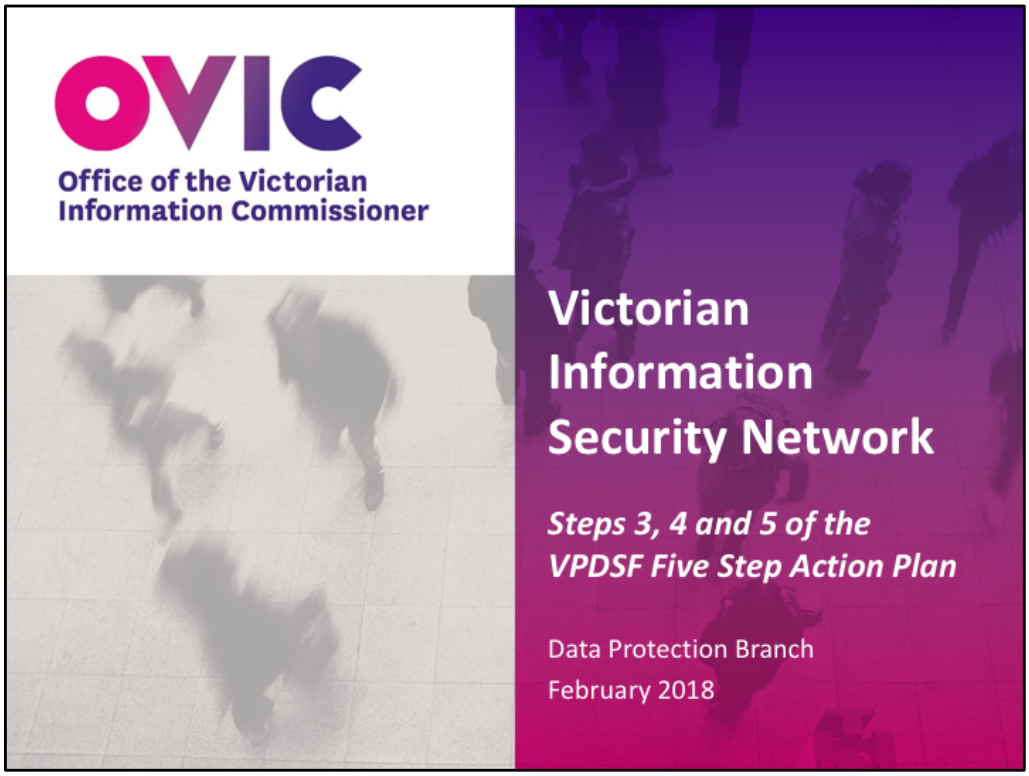
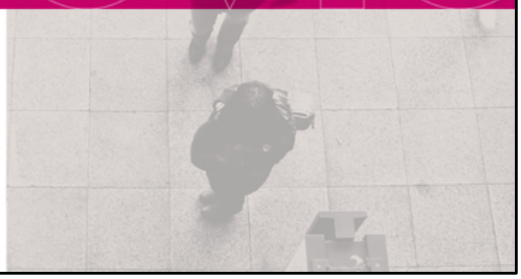

OVIC
Office of the Victorian Information Commissioner
Victorian Information Security Network
Steps 3, 4 and 5 of the VPDSF Five Step Action Plan
Data Protection Branch
February 2018

Acknowledgement

We acknowledge the Traditional Owners of the land on which we are meeting today and pay our respects to their Elders, past and present, and the Elders from other communities who may be here today.

OVIC
Office of the Victorian Information Commissioner



Sli.do

sli.do

Sli.do is an online tool designed to help audiences engage in meetings and events.

Those using the tool can submit questions for Q&A session, get instant feedback via live polls and access or download a copy of these slides on their device for future reference

Simply navigate to www.slido.com

Enter code B458

OVIC
Office of the Victorian Information Commissioner

Recording

This session is being live streamed and recorded on periscope.

The recording will be available after the session for those who could not attend.

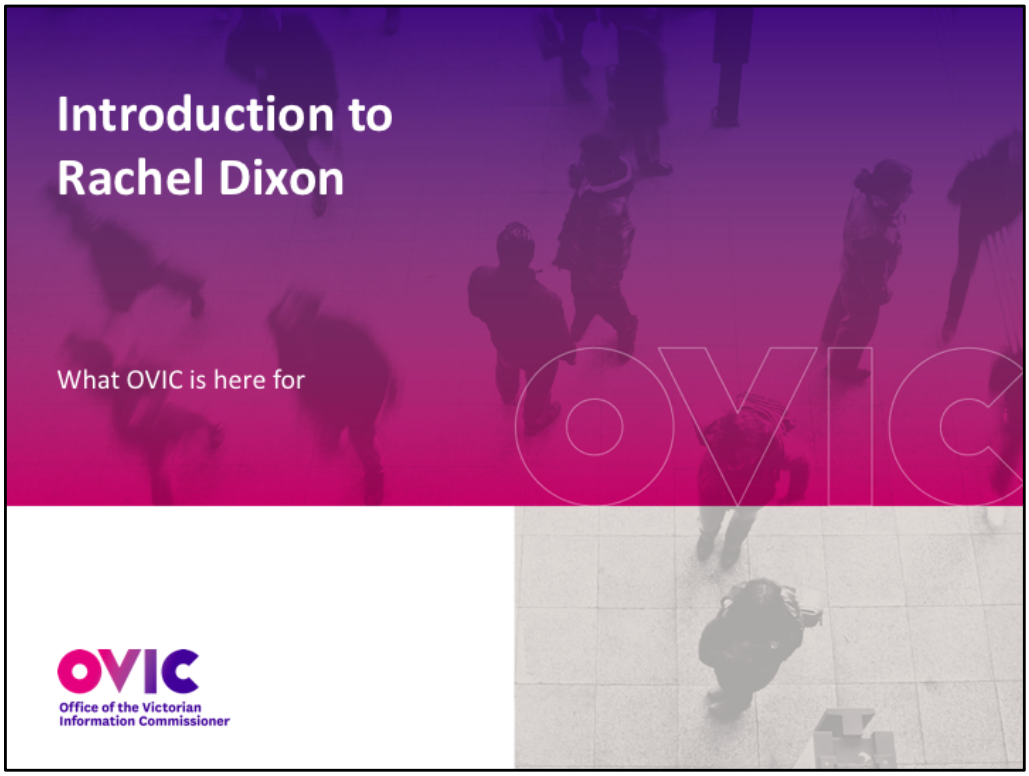
Go to our twitter page https://twitter.com/OVIC_AU

And click on the VISN tweet to navigate to periscope

OVIC
Office of the Victorian Information Commissioner

Agenda

1. **Introduction to Rachel Dixon, Privacy and Data Protection Deputy Commissioner**
2. **Adding security to the risk discussion** by Jonathon Masom, Victorian Managed Insurance Authority (VMIA)
3. **Steps 3, 4, and 5 of the VPDSF five step action plan** by Data Protection Branch, OVIC
4. **A VPS organisation's experience** by Tony Smith, East Gippsland Water
5. **2018 Reporting requirements** by Data Protection Branch, OVIC
6. **Question and Answer panel**, All presenters



Rachel Dixon was the former head of digital identity projects at the Digital Transformation Agency and is now responsible for privacy and data protection in the office of the Victorian Information Commissioner

Rachel has had “a diverse and impressive career holding senior positions in the private sector for Australian and International technology companies, where she led large teams and developed expertise in the areas of data, privacy, cybersecurity and information security”

Welcome Rachel

What OVIC is here for

OVIC is an independent regulator.

- Responsible under the Privacy and Data Protection Act 2014
- Responsible for the Victorian Protective Data Security Framework and the VPDS Standards

OVIC wants to facilitate cultural change - from 1990s IT, to contemporary corporate governance

There is no perfect security, only better security

OVIC
Office of the Victorian Information Commissioner

To speak to you about considering information security in risk management, we have Jonathon Masom from the Victorian Managed Insurance Agency (VMIA)

Welcome Jonathon.

- VMIA's purpose is to build a confident, resilient Victoria through world leading harm prevention and recovery.

About us

- As the State's insurer, we have developed tailored insurance products which cover government operations and infrastructure.

More than
4,300
clients across the State

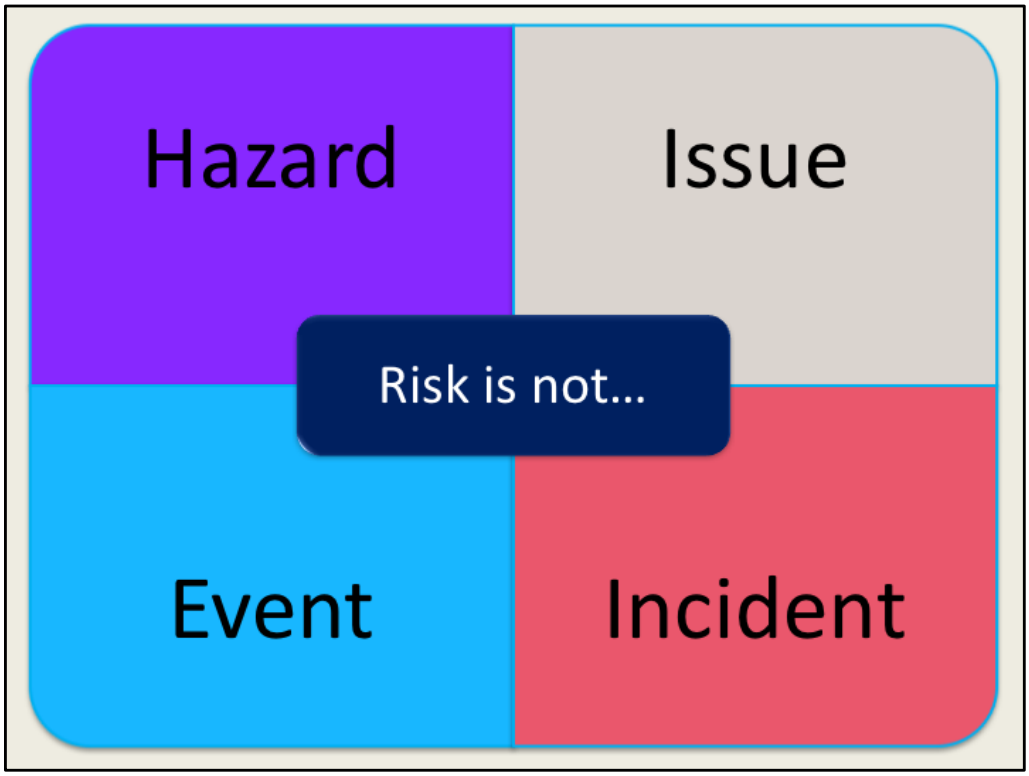
$195 billion
of the State's assets

79%
client engagement score

Appetite for risk

Risk definition:
the effect of uncertainty on objectives

vmia
Risk Management and Insurance



The concept of risk is related to other concepts which have a slightly different emphasis.

