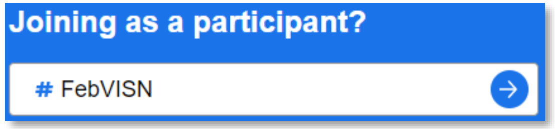
Housekeeping

Cameras and mics are muted. If your Teams is running slow, try disconnecting from your VPN.

The session is being recorded and a copy (including slides) will be made available following the session.

Go to slido.com



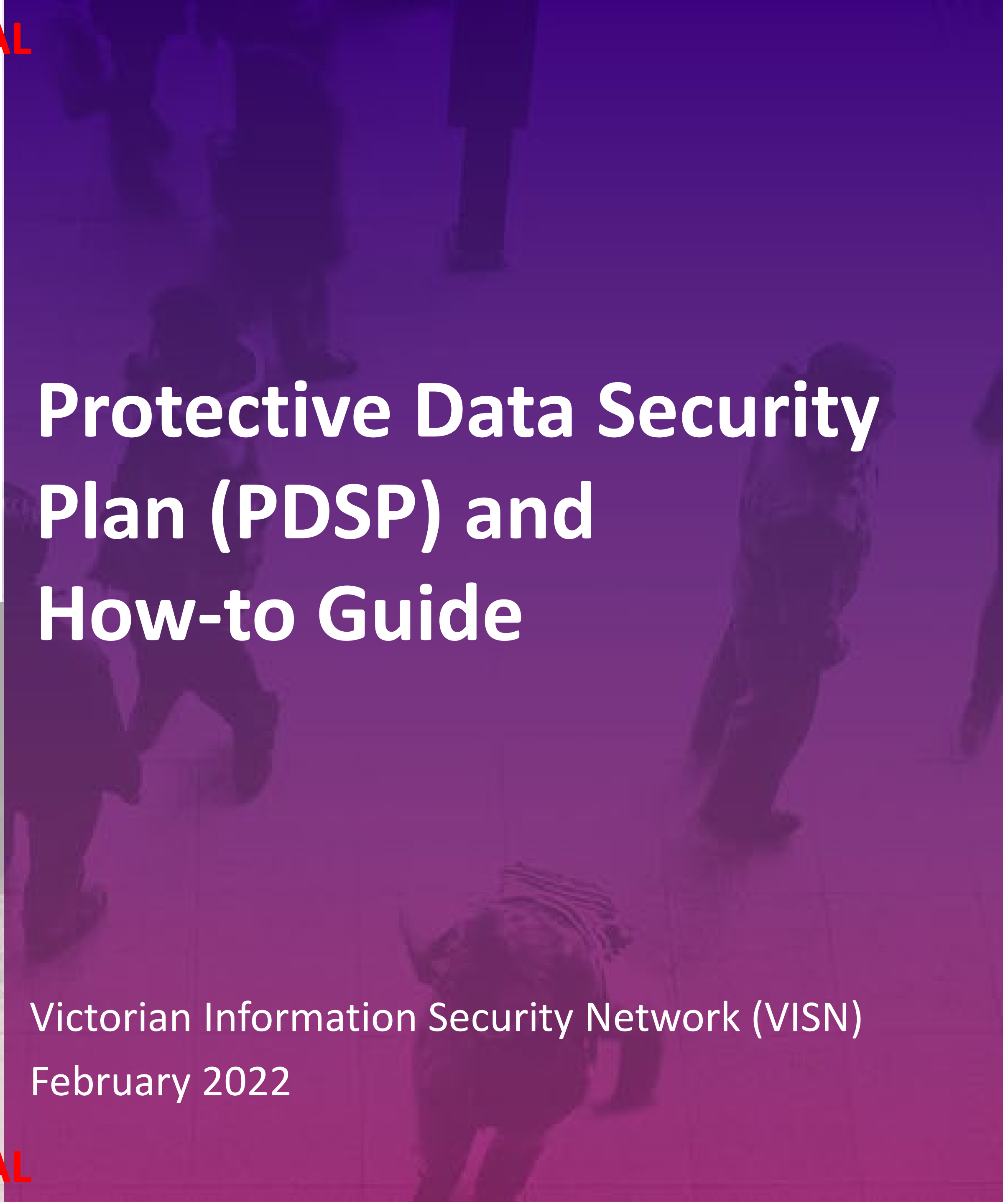
Joining as a participant?

FebVISN

Join the Q&A using #FebVISN or using the chat feature in MS Teams.

