

# Victorian Protective Data Security Framework

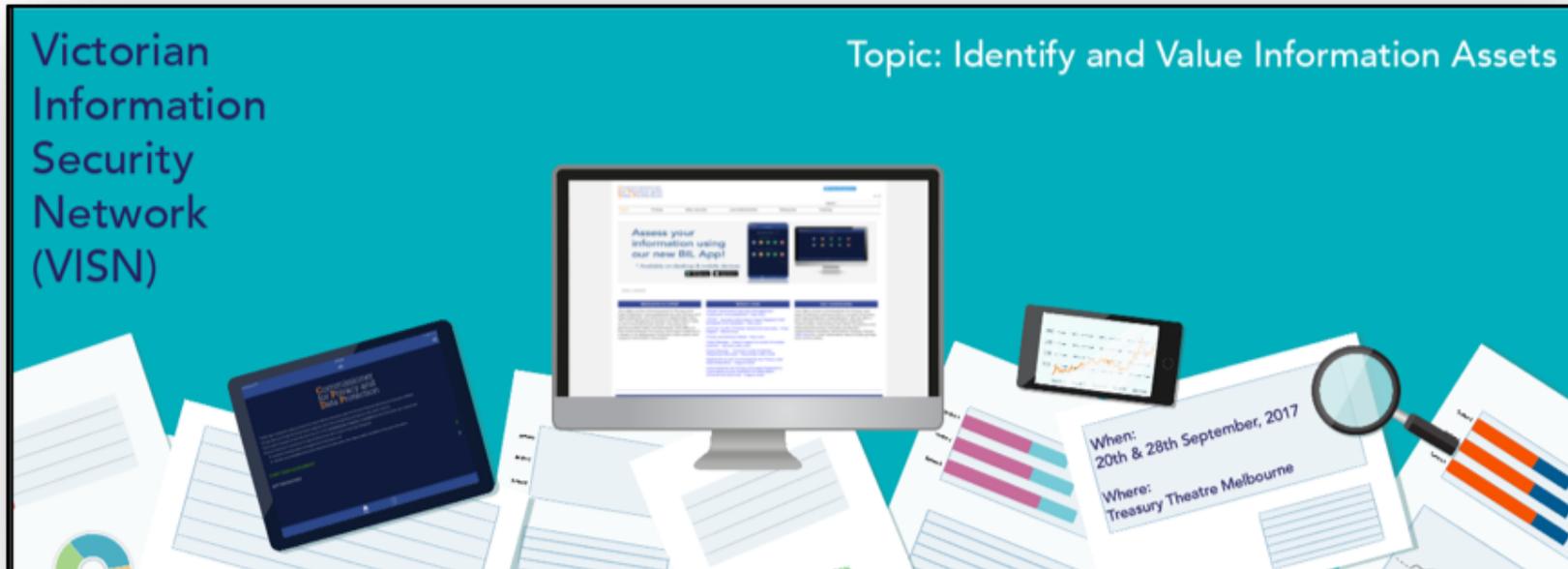
---

Identify and Value Information Assets  
September 2017

---

**OVIC**

Office of the Victorian Information Commissioner  
Privacy and Data Protection



slido

Navigate to [slido.com](https://www.slido.com)

Enter code V906

## We are OVIC

### Freedom of Information Amendment (Office of the Victorian Information Commissioner) Act 2017



#### OVIC

The Victorian Government created OVIC as a primary regulator and source of independent advice to the community and the Victorian Government about how the public sector collects, uses and shares information.

OVIC commenced operating on 1 September 2017 and comprises the functions that previously sat with the Offices of the Freedom of Information Commissioner and the Commissioner for Privacy and Data Protection.

# OVIC

Office of the Victorian Information Commissioner

Privacy and Data Protection

## We are OVIC

OVIC takes on the functions that are currently performed by two separate bodies, the Office of the Commissioner for Privacy and Data Protection (CPDP) and Office of the Freedom of Information (FOI) Commissioner.

Commissioner  
for Privacy and  
Data Protection



OVIC will manage Data Protection, Privacy and FOI regimes as well as maintaining broad oversight of the Victorian Government's information access and management practices.

## We are OVIC

The establishment of OVIC with its new statutory powers is intended to:

- provide more proactive and integrated FOI, privacy and data protection leadership in Victoria, particularly by driving the cultural shifts necessary to improve how government manages and provides access to information
- ensure greater transparency by increasing Victorians' access to government-held information and expanding the scope of FOI decisions made by agencies and Ministers, which are reviewable by the OVIC, and
- ensure the effectiveness and independence of the regulator by giving OVIC greater investigative powers, an increased education function, the ability to set binding professional standards and independence from ministerial direction

**OVIC**

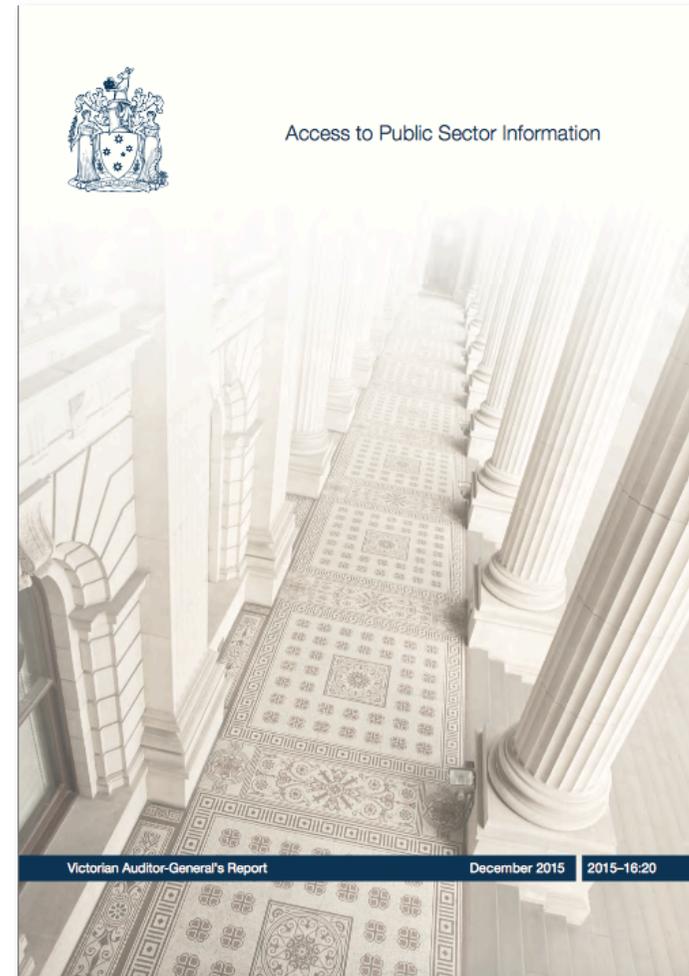
Office of the Victorian Information Commissioner  
Privacy and Data Protection