An issue: A present problem or concern influencing organisational objectives. A risk can become an issue, but an issue is not a risk!

A hazard: Anything that has the potential to harm people, property. A risk arises when it is possible that a hazard will actually cause harm.

An event: An occurrence or change of a particular set of circumstances. An event can:

Be one or more occurrences, and can have several causes
Consist of something not happening
Sometimes be referred to as an 'incident' or 'accident'.
Without consequences can also be referred to as a 'near miss'.

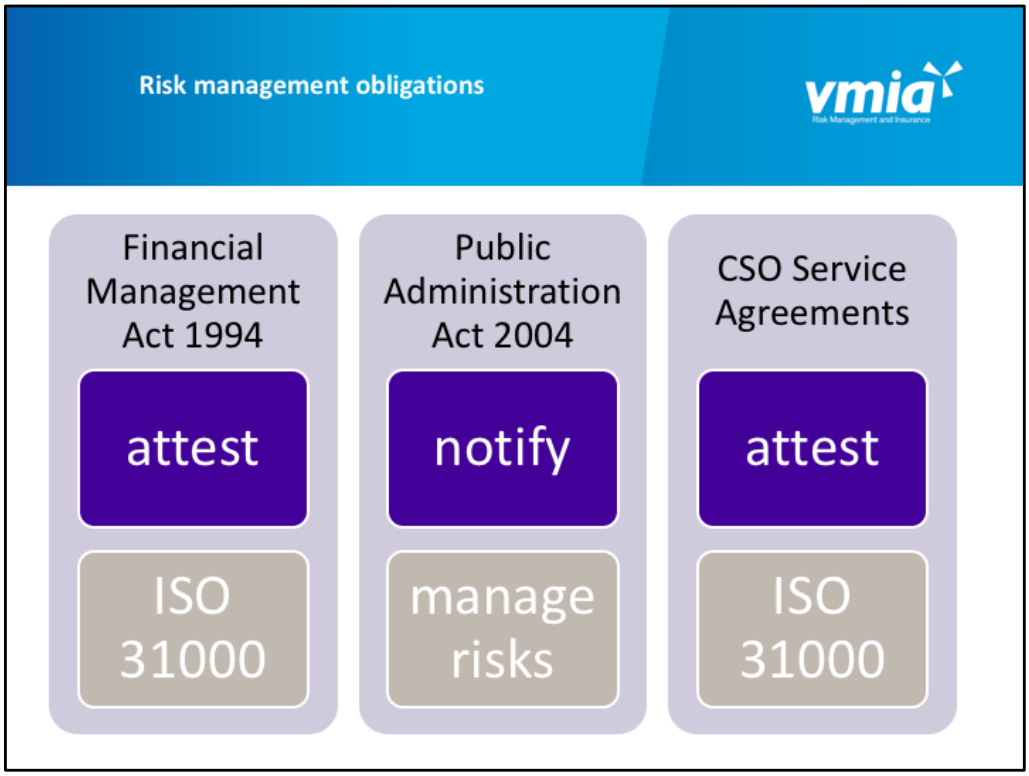
An incident is: An event or circumstance which could have, or did lead to, unintended and/or unnecessary **harm** to a person and/or a complaint, loss or damage.

Examples

Objective	Risk
Financial	**fraud** attributed to poor IT access control systems, resulting in financial loss
Operations	**flood** resulting in possible injury/ loss of life and damage to natural assets
Strategic	**loss of staff** resulting in loss of skills / corporate knowledge and inability to deliver on targets
Reputational	**negative PR around key sports identity** not in line with company's brand message harms sales

Cabinet video

- Don’t have to go far to see information security risks!
- http://www.abc.net.au/insiders/the-cabinet-files/9394426



Key Message

Risk management is not a 'nice to have' - agencies have legislated obligations with respect to risk management and as an employee you need to be aware of what those obligations are and operate within them.

Agencies are expect to attest in their annual reports that:

they have risk management processes in place consistent with the Standard (or its successor);
these processes are effective in controlling risks to a satisfactory level; and
a responsible body or Audit committee verifies that view.

Agencies have obligations with respect to Risk Management that come from standing direction 4.5.5. and supported by VGRMF

Key points:

The Board or Accountable Officer:

Is ultimately responsible for the risk management framework.

Must ensure that it understands its responsibilities and has in place a mechanism to assure itself that it is meeting those.

May choose to delegate some responsibilities to a committee or Executive and senior management.

Delegation of responsibilities does not negate the Board's or Accountable Officer's responsibilities and accountabilities with respect to risk management.

- A board is ultimately responsible for oversight of the risk management framework

Under the Public Administration Act 2004 (s. 81(1)(b)) a Board of a public entity governed by Division 2 of Part 5 of the Public Administration Act must inform the responsible Minister and the relevant Department

Sources of risk

Strategic

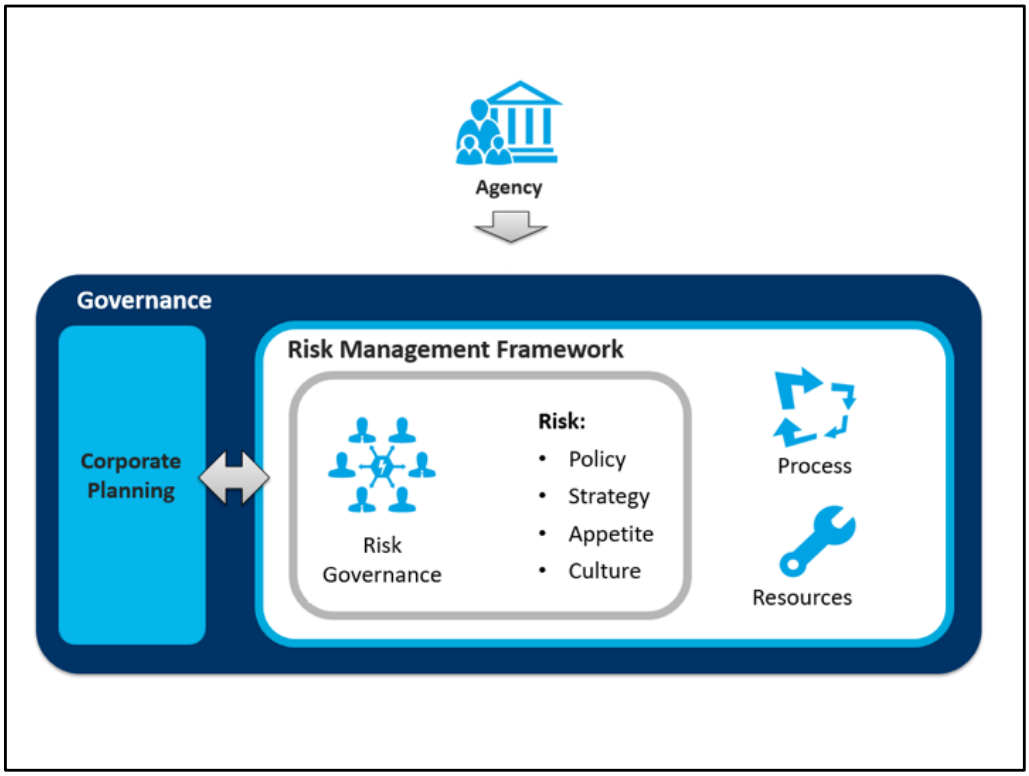
- Risk we make

Operational

- Internal capability

External

- Nature, markets



Talk through the three VMIA's model RM framework: key elements – Risk Governance, Resources & Capability and Process. "Process" will be dealt with in more detail later in the training.

Also highlight the link to an agency's overall corporate governance and its corporate planning process.

The Risk Management Framework includes a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

A risk management framework is not one discrete policy or document, it comprises the totality of the structures, policies, strategies, procedures and resources within an organisation that support risk management. Each organisation is unique and must ensure that a risk management framework is implemented and appropriate to the activity, size and complexity of the organisation, aligns with the defined risk profile and meets legislative or government policy requirements.

Q. What do you know about your organisation's risk management framework?

Agencies must adopt the approach outlined in this VGRMF and have in place a risk management framework to provide for consistent risk management practices across the public sector; which is aligned with the AS/NZS Standard or its successor.

A Risk Management Framework provides:

Systematic approach to risk identification & management.

Consistent risk assessment criteria.

Accurate and concise risk information, for decisions.

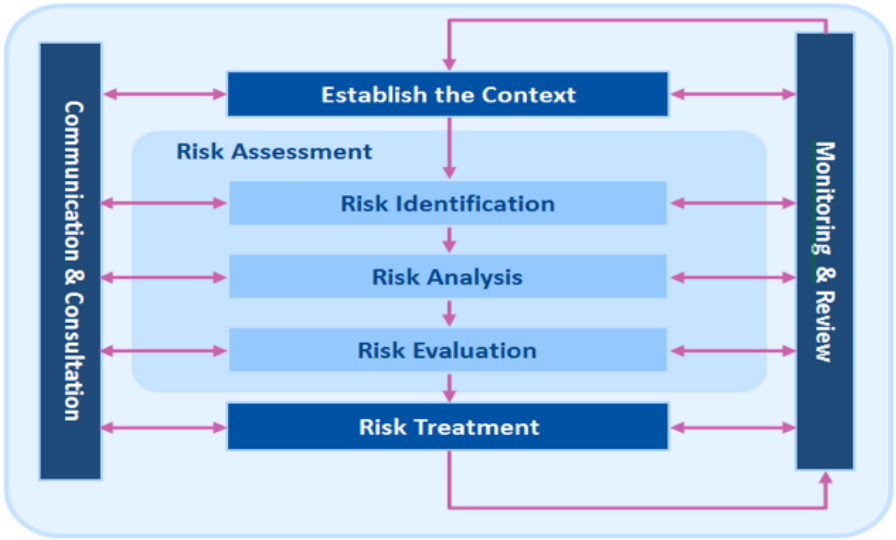
Cost effective and efficient risk treatment strategies.

