OVIC

Office of the Victorian Information Commissioner

Victorian Information Security Network (VISN) Forum - Melbourne

February 2020

Acknowledgement

We acknowledge the traditional custodians of the land on which we are meeting today, and pay our respects to them, their culture and their Elders past, present and emerging. We also acknowledge the Elders from other communities who may be here today.

OVIC

Office of the Victorian
Information Commissioner

Agenda – Session 13

1. **Welcome by Sven Bluemmel, Victorian Information Commissioner**

2. **Release of the updated Framework**

3. **Release of supporting products**

4. **Upcoming release of Practitioner Guide: Information Security Risk Management**
   Former Chapter 1 – Assurance Collection

4. **Deep dive into the new Protective Data Security Plan**

5. **Multi-Organisational Reporting and supporting processes**

6. **Questions**

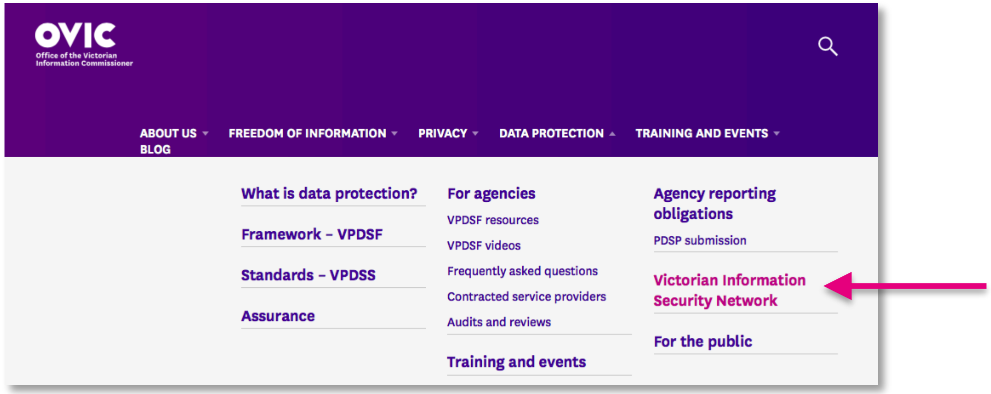
Live Streaming/Recording of Event & Copies of Slides

Live streaming / recording

This event is being live streamed on Periscope. A recording of this be posted on our website after the event.

Slides

For those who want to access a copy of this slide deck please refer to the **Victorian Information Security Network** page on the OVIC website.



Office of the Victorian Information Commissioner

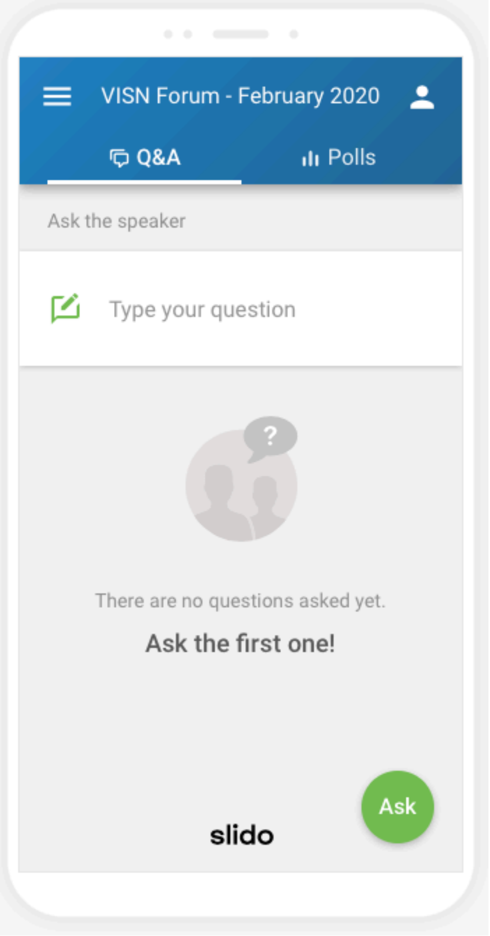
SLiDo

During

be using an online tool (Sli.do) offering you an opportunity to interact with our presentation, engage in polls and ask questions.

For those using the tool you will have the option of asking questions anonymously and can also access a link

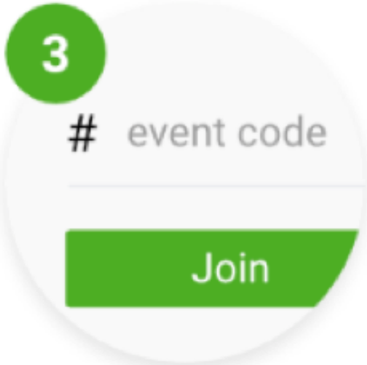
The team will moderate the tool and will post any relevant comments or material to the audience…



SLiDo

Open browser

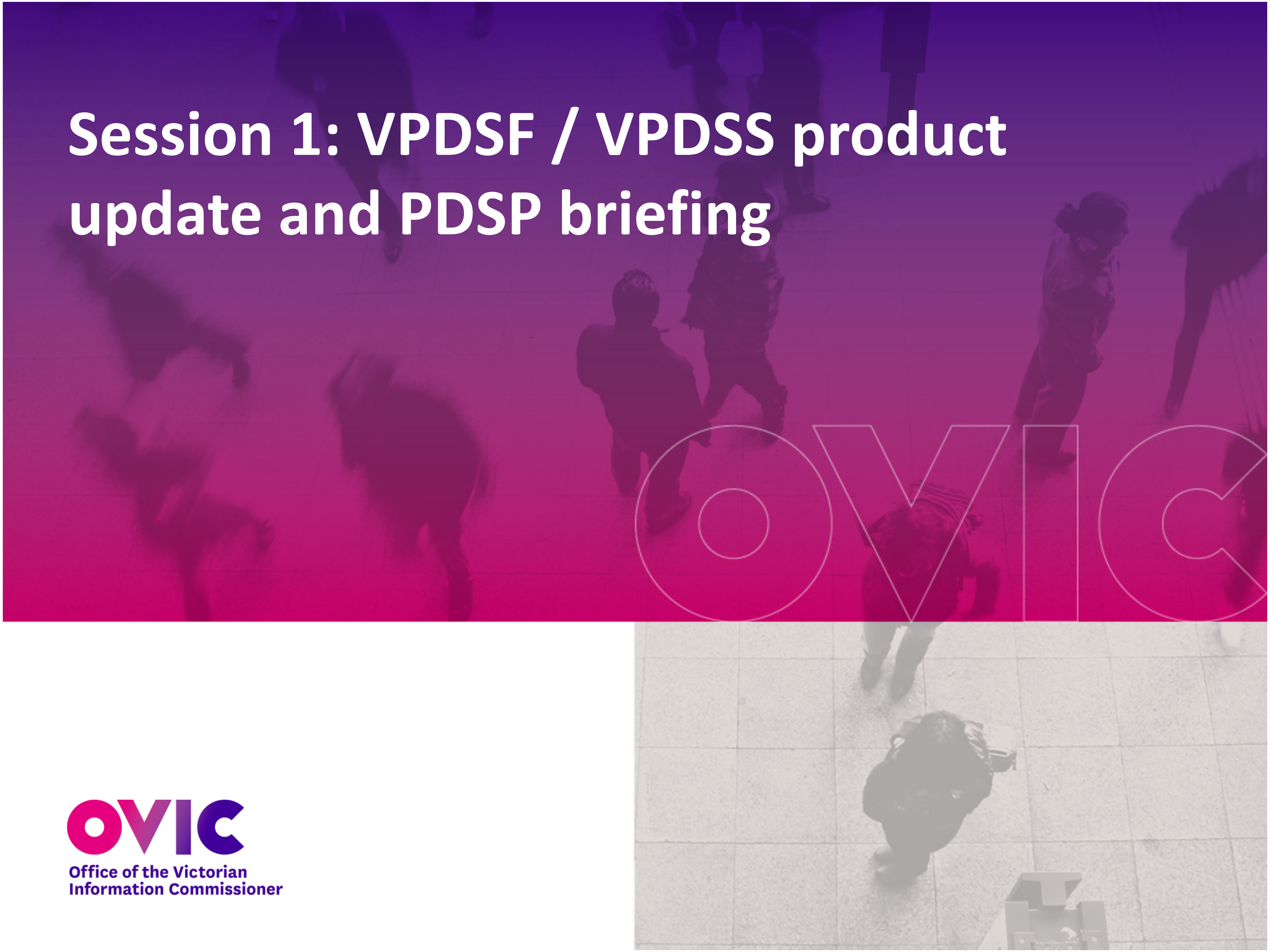
Go to slido.com



Join with event code

Q507 JOIN

Session 1: VPDSF / VPDSS product update and PDSP briefing



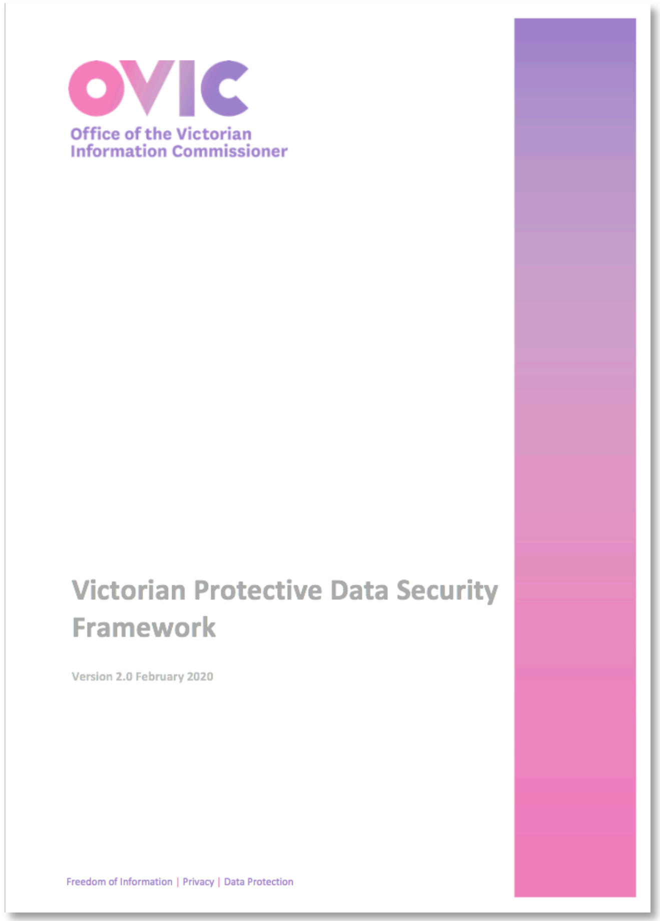
Office of the Victorian Information Commissioner

The Framework re-cast (v2.0)

Following an extensive review of our product suite, the Victorian Protective Data Security Framework (the **Framework**) document has been heavily revised.

The Framework document now:

- outlines the monitoring and assurance activities of VPS Organisations and OVIC, and
- articulates the relationship of the Standards to the Framework and Regulatory Action Plan (RAP).



OVIC
Office of the Victorian
Information Commissioner

Victorian Protective Data Security Framework

Version 2.0 February 2020

Freedom of Information | Privacy | Data Protection

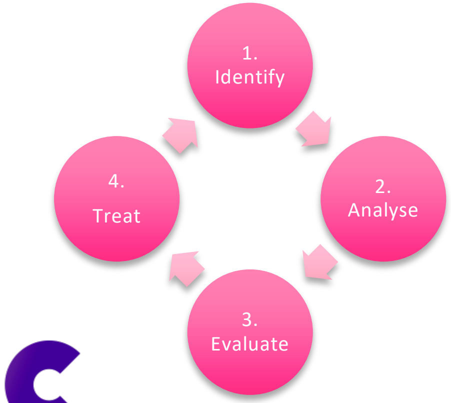
SRPA and PDSP re-framed

As part of this broader product review, OVIC has also updated some of its monitoring and assurance tools.

This included re-framing what a Security Risk Profile Assessment (**SRPA**) and a Protective Data Security Plan (**PDSP)** were.

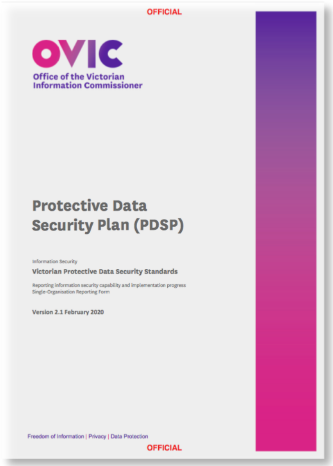
SRPA

A SRPA is an **end to end, 4 stage process** that enables VPS organisations to identify, analyse, evaluate and treat information security risks.