# VAGO Guest Presenter

**Michelle Tolliday**

Manager Performance Audit

Victorian Auditor General's  
Office (VAGO)



# Information Asset Registers

Michelle Tolliday  
Manager, Performance Audit  
Victorian Auditor-General's Office

## Outline

- VAGO's mandate and role
- *Audit: Access to public sector information (PSI)(2015)*
- Information Asset Registers (IAR)

# Why does Victoria have an Auditor-General?

9

## *What do we do?*

provide assurance to Parliament on the accountability and performance of the Victorian public sector

## *How do we do it?*

- under the *Audit Act 1994*
- independently of Parliament (i.e. not subject to direction)
- by reporting on what we find without fear, favour or affection

# ***Access to Public Sector Information (2015)***

## Access to PSI

11

### *Inquiry into Improving Access to Victorian Public Sector Information and Data (2009) (EDIC Inquiry)*

Government's response: commitment to an 'open access' approach to all Victorian PSI, through:

- standardised method for categorising, storing & managing PSI (i.e. an Information Management Framework — IMF)
- **agencies publishing comprehensive information asset registers (IARs)**

## Access to PSI

12

### *Key audit finding*

examined agencies were not providing the public with full and open access to the PSI to which they are entitled.

### *Why?*

the critical foundation of comprehensive and sound information management had been neglected

### *How come?*

ineffective whole-of-government information management leadership and governance led to a failure to drive the operational and cultural changes needed to achieve open access to PSI

## Access to PSI

- absence of a rigorous approach to managing information has significant implications for
  - public access
  - the sharing of information across government
- agencies fell 'well-short' of compliance with Part II of the FOI Act by not publishing registers of the PSI they hold
- So.....'current system' is in disarray— where we are:
  - **not confident** that agencies understand what PSI they hold
  - **certain** that they are not providing the public with the means to request PSI that agencies own and hold

## Key audit recommendations

- mandatory standardised method for categorising, storing & managing PSI (i.e. a WoG Information Management Framework)
- agencies develop a proactive public sector information release program, using comprehensive **information asset registers** as a core tool for release decisions

## Information Asset Registers

15

So...

what's the big deal about  
Information Asset Registers?

PSI is an asset just the same as chairs, tables, and cars—and can be managed using registers in the same way

## Information Asset Registers

Properly identifying and describing PSI is critical to an agency being able to:

- **fully understand what it owns and holds**

It is from this point that well-informed decisions can be made about all aspects of information management:

*creation—capture—storage—access—use/re-use—disposal*

## Information Asset Registers

IARs are able to 'serve many masters', including:

- compliance with legislative and regulatory access obligations (e.g. privacy, security, FOI, proactive release, inter-agency PSI sharing)
- knowledge management and informed decision-making (single source of truth/authoritative assets)
- efficiency (time needed to locate, retrieve and use PSI)
- accountability (assigning responsibility for the quality of particular assets)
- storage management (identification and removal of duplicated assets, ease of migration to new systems, reduction of shadow systems)
- And many **many** more!

## In summary

### Understanding your PSI enables:

- more efficient processes
- increased confidence in access controls (security and release)
- better decision-making (including joined-up government decision making)

One of the easiest ways to achieve and maintain this understanding is through Information Asset Registers

## Questions?...

### Contacting VAGO:

[www.audit.vic.gov.au](http://www.audit.vic.gov.au)