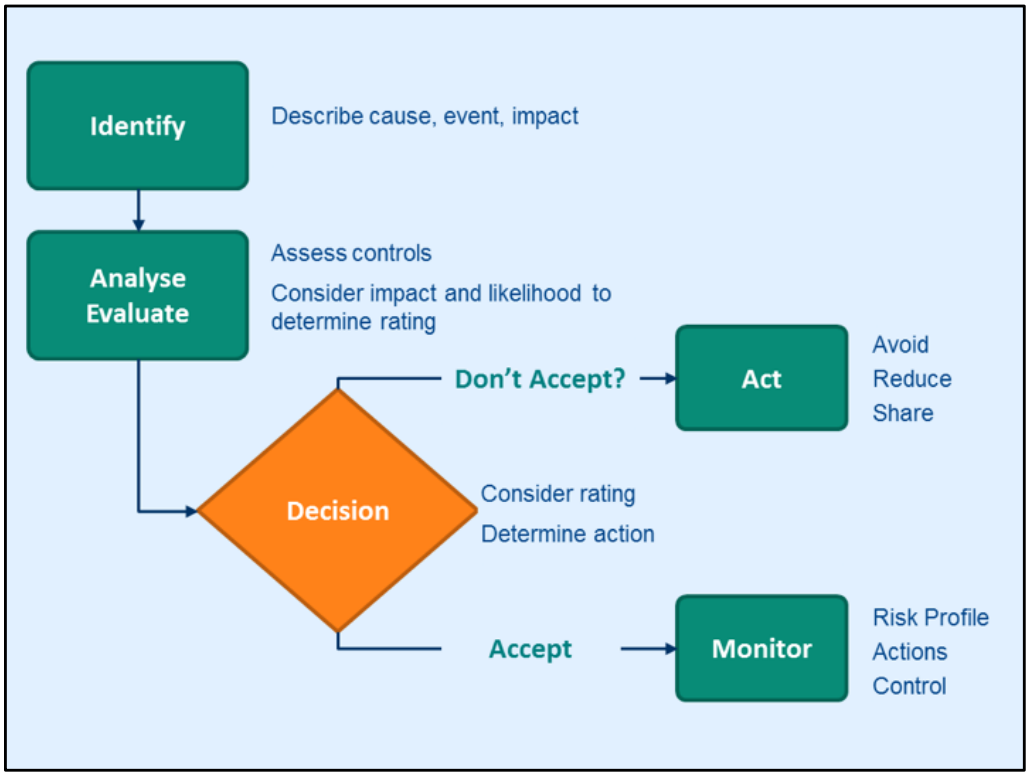
Ensure risk exposure remains within acceptable level.

'Cyberrisk' AND 'Data fraud or theft' rank highly
World Economic Forum – global risks report

- http://reports.weforum.org/global-risks-2018/global-risks-of-highest-concern-for-doing-business-2018/

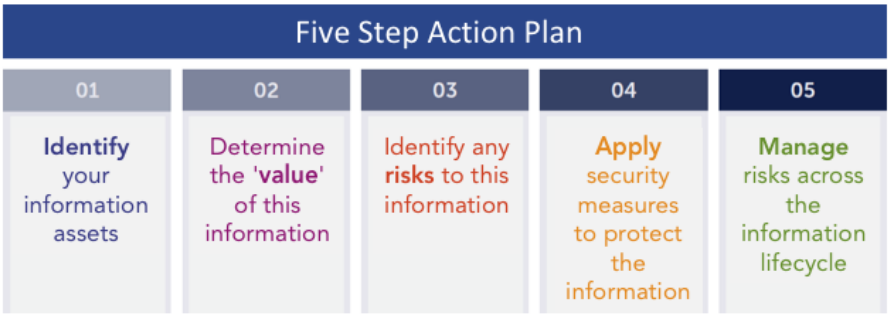
Process based approach

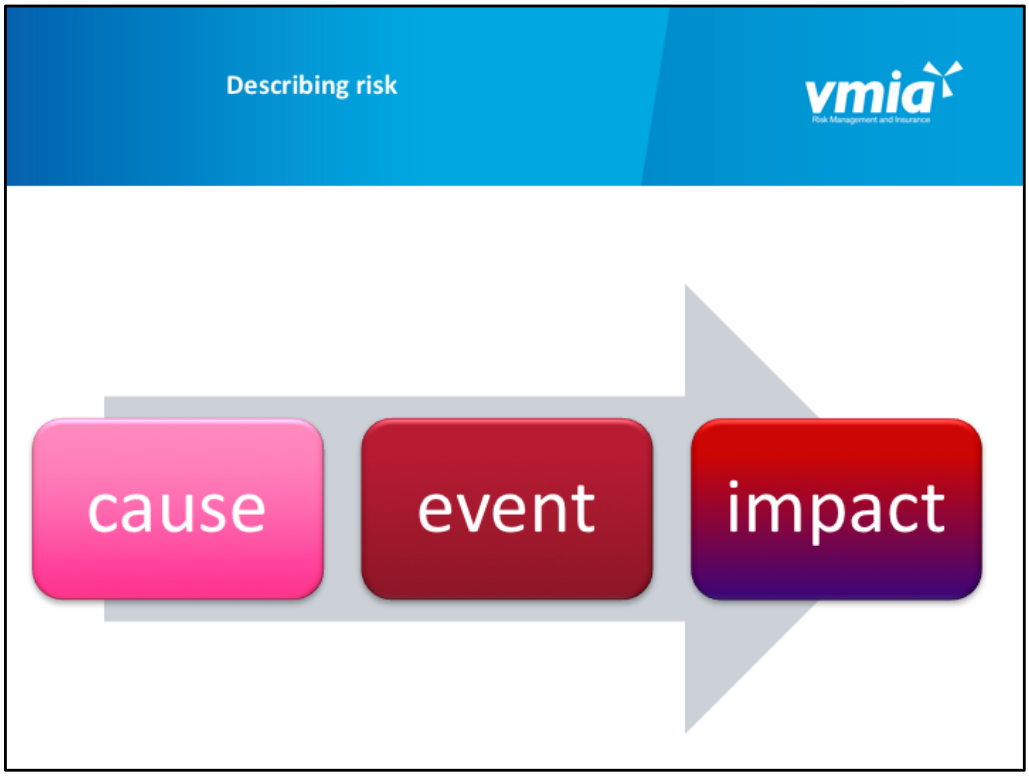




Refer participants to the template towards the back of the PG.

Risk management & the five step action plan



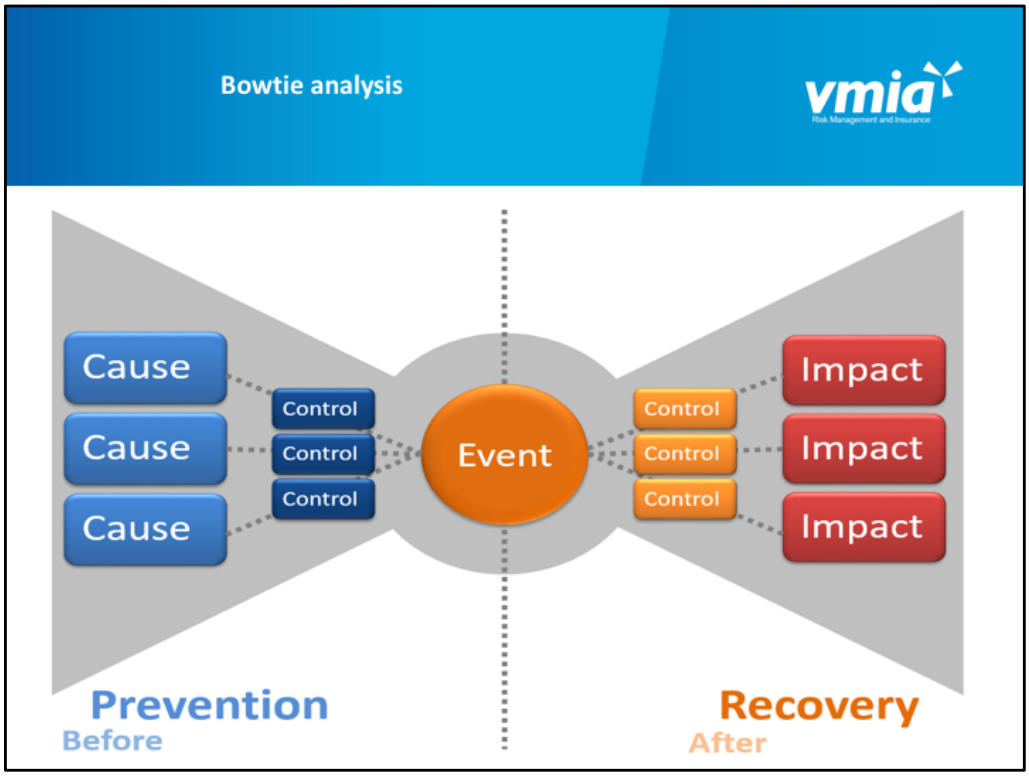


Group Activity – Card "Write a Risk"

The aim of this is to get them to **practice identifying a few risks** before we get into risk assessment and evaluation

There are varying ways to identify a risk and the Standard doesn't prescribe **1 way**. How a risk is described will influence how it will be addressed or understood. The risk needs to reflect what is useful and makes sense to people who are reading it. For example, it is no good saying 'OHS' is a risk as it is too broad.

There are categories of risks that an organisation puts together to help make sense of risk.