OVIC

Office of the Victorian Information Commissioner



Protective Data Security Plan (PDSP) and How-to Guide

Victorian Information Security Network (VISN)

February 2022

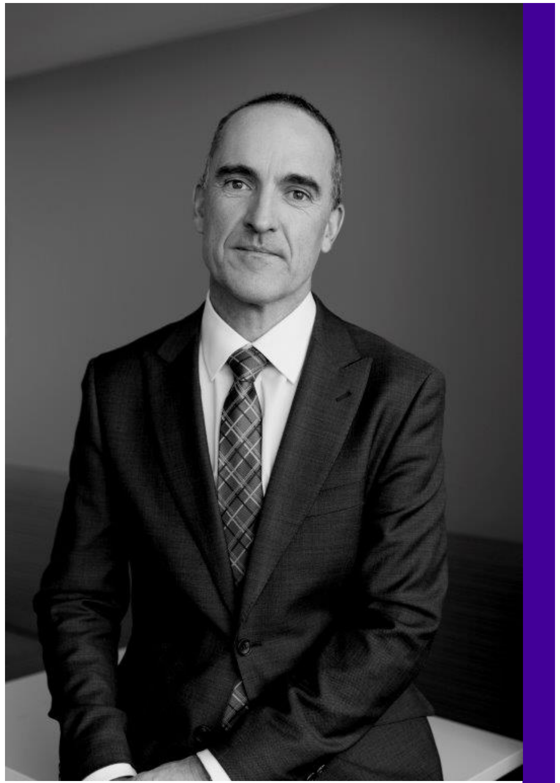
Acknowledgement

We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.

Many of you will be joining from the traditional lands of other traditional owners. We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

OVIC
Office of the Victorian
Information Commissioner

Commissioner’s Welcome



Sven Bluemmel
Information Commissioner

OFFICIAL

Standard 3 – Information Security Risk Management

An organisation utilises its risk management framework to undertake a Security Risk Profile Assessment to manage information security risks.

VPDSS Standard 3 Element Assessment

	Entity Risk	Supporting	Proposed
E3.010			
E3.020			
E3.030			
E3.040			
E3.050			

Freedom of Info

OFFICIAL

Standard 2 – Information Security Value

An organisation identifies and assesses the security value of public sector information.

VPDSS Standard 2 Element Assessment

	Entity Risk	Supporting	Proposed
E2.0			
E2.0			
E2.0			
E2.0			
E2.0			
E2.0			
E2.0			
E2.0			
E2.0			

Freedom o

OFFICIAL

Standard 1 – Information Security Management Framework

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

VPDSS Standard 1 Element Assessment

	VPDSS Standard
E1.010	The organisation documents a contextualised infor (e.g., strategy, policies, procedures) covering all sec
E1.020	The organisation’s information security manageme all legislative and regulatory drivers.
E1.030	The organisation’s information security manageme management framework.
E1.040	Executive management defines information securit competencies and authorities.
E1.050	Executive management nominates an information : changes to this point of contact.
E1.060	Executive management owns, endorses and sponsc information security program(s) including the imple
E1.070	The organisation identifies information security pe information security obligations against these.
E1.080	Executive management commits to providing suffic organisation’s ongoing information security progra
E1.090	The organisation sufficiently communicates its info framework and ensures it is accessible.

Freedom of Information | Privacy | Data Protection

OFFICIAL

OVIC
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 3.1

This form is intended to be completed electronically.
Different softwares may preview form fields differently.

The 2022 PDSP form was developed using Acrobat 2020 (20.004.30020).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

SUBMISSION, NEXT STEPS, AND USEFUL LINKS

PART C OF THE PDSP FORM

PART B OF THE PDSP FORM

PART A OF THE PDSP FORM

FREQUENTLY ASKED QUESTIONS

OVIC
Office of the Victorian
Information Commissioner

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

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

Commissioner’s Welcome

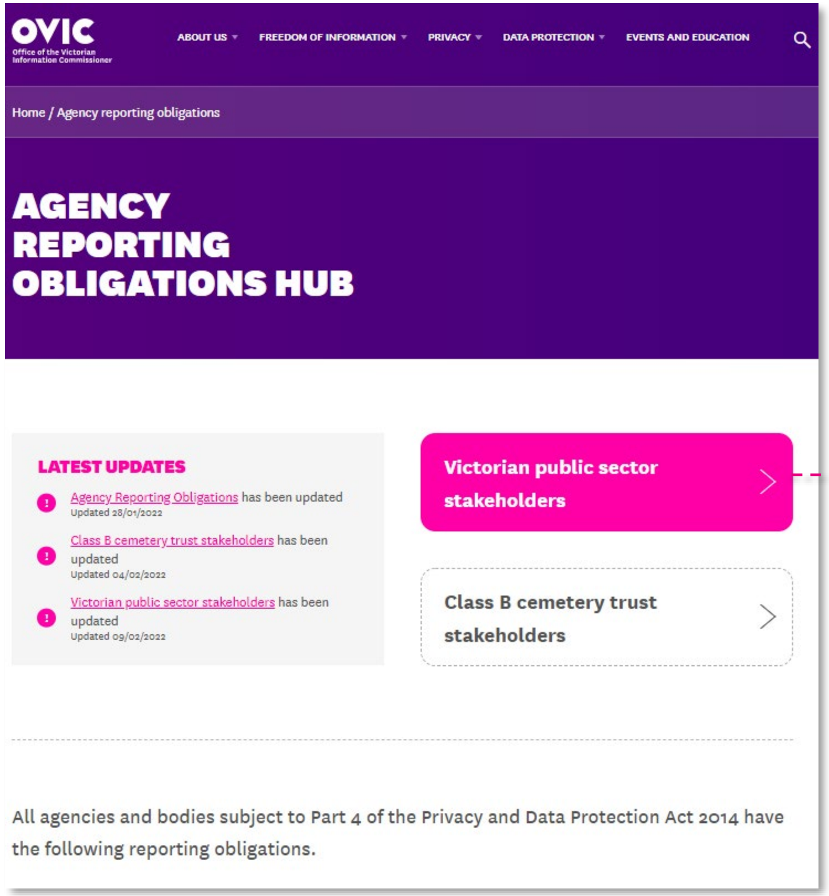
VICTORIAN PUBLIC SECTOR STAKEHOLDERS
OVIC
Office of the Victorian Information Commissioner
Sven Bluemmel
INFORMATION COMMISSIONER
01:40
vimeo