+61 3 8601 7000

Level 31, 35 Collins Street Melbourne

Victoria 3000

Australia

# Introducing the Data Protection team

## Data Protection Branch

Assistant Commissioner, Data Protection

Anthony Corso

Senior Data Protection Advisor

Laurencia Dimelow

Senior Data Protection Officer

Anna Harris

GRC Security Manager

Karl Will

Specialist Data Protection Advisor

Martin Harris

Law Enforcement Liaison Officer

Matthew Fiford

Project Officer

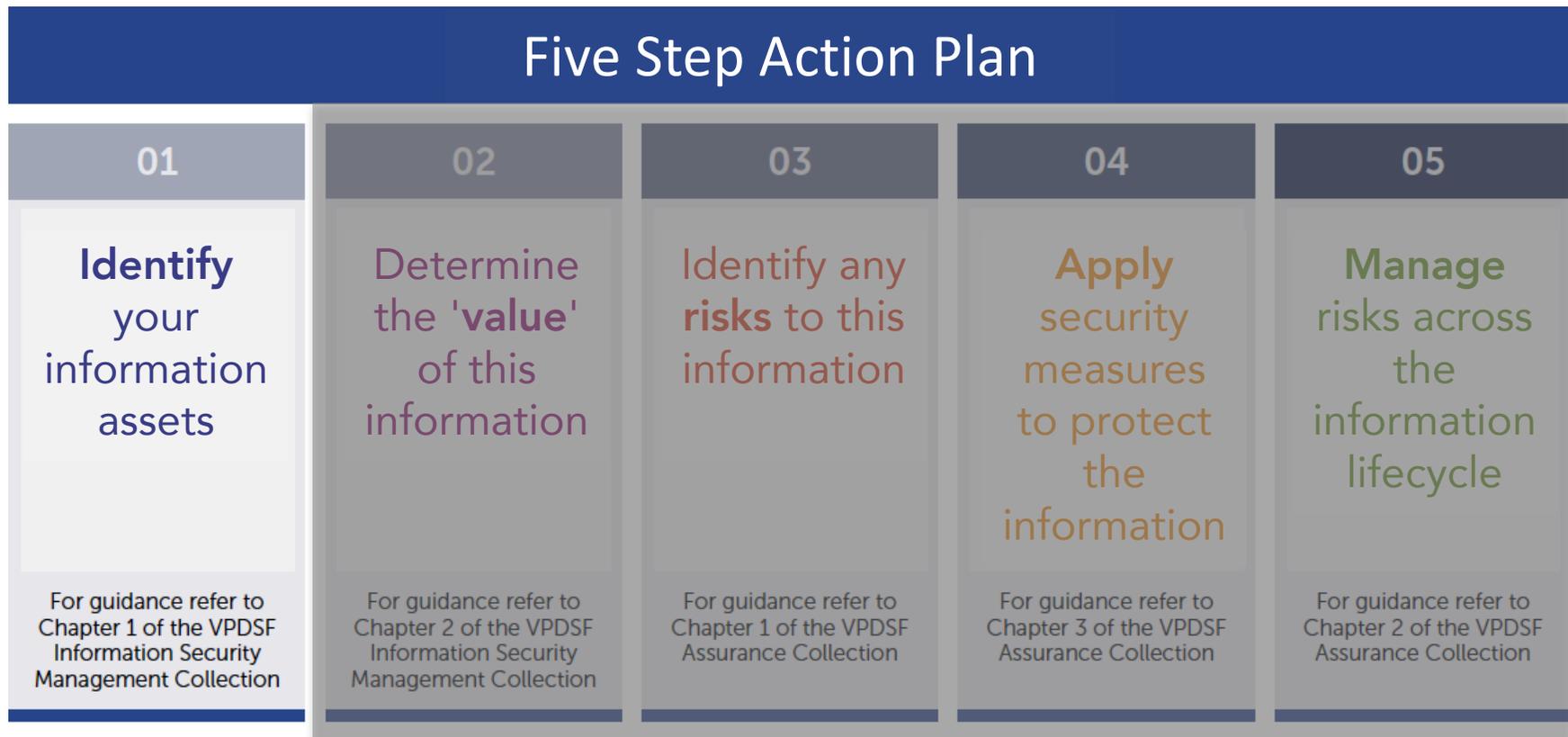
Marilyn McPherson

### Contact details

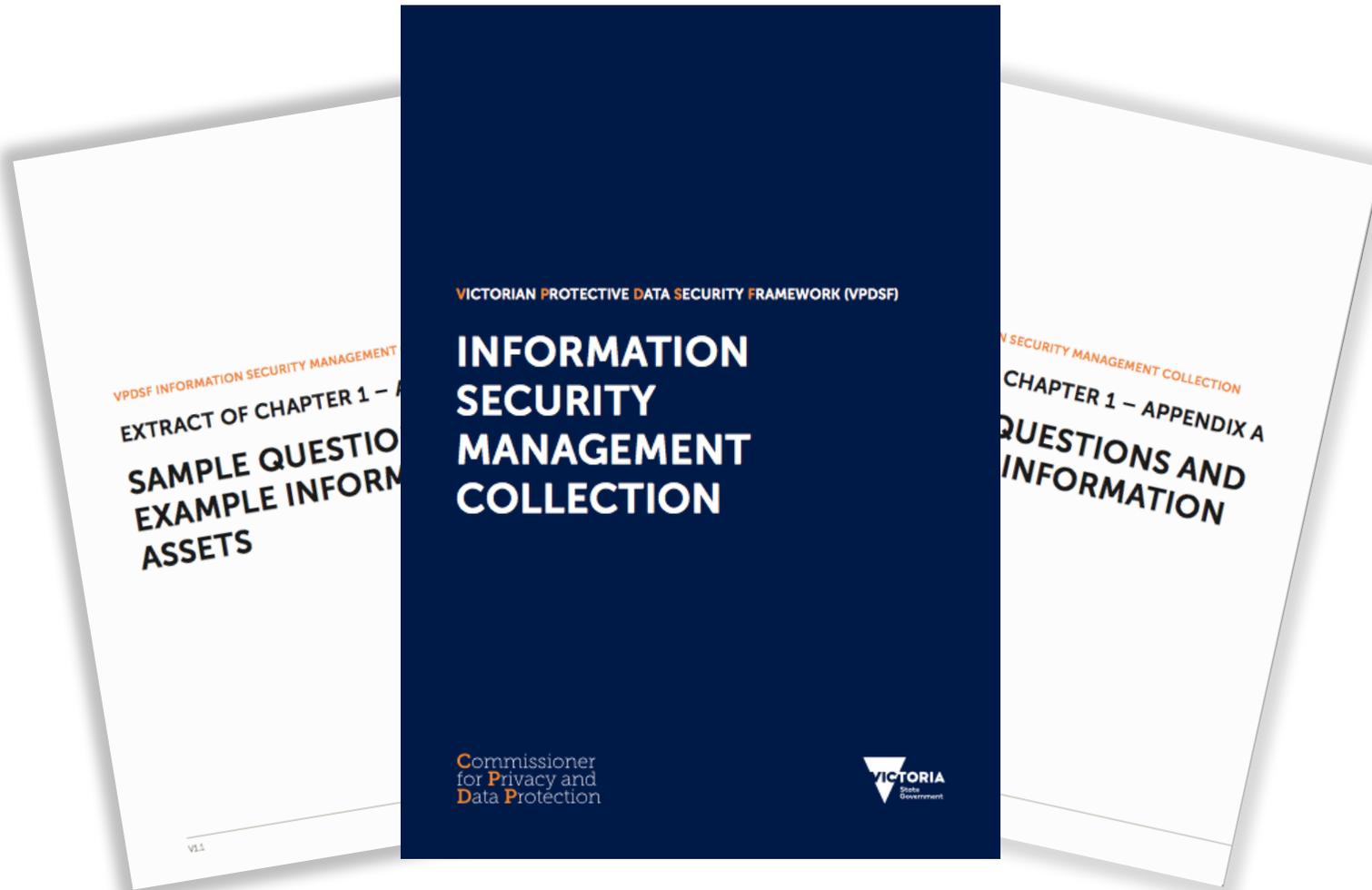
Email: [security@cpdp.vic.gov.au](mailto:security@cpdp.vic.gov.au)

Ph. 8684 1660

# Topic 1 – Identify your information assets



# How to do this?



## How did we form this guide?

Chapter 1 of the VPDSF Information Security Management Collection was developed with reference and input from the following bodies and subject matter experts from the WoVG Information Management community



Premier  
and Cabinet

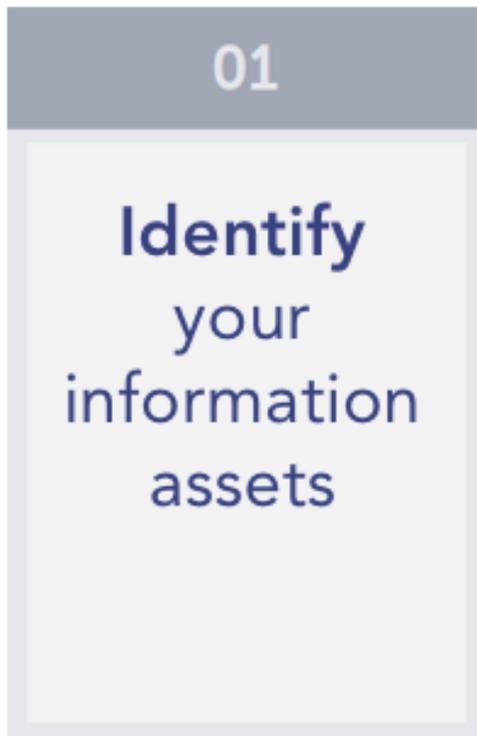
### VAGO

Victorian Auditor-General's Office

*Auditing in the Public Interest*



# Why do we need to do this?



01

**Identify**  
your  
information  
assets

Simply put, agencies can't protect what they don't know...