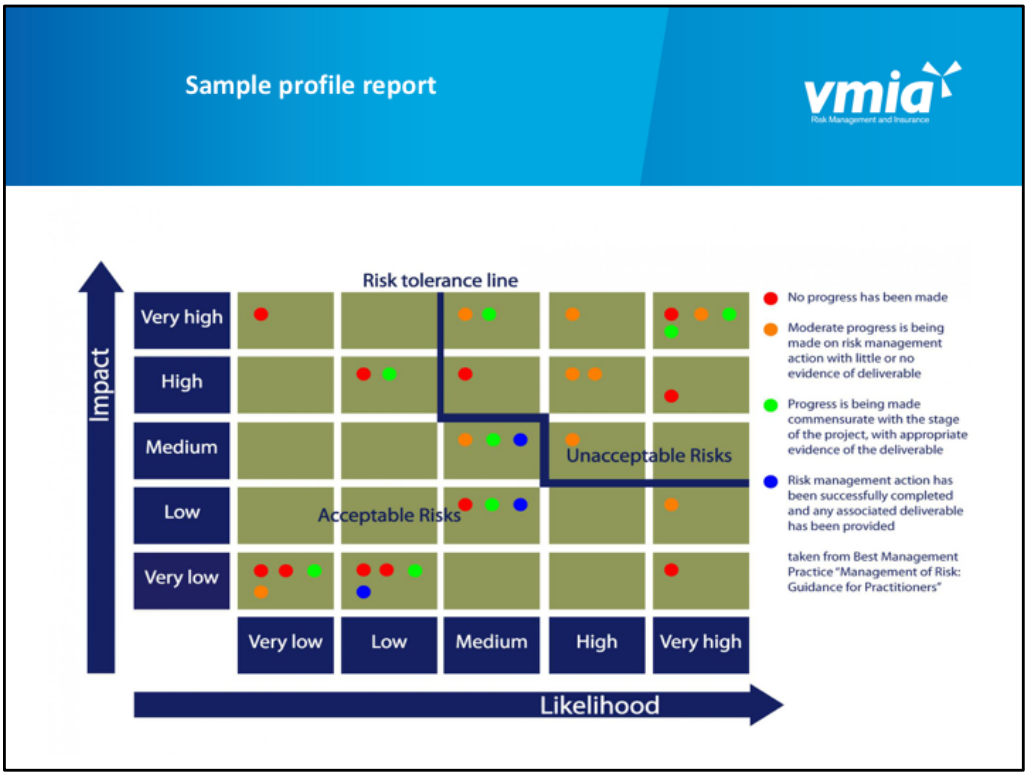

Bowtie analysis
vmia
Risk Management and Insurance
Cause
Cause
Cause
Control
Control
Control
Event
Control
Control
Control
Impact
Impact
Impact
Prevention
Before
Recovery
After

Nature of controls

Table 1: Examples of Timing- and Nature-Related Controls

Timing		
Control type	**Description**	**Example**
Preventive	Controls designed to prevent incidents from occurring	Access controls to applications and systems that prevent unauthorized individuals from performing transactions
Detective	Controls designed to alert management when incidents occur	Reports that show suspicious activity
Corrective	Controls that lessen impact to the institution when adverse incidents occur	Business continuity plans
Nature		
Control type	**Description**	**Example**
Administrative	Controls that align with the board-approved risk appetite and inform employees of management's expectations	Policies or procedures that guide implementation of the information security program
Technical	Software or hardware (or both) that prevents unauthorized activity	A firewall that prevents unauthorized logical access to or from a network
Physical	Devices to prevent unauthorized physical access to a facility or computer system	A deadbolt lock on a door

Sample profile report



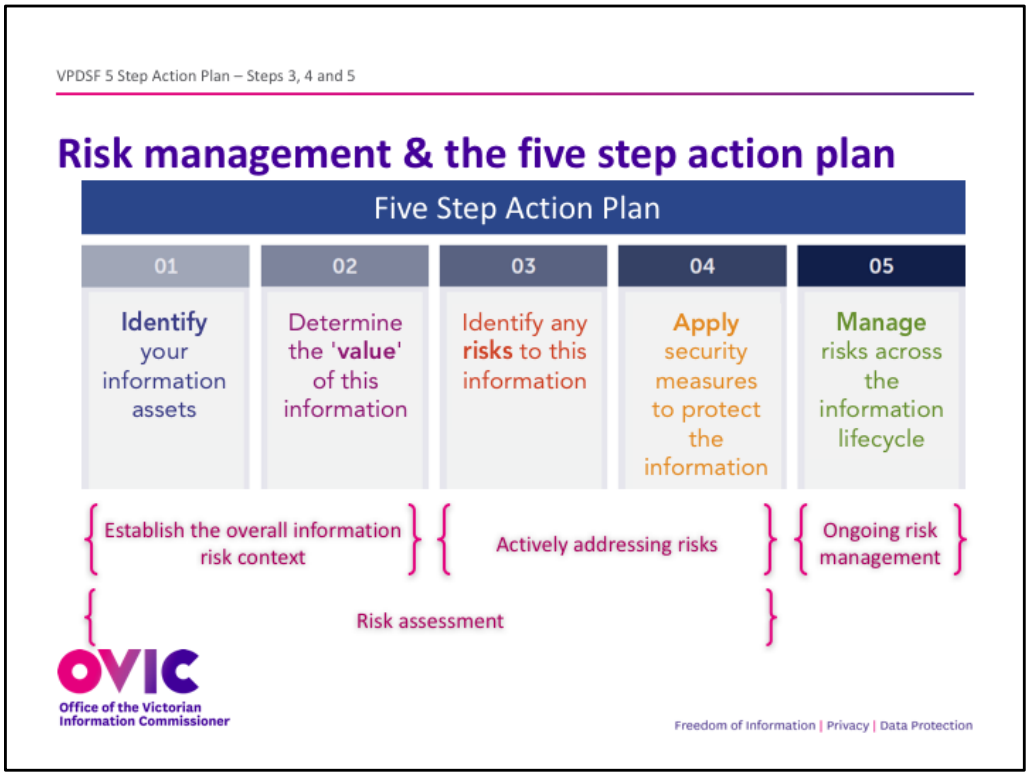

Our learning program
vmia
Risk Management and Insurance
Foundation
Introduction workshop and eLearn
Boards
IPAA CoP
Leadership
Interagency risk
Planning
Culture
Focus
Health topics
Employment issues
Collaboration masterclass

Thanks and see you next time
(when I get back from Mars)

vmia
Risk Management and Insurance

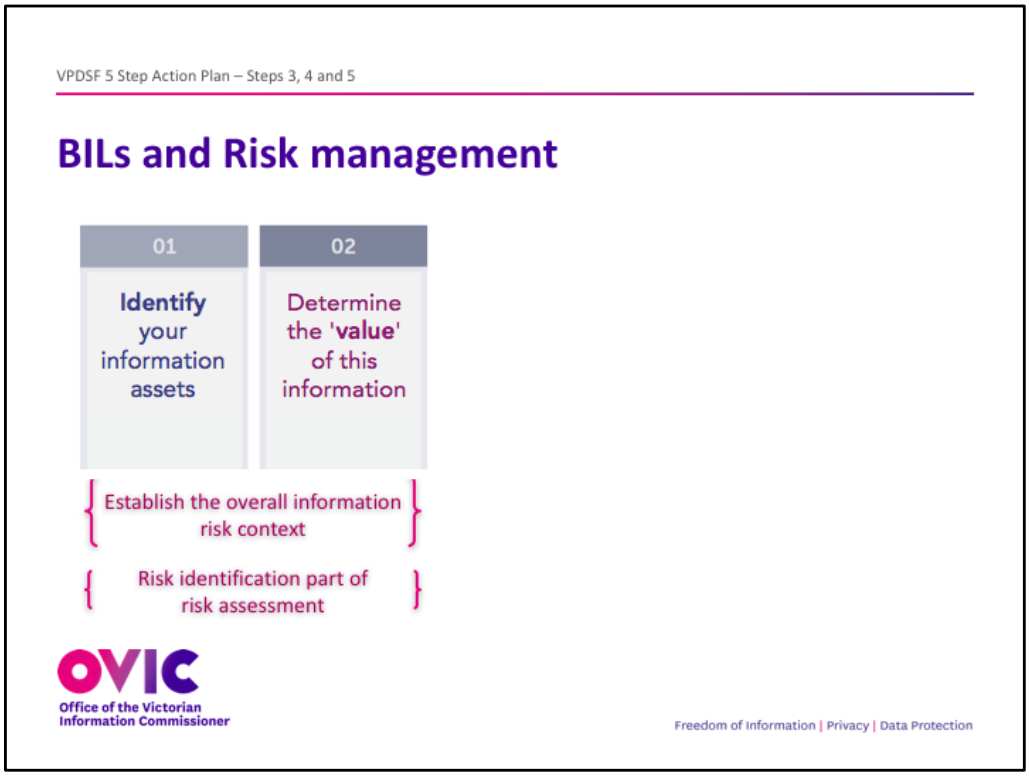
Thank you Jonathon

Now I am pleased to welcome Anna Harris where we will cover steps 3-5 of the VPDSF 5 step action plan in more detail



The VPDSF five step action plan neatly ties in with the existing risk management process as Jonathon discussed to assist you in identifying your security risks. It is no different to your current risk management process.