PDSP

A PDSP is a **reporting tool** for VPS organisations to submit to OVIC.


OFFICIAL

Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards

Reporting information security capability and implementation progress
Single-Organisation Reporting Form

Version 2.1 February 2020

Freedom of Information | Privacy | Data Protection

OFFICIAL

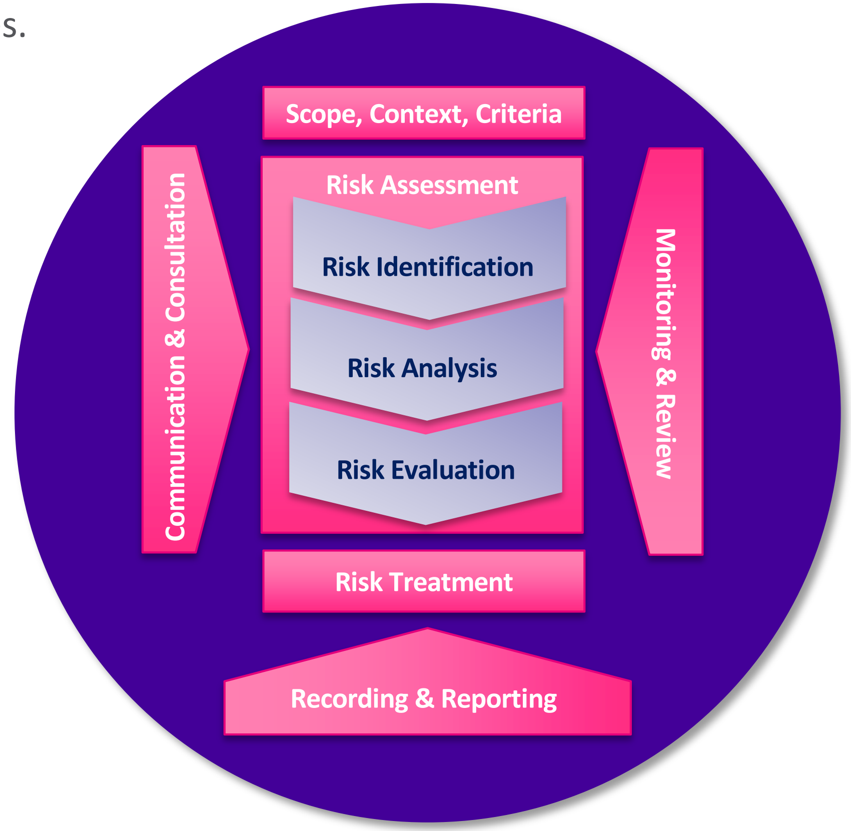
Office of the Victorian Information Commissioner

The SRPA explained

To perform a SRPA, organisations should adopt the risk management process outlined in ISO31000, applying a security lens to the risk assessment and subsequent management activities.

- VPS organisations should undertake a SRPA regularly (**at least annually**)
- The SRPA process **must include assessments of 3rd parties** that deal with public sector information for the VPS organisation, for example, contracted service providers
- The **outcomes** of a SRPA should be **documented in a VPS organisation's risk register**

Risk Management process outlined in ISO31000



Practitioner Guide: Information Security Risk Management

Chapter 1 of the **former Assurance Collection** has been refreshed and will be presented as a Practitioner Guide.

This guide will walk organisations through the SRPA process.

This Practitioner Guide will be published in the coming weeks.

The remaining chapters of the former Assurance Collection relate to obsolete resources that are no longer relevant, but an archived version of the collection is available on **GovTEAMS**.

OVIC
Office of the Victorian
Information Commissioner

INFORMATION SECURITY

Information Security Risk Management

Version 2.0

Formerly Chapter 1 of the Assurance Collection

Freedom of Information | Privacy | Data Protection

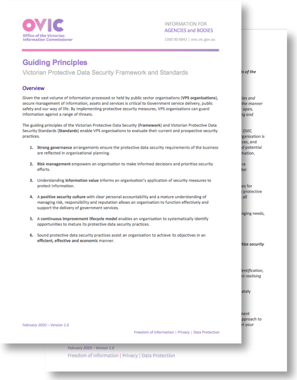
Coming Soon!

Accessing Former Framework content

Relevant material previously included in the former version of the Framework document, will be represented as supplementary resources within the **GovTEAMS** community and on the OVIC website.

Example resources include:

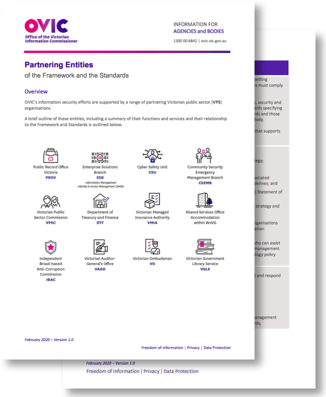
InfoSheet Guiding Principles



Guiding Principles

Victorian Protective Data Security Framework and Standards

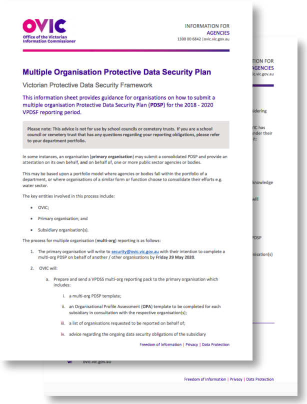
InfoSheet Partnering Entities



Partnering Entities

of the Framework and the Standards

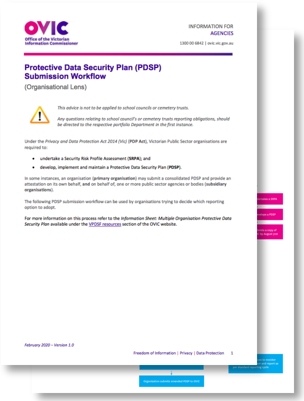
InfoSheet Multi-Organisation Reporting



Multiple Organisation Protective Data Security Plan

Victorian Protective Data Security Framework

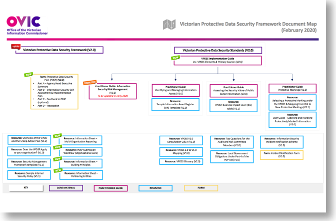
PDSP Submission Process



Protective Data Security Plan (PDSP) Submission Workflow

(Organisational Lens)

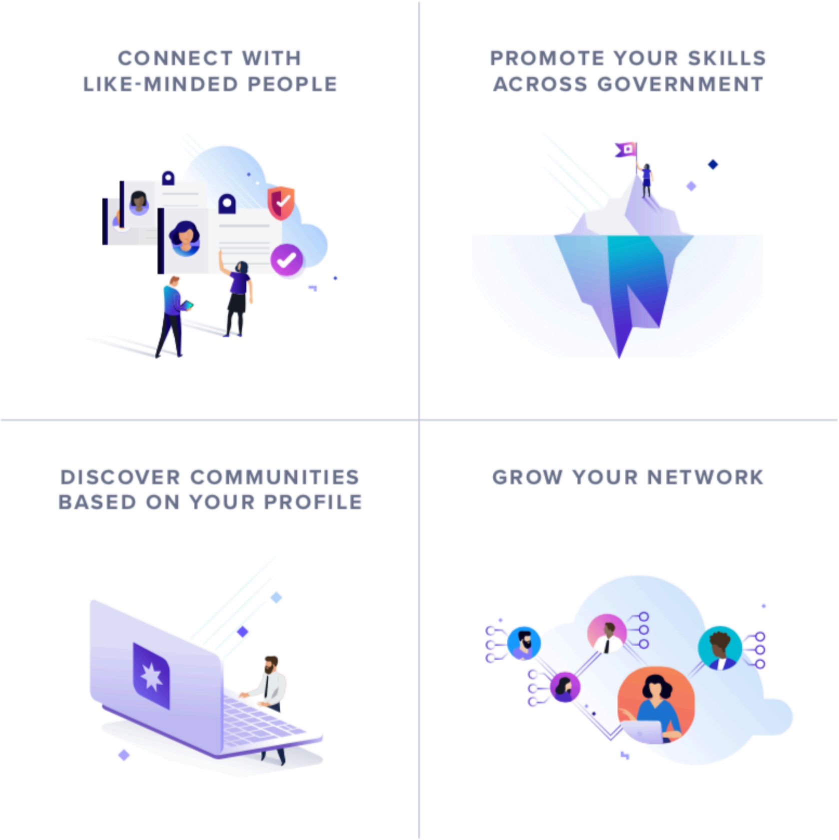
Feb 2020 Document Map



Victorian Protective Data Security Framework Document Map (February 2020)

Office of the Victorian Information Commissioner

GovTEAMS



CONNECT WITH LIKE-MINDED PEOPLE

PROMOTE YOUR SKILLS ACROSS GOVERNMENT

DISCOVER COMMUNITIES BASED ON YOUR PROFILE

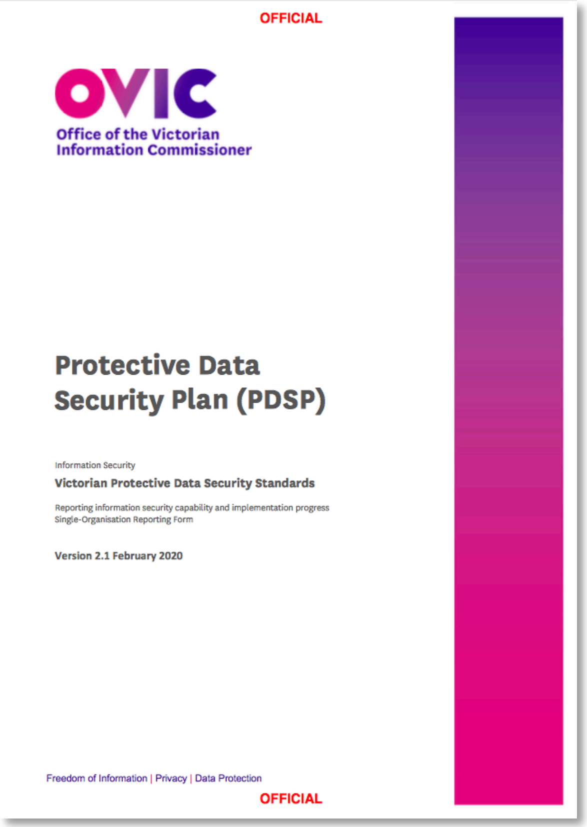
GROW YOUR NETWORK

Email security@ovic.vic.gov.au to request to join the online VISN community!

Deep dive into the new PDSP form

Office of the Victorian
Information Commissioner

What is a PDSP?



OFFICIAL

Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards

Reporting information security capability and implementation progress
Single-Organisation Reporting Form

Version 2.1 February 2020

Freedom of Information | Privacy | Data Protection

OFFICIAL

A Protective Data Security Plan (**PDSP**) is a reporting tool, used by VPS organisations to:

- advise OVIC of their maturity level, and implementation status of the Standards, referencing information security risks as identified as part of the SRPA process;
- articulate the VPS organisation's security profile; and
- attest to the implementation activities as required by the Standards.

Commonly asked questions

Who fills in the PDSP?

The PDSP should be completed by a person with sufficient knowledge of the security operations of the organisation.

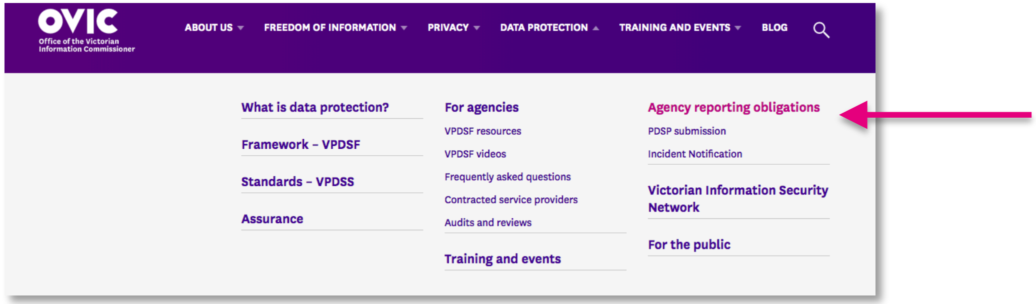
Who signs the Attestation (*Part D* of the PDSP form)?

