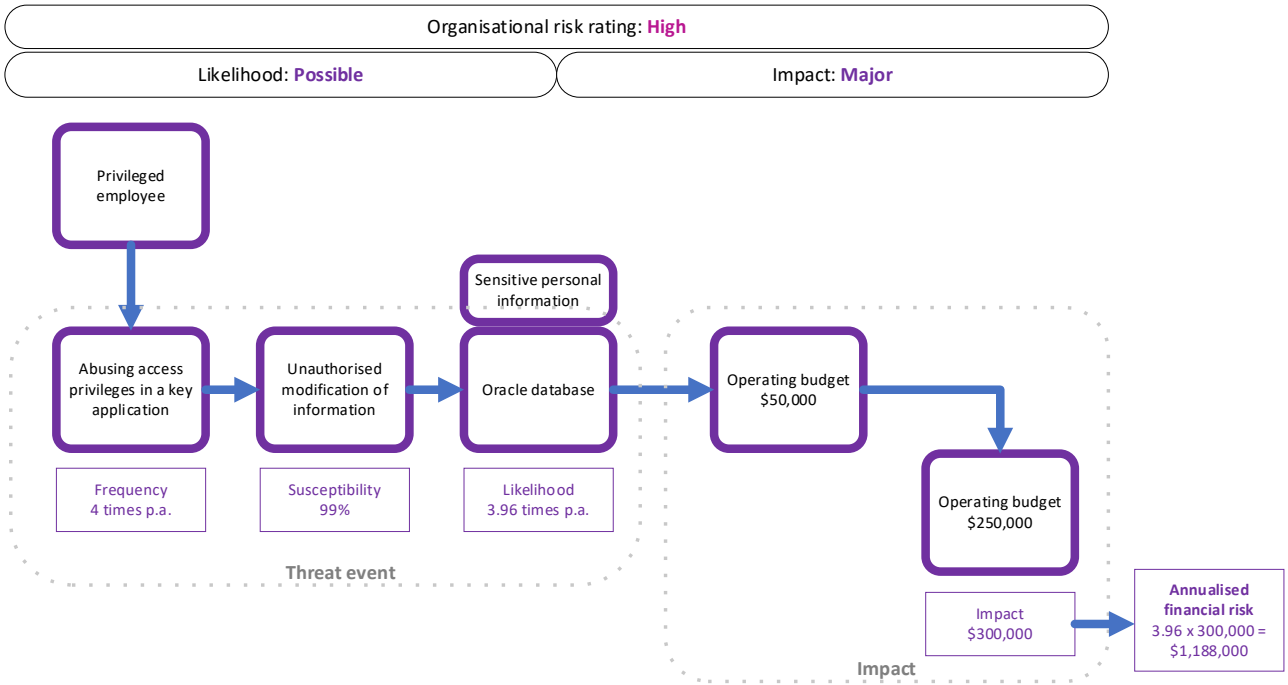
Action 5 – Calculate the annualised financial risk	☑ Check the box once the action is finalised

Risk	Input (in financial terms)
Annualised financial risk	*3.96* ***x*** *$300,000 = $ 1,188,000*

The organisation *risk rating [according to organisational risk matrix].*

Likelihood	Consequence / Impact	Organisation risk rating
3.96 times per year maps to ***'3 – Possible'*** *(using sample likelihood table)*	*$ 1,188,000 maps to* ***'4 – Major'*** *(using sample consequence table)*	***High*** *(intersection of 'Possible' and 'Major' using sample risk table)*

The risk story can now be illustrated as follows:



Step 2 – Categorise and analyse existing controls

Action 1 – Conduct an inventory of existing controls	☑ Check the box once the action is finalised

In this example, the organisation's current controls are below.