# What is an information asset?

An information asset is described as a body of information, defined and practically managed so it can be understood, shared, protected and used to its full potential. Information assets support business processes and are stored across a variety of media and formats (i.e. both paper based as well as electronic material).

Information assets have a recognisable and manageable value, risk, content and lifecycle.

An information asset can be a specific report, a collection of reports, a database, information contained in a database, information about a specific function, subject or process.



## What is an Information Asset Register (IAR)?

An IAR is a tool used to record collections of information (information assets) regardless of media or format.

It can take many forms, with no set system or tool mandated for use.



# Sample IAR template

To help organisation's develop their own IAR we produced a sample template for you to either use or reference.

This template was developed in conjunction with partner agencies across Victorian Government, mapping common information and records management requirements.



# What to include on your IAR?



Not all fields on the sample IAR template are mandatory

You should consider your organisation's specific operating requirements when defining what is, and isn't appropriate to include in your final organisational IAR.

**Add or remove fields as required.**

Before building or procuring a tool, first talk with the business to see if something is already available to use to input information into, or extract from.

# Sample IAR template

The sample IAR template is set out over 3 tabs –

## 1 - VPDSF requirements

Minimum fields needed for the VPDSF

## 2 - Core

This includes the VPDSF requirements as well as other common existing legal and regulatory references across Victorian Government

## 3 - Supplementary

Additional fields to add business benefit or context



# VPDSF requirements

The first tab of the sample IAR template lists the required fields for the VPDSF.

The fields on this tab will help you manage the security aspects of your information assets.

They also act as an important input into your Security Risk Profile Assessment (SRPA) and Protective Data Security Plan (PDSP).

VPDSF REQUIREMENTS					
INFORMATION ASSET REGISTER					
	ASSET NAME	ASSET DESCRIPTION	FORMAT	LOCATION	CREATION DATE (INCLUDING ACQUIRED DATE)
DESCRIPTION	The name or title of the information asset	Description of the contents and / or an outline of the components of the information asset	Describe the form and format of the information asset. This includes both soft and hard copy material	Describe the location where the information asset is most commonly used and stored	Input the date that this version of the information asset or associated records were generated
SUPPORTING COMMENTS	List name of the information asset  Include any alternative names for the information asset may be captured in description field. Make sure the title describes the information asset, is meaningful to the user and is keyword rich to support any search functions in the future	Provide a detailed description of the information asset (data) or program  As a minimum, organization's should identify if the information asset contains one of more of the following information types:  <ul style="list-style-type: none"> <li>Personal Information (as defined in the Privacy and Data Protection Act, 2014)</li> <li>Law Enforcement Data (as defined in the Privacy and Data Protection Act, 2014)</li> <li>Crime Statistics Data (as defined in the Privacy and Data Protection Act, 2014)</li> <li>Health records (as defined in the Health Records Act, 2001), or</li> <li>any other forms of data or records not already specified above</li> </ul>	Provide a detailed description of the format of the information asset (i.e. soft copy excel, hard copy records).  e.g. Whether the material is stored in: <ul style="list-style-type: none"> <li>hard copy, or</li> <li>soft copy.</li> </ul> Format types such as: <ul style="list-style-type: none"> <li>word documents,</li> <li>excel sheets,</li> <li>audio files.</li> </ul> N.B. There may be multiple format options, depending on the makeup of the information asset	Describe location of the information asset  This can be a physical location and / or digital location where the information is used and stored (including any ICT systems)	List the original creation date of the information asset or when the information asset was acquired or transferred to the organisation (i.e. either capture or collection)  If the information asset originated outside the organisation, a description of where it came from and the business area that originally created it should also be included.

## Broader IM considerations

The other tabs on the sample IAR spreadsheet set out some of the more common Victorian Government IM obligations.

The tabs titled 'Core' and 'Supplementary' include references from:

- VPDSF
- Public Record Office Victoria (PROV)
- DataVic Access Policy
- Enterprise Solutions Branch (ESB)
- Freedom of Information (FOI)
- Privacy

INFORMATION ASSET REGISTER		
	DEFINITION OF THE METADATA / ELEMENT	SUPPORTING INFORMATION AND IMPLEMENTATION NOTES
Asset Name / Data Title	The title of the information asset.	This is the definitive name of the information asset. Alternative names for the information asset may be captured in description field. When providing a title for your information asset please make sure the title describes the asset, is meaningful to the user and is keyword rich to support search engine optimisation.
Asset Description	Particular description of the information asset (field is optional).	
INFORMATION ASSET REGISTER		
	DEFINITION OF THE METADATA / ELEMENT	SUPPORTING INFORMATION AND IMPLEMENTATION NOTES
Extract		
Format	IAIR entry review date	It is recommended that this field be generated automatically when changes occur to the metadata associated with the information asset.
Location	Unique ID	It is recommended that this identifier be unique at least within the Victorian government. Note that this identifier primarily identifies the record. The contained records/files/database may have other identifiers.
Asset Status	Purpose (primary purpose of collection)	This helps organisations determine the original intent or purpose for generation or collection of that information asset. This is particularly important for information assets containing personal information. The Privacy and Data Protection Act (2014) prohibits the use of personal information collected for one purpose from being reused for a secondary purpose. This field documents the original purpose for which the personal information was collected (including any mandates for collecting the information and whether the information asset contains personal information).
Related Information Asset	Link to related information assets	A link to a related information asset (e.g. previous instances of the information asset). Organisations to define whether this information asset is an input or an output.
	Type of relationship	Typical values would be: Replaces / Replaced By, New Version / Old Version, Derived From / Derivation, Related information assets. Other values are allowed.
	Value	Value refers to the URL, (webpage address) of a metadata record of another dataset.
Disposal requirements	How must the asset be disposed of?	Organisations should consider: <ul style="list-style-type: none"> <li>the format type of the information asset (including any associated records or elements)</li> <li>related Retention and Disposal Authority &amp; Single Instance Disposal Authority and</li> <li>the procedure marking of the information (see the will inform relevant security measures required to securely dispose of the asset)</li> </ul>