Under the PDP Act, your public sector body Head is responsible for providing a copy of your organisation's PDSP to OVIC. However, your organisation's PDSP can be submitted to OVIC by anyone authorised by your organisation.

Part A of the PDSP form provides a section where the public sector body Head can nominate an authorised person.

Where do I get a copy of the PDSP template?

A current copy of the PDSP template, refer to the **Agency Reporting Obligations** page on the OVIC website.



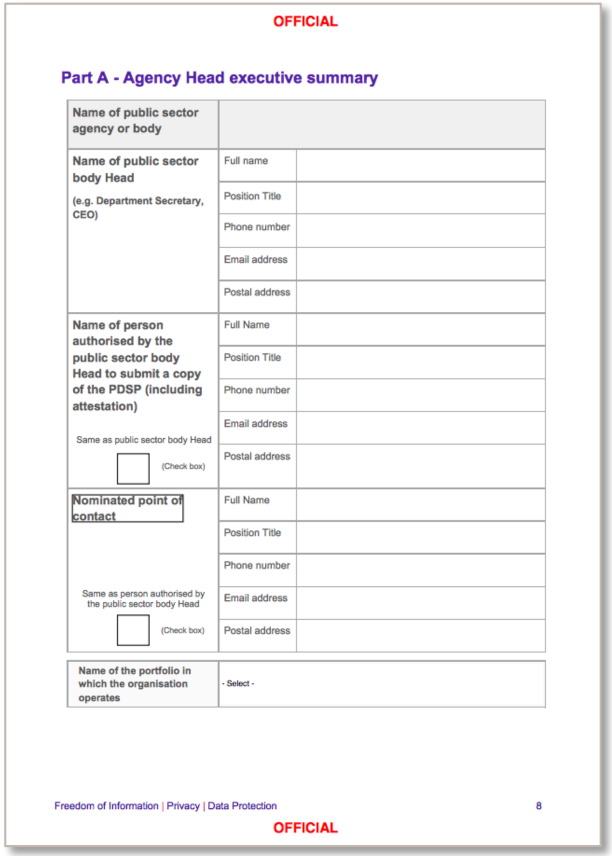
Part A – Agency Head Executive Summary

Agency Head

Authorised Person
(authorised by Agency Head)

Point of Contact

Portfolio Dept.



OFFICIAL

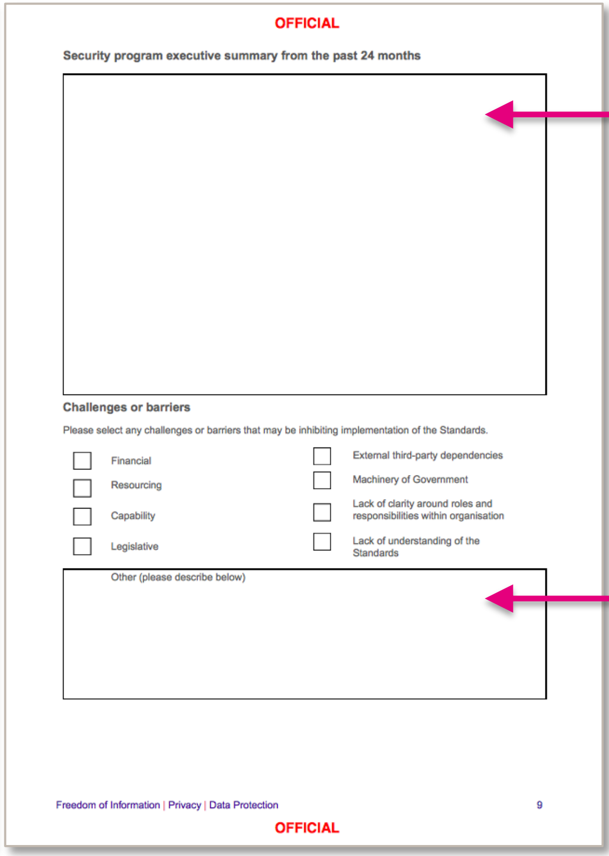
Part A - Agency Head executive summary

Name of public sector agency or body		
Name of public sector body Head **(e.g. Department Secretary, CEO)**	Full name	
	Position Title	
	Phone number	
	Email address	
	Postal address	
Name of person authorised by the public sector body Head to submit a copy of the PDSP (including attestation) Same as public sector body Head □ (Check box)	Full Name	
	Position Title	
	Phone number	
	Email address	
	Postal address	
Nominated point of contact Same as person authorised by the public sector body Head □ (Check box)	Full Name	
	Position Title	
	Phone number	
	Email address	
	Postal address	

Name of the portfolio in which the organisation operates	- Select -

Freedom of Information | Privacy | Data Protection 8

OFFICIAL



OFFICIAL

Security program executive summary from the past 24 months

Challenges or barriers

Please select any challenges or barriers that may be inhibiting implementation of the Standards.

- □ Financial
- □ Resourcing
- □ Capability
- □ Legislative
- □ External third-party dependencies
- □ Machinery of Government
- □ Lack of clarity around roles and responsibilities within organisation
- □ Lack of understanding of the Standards

Other (please describe below)

Freedom of Information | Privacy | Data Protection 9

OFFICIAL

*Free text field, where you can describe **achievements** since the last PDSP submission*

*Free text field, where you can describe **challenges / barriers***

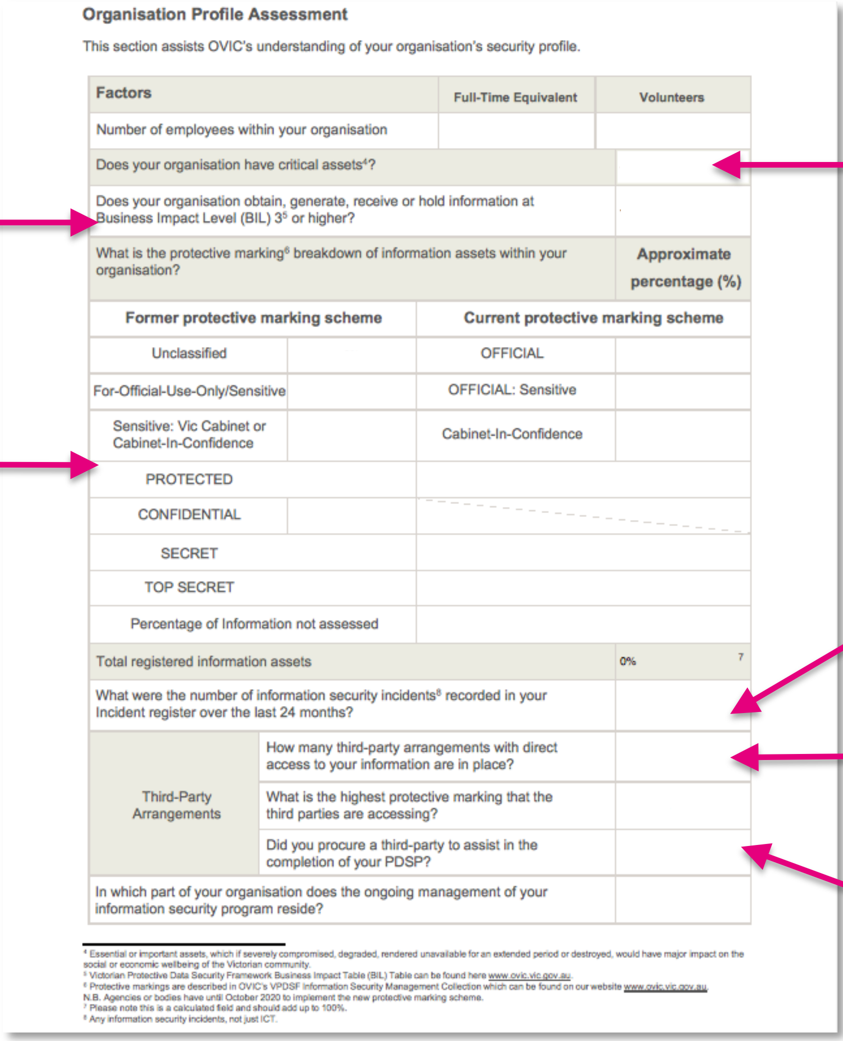
Part A – Organisation Profile Assessment

Refer to the Business Impact Level (**BIL**) table and your organisation's Information Asset Register (**IAR**).

Enter the percentage **(%)** breakdown of information assets as per their **protective marking**.

N.B. Your **IAR** may help you with these responses, however if this is not available please provide an estimate.

N.B. This section provides both the former and new protective marking scheme options.



Organisation Profile Assessment

This section assists OVIC's understanding of your organisation's security profile.

Factors		**Full-Time Equivalent**	**Volunteers**
Number of employees within your organisation			
Does your organisation have critical assets[4]?			
Does your organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3[5] or higher?			
What is the protective marking[6] breakdown of information assets within your organisation?			**Approximate percentage (%)**
Former protective marking scheme		**Current protective marking scheme**	
Unclassified		OFFICIAL	
For-Official-Use-Only/Sensitive		OFFICIAL: Sensitive	
Sensitive: Vic Cabinet or Cabinet-In-Confidence		Cabinet-In-Confidence	
PROTECTED			
CONFIDENTIAL			
SECRET			
TOP SECRET			
Percentage of Information not assessed			
Total registered information assets			0%[7]
What were the number of information security incidents[8] recorded in your Incident register over the last 24 months?			
Third-Party Arrangements	How many third-party arrangements with direct access to your information are in place?		
	What is the highest protective marking that the third parties are accessing?		
	Did you procure a third-party to assist in the completion of your PDSP?		
In which part of your organisation does the ongoing management of your information security program reside?			

[4] Essential or important assets, which if severely compromised, degraded, rendered unavailable for an extended period or destroyed, would have major impact on the social or economic wellbeing of the Victorian community.
[5] Victorian Protective Data Security Framework Business Impact Table (BIL) Table can be found here www.ovic.vic.gov.au.
[6] Protective markings are described in OVIC's VPDSF Information Security Management Collection which can be found on our website www.ovic.vic.gov.au.
N.B. Agencies or bodies have until October 2020 to implement the new protective marking scheme.
[7] Please note this is a calculated field and should add up to 100%.
[8] Any information security incidents, not just ICT.

Critical assets are defined as:

Essential or important assets, which if compromised, degraded, rendered unavailable for an extended period or destroyed, would significantly impact on the social or economic wellbeing of the organisation or Victorian community.