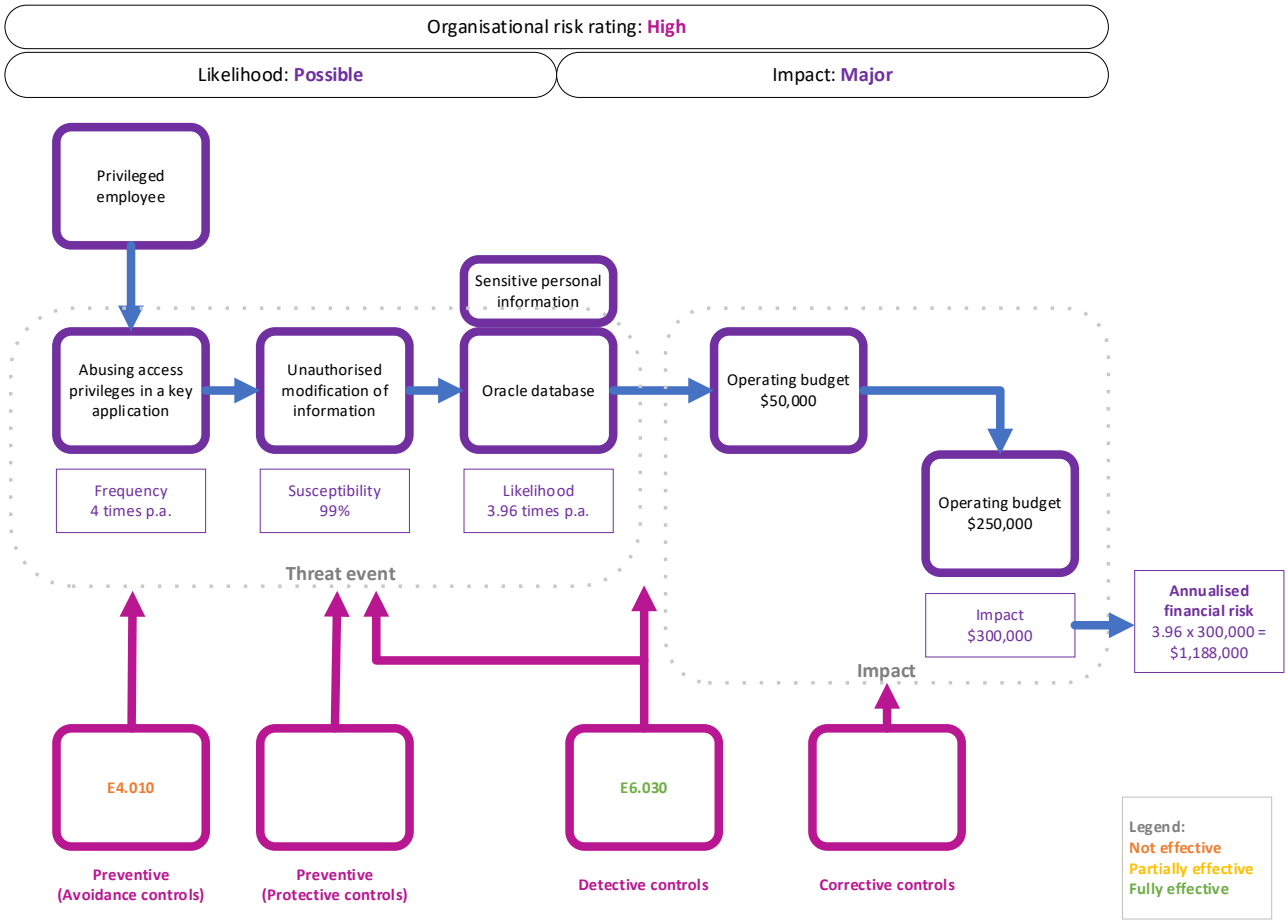
Element(s)	Control type	Control
E4.010 *The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know.*	***Preventive***	*The organisation established appropriate roles and assigned those to users based on their need to access certain information asset types.*
E6.030 *The organisation has an incident management process and plan consisting of the five (5) phases.*	***Detective***	*The organisation detects an incident that allows them to respond. Logs are reviewed on a weekly basis and mechanisms exist for the public to notify if they believe information has been inappropriately disclosed.*

Action 2 – Conduct an analysis of existing controls	☑ Check the box once the action is finalised

Once all the controls have been identified and recorded, they can be analysed for their effect on the reduction of risk. This includes analysing the effect of the controls based on their profile (the design and operating effectiveness at which the control is implemented and operating).