# Identifying what you have...

## Discovery process -

There is no set way to conduct an information review. Each organisation has varied needs and will use their resources differently. A suggested approach includes –

- ✓ Defining the scope of the review
- ✓ Establishing a sponsor
- ✓ Identifying key personnel (roles and responsibilities)
- ✓ Drafting communications explaining the review / discovery process
- ✓ Determining how you will collect and capture responses from the business
- ✓ Reviewing existing resources
- ✓ Engaging all stakeholders and providing ongoing support
- ✓ Reviewing responses and recording outcomes into the organisation's IAR

# So how did we do it?

Action	CPDP Action
Scope	<p>Our information review included all information assets (both hard and soft copy material) in active use. Inactive material was also discovered during the review exercise.</p> <p>We also considered the sample IAR template fields and developed our own internal IAR, including the appropriate fields for our organisation.</p>
Sponsor	An Executive Sponsor was appointed for the project. Assistant Commissioner Projects and Operations
Key personnel (RACI)	Key personnel were identified (including the Executive Sponsor) Data Protection Branch (DPB) members, workgroup heads, and other CPDP personnel across the business
Comms	Comms were drafted by the DPB and initially sent out by the Executive Sponsor to all personnel. Supplementary comms were then followed up by the DPB leads, including invites to workshops

# So how did we do it?

Action	CPDP Action
Collect & capture responses	To capture the responses from the business an editable version of the IAR was saved on a shared network drive. Users from each workgroup were then able to populate the worksheet with their initial responses
Existing resources	DPB considered existing resources to help conduct the review including CPDP staff, IAR template, network drive structure and external CPDP website
Stakeholder engagement	DPB engaged with all stakeholders via a range of facilitated workshops and were available for follow up assistance as required
Record outcomes into IAR	DPB then updated the master IAR using responses from each of the individual workgroups. The IAR will continue to be refined and adjusted as information assets across the organisation are created or changed

# DJR Guest Presenter

Jacinta Thomson

Director, Security Management  
& Assurance Finance,  
Infrastructure & Governance  
Division

Department of Justice &  
Regulation



# Victorian Information Security Network

## Valuing Information Assets

Jacinta Thomson  
Director Security Management & Assurance Directorate  
Department of Justice and Regulation  
20 September 2017

# Presentation overview

## The Justice Landscape

Our Information  
Diversity of Information  
Information is an Enabler and Important

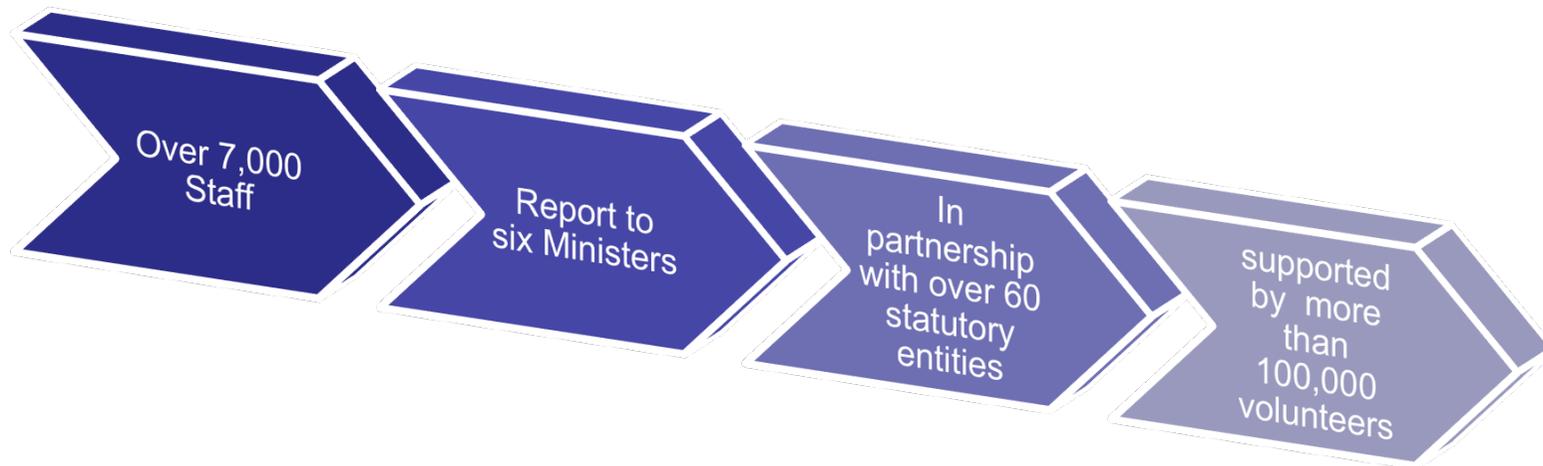
## Information Asset Register

The Journey  
Lessons Learned

## The Justice Security Management Framework

Next Steps – The Journey Continues

Vision – providing a safe, just, innovative and thriving Victoria, where the rule of law is upheld, and rights and responsibilities are respected



Leading extensive justice and regulation service delivery across four regional areas and responsibilities including managing the state's prison system, development of laws and policy through to implementation

# Diversity of information

Departments information supports the delivery of capabilities and functions for:



# Our Information



# Information is an enabler and important

In 2016 Justice information was critical to support and enable:

- Evidence base data to expand critical infrastructure and various justice services
- Applications processing, delivering and supporting services to the community as required by legislation
- Informed approaches to address the overrepresentation of Aboriginal people in the criminal justice system
- Decisions about the organisation structure and recruitment
- Preparation of a high volume of Bills that were passed by the Parliament
- Introduction of new capabilities to support various government initiatives

These achievements, and the many other accomplishments throughout the year, have been made possible through the information we have and efforts of more than 7K+ departmental staff and 100,000+ volunteers who support our work.