So lets revise steps 1 and 2 briefly and where they fit in…

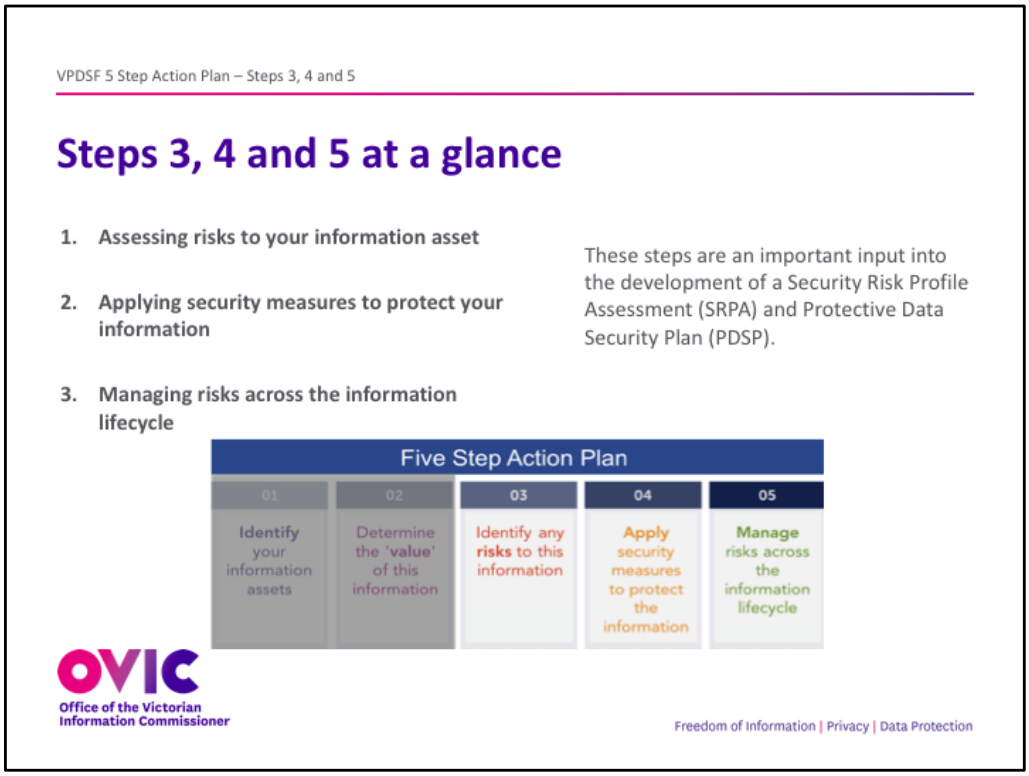


Steps 1 and 2 have the beauty of assisting 2 fold.

First you have already undertaken steps 1 and 2 to identify **ALL** the information handled in your organisation and undertaken a valuation assessment on these which will form part of establishing your overall risk context when you look at the risk methodology i.e. internal operating environment (organisational context) along with other internal and external factors affecting your organisation such as regulatory and operational requirements.

Second, these two steps also play a part in the risk identification stage of the risk assessment process whereby you take the information assets that you have identified in step 2 as the more critical information in your organisation. This is a prioritisation step so you can focus on the more important assets and undertake the risk assessment process on these rather than all your assets. We will touch upon this a little more further in the presentation.

For more information regarding the actual step 1 and 2 process refer to our published information security management collection and check out our September VISN forum recording (available on our website)



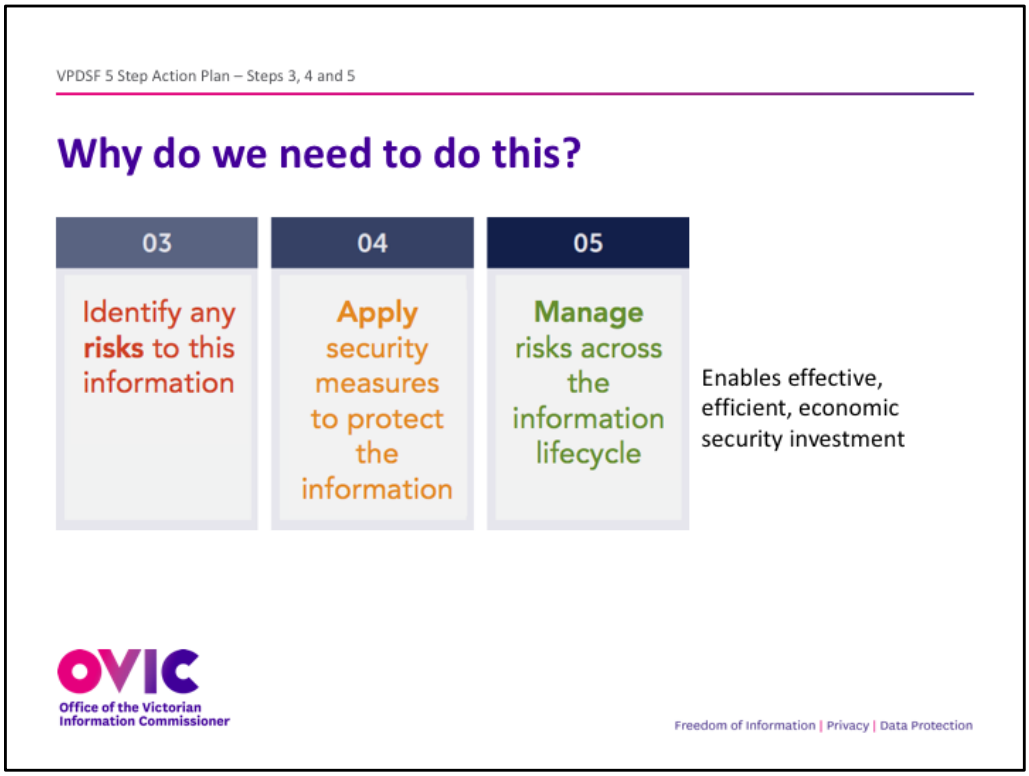
The focus of this session are steps 3, 4 and 5 of the five step action plan where you take the input from both steps 1 and 2 as well the VPDSS self assessment process that organisations are asked to undertake where you may have identified some gaps you wish to risk assess if they cannot be implemented.

These three steps focus on identifying and assessing your security risks, making good choices on which security measures to apply to protect your information and managing the risks across the information lifecycle

How do you complete this?
As well as making sure you follow your organisations existing risk methodology, we have tried to assist you by developing the assurance collection published on our website which contains all the answers and also includes examples and some appendices such as

- sample templates such as the risk assessment and treatment plan which we will discuss further, the VPDSS self assessment and
- Summaries of the various assessment steps

The information contained in this collection will assist you in completing steps 3 – 5 of the VPDSF 5 step action plan

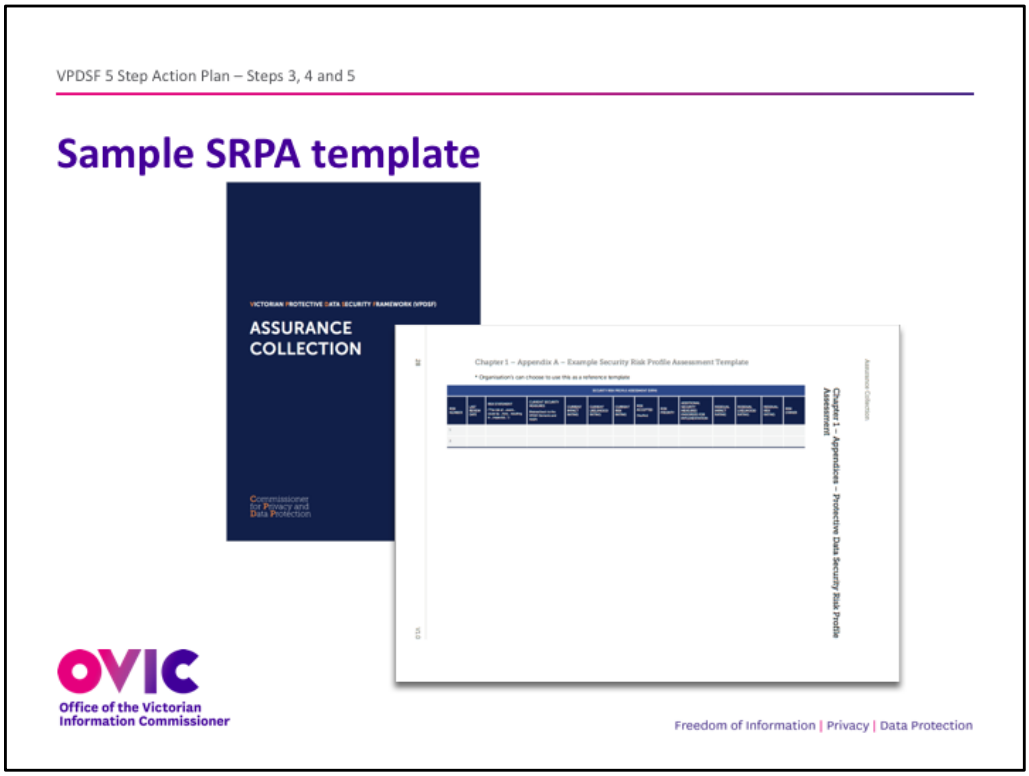


So why do we need to do this? Now that you know what information you have and its corresponding value to your organisation, you can identify the security risks to your more important assets (your crown jewels) so you can ensure effective, efficient and economic investment in security.

The value of this exercise to your organisation which Tony will touch upon in his presentation includes

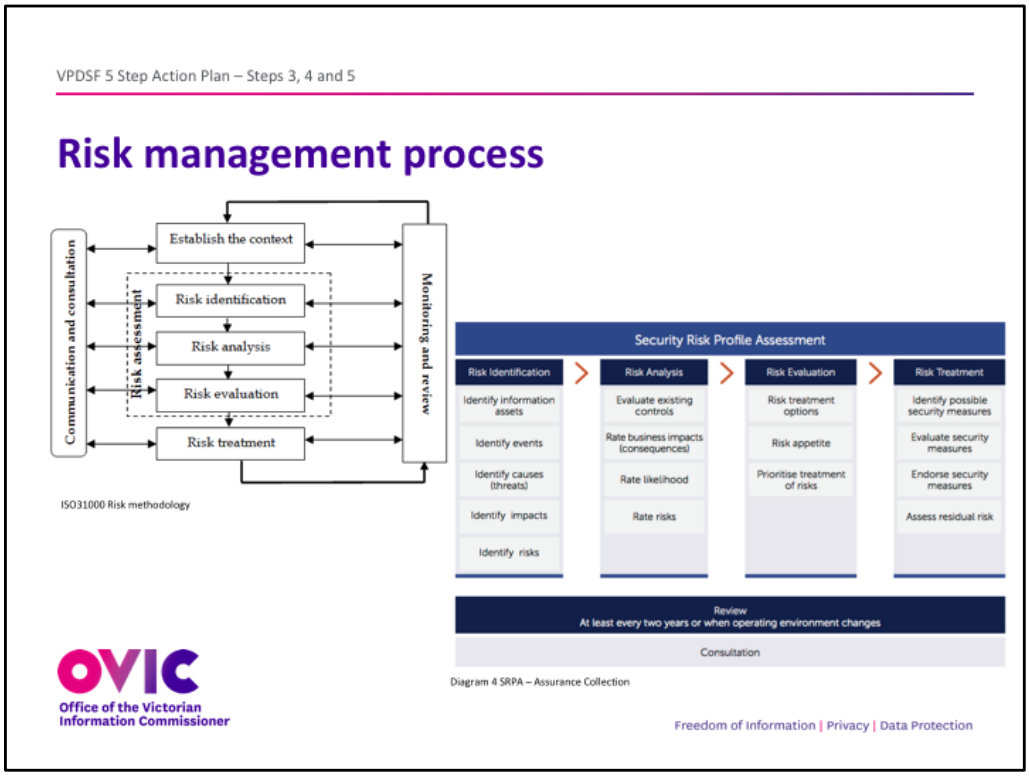
- providing context and meaning of the event, cause and impact for each risk for ongoing management and oversight
- assisting in directing outcomes of treatment planning
- providing meaningful information for reporting
- reducing over or under investment in measures, and
- aligning the 'uncertainty' to the business objectives