Element(s)	Control attributes
E4.010	***Design effectiveness:*** *Fully effective* ***Operating effectiveness:*** *Partially effective* *Through both self-assessment and internal audit, the control was assessed to be reasonably mature but not fully operating effectively. While roles were appropriately defined based on information asset types, roles were often cloned i.e., "copied and pasted" for new users rather than undertaking an appropriate assessment to determine the actual role a user would need.* *As a result, there were instances when a user was assigned a role that would provide a higher level of privilege than they needed for their role. And as there was no periodic review control in place to validate user access, the reduction in likelihood of the risk occurring was minimal.* ***Effect:*** *This has minimal reduction to the probable likelihood of the risk, as the threat event is based on a user which has a level of privilege assigned to their role.*
E6.030	***Design effectiveness:*** *Fully effective* ***Operating effectiveness:*** *Fully effective* *Through both self-assessment and internal audit, the control was assessed to be fully effective in how the organisation identifies and manages a potential incident.* ***Effect:*** *Based on the assessment of the control and the weekly review of logging data, the reduction to the probable risk impact is minimal.* *Despite how effective the control is, the challenge is that logging of the actual risk story (user accessing and then modifying data in an unauthorised manner) is not being performed. As such, even at a good level of effectiveness, the event would not be detected (and as a result, not responded to accordingly).*

Taking these controls into consideration, the overall risk position is at **High**. Our risk story including controls can be illustrated as follows:



Step 3 – Analyse proposed treatments

Action 1 – Identify the target risk rating	☑ Check the box once the action is finalised

In this example, with the current risk rating of **High** not acceptable, it is important for management to agree on a target risk rating commensurate to the risk appetite of the organisation. In this instance, management has chosen the target risk rating to be **Low**.

Based on the current risk story, possible ways of reducing the risk level to **Low** includes reducing the:

- likelihood from **Possible** to **Unlikely**, and
- impact from **Major** to **Insignificant**.

Risk Rating	Input
Target risk rating	*Low*

Action 2 – Determine the treatments and control type(s) to reduce risk to the target risk rating

☑ Check the box once the action is finalised

Based on the risk story, the impacts (specifically the secondary impact) contribute significantly to the assessment of the risk and to some extent, can be managed by the organisation through appropriate uplift of controls.

The risk story provides visibility of difficulties protecting the supporting asset when a privileged user has legitimate access. The susceptibility rate will always be **High**. Users with appropriate access will always have reasons around why they need to access certain information holdings. The objective in this instance, is not to apply an excessive number of controls, but identify the most effective controls to reduce overall risk.

Some considerations in reducing the risk based on visibility of the risk story could include:

- Improve personnel pre-engagement screening and maintain ongoing eligibility and suitability checks of personnel in high risk roles;
- Improve the effectiveness of access management controls so that all users are assigned to appropriate roles that adhere to the principles of least privilege;
- Perform periodic user revalidation to ensure role assignments are current and valid. Where necessary, update or have different levels of frequency that reflect the criticality/sensitive of the information asset and supporting systems e.g., more critical systems could have revalidation of one month while less critical systems could have a revalidation of six (6) months;
- Whilst it is not possible to “prevent” a system from a legitimate user who requires access to it, controls can be introduced to improve the logging of their activity. In this situation, the control provides a two-fold risk reduction. As a detective control, it provides the ability to enhance logging so that inappropriate activity including abuse of privileged access can be logged. When integrated into an effective incident response process, this can allow for more rapid incident management. In addition, with appropriate visibility of the control, it can function as a protective (preventive) control by deterring users from “doing the wrong thing” because all their activity is logged and monitored; and
- Uplift the incident response process so the organisation is better prepared to respond to the incident and manage the impact – namely improved alerting and visibility of more critical events so logs are reviewed more frequently.