# Information Asset Register – the Journey

## Information Management Strategy 2015 - 2018

- Focused on the importance of managing information as a strategic asset
- Provided a roadmap for improving information management capability, systems and processes
- Focused on addressing strategic priorities of digital service delivery to continue to build workforce capability and make evidence-based decisions
- Victorian Protective Data Security Framework

## Key initiative – Valuing our information

- Information Asset Register (IAR)

# The Journey continues – Where it started

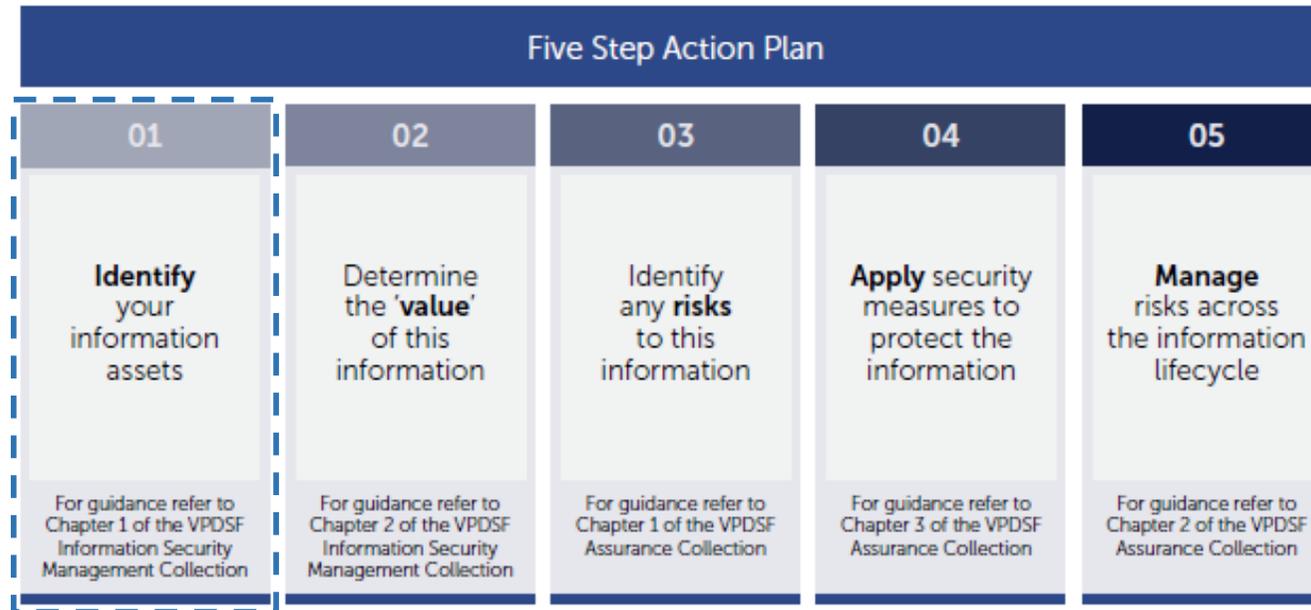


Figure 1 from CPDP, Victorian Protective Data Security Framework (VPDSF) Assurance Collection, July 2017, p.11

- Identified the information assets
- Developed the IAR
- Approximately 80 business units
- Workshops with key representatives
- Review and validation of content

# Sharing our experience...



# Lessons Learned – Considerations for your IAR



# Security Management Framework



Strategically driving and supporting WoVG initiatives and departmental reform. We care about the security of DJR's data and resources, and want to support each other to put DJR in the best possible position when it comes to attesting to the security of our data and resources...

*...but*

... It's not just about attestation, we want to be **leaders** and **exemplars** in the field of data security for the State.



A holistic **Security Management Framework** that **embeds security into the design** of our everyday processes and systems, and that is **governed through shared responsibility**.

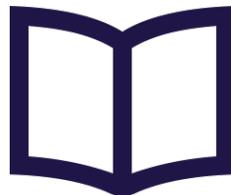
*This enables us to do more than merely comply with the Victorian Protective Data Security Framework.*



**Strategy**



**Security Manual**



**Assurance Framework**

*Security Risk Profile Assessment (SRPA)*



*Protective Data Security Plan (PDSP)*



**Stakeholder Engagement Strategy & Communications**



<46>



Justice and Regulation

# Justice Security Management Framework

- 1 A DJR Security Management Framework**

Strategically drives and supports whole-of-government initiatives and departmental reforms to deliver consistent, innovative, risk-based security outcomes supported by a **Protective Data Security Strategy and Capability Plan**
- 2 Governed representationally & skills-based**

Redefined the Security Executive Committee and established a Security Program Board - a shared responsibility for the department's planning and security risk-profile
- 3 New Directorate**

Strategic centralised oversight of protective data security across the department
- 4 With strong relationships**

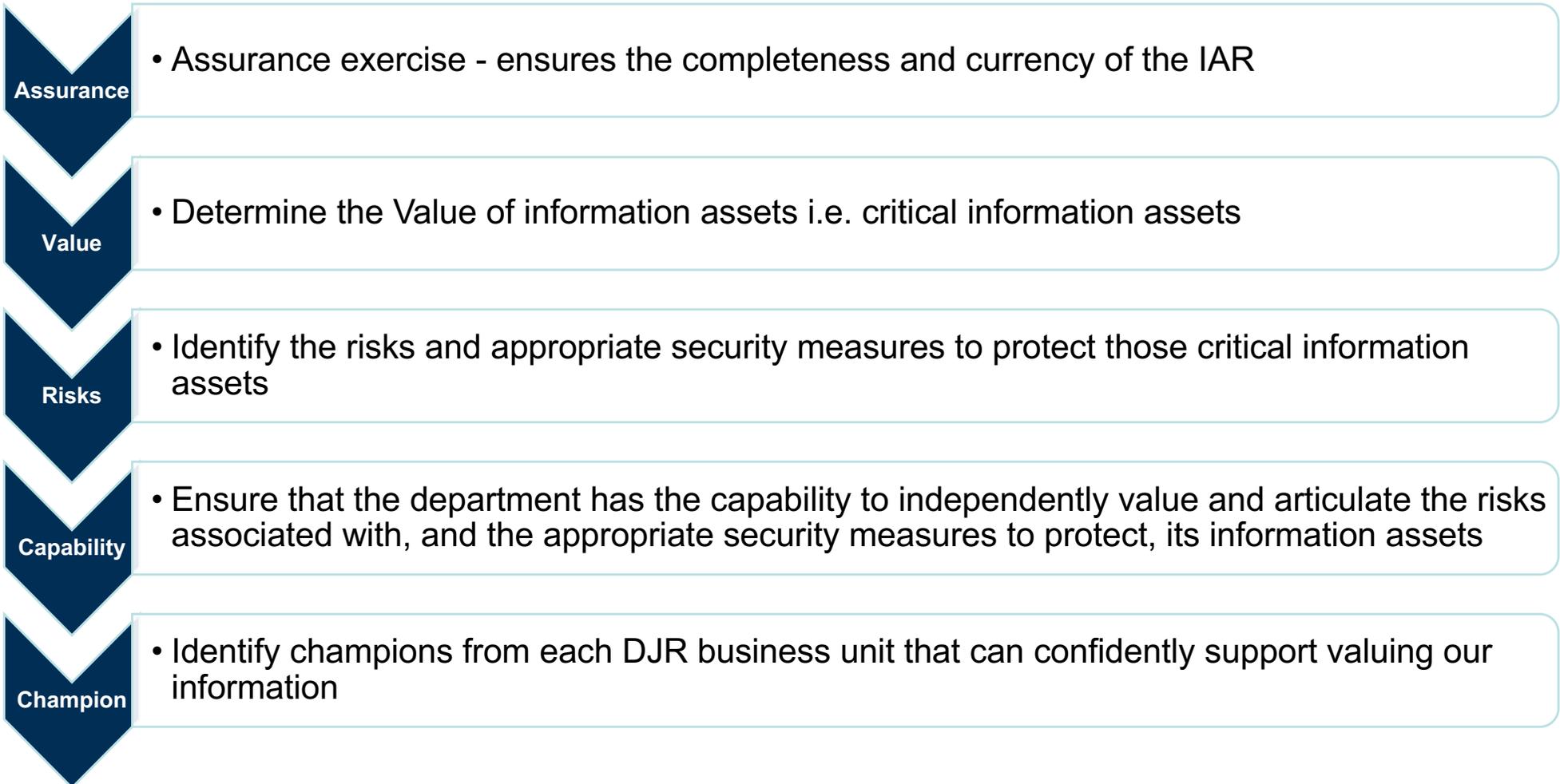
Both internally and externally, especially with the Office of the Victorian Information Commissioner
- 5 A clear program of work and **Capability Plan****