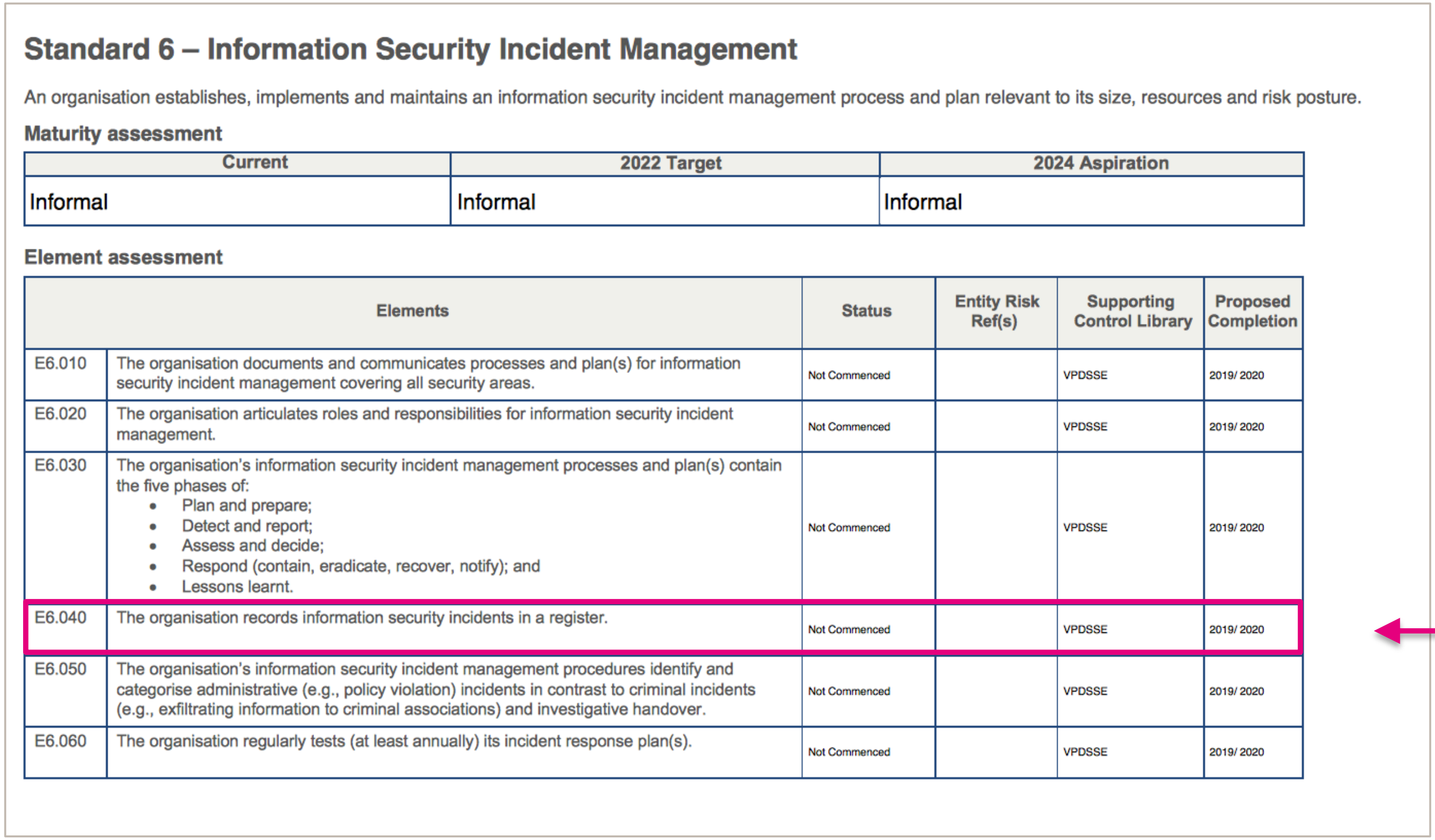
Refer to your incident register for this figure. If your organisation does not have an incident register (***element E6.040***), enter an estimate

If your organisation does not have a register of third party arrangements (***element E8.050***), enter an estimate

Did a consultant or 3rd party assist the organisation in completing the PDSP?

Office of the Victorian Information Commissioner

Part B – A working example



Standard 6 – Information Security Incident Management

An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

Maturity assessment

Current	2022 Target	2024 Aspiration
Informal	Informal	Informal

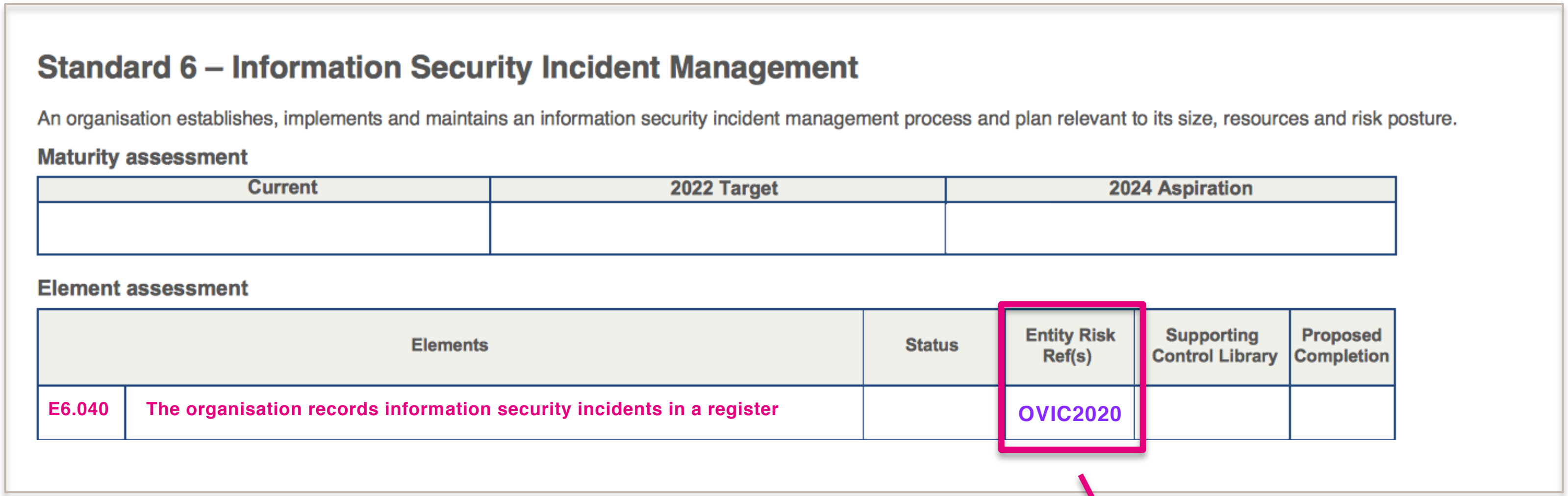
Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E6.010	The organisation documents and communicates processes and plan(s) for information security incident management covering all security areas.	Not Commenced		VPDSSE	2019/ 2020
E6.020	The organisation articulates roles and responsibilities for information security incident management.	Not Commenced		VPDSSE	2019/ 2020
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.	Not Commenced		VPDSSE	2019/ 2020
E6.040	The organisation records information security incidents in a register.	Not Commenced		VPDSSE	2019/ 2020
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.	Not Commenced		VPDSSE	2019/ 2020
E6.060	The organisation regularly tests (at least annually) its incident response plan(s).	Not Commenced		VPDSSE	2019/ 2020

E6.040

Part B – *A working example*

*What should you record in the **Entity Risk Ref(s)** field?*



Standard 6 – Information Security Incident Management

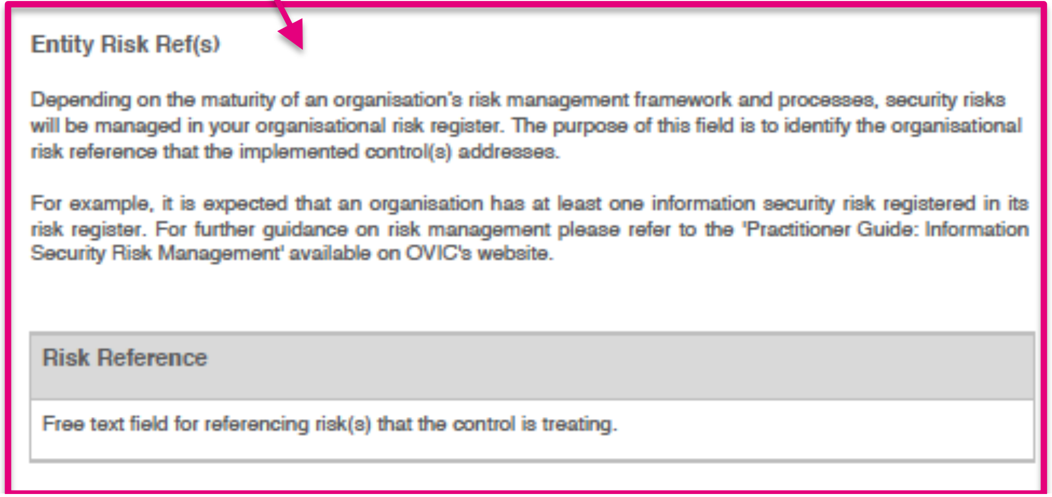
An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

Maturity assessment

Current	2022 Target	2024 Aspiration

Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E6.040	The organisation records information security incidents in a register		OVIC2020		



Entity Risk Ref(s)

Depending on the maturity of an organisation's risk management framework and processes, security risks will be managed in your organisational risk register. The purpose of this field is to identify the organisational risk reference that the implemented control(s) addresses.

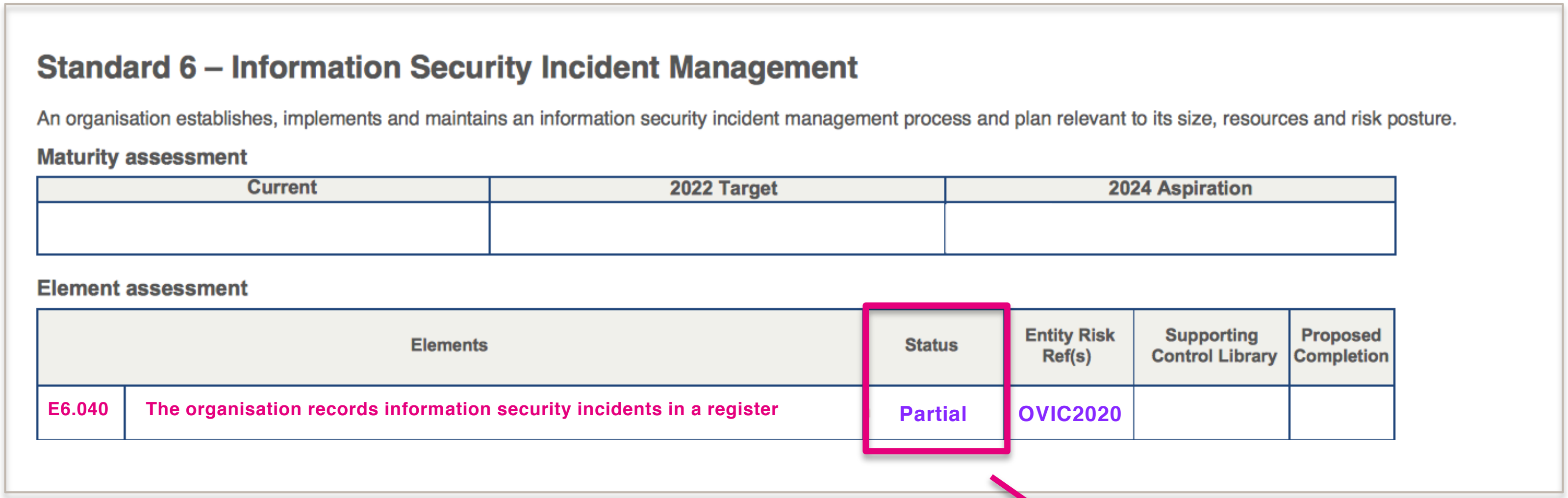
For example, it is expected that an organisation has at least one information security risk registered in its risk register. For further guidance on risk management please refer to the 'Practitioner Guide: Information Security Risk Management' available on OVIC's website.

Risk Reference
Free text field for referencing risk(s) that the control is treating.

Office of the Victorian Information Commissioner

Part B – *A working example*

*What should you record in the **Status** field?*



Standard 6 – Information Security Incident Management

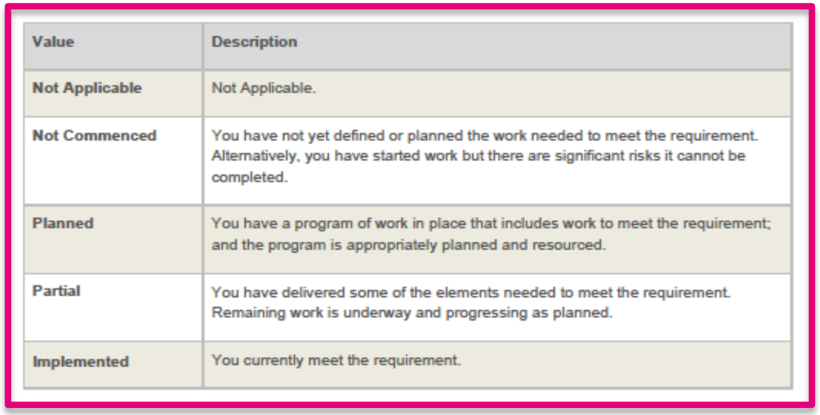
An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

Maturity assessment

Current	2022 Target	2024 Aspiration

Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E6.040	The organisation records information security incidents in a register	Partial	OVIC2020		