Risk reduction may not necessarily involve the introduction of new controls as there may be benefit in uplifting existing controls. Risk treatments that may be considered in this example include:

Proposed treatment	Control type	Control
E4.010 – Proposed uplift *The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know.*	***Preventive***	*The organisation improves definition of access roles and develops a checklist to place the right users into the appropriate role types. This is then validated by the information owner before the role assignment is approved and implemented.*
E6.030 – Proposed uplift *The organisation has an incident management process and plan consisting of the 5 (five) phases.*	***Detective***	*The organisation proposes an improvement to the incident management control including performing alerting to key stakeholders as soon as an incident is detected. It also includes identifying an increased frequency for monitoring key risk stories.*
E4.070 – New treatment *The organisation regularly reviews and adjusts physical and logical access rights considering operational changes.*	***Preventive***	*The organisation introduces a periodic revalidation of user access. The revalidation periods are aligned to information asset criticality/ sensitivity and supporting systems. Access to the internal database for example is revalidated every two months.*
E10.040 – New treatment *The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.*	***Preventive*** ***Detective***	*The organisation conducts regular personnel checks e.g., police checks, probity checks on staff in identified roles.*

Proposed treatment	Control type	Control
E11.110 – New treatment *The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/prevention systems (IDS/IPS)).*	***Detective***	*The organisation implements specific user activity monitoring across key systems that support critical information assets. For the internal database, it includes logging all activity including the definition of "normal" and "abnormal" activity so events of interest can be more rapidly fed into the incident response process and be alerted.*

Action 3 – Analyse the effect of proposed treatments ☑ Check the box once the action is finalised

Analyse the treatments and estimate the risk buy-down value (the level of investment in the control for the level of risk reduction).

The probable effect of the proposed treatments (assuming the controls are designed and operating effectively) are as follows:

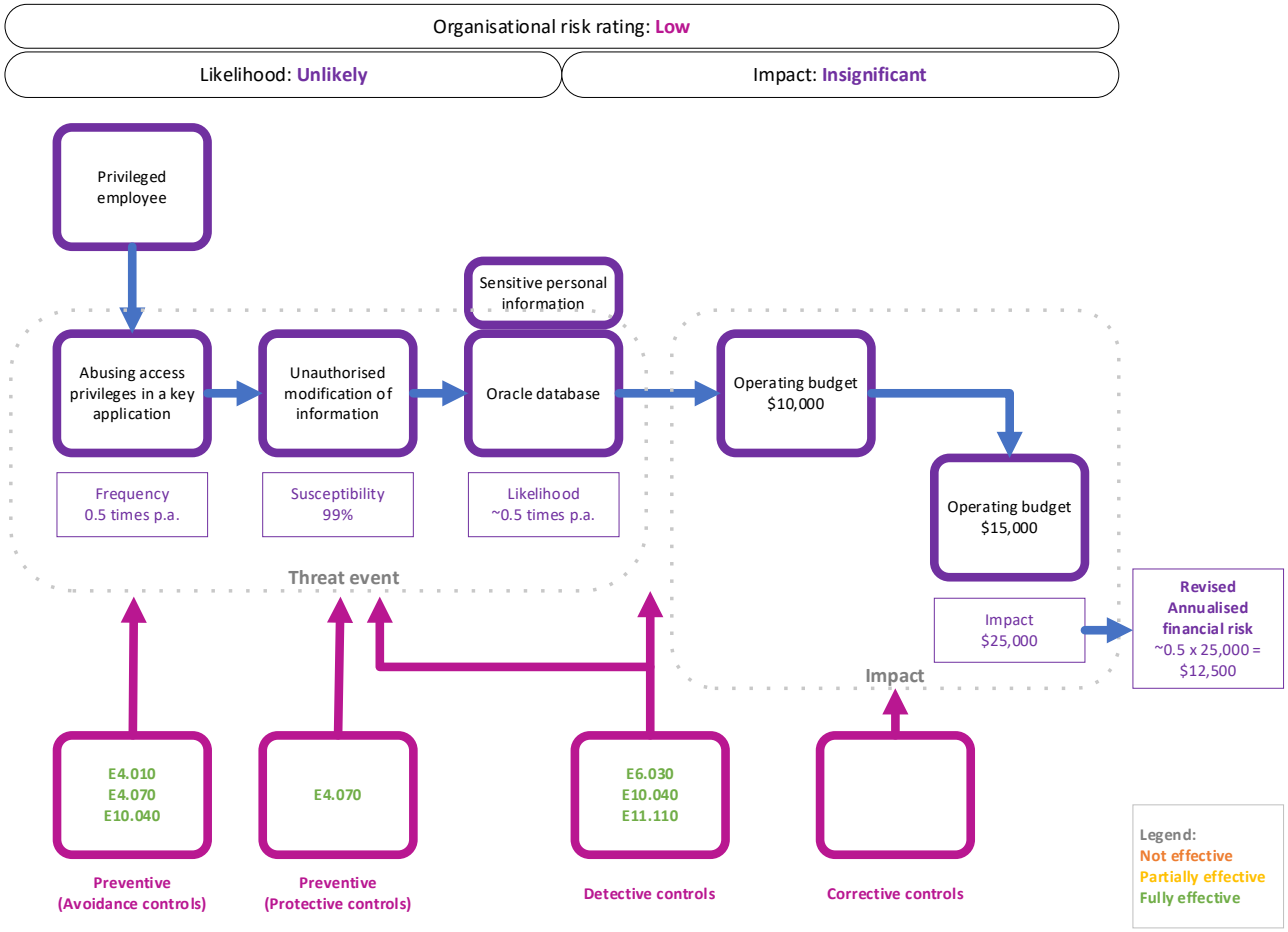
Risk attribute	Measure
Revised likelihood	***Unlikely*** *Hiring appropriate personnel as well as improved access management including revalidation as well as monitoring of user activity creates a significant reduction in the likelihood of ability/ attempts to abuse privileged access. This reduces the frequency of the event from 4 times a year to once every 2 years (or 0.5 times a year). The revised likelihood is 0.5 times a year x 99% susceptibility ≈ 0.5% events per annum*
Revised annualised financial risk	***Insignificant*** *Primary impact = $10,000 per incident* *Secondary impact = $15,000 per incident* *Revised impact: $10,000 **+** $15,000 = $25,000 per incident* *Revised annualised financial risk: $12,500 per annum ($25,000 **x** ~0.5)* *With both an uplift in incident response processes, as well as improving the review of logs from seven (7) days to one day for critical systems, the organisation is better able to detect and respond to the incident and therefore minimises the initial impact of the incident. This includes the ability to log specific user activity and identify when abnormal activity is occurring e.g., someone making a significant number of unauthorised changes to the database. This results in the ability to minimise the primary impact (limiting the amount of change that is possible) and therefore the secondary impacts of the event.*
Revised organisational risk rating	*By using the organisational risk matrix and mapping the revised likelihood with the revised annualised financial risk, the risk rating has now been reduced to **Low***

Risk attribute	Measure

Revised financial risk

The example demonstrates that if the investment is placed in the suitable controls, there is an opportunity for the organisation to achieve a considerable reduction of risk. This results in the probable risk moving from **High** to **Low** or a reduction in financial impact terms of $1,188,000 to **~$12.5K** (a 99% impact reduction). Therefore, even if the control investment required $300,000 for upfront cost, the return of the controls would still be considerable.

Our risk story, considering the control improvements, can now be illustrated as follows:



Step 4 – Monitor control effectiveness

The organisation utilises its risk management tools to manage the risk.

11 Part Four - Appendix

11.1 VPDSS Element to control type chart

The following chart maps each of the VPDSS Elements to their control type (preventive, detective, and corrective). It is important to note that assignment of control type is applied at the element level and specific controls under an element may have a more specific effect.