Lastly, the other plus is that after this process you will have completed some of your obligations under the Privacy and Data Protection Act including the security risk profile assessment, SRPA and the detailed protective data security plan, PDSP



To that end, to assist with the risk assessment stage, Chapter 1 Appendix A of the Assurance Collection has a sample SRPA template that organisations who do not have a risk register can adopt and those who do have a register can use to check against.

Feel free to continue to use VMIA's risk templates as well if these are already used within your organisation. This is just an additional resource



The risk management process outlined in Chapter 1 of the Assurance collection follows the same risk management process as the international standard 31000 that Jonathon discussed. We did not set out to develop something bespoke to security that everyone needed to learn about. The same risk process is followed to identify the security risks to your information as other risks in your organisation such as financial, OHS risks etc.

VPDSF 5 Step Action Plan – Steps 3, 4 and 5

Risk identification

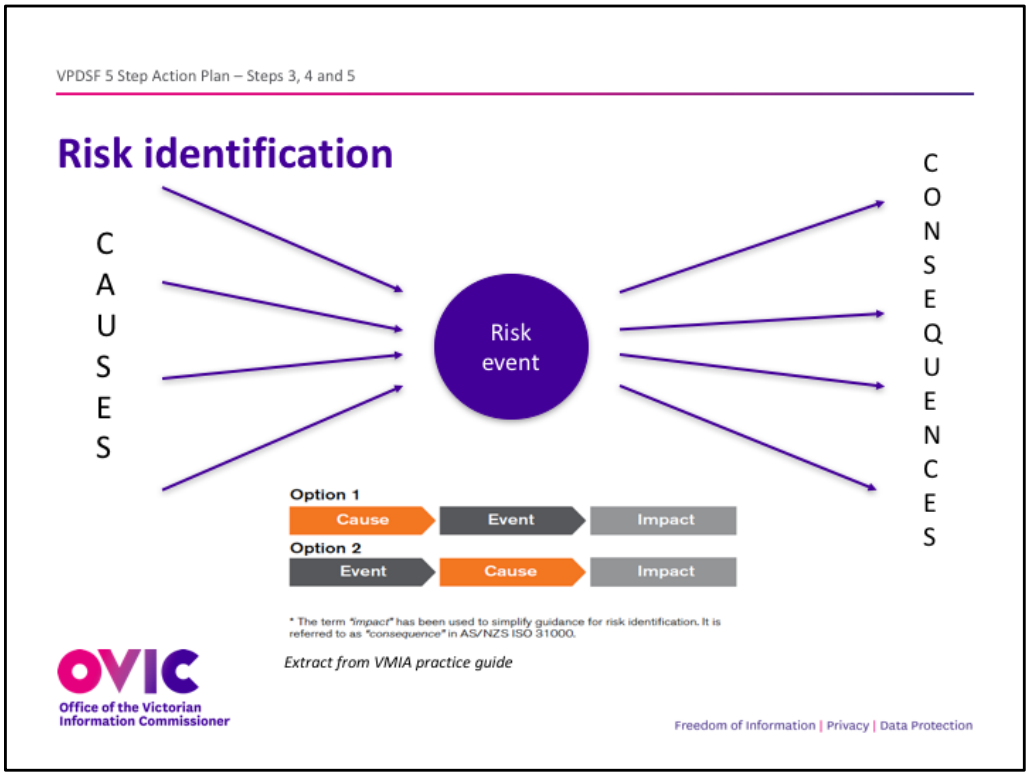
OVIC
Office of the Victorian Information Commissioner

Freedom of Information | Privacy | Data Protection

So lets start at the start - risk identification which is outlined in section 10 of the collection. Lets work our way down

Now that you have completed steps 1 and 2 to establish your overall information risk context, its time to select the crown jewels or the information with the higher value (more critical) information assets to focus on, and
The possible events that may occur to these,
The potential causes of these events,
The possible impacts which have already been identified in step 2, so you can keep that in your back pocket
And these will enable you to formulate your risk statement

So lets walk through an example…



The bow tie approach is one way to assist with formulating your risk statement. It's a great visualisation tool to identify the possible risk scenarios for a particular event

Its time to tell the risk story…

When you are looking at a risk event (in the centre of your bow tie) for your most critical information that you have identified, it may be something like

- unauthorised access leading to compromise of the information (whether that's a compromise to either its confidentiality, integrity or availability may be theft / modification / disclosure / destruction)

In terms of causes to the left of the bow tie, you are looking at how this event may eventuate be it natural, accidental or deliberate. The International Standard ISO 27005 has a list of threats in its Annex. For example, this risk event may occur due to:

- A disgruntled employee
- Malicious outsider
- Opportunistic contractor
- A natural weather occurrence

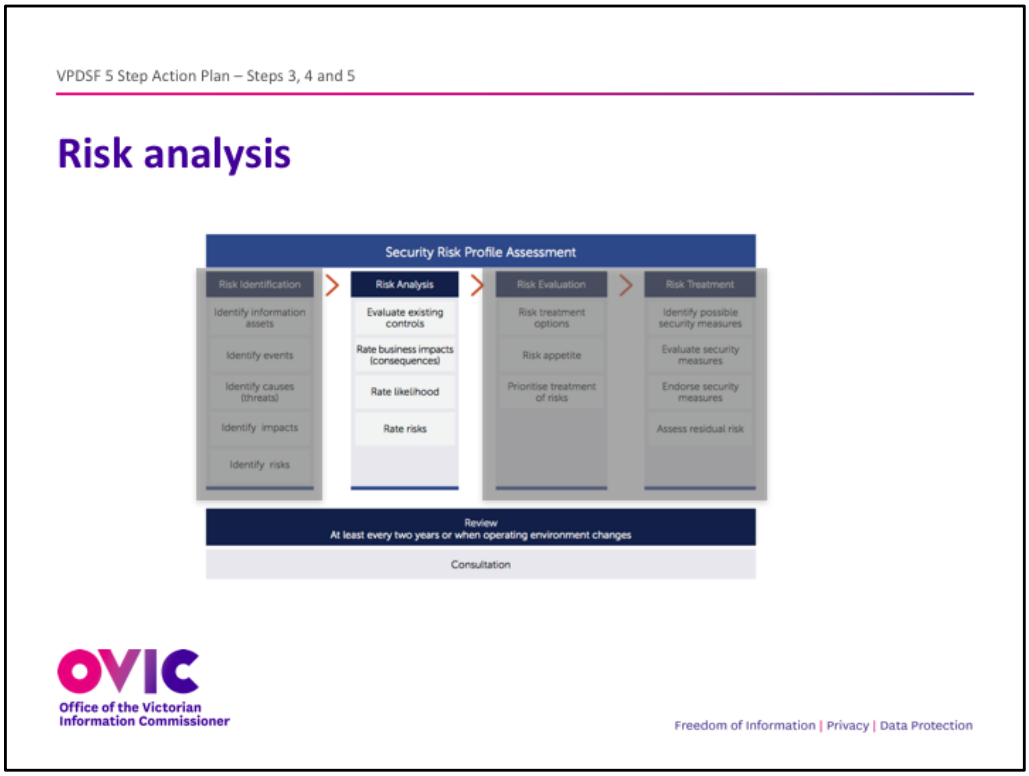
The consequences on the right hand side thankfully have already been taken care of for this asset via your business impact level valuation assessment (Step 2) so you plug

the outputs of the affected categories that gave rise to the higher value rating in here. For example this event may result in:

- Personal injury
- Compliance issues
- Financial loss

Bring this together to now formulate your risk statement. For example,
The risk of unauthorised access leading to disclosure of information
Caused by a malicious outsider (upset about the organisations stance on a topic) / or a malicious insider upset about being overlooked for a promotion and exploiting a system/other personnel
Resulting in harm to an individuals safety / loss of public confidence and trust / financial loss

What you may find is that your identified security risks are not all that different to your neighbour, but what may differ is your internal risk criteria to rate the risks, your organisation's risk tolerance, the current controls you have in your environment and the controls you plan to implement to mitigate/reduce the risk.



So you have your risk statement, lets move to risk analysis
Its time to rate the likelihood of this risk occurring understanding the current controls you have in place and the level of consequence e.g. insignificant vs major.