With defined projects, and work packages illustrating the work and effort that underpins the first year of a successful security program
- 6 And a strong vision**

With a clear end state of what success looks like in three years
- 7 Next steps**

Understanding and promoting the Value of our Information

# Next Steps



# The Journey Continues

Support the efforts of the  
Office of the Victorian  
Information Commissioner

Support our people to value  
and protect our information  
seamlessly and as BAU

# Thank you

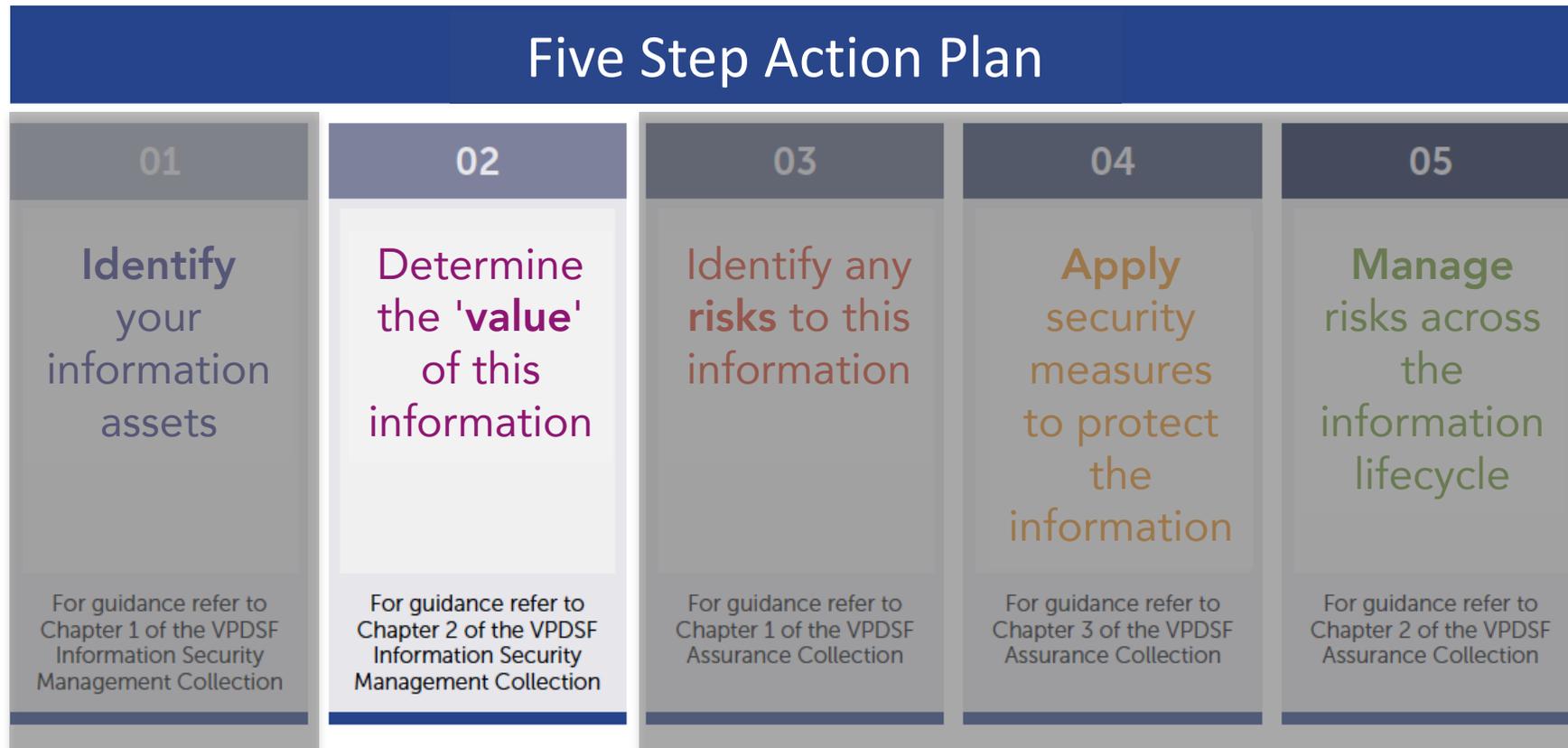
## **Security Management & Assurance**

Finance, Infrastructure & Governance Division  
Department of Justice & Regulation

(03) 8684 1585 | 0429 889712  
[smaenquiries@justice.vic.gov.au](mailto:smaenquiries@justice.vic.gov.au)