Element	Description	Control Type
Standard 1 - Information Security Management Framework		
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.	Preventive, Detective and Corrective
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.	Preventive (Avoidance and Protective)
E1.030	The organisation's information security management framework aligns with its risk management framework.	Preventive (Avoidance and Protective)
E1.040	Executive management defines information security functions, roles, responsibilities, competencies, and authorities.	Preventive (Avoidance and Protective)
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.	Preventive (Avoidance and Protective)
E1.060	Executive management owns, endorses, and sponsors the organisation's ongoing information security program(s) including the implementation plan.	Preventive, Detective and Corrective
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.	Detective and Corrective
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).	Preventive, Detective and Corrective
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.	Preventive (Avoidance)
E1.100	The organisation documents its internal control library that addresses its information security risks.	Preventive (Avoidance and Protective)

Element	Description	Control Type
E1.110	The organisation monitors, reviews, validates, and updates the information security management framework.	Preventive (Avoidance)
Standard 2 - Information Security Value		
E2.010	The organisation's Information Management Framework incorporates all security areas.	Preventive (Avoidance and Protective)
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.	Preventive (Avoidance and Protective)
E2.030	The organisation uses a contextualised VPDSF business impact level (BIL) table to assess the security value of public sector information.	Preventive (Avoidance and Protective)
E2.040	The organisation identifies and documents the security attributes (confidentiality, integrity, and availability business impact levels) of its information assets in its information asset register.	Preventive (Avoidance and Protective)
E2.050	The organisation applies appropriate protective markings to information throughout its lifecycle.	Preventive (Avoidance and Protective)
E2.060	The organisation manages the aggregated (combined) security value of public sector information.	Preventive (Avoidance and Protective)
E2.070	The organisation continually reviews the security value of public sector information across the information lifecycle.	Preventive (Avoidance and Protective)
E2.080	The organisation manages externally generated information in accordance with the originator’s instructions.	Preventive (Avoidance and Protective)
E2.090	The organisation manages the secure disposal (archiving/destruction) of public sector information in accordance with its security value.	Preventive (Avoidance and Protective)
Standard 3 - Information Security Risk Management		

Element	Description	Control Type
E3.010	The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: Risk identification; Risk analysis; Risk evaluation; and, Risk treatment.	Preventive, Detective and Corrective
E3.020	The organisation records the results of information security risk assessments and treatment plans in its risk register.	Preventive (Avoidance)
E3.030	The organisation considers information security risks in organisational planning.	Preventive, Detective and Corrective
E3.040	The organisation communicates and consults with internal and external stakeholders during the information security risk management process.	Preventive (Avoidance and Protective)
E3.050	The organisation governs, monitors, reviews, and reports on information security risk (e.g., operational, tactical, and strategic through a risk committee (or equivalent, e.g., audit, finance, board, corporate governance)).	Preventive, Detective and Corrective
Standard 4 - Information access		
E4.010	The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know	Preventive (Avoidance)
E4.020	The organisation documents a process for managing identities and issuing secure credentials (registration and de-registration) for physical and logical access to public sector information.	Preventive (Avoidance and Protective)
E4.030	The organisation implements physical access controls (e.g., key management, swipe card access, visitor passes) based on the principles of least-privilege and need-to-know.	Preventive (Protective)

Element	Description	Control Type
E4.040	The organisation implements logical access controls (e.g., network account, password, two-factor authentication) based on the principles of least-privilege and need-to-know.	Preventive (Protective)
E4.050	The organisation manages the end-to-end lifecycle of access by following provisioning and de-provisioning processes.	Preventive (Avoidance)
E4.060	The organisation limits the use of, and actively manages, privileged physical and logical access, and separates these from normal access (e.g., executive office access, server room access, administrator access).	Preventive (Avoidance and Protective)
E4.070	The organisation regularly reviews and adjusts physical and logical access rights taking into account operational changes.	Preventive (Avoidance and Protective)
Standard 5 - Information security obligations		
E5.010	The organisation documents its information security obligations and communicates these to all persons with access to public sector information (e.g., policies, position descriptions).	Preventive (Avoidance)
E5.020	The organisation's information security training and awareness content covers all security areas.	Preventive (Avoidance)
E5.030	The organisation delivers information security training and awareness to all persons with access to public sector information, upon engagement and at regular intervals thereafter in accordance with its training and awareness program and schedule.	Preventive (Avoidance)
E5.040	The organisation provides targeted information security training and awareness to persons in high-risk functions or who have specific security obligations (e.g., executives, executive assistants, procurement advisors, security practitioners, risk managers).	Preventive (Avoidance)
E5.050	The organisation reviews and updates the information security obligations of all persons with access to public sector information.	Preventive (Avoidance)