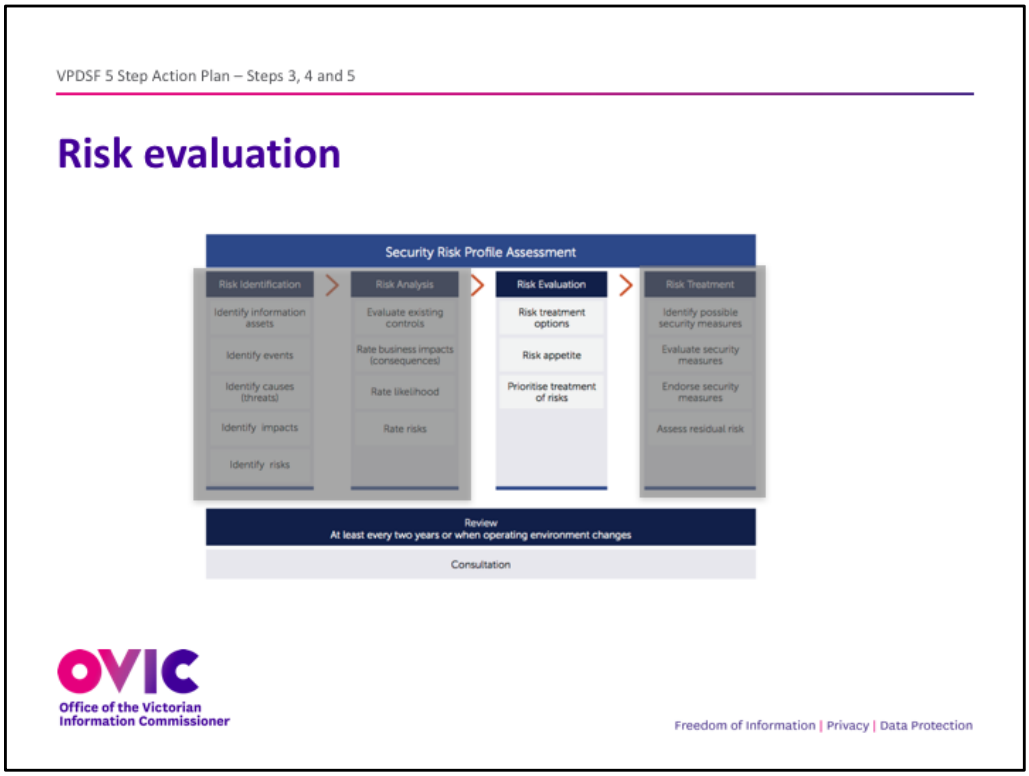
Generally, the controls you have in place won't necessarily change the impact level if the risk was to eventuate but will affect whether the risk actually occurs in the first instance i.e. what is the likelihood of this event happening with the current controls? e.g. rare, possible, almost certain

We recommend you use your organisations enterprise risk criteria/matrix to complete this step to arrive at your corresponding risk rating.

We often get the question, what is the difference between the business impact level ratings in step 2 and the consequences rating table used in risk?
The BILs look specifically at the impact related to the compromise of the confidentiality, integrity and availability CIA of information and are closely aligned with other BIL tables on purpose to enable information sharing across jurisdictions. Consequence criteria take into consideration other factors including the organisation's tolerances. We recommend that business impacts are mapped to your organisation's risk consequence criteria. Whilst not always an easy match, the categories identified in the BIL table are covered more loosely/broadly in risk criteria so a mapping of sorts should be made to enable the application of your enterprise

risk framework to your information security risks.

The business impact level you came up with in step 2 when doing your valuation assessment for this asset can be used to map to your consequence criteria. Section 10.2.2 in the Collection discusses aligning the business impact levels with your risk consequence criteria so you can make sure the risks ratings for your information assets are proportionate with your other risks in your organisation's risk framework and application of treatment options is consistent.



The risk evaluation process is no different to normal risk management and also covered in the VMIA practice guide and assurance collection so we will quickly go over this…

10.3.1 Risk treatment options
The four potential options for treating each risk are the same as normal risk management of accept the risk as is, avoid or share the risk, or reduce the risk by adding additional treatment options

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

10.3.3 Prioritisation of risk treatment
To determine with what urgency you should address risks, they must first be prioritised. Risks with the highest risk rating are normally attended to first.
Typically, additional considerations may include:
safety – what are the implications if the risk is not addressed?
cost – how much will it cost to reduce the risk (and will the benefits outweigh the

expenditure)?
reputation – what is the likely effect on reputation if the risk is not treated?
legal obligations – is the organisation likely to be unable to meet its legal obligations if the risk is left in its current state?
occurrence – which risks are more likely to occur? which you would have identified with your likelihood rating (tackle the ‘almost certain’ ones first)

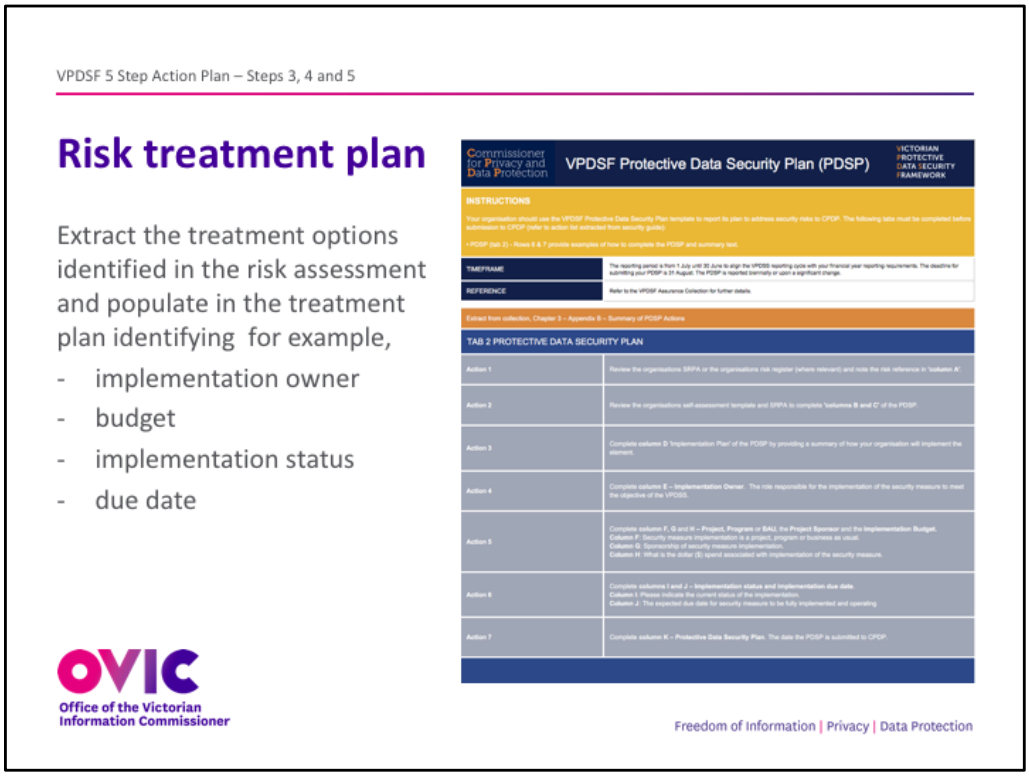
Lastly, you have reached risk treatment where you identify possible security measures across the security domains of

- Information
- Personnel
- ICT
- Physical

They may be additional equipment, stronger personnel screening, specific contract clauses, governance arrangements, policies and procedures, training…

The VPDSS elements may also assist here to identify what measures to consider and they are not always IT controls!

And then, once you have selected your security measures to mitigate the risk from occurring, re-assess the likelihood and consequence to get the residual risk for acceptance by management

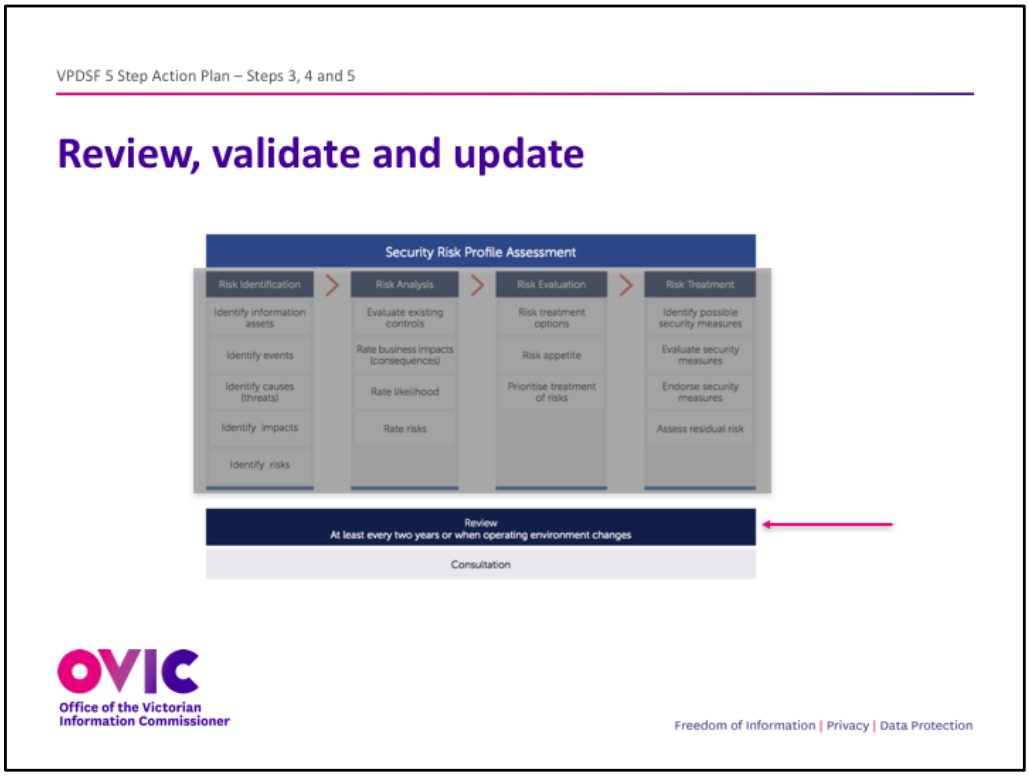


Now that you have a list of security measures to implement from the risk assessment to minimise the risks to your information to a manageable level for your organisation, extract this list of security measures and populate your detailed protective data security plan (PDSP) which is in the Assurance Collection identifying details such as the

- implementation plan
- Implementation owner
- Tying it back to corresponding VPDSS element to help you with your reporting
- Any project sponsors if its not a BAU activity
- Budget
- Status
- Due date

You should also add the gaps of elements not implemented that were identified in your VPDSS self-assessment to this treatment plan (if not already listed) so they are in the one document.