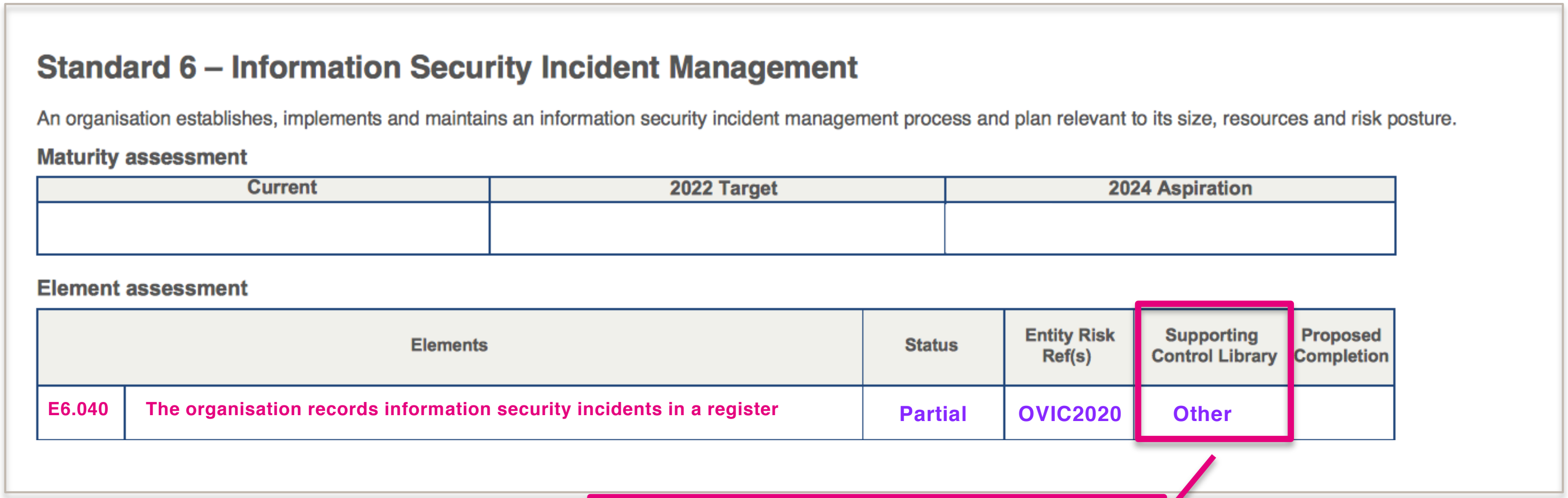


Value	Description
Not Applicable	Not Applicable.
Not Commenced	You have not yet defined or planned the work needed to meet the requirement. Alternatively, you have started work but there are significant risks it cannot be completed.
Planned	You have a program of work in place that includes work to meet the requirement; and the program is appropriately planned and resourced.
Partial	You have delivered some of the elements needed to meet the requirement. Remaining work is underway and progressing as planned.
Implemented	You currently meet the requirement.

Office of the Victorian Information Commissioner

Part B – *A working example*

*What should you record in the **Supporting Control Library** field?*



Standard 6 – Information Security Incident Management

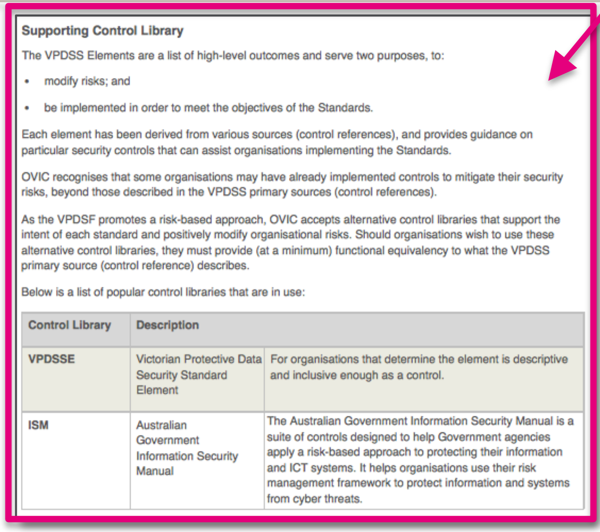
An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

Maturity assessment

Current	2022 Target	2024 Aspiration

Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E6.040	The organisation records information security incidents in a register	Partial	OVIC2020	Other	



Supporting Control Library

The VPDSS Elements are a list of high-level outcomes and serve two purposes, to:

- modify risks; and
- be implemented in order to meet the objectives of the Standards.

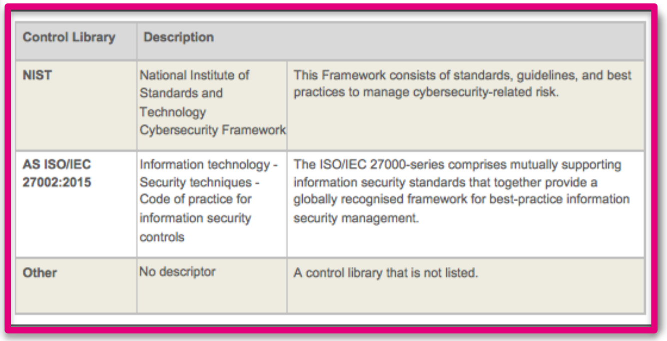
Each element has been derived from various sources (control references), and provides guidance on particular security controls that can assist organisations implementing the Standards.

OVIC recognises that some organisations may have already implemented controls to mitigate their security risks, beyond those described in the VPDSS primary sources (control references).

As the VPDSF promotes a risk-based approach, OVIC accepts alternative control libraries that support the intent of each standard and positively modify organisational risks. Should organisations wish to use these alternative control libraries, they must provide (at a minimum) functional equivalency to what the VPDSS primary source (control reference) describes.

Below is a list of popular control libraries that are in use:

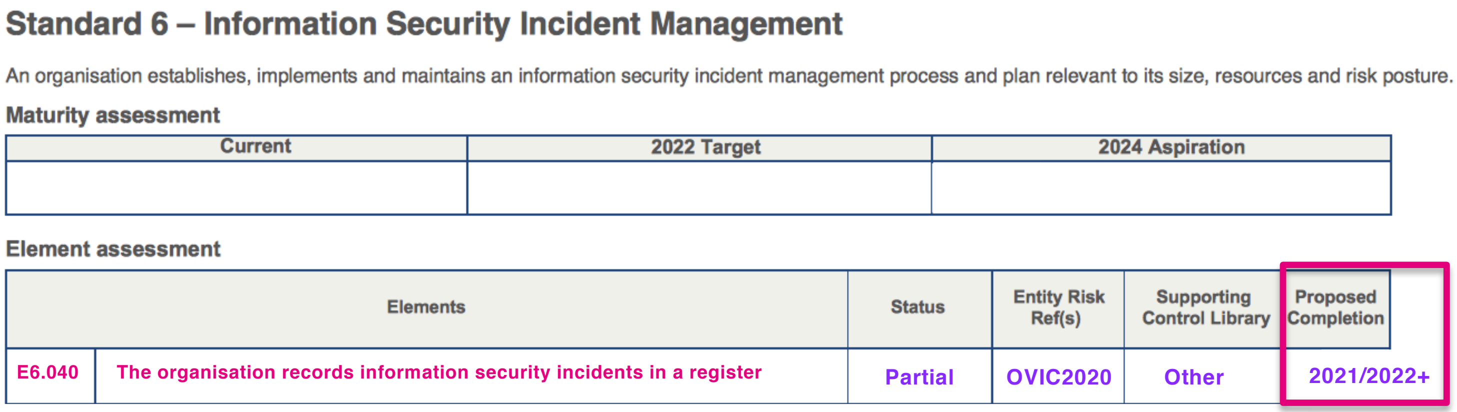
Control Library	Description	
VPDSSE	Victorian Protective Data Security Standard Element	For organisations that determine the element is descriptive and inclusive enough as a control.
ISM	Australian Government Information Security Manual	The Australian Government Information Security Manual is a suite of controls designed to help Government agencies apply a risk-based approach to protecting their information and ICT systems. It helps organisations use their risk management framework to protect information and systems from cyber threats.



Control Library	Description	
NIST	National Institute of Standards and Technology Cybersecurity Framework	This Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
AS ISO/IEC 27002:2015	Information technology - Security techniques - Code of practice for information security controls	The ISO/IEC 27000-series comprises mutually supporting information security standards that together provide a globally recognised framework for best-practice information security management.
Other	No descriptor	A control library that is not listed.

Part B – *A working example*

*What should you record in the **Proposed Completion** field?*



Standard 6 – Information Security Incident Management

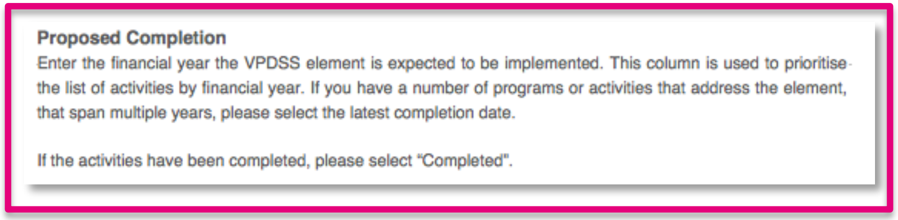
An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

Maturity assessment

Current	2022 Target	2024 Aspiration

Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E6.040	The organisation records information security incidents in a register	Partial	OVIC2020	Other	2021/2022+

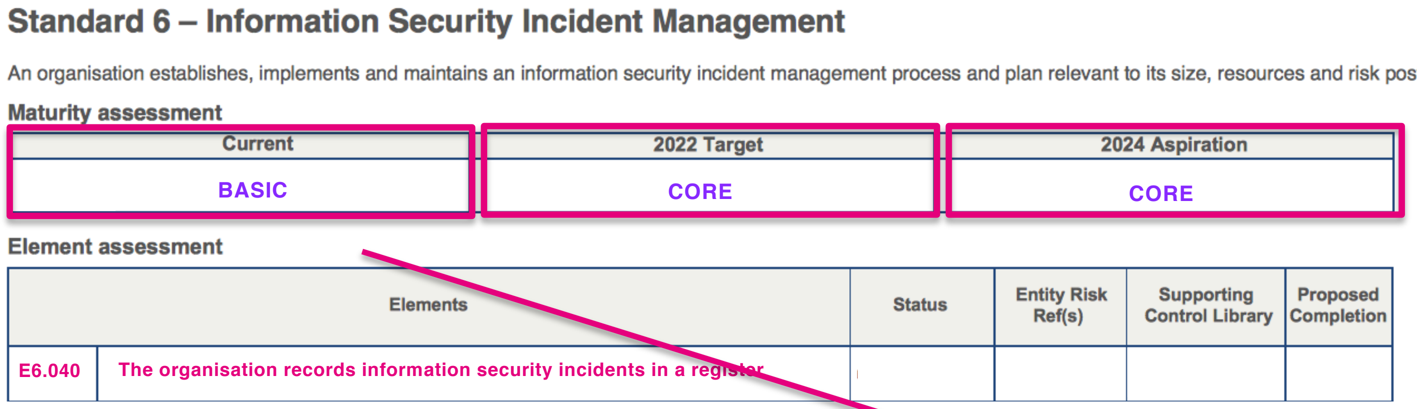


Proposed Completion

Enter the financial year the VPDSS element is expected to be implemented. This column is used to prioritise the list of activities by financial year. If you have a number of programs or activities that address the element, that span multiple years, please select the latest completion date.

If the activities have been completed, please select "Completed".

Part B – *A working example*



Standard 6 – Information Security Incident Management

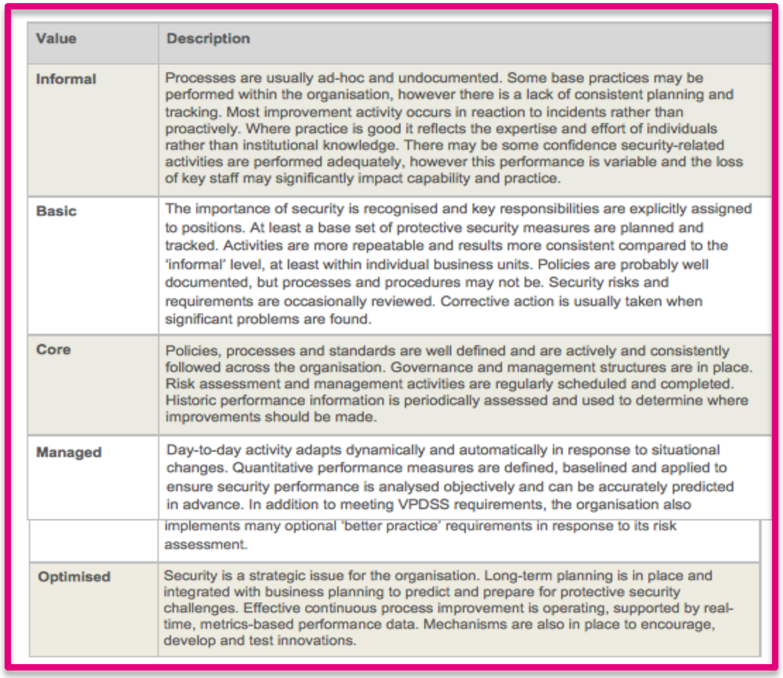
An organisation establishes, implements and maintains an information security incident management process and plan relevant to its size, resources and risk posture.