Element	Description	Control Type
E5.060	All persons with access to public sector information acknowledge their information security obligations at least annually (e.g., during performance development discussions, attending security briefings, completing security training).	Preventive (Avoidance)
E5.070	The organisation monitors, reviews, validates, and updates its information security training and awareness program and schedule.	Preventive and Detective
Standard 6 - Information security Incident Management		
E6.010	The organisation documents and communicates processes and plan(s) for information security incident management covering all security areas.	Preventive (Avoidance) and Detective
E6.020	The organisation articulates roles and responsibilities for information security incident management.	Detective
E6.030	The organisation's information security incident management processes and plan(s) contain the five phases of: Plan and prepare; Detect and report; Assess and decide; Respond (contain, eradicate, recover, notify); and, Lessons learnt.	Detective
E6.040	The organisation records information security incidents in a register.	Detective
E6.050	The organisation's information security incident management procedures identify and categorise administrative (e.g., policy violation) incidents in contrast to criminal incidents (e.g., exfiltrating information to criminal associations) and investigative handover.	Detective
E6.060	The organisation regularly tests (at least annually) its incident response plan(s).	Detective

Element	Description	Control Type
Standard 7 - Information Security Aspects of Business Continuity and Disaster Recovery		
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.	Corrective
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.	Corrective
E7.030	The organisation regularly tests (at least annually) its business continuity and disaster recovery plan(s).	Corrective
Standard 8 - Third party agreements		
E8.010	The organisation's information security policies, procedures and controls cover the entire lifecycle of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).	Preventive, Detective and Corrective
E8.020	The organisation includes requirements from all security areas in third-party arrangements (e.g., contracts, MOUs and information sharing agreements) in accordance with the security value of the public sector information.	Preventive, Detective and Corrective
E8.030	The organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement.	Preventive (Avoidance and Protective)
E8.040	The organisation identifies and assigns information security roles and responsibilities in third-party arrangements (e.g., contracts, MOUs and information sharing agreements).	Preventive (Avoidance and Protective)
E8.050	The organisation establishes, maintains, and reviews a register of third-party arrangements (e.g., contracts, MOUs and information sharing agreements).	Preventive (Avoidance and Protective) and Detective
E8.060	The organisation monitors, reviews, validates, and updates the information security requirements of third-party arrangements and activities.	Preventive (Avoidance and Protective) and Detective

Element	Description	Control Type
E8.070	The organisation documents its information release management requirements (e.g., social media, news, DataVic).	Preventive (Protective) and Corrective
E8.080	The organisation manages the delivery of maintenance activities and repairs (on-site and off-site).	Detective
E8.090	The organisation applies appropriate security controls upon completion or termination of a third-party arrangement (e.g., contracts, MOUs and information sharing agreements).	Preventive (Avoidance)
Standard 9 - Information Security Reporting to OVIC		
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (BIL) of 2 (limited) or higher.	Detective
E9.020	The organisation submits its Protective Data Security Plan (PDSP) to OVIC every two years.	Preventive, Detective and Corrective
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.	Preventive, Detective and Corrective
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	Preventive, Detective and Corrective
Standard 10 - Personnel Security		
E10.010	The organisation's personnel security policies and procedures address the personnel lifecycle phases of: Pre-engagement (eligibility and suitability); Engagement (ongoing and re-engagement); and, Separating (permanently or temporarily).	Preventive (Avoidance and Protective)
E10.020	The organisation verifies the identity of personnel, re-validates, and manages any changes as required.	Preventive and Detective
E10.030	The organisation undertakes pre-engagement screening commensurate with its security and probity obligations and risk profile.	Preventive (Avoidance) and Detective