Level 26, 121 Exhibition Street  
Melbourne Victoria 3000

# Topic 2 - Determine the value of this information



# Business Impact Levels (BILs)

VPDSF INFORMATION SECURITY MANAGEMENT COLLECTION

EXTRACT OF CHAPTER 2 – APPENDIX B

**VPDSF BUSINESS IMPACT LEVEL (BIL) TABLE**

V11

Appendix – VPDSF Business Impact Level (BIL) Table

IMPACT CATEGORY >	ECONOMY AND FINANCE				
	Impact Levels				
	NEGLIGIBLE 0	LOW-MEDIUM 1	HIGH 2	VERY HIGH 3	EXTREME 4
	Compromise of the information could be expected to cause insignificant harm/damage to government operations, organisations and individuals	Compromise of the information could be expected to cause limited harm/damage to government operations, organisations and individuals	Compromise of the information could be expected to cause major harm/damage to government operations, organisations and individuals	Compromise of the information could be expected to cause significant harm/damage to government operations, organisations and individuals	Compromise of the information could be expected to cause serious harm/damage to government operations, organisations and individuals
SUB IMPACT CATEGORY ✓					
Organisation's operating budget (impact on public finances) >	Resulting in insignificant loss of < 1% of organisation's annual operating budget	Resulting in limited loss of > 1% – 10% of organisation's annual operating budget	Resulting in major loss of > 10% – 15% of organisation's annual operating budget	Resulting in significant loss of > 15% – 20% of organisation's annual operating budget	Resulting in serious loss of > 20% of organisation's annual operating budget
CONSEQUENCES >					
Non-public finances >	None	Resulting in limited financial hardship to an individual or business	Resulting in major financial hardship to an individual or business	Resulting in significant financial hardship to an individual or business	Resulting in serious financial hardship to an individual or business
CONSEQUENCES >					

# Compromise of...



**CONFIDENTIALITY**



**INTEGRITY**



**AVAILABILITY**



**RIGHT PEOPLE**



**RIGHT INFORMATION**



**RIGHT TIME**



# Performing an assessment

A value assessment involves three core stages:

1. Review the content
2. Consider potential impacts if the information were compromised
3. Understand the overall value of the information, in order to apply the appropriate security measures



## Working example

The Country Fire Authority (CFA) regularly publish a range of information on their website, notifying members of the community about warnings or events.



The image shows a screenshot of the CFA website. At the top left is the CFA logo, which consists of a red and white checkered square above the letters 'CFA' in red. To the right of the logo is a black horizontal bar with the text 'WARNINGS & RESTRICTIONS' in white. Below this bar is a section titled 'CURRENT WARNINGS' in bold red text. Underneath this title are two warning icons (yellow triangles with a black exclamation mark) followed by text: 'GREATER MELBOURNE, ADVICE' and '14/09/17 04:15 pm' in red; and 'WEST AND SOUTH GIPPSLAND, ADVICE' and '14/09/17 04:01 pm' in red.

**CFA**

**WARNINGS & RESTRICTIONS**

**CURRENT WARNINGS**

-  GREATER MELBOURNE, ADVICE  
14/09/17 04:15 pm
-  WEST AND SOUTH GIPPSLAND, ADVICE  
14/09/17 04:01 pm

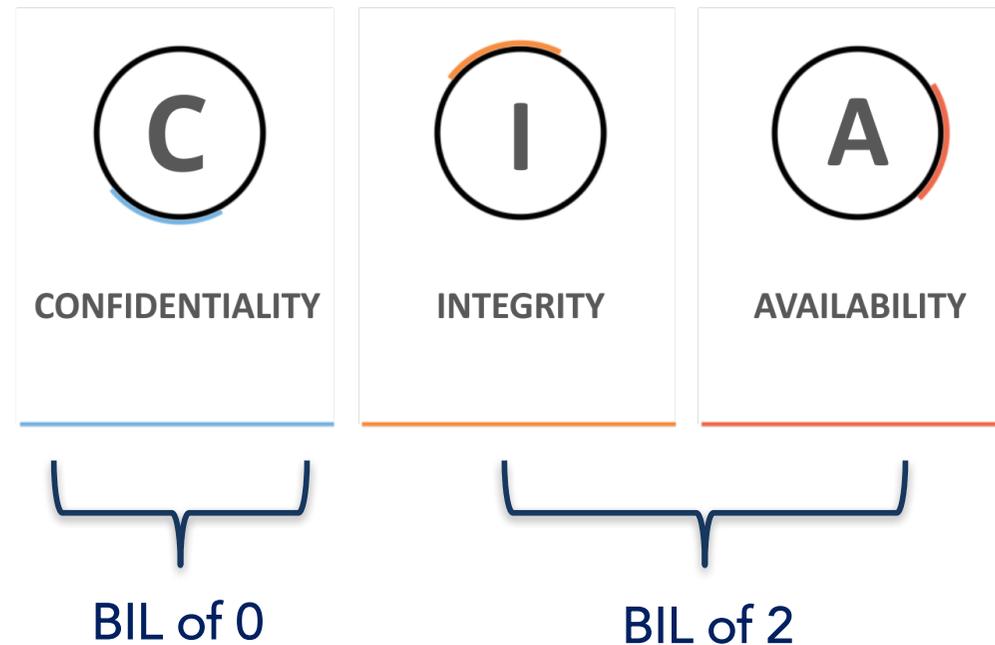
## Outcomes

Work through each impact category in the Business Impact Level table using either the BIL mobile/web app or other methods to identify the highest impact if this information was compromised

### WORK SHEET

Information Type 1 – EXAMPLE ONLY - CFA Warnings and Events					
Impact Type <i>(Refer to the BIL table for detailed information of each impact type)</i>	Severity				
	0 Negligible	1 Low - Medium	2 High	3 Very High	4 Extreme
Organisation's operating budget	CIA				
Non-public finances	C	IA			
Legal and regulatory compliance	C	IA			
Personal impact (injury)	C		IA		
Organisation reputation, confidence and utilisation of services	C		IA		
Companies operating in Victoria	CIA				
Organisation's material or physical assets	C	IA			
Service delivery	C		IA		
Relationships with other governments	CIA				
Provision of emergency services	C		IA		
Crime fighting	CIA				
Judicial proceedings	CIA				
Public unrest / order	CIA				
	↓	↓	↓	↓	↓
	<b>PUBLIC DOMAIN UNCLASSIFIED</b>	<b>UNCLASSIFIED</b>	<b>PROTECTED</b>	<b>CONFIDENTIAL</b>	<b>SECRET</b>
(C) Protective Marking	<b>PUBLIC DOMAIN X</b>	DLM:	DLM:	DLM:	DLM:
(I)			X		
(A)			X		

## Outcomes



The value of the information, is based on the overall highest BIL rating

In this scenario, the example arrived at a BIL of 2 so you should implement security measures to support protection of information at this level

## Questions?



For any other feedback or enquiries please direct your comments to the the [security@cpdp.vic.gov.au](mailto:security@cpdp.vic.gov.au) mailbox