Maturity assessment

Current	2022 Target	2024 Aspiration
BASIC	CORE	CORE

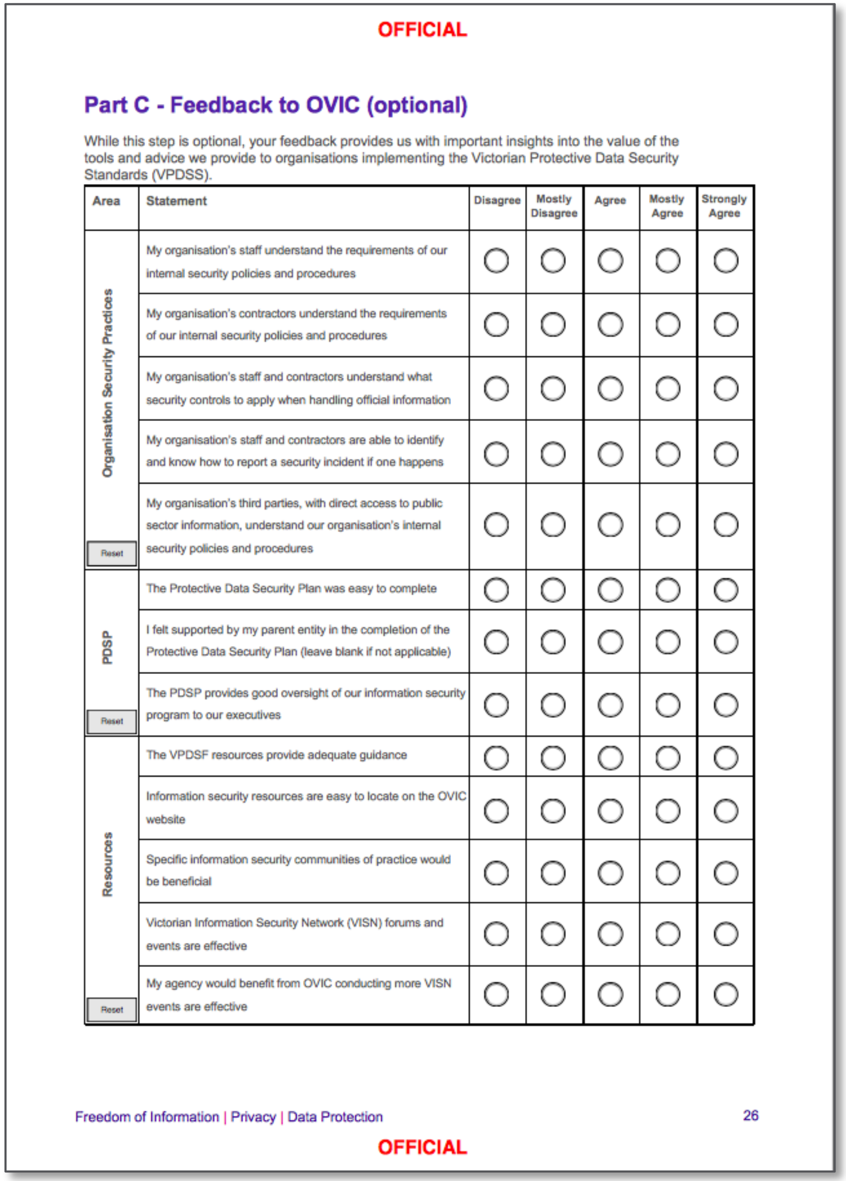
Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E6.040	The organisation records information security incidents in a register				



Value	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.

Part C



OFFICIAL

Part C - Feedback to OVIC (optional)

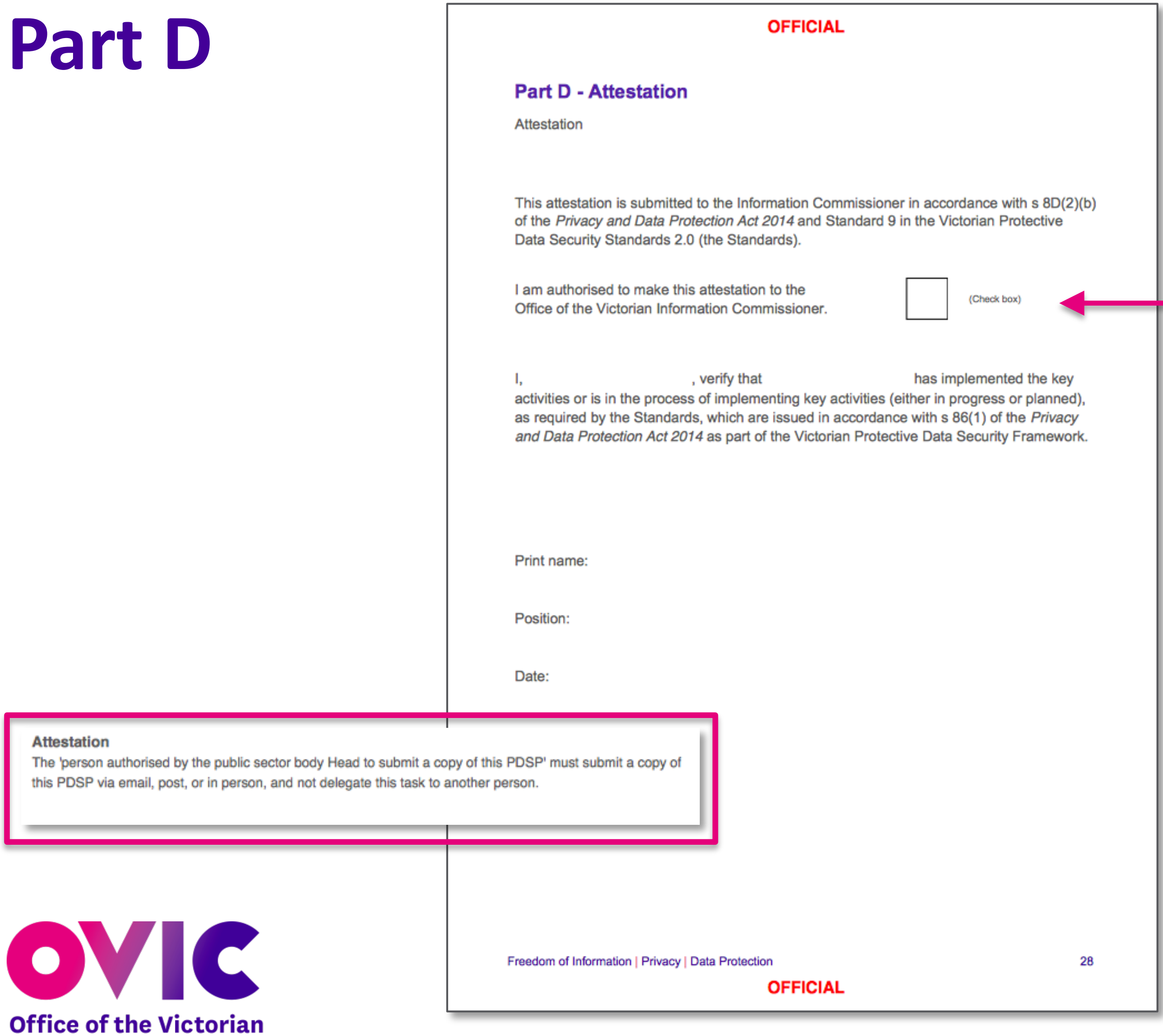
While this step is optional, your feedback provides us with important insights into the value of the tools and advice we provide to organisations implementing the Victorian Protective Data Security Standards (VPDSS).

Area	Statement	Disagree	Mostly Disagree	Agree	Mostly Agree	Strongly Agree
Organisation Security Practices Reset	My organisation's staff understand the requirements of our internal security policies and procedures	○	○	○	○	○
	My organisation's contractors understand the requirements of our internal security policies and procedures	○	○	○	○	○
	My organisation's staff and contractors understand what security controls to apply when handling official information	○	○	○	○	○
	My organisation's staff and contractors are able to identify and know how to report a security incident if one happens	○	○	○	○	○
	My organisation's third parties, with direct access to public sector information, understand our organisation's internal security policies and procedures	○	○	○	○	○
PDSP Reset	The Protective Data Security Plan was easy to complete	○	○	○	○	○
	I felt supported by my parent entity in the completion of the Protective Data Security Plan (leave blank if not applicable)	○	○	○	○	○
	The PDSP provides good oversight of our information security program to our executives	○	○	○	○	○
Resources Reset	The VPDSF resources provide adequate guidance	○	○	○	○	○
	Information security resources are easy to locate on the OVIC website	○	○	○	○	○
	Specific information security communities of practice would be beneficial	○	○	○	○	○
	Victorian Information Security Network (VISN) forums and events are effective	○	○	○	○	○
	My agency would benefit from OVIC conducting more VISN events are effective	○	○	○	○	○

Freedom of Information | Privacy | Data Protection 26

OFFICIAL

Part D



OFFICIAL

Part D - Attestation

Attestation

This attestation is submitted to the Information Commissioner in accordance with s 8D(2)(b) of the *Privacy and Data Protection Act 2014* and Standard 9 in the Victorian Protective Data Security Standards 2.0 (the Standards).

I am authorised to make this attestation to the Office of the Victorian Information Commissioner. □ (Check box)

I, , verify that has implemented the key activities or is in the process of implementing key activities (either in progress or planned), as required by the Standards, which are issued in accordance with s 86(1) of the *Privacy and Data Protection Act 2014* as part of the Victorian Protective Data Security Framework.

Print name:

Position:

Date:

Freedom of Information | Privacy | Data Protection 28

OFFICIAL

Attestation

The 'person authorised by the public sector body Head to submit a copy of this PDSP' must submit a copy of this PDSP via email, post, or in person, and not delegate this task to another person.

If you check this box, the **authorised person** identified in **Part A** of the PDSP template will be automatically filled in here.

Should your agency head wish to manually enter their information here, they still can.

Multi-Organisation Reporting

Office of the Victorian
Information Commissioner

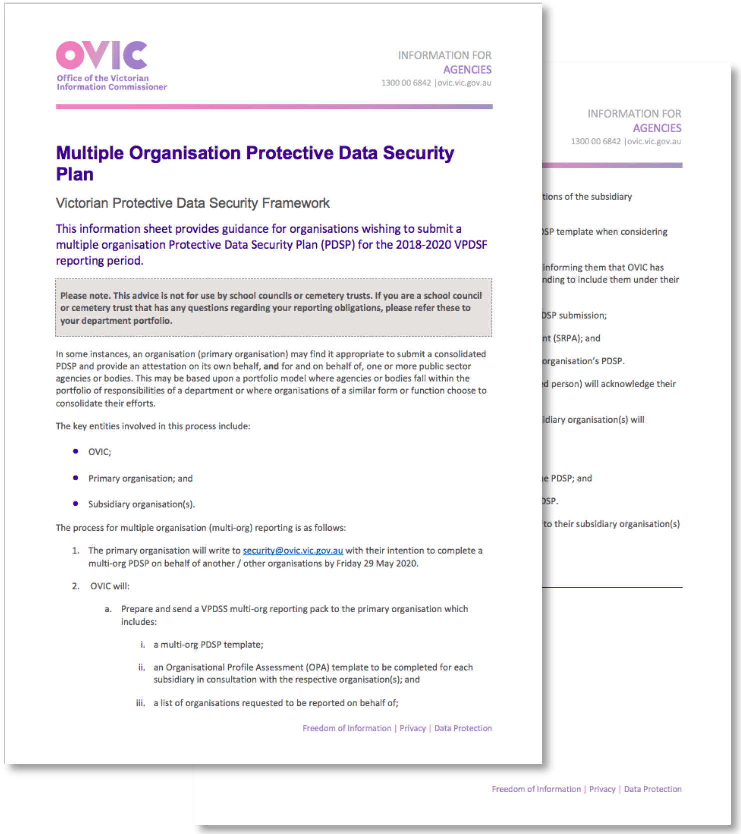
Updates to the Multi-Organisation Reporting Process

The multi-organisation PDSP reporting process has changed!