This will ensure you have an approved security program for the next period to focus your security investment and you also fulfil your detailed PDSP obligations.



As part of the lifecycle and the final step in the 5 step action plan, is the review stage.

Remember this is not a set and forget exercise and these risks should be managed with regular reviews across the information lifecycle

Triggers for this review may be:

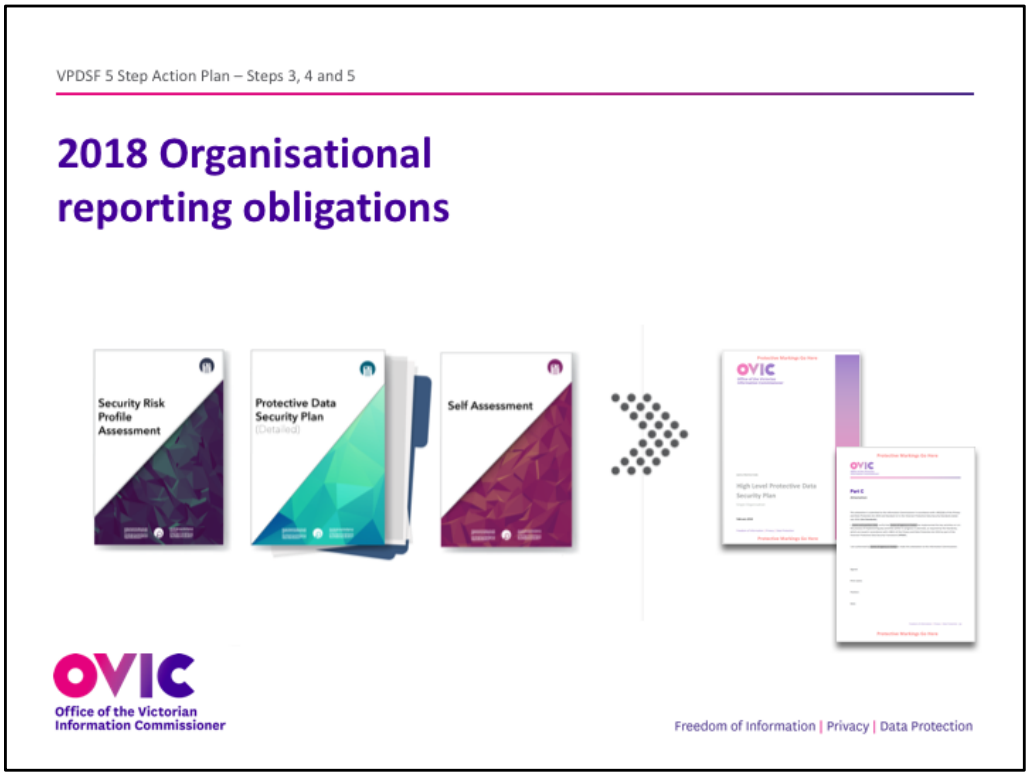
- Change of business context e.g. machinery of government
- Additional / removal of information asset
- Regular risk review cycle
- Incident where the risk has eventuated

If these risks are fed into your enterprise risk register this will be included as part of this exercise.

The first time the 5 step action plan is done, it will be quite a big task but once the hard yards have been done hopefully it will get easier each time it is undertaken and with each review.

And now to hear from a VPS agency's experience with the five step action plan, we are pleased to welcome Tony Smith from East Gippsland Water.
Thank you Tony

Thank you Tony and before we finish up and take questions, Laurencia will provide an update on the upcoming 2018 reporting obligations



After hearing feedback from executives across the VPS, our office has published a high-level Protective Data Security Plan (PDSP) with built in attestation for organisations to use to report to us in August this year.

This is essentially an executive summary of the detailed templates provided in our assurance collection. This will make it easier for your executive to sign off.

VPDSF 5 Step Action Plan – Steps 3, 4 and 5

OVIC reporting templates

Protective Data Security Plan and Attestation

OVIC
Office of the Victorian Information Commissioner

Freedom of Information | Privacy | Data Protection

And here is one we prepared earlier… Sven has written to agencies to advise of the new reporting template that will need to be submitted to our office in August 2018.

As part of the updated reporting templates, we have also provided options for organisation reporting to our office such as single or multiple reporting.

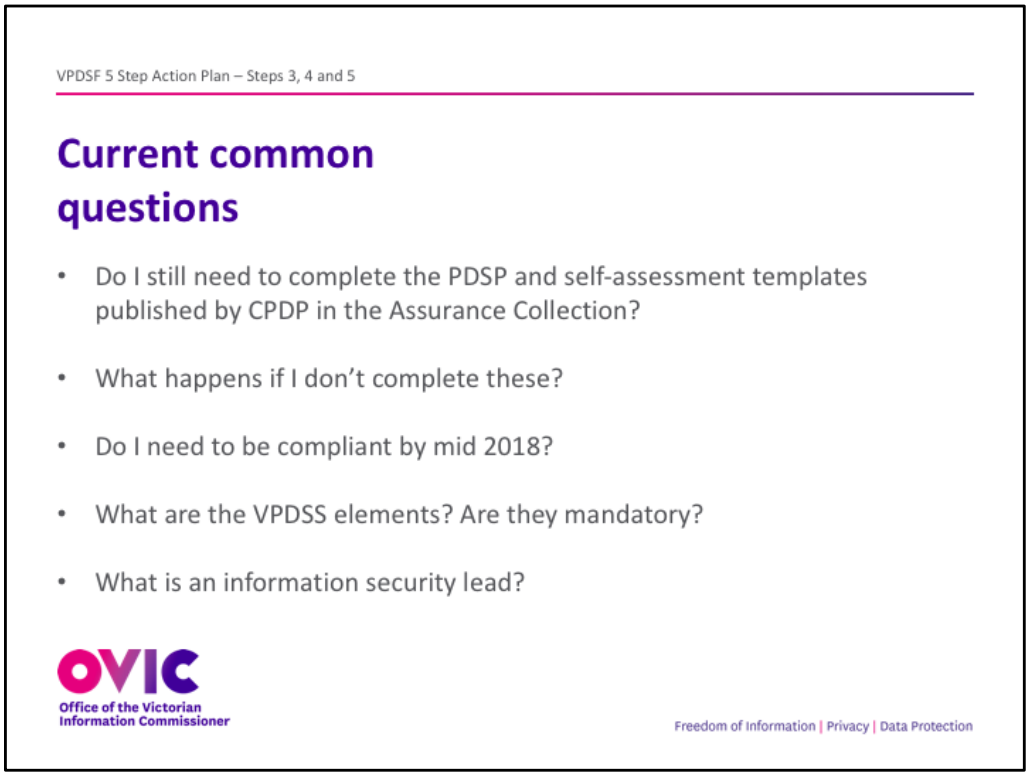
The reporting options in template are just that 'OPTIONS'!
The options are designed to reflect the unique operating arrangements that exist across Victorian government.
This includes governance structures that often exist between larger lead agencies and smaller organisations that fall within the lead agency's portfolio of responsibilities and the provision of shared resources (including information technology and corporate functions). It also provides an opportunity for collaboration across agencies or bodies that perform a similar function.

Single organisation model – An organisation submits a high level PDSP and provides an attestation on its own behalf only.
Multiple organisation model – An organisation submits a consolidated high level PDSP and provides an attestation on its own behalf, and for and on behalf of one or more additional public sector agencies or bodies.

The multiple organisation model may be used in a portfolio setting where agencies or bodies fall within the portfolio of responsibilities of a Department or where a number of organisations of a similar form or function choose to consolidate their efforts. While this approach will assist you in meeting your reporting obligations, your

public sector body Head is still accountable for the protection of its information assets. Accountability cannot be transferred or outsourced.

Before we open the floor to questions from the audience and those that have come in via slido, these are a handful of questions we commonly receive in the data protection branch



Do I need to complete the templates in the collection?
The PDSP and VPDSF self-assessment templates in the assurance collection will actually help you to complete the new reporting templates. Think of them as the detail to enable you to write your executive summary for your public sector body head and relevant committees to get a high level understanding of your security posture and the plans to improve this.

What happens if I don't?
Without completing these more detailed documents, it will be difficult to write the summary for the executive to attest as these will provide you with reasons/explanations/justification for why and how the security status was derived. These documents will also be requested by our office in the event we conduct one of our assurance activities under the assurance model e.g. walkthrough, reviews.

Do I need to be compliant by 2018?
We still get organisations calling us asking if they need to be compliant with the standards by mid this year? To be compliant with the legislation, your organisation needs to submit the high level PDSP and attestation to our office – that is the compliance part. In terms of whether you need to have all 18 standards fully implemented by August 2018, the simple answer is NO, and hopefully the executive summary report that is submitted to our office re-iterates that this is just a plan of your security activities for the next two years to improve information security in your

organisation.

What are the VPDSS elements? Are they mandatory?
We introduced the elements into the VPDSS to assist organisations with the baseline measures they should consider when implementing the Standards. These are not additional measures, all they are is a consolidated extract from each of the reference libraries listed under each standard. This helps organisations to not have to trawl through all the literature to determine the key actions to meet the intent of each standard. In a way they are mandatory – the ones that you determine to be applicable to your organisation will be the ones we expect to see operating in your environment if you reported full compliance to our office

What is an information security lead?
As many of you may be aware, in the second half of 2017, our office sought nominations for an information security lead from each organisation to enable us to have a point of contact to liaise on information security matters including informing them of new material we produce, upcoming events such as the VISN and any changes to the framework. This 'lead' should not stop others from contacting us. We will continue to answer any security enquiries we receive. If your organisation does not want anyone else other than the lead to contact us, this is an internal governance issue for your organisation to work out. If your information security lead would like visibility of the type of questions that come from others within your organisation, we can include the lead in our return correspondence. We do encourage organisations to keep us informed of any changes to information security leads so we can ensure your organisation is getting the latest information from us.

Contact Us

Data Protection Branch
Email: security@ovic.vic.gov.au
Phone: 8684 1660

VMIA
Email: contact@vmia.vic.gov.au
Phone: 9270 6900

OVIC
Office of the Victorian Information Commissioner

And to book into a risk training session, contact VMIA