Element	Description	Control Type
E10.040	The organisation manages ongoing personnel eligibility and suitability requirements commensurate with its security and probity obligations and risk profile.	Preventive (Avoidance) and Detective
E10.050	The organisation manages personnel separating from the organisation commensurate with its security and probity obligations and risk profile.	Preventive (Avoidance) and Detective
E10.060	The organisation develops security clearance policies and procedures to support roles requiring high assurance and/ or handling security classified information.	Preventive (Avoidance and Protective)
E10.070	The organisation undertakes additional personnel screening measures commensurate with the risk to support roles requiring high assurance and/ or handling security classified information.	Preventive (Avoidance) and Detective
E10.080	The organisation actively monitors and manages security clearance holders.	Preventive (Avoidance) and Detective
Standard 11 - Information Communications Technology (ICT) Security		
E11.010	The organisation manages security documentation for its ICT systems (e.g., system security plans).	Preventive (Avoidance and Protective)
E11.020	The organisation manages all ICT assets (e.g., on-site, and off-site) throughout their lifecycle.	Preventive (Avoidance and Protective)
E11.030	The organisation conducts a security assessment for authorising systems to operate prior to transmitting, processing, or storing public sector information.	Preventive (Avoidance) and Detective
E11.040	The organisation undertakes risk-prioritised vulnerability management activities (e.g., patch management, penetration testing, continuous monitoring systems).	Preventive (Avoidance and Protective), Detective
E11.050	The organisation documents and manages changes to ICT systems.	Preventive (Avoidance and Protective), Detective
E11.060	The organisation manages communications security controls (e.g., cabling, telephony, radio, wireless networks).	Preventive (Avoidance and Protective)

Element	Description	Control Type
E11.070	The organisation verifies the vendors security claims before implementing security technologies.	Preventive (Avoidance)
E11.080	The organisation manages security measures (e.g., classification, labelling, usage, sanitisation, destruction, disposal) for media.	Preventive (Avoidance and Protective)
E11.090	The organisation manages standard operating environments (SOEs) for all ICT assets, including end user access devices (workstations, mobile phones, laptops), network infrastructure, servers, and Internet of Things (IoT) commensurate with security risk.	Preventive (Avoidance and Protective)
E11.100	The organisation manages security measures for email systems.	Preventive (Avoidance and Protective), Detective
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (IDS/ IPS)).	Detective
E11.120	The organisation uses secure system administration practices.	Preventive (Avoidance and Protective)
E11.130	The organisation designs and configures the ICT network in a secure manner (e.g., segmentation, segregation, traffic management, default accounts).	Preventive (Avoidance and Protective)
E11.140	The organisation manages a process for cryptographic keys (e.g., disk encryption, certificates).	Preventive (Protective)
E11.150	The organisation uses cryptographic controls for confidentiality, integrity, non-repudiation, and authentication commensurate with the risk to information.	Preventive (Avoidance and Protective)
E11.160	The organisation manages malware prevention and detection software for ICT systems.	Preventive (Protective)
E11.170	The organisation segregates emerging systems from production systems (e.g., physical and/ or logical) until their security controls are validated.	Preventive (Avoidance)
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing, retention).	Corrective

Element	Description	Control Type
E11.190	The organisation manages a secure development lifecycle covering all development activities (e.g., software, web based applications, operational technology (Supervisory Control and Data Acquisition/ Industrial Control Systems (SCADA/ICS)).	Preventive (Avoidance and Protective)
E11.200	The organisation manages security measures for enterprise mobility (e.g., mobile device management, working from home).	Preventive (Avoidance and Protective)
Standard 12 - Physical Security		
E12.010	The organisation plans and documents physical security measures.	Preventive, Detective and Corrective
E12.020	The organisation applies defence-in-depth physical security measures.	Preventive, Detective and Corrective
E12.030	The organisation selects physical security measures commensurate with the business impact level of the information.	Preventive, Detective and Corrective
E12.040	The organisation has scalable physical security measures ready for activation during increased threat situations.	Preventive
E12.050	The organisation implements physical security measures when handling information out of the office.	Preventive
E12.060	The organisation manages physical security measures throughout their lifecycle.	Preventive, Detective and Corrective