An information sheet and supporting workflow has been produced to assist organisations in this updated process.

Organisations must advise OVIC, no later than May, of their intention to submit a Multi-Organisation PDSP.

These resources are available for download from the OVIC website.



Office of the Victorian Information Commissioner

INFORMATION FOR
AGENCIES
1300 00 6842 |ovic.vic.gov.au

Multiple Organisation Protective Data Security Plan

Victorian Protective Data Security Framework

This information sheet provides guidance for organisations wishing to submit a multiple organisation Protective Data Security Plan (PDSP) for the 2018-2020 VPDSF reporting period.

Please note. This advice is not for use by school councils or cemetery trusts. If you are a school council or cemetery trust that has any questions regarding your reporting obligations, please refer these to your department portfolio.

In some instances, an organisation (primary organisation) may find it appropriate to submit a consolidated PDSP and provide an attestation on its own behalf, **and** for and on behalf of, one or more public sector agencies or bodies. This may be based upon a portfolio model where agencies or bodies fall within the portfolio of responsibilities of a department or where organisations of a similar form or function choose to consolidate their efforts.

The key entities involved in this process include:

- OVIC;
- Primary organisation; and
- Subsidiary organisation(s).

The process for multiple organisation (multi-org) reporting is as follows:

1. The primary organisation will write to security@ovic.vic.gov.au with their intention to complete a multi-org PDSP on behalf of another / other organisations by Friday 29 May 2020.
2. OVIC will:
    a. Prepare and send a VPDSS multi-org reporting pack to the primary organisation which includes:
        i. a multi-org PDSP template;
        ii. an Organisational Profile Assessment (OPA) template to be completed for each subsidiary in consultation with the respective organisation(s); and
        iii. a list of organisations requested to be reported on behalf of;

Freedom of Information | Privacy | Data Protection

INFORMATION FOR
AGENCIES
1300 00 6842 |ovic.vic.gov.au

tions of the subsidiary

SP template when considering

informing them that OVIC has
nding to include them under their

DSP submission;

nt (SRPA); and

organisation's PDSP.

d person) will acknowledge their

idiary organisation(s) will

e PDSP; and

DSP.

to their subsidiary organisation(s)

Freedom of Information | Privacy | Data Protection

Session 2: Information Security Incident Notification Scheme

Office of the Victorian Information Commissioner

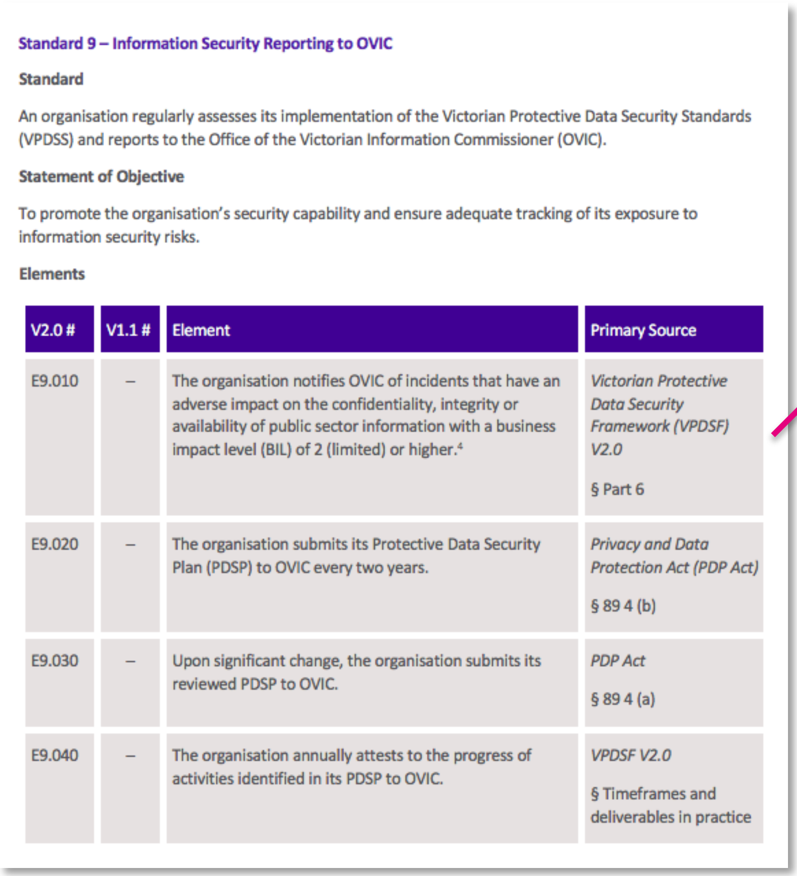
Overview of the Scheme

The Notification Scheme was introduced in October 2019 and is currently in play…

We acknowledge there will be subtleties assessing incidents

If in doubt about whether an incident needs to be reported, notify OVIC regardless

What's actually required under the scheme



Standard 9 – Information Security Reporting to OVIC

Standard

An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (VPDSS) and reports to the Office of the Victorian Information Commissioner (OVIC).

Statement of Objective

To promote the organisation's security capability and ensure adequate tracking of its exposure to information security risks.

Elements

V2.0 #	V1.1 #	Element	Primary Source
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.[4]	*Victorian Protective Data Security Framework (VPDSF) V2.0* § Part 6
E9.020	–	The organisation submits its Protective Data Security Plan (PDSP) to OVIC every two years.	*Privacy and Data Protection Act (PDP Act)* § 89 4 (b)
E9.030	–	Upon significant change, the organisation submits its reviewed PDSP to OVIC.	*PDP Act* § 89 4 (a)
E9.040	–	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	*VPDSF V2.0* § Timeframes and deliverables in practice

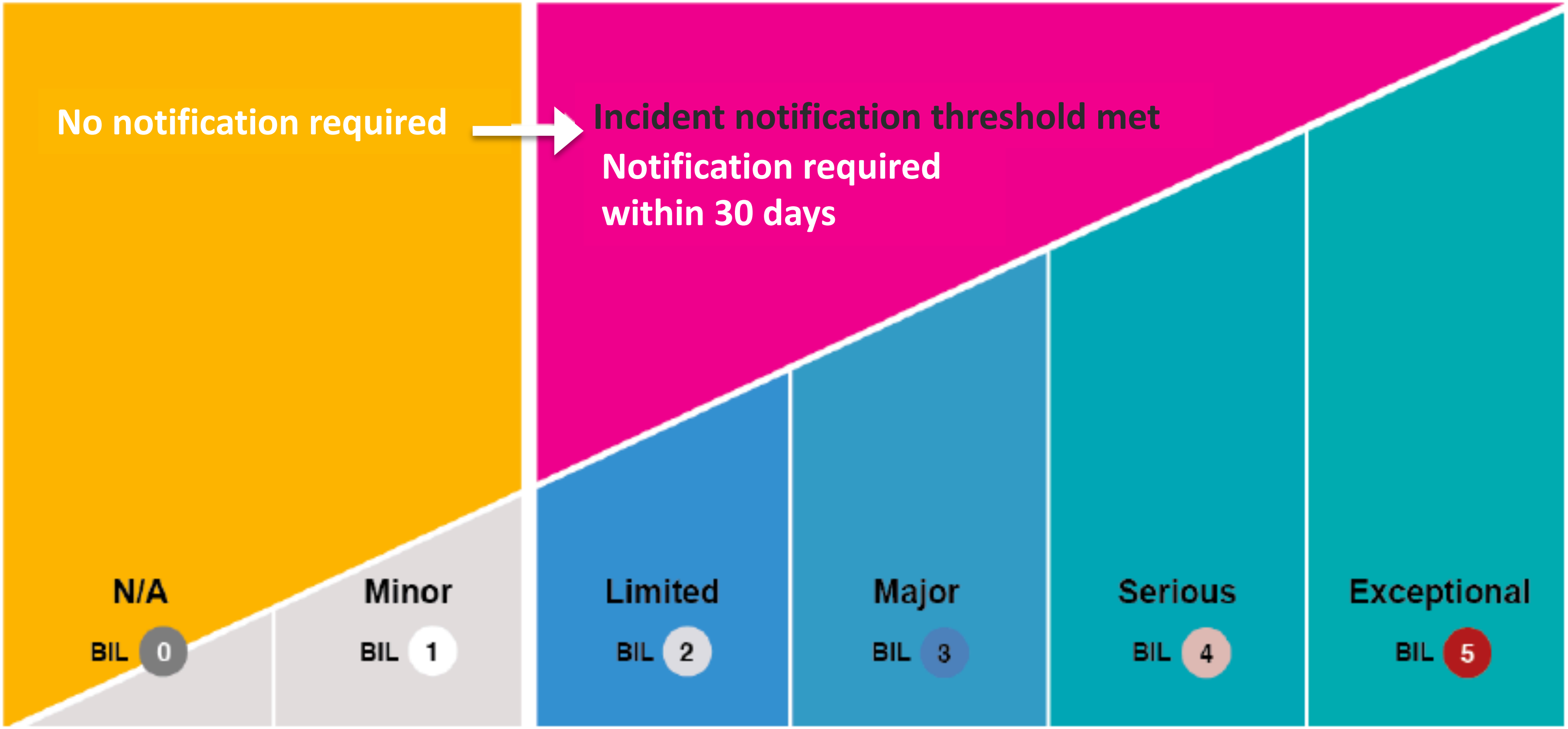
Standard 9 - Element E9.010

Notify 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.**

Visual representation of the scheme



No notification required

Incident notification threshold met

Notification required within 30 days

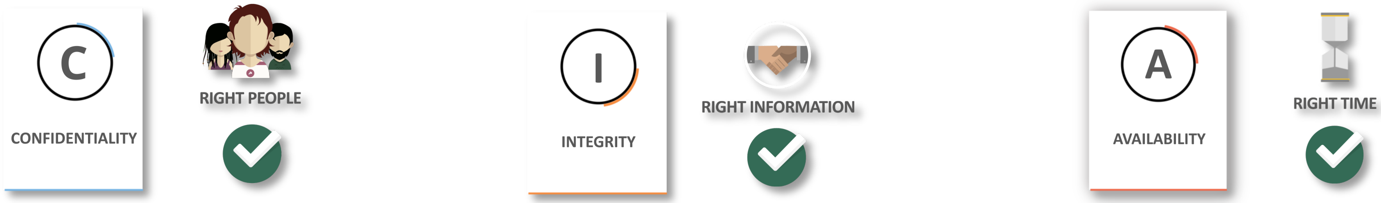
Key points about the scheme

Incident vs. Breach

- These two terms are quite distinct, and have different meanings

- Under the <u>**incident**</u> **notification scheme**, the ***confidentiality*** of the information is not the only focus.

  If there is an adverse impact to the ***integrity*** and/or ***availability*** of the information or information system(s), the incident would qualify under this scheme



- A **breach** however**,** primarily focuses on a compromise to the confidentiality of information

Key points about the scheme

Coverage

The scheme applies to ALL:

- **Types** of information, for example:
  - financial records,
  - personal information,
  - general corporate information, and
  - health information.
- **Forms** of information, for example:
  - Soft copy / Digital,
  - Hard copy /Physical Documents, and
  - Verbal disclosures

Key points about the scheme

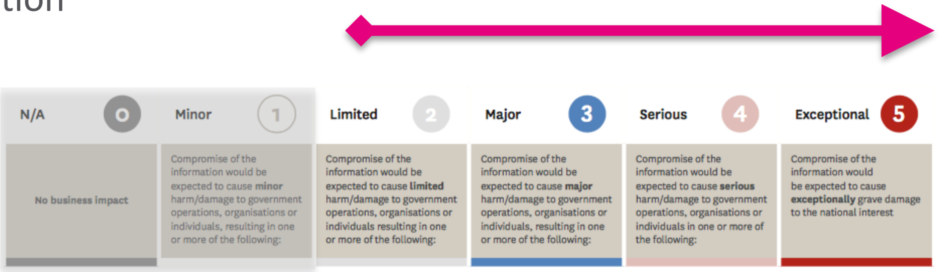
Business Impact Level (BIL) 2 or higher

- The scheme only applies to information assessed at a **BIL of 2 or higher**

- This means compromise of the Confidentiality, Integrity or Availability of the information would be expected to cause either:
    - **limited** (BIL of 2)
    - **major** (BIL of 3)
    - **serious** (BIL of 4) or
    - **exceptional** (BIL of 5)

  harm or damage

- BILs are determined by the originator the information



N/A 0	Minor 1	Limited 2	Major 3	Serious 4	Exceptional 5
No business impact	Compromise of the information would be expected to cause **minor** harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Compromise of the information would be expected to cause **limited** harm/damage to government operations, organisations or individuals resulting in one or more of the following:	Compromise of the information would be expected to cause **major** harm/damage to government operations, organisations or individuals, resulting in one or more of the following:	Compromise of the information would be expected to cause **serious** harm/damage to government operations, organisations or individuals in one or more of the following:	Compromise of the information would be expected to cause **exceptionally** grave damage to the national interest

Refer to the VPDSF BIL table on the OVIC website for more information on BILs

SCENARIO

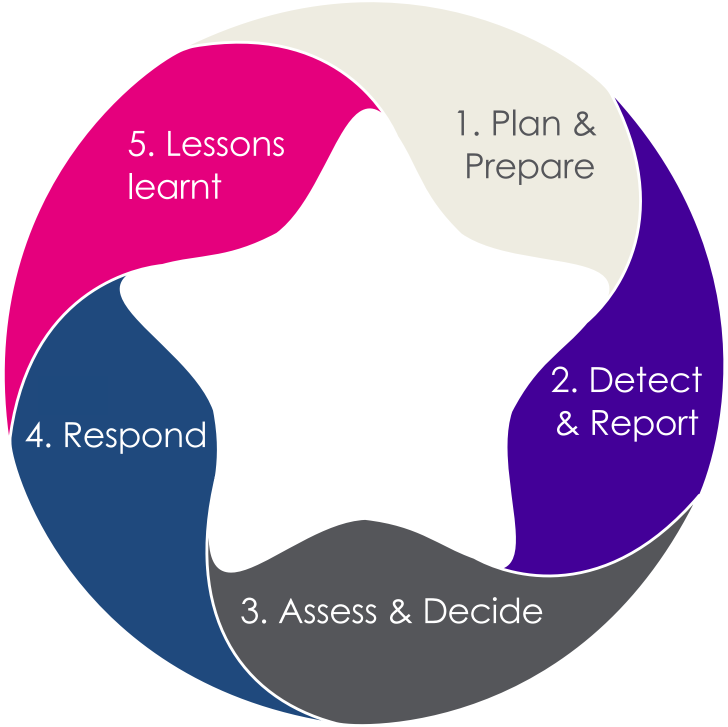
Before we jump in…

The purpose of walking through a scenario is to show how your organisation may interact with OVIC and DPC, once a notifiable incident has been identified.

There may be multiple players involved in the oversight and management of an incident, but primarily today we will focus on:

- Information Security Unit within OVIC
- Privacy Guidance Unit within OVIC
- Cyber Incident Response Service (CIRS)

We won't be stepping though the full incident response process, but will go through each of the units roles and responsibilities.



Introduction of key players in this scenario

Information Security Unit within OVIC

Oversight of all information security incidents for organisations that fall under Part 4, Privacy and Data Protection Act 2014

- No response capability
- Operate 9am – 5pm, Monday to Friday

Data Protection

Privacy Guidance Unit within OVIC

- Receive voluntary reports of data breaches involving personal information
- Provide guidance – contemporaneous and after the fact – mainly focused on minimising harm to affected individuals
- 9 – 5 business days – mix of telephone/written report

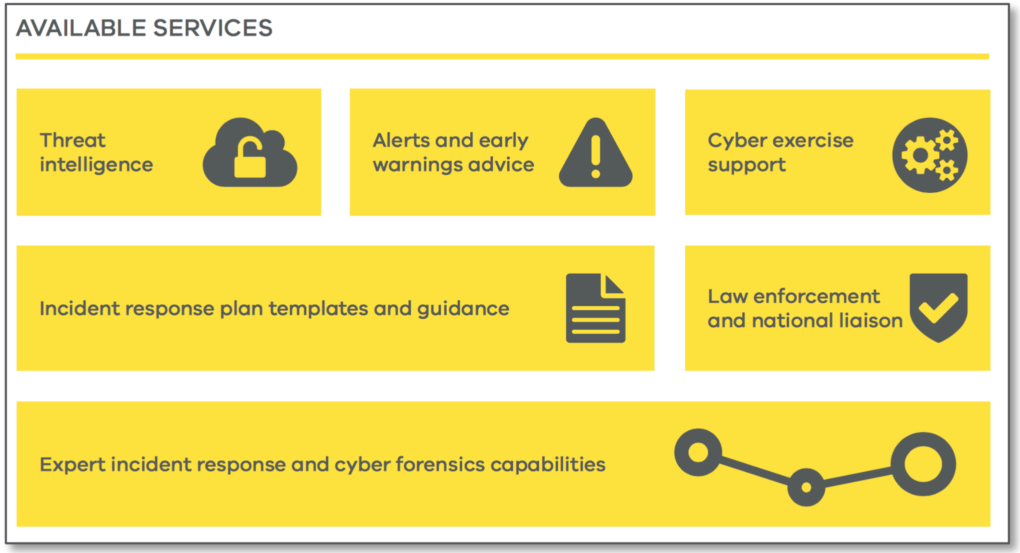
Privacy

Introduction of key players in this scenario

Cyber Incident Response Service within CSU

24/7 Cyber Incident Response Service (CIRS):

- coordinates government responses for cyber security incidents
- provides cyber threat intelligence
- provides remote and onsite services



AVAILABLE SERVICES

Threat intelligence

Alerts and early warnings advice

Cyber exercise support

Incident response plan templates and guidance

Law enforcement and national liaison

Expert incident response and cyber forensics capabilities

Scenario: Incident Summary

"Unauthorised access to HR system, resulting in exfiltration of information"

Incident attributes: *Compromise of the confidentiality of soft copy information*

Status: *Ongoing*

Incident Identified: *02/02/2020*

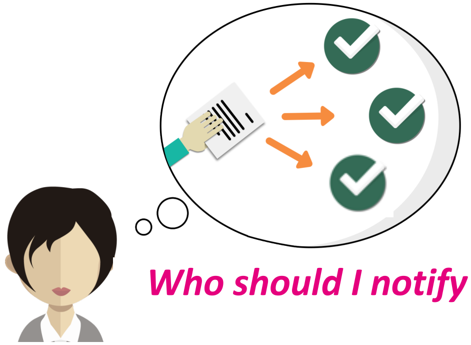
BIL assessment of information: *BIL 2 - Compromise of the **C**, **I** and **A** resulted in limited harm or damage to -*

- ***Individuals***: *limited breach of personal information (including sensitive information as defined in Schedule 1 of the PDP Act 2014) (Personal Injury category in VPDSF BIL table)*
- ***The organisation***: *limited reputational damage or embarrassment for the organisation (Public Services category in VPDSF BIL table)*

Organisation's ability (capability and capacity) to respond: *Minimal*

So what players could be involved?

Based on the incident attributes, the following players may be involved -



Who should I notify?

Cyber response required ✓

>> *Engage the **Cyber Safety Unit***

Privacy advice required ✓

>> *Engage the **OVIC Privacy Unit***

Threshold met for Information Security Incident **notification scheme** ✓

>> *Engage the **OVIC Information Security Unit***

Where to start?

Step One

First, you need to stop the bleed…

After dusting off your incident response plan you recognise that your organisation doesn't have the capacity or capability to effectively respond to the incident.

Given that this is a cyber incident, you may seek assistance from the Cyber Incident Response Service (CIRS) within the Cyber Safety Unit.

James McMillan, Advisor - Cyber Incident and Emergency Management can tell us more about what to expect when you call **1300 CSU VIC** or email cybersecurity@dpc.vic.gov.au

DATE: 07/2019

Cyber Incident Response Plan

<organisation name>

Contact the Victorian Government Cyber Incident Response Service for assistance in responding to cyber incidents. Contact 1300 CSU VIC or cybersecurity@dpc.vic.gov.au

[INSERT APPROPRIATE SECURITY CLASSIFICATION]

Working through the issues…

Step Two

Once you have managed to contain the incident, you can now turn your attention to limiting the impact.

Turning to our privacy colleagues, we pose the question - *What sort of things should you need to take into account in an incident like this*?

Dermot Dignam, Manager Privacy Guidance can tell us more about what to expect when you call **1300 006 842** or email privacy@ovic.vic.gov.au

OVIC
Office of the Victorian Information Commissioner

PRIVACY

Managing the privacy impacts of a data breach

May 2019

Freedom of Information | Privacy | Data Protection

OVIC
Office of the Victorian Information Commissioner

Formally notifying OVIC

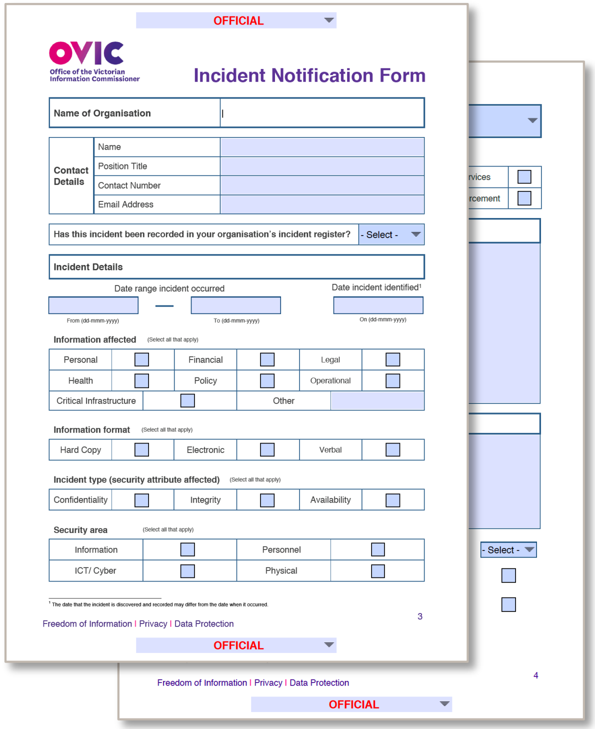
Step Three

VPS organisations need to notify OVIC within 30 business days of identifying an reportable incident (BIL of 2 or higher).

It is important that the notification process should not get in the way of responding or addressing your incident.

If you have already spoken to the OVIC Privacy Unit, you will have satisfied this requirement and don't need to notify OVIC again.

Anthony Corso, Assistant Commissioner Information Security can tell us more about what to expect when you submit a notification form to incidents@ovic.vic.gov.au



OFFICIAL

Office of the Victorian Information Commissioner

Incident Notification Form

Name of Organisation	

Contact Details	Name	
	Position Title	
	Contact Number	
	Email Address	

Has this incident been recorded in your organisation's incident register?	- Select -

Incident Details

Date range incident occurred — Date incident identified[1]

From (dd-mmm-yyyy) — To (dd-mmm-yyyy) — On (dd-mmm-yyyy)

Information affected (Select all that apply)

Personal	□	Financial	□	Legal	□
Health	□	Policy	□	Operational	□
Critical Infrastructure	□	Other			

Information format (Select all that apply)

Hard Copy	□	Electronic	□	Verbal	□

Incident type (security attribute affected) (Select all that apply)

Confidentiality	□	Integrity	□	Availability	□

Security area (Select all that apply)

Information	□	Personnel	□
ICT/ Cyber	□	Physical	□

[1] The date that the incident is discovered and recorded may differ from the date when it occurred.

Freedom of Information | Privacy | Data Protection 3

OFFICIAL

rvices □

rcement □

- Select -

□

□

Freedom of Information | Privacy | Data Protection 4

OFFICIAL

Key things to remember

We are trying to minimize the reporting burden by allowing multiple avenues to not only notify, but also request assistance.

Depending on the particular incident, you may choose a different path and that's ok - we will be there to direct you.

Organisations:

- need to ensure their teams are coordinating internally on incident management
- may need to update their internal processes to address the notification scheme
- should ensure that they:
    - have an Incident Management Plan –
        - ○ CSU have a sample *Cyber Incident Management Plan* (CIMP) available
    - test their incident management plan at least annually

Questions

For those with questions following this forum, please email ***security@ovic.vic.gov.au***

OVIC
Office of the Victorian
Information Commissioner