Following positive feedback from stakeholders in 2020 and 2021, we understood the importance of engaging executives and highlighting the upcoming reporting deadline.

This video seeks to clarify public sector body Head’s accountability for the PDSP submission and ensure appropriate attention is given to resourcing in support of information security efforts across the organisation.

Access the video by visiting the OVIC website: https://ovic.vic.gov.au/agency-reporting-obligations-hub/vps-stakeholders/

Commissioner’s Welcome



Home / Agency reporting obligations

AGENCY REPORTING OBLIGATIONS HUB

LATEST UPDATES

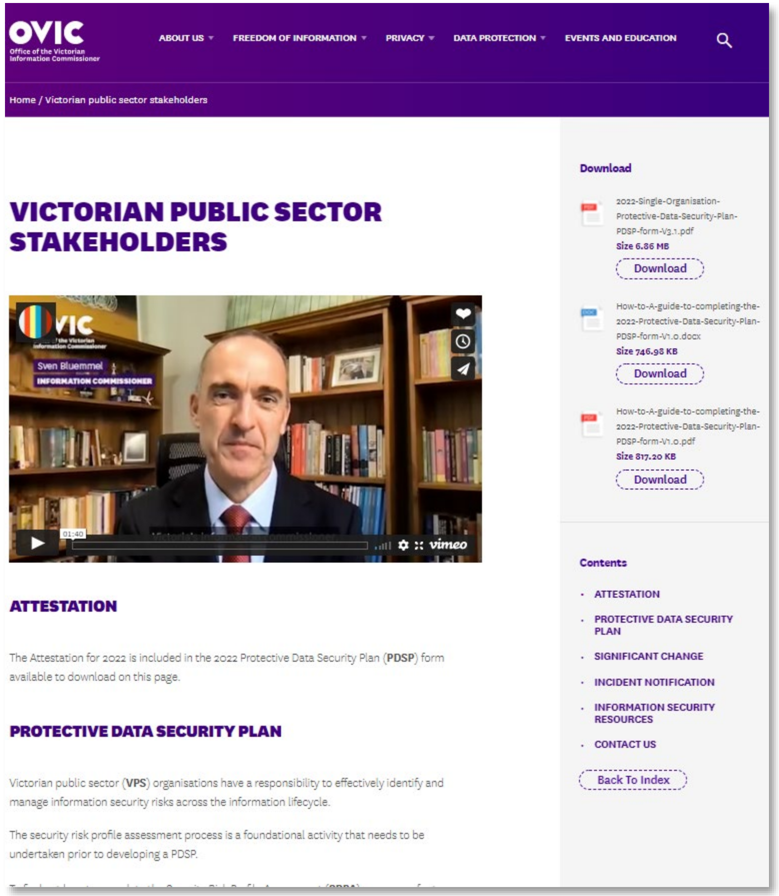
- Agency Reporting Obligations has been updated
  Updated 28/01/2022
- Class B cemetery trust stakeholders has been updated
  Updated 04/02/2022
- Victorian public sector stakeholders has been updated
  Updated 09/02/2022

Victorian public sector stakeholders

Class B cemetery trust stakeholders

All agencies and bodies subject to Part 4 of the Privacy and Data Protection Act 2014 have the following reporting obligations.

We’ve refreshed our website to include an **Agency Reporting Obligations Hub**.



Home / Victorian public sector stakeholders

VICTORIAN PUBLIC SECTOR STAKEHOLDERS

ATTESTATION

The Attestation for 2022 is included in the 2022 Protective Data Security Plan (**PDSP**) form available to download on this page.

PROTECTIVE DATA SECURITY PLAN

Victorian public sector (**VPS**) organisations have a responsibility to effectively identify and manage information security risks across the information lifecycle.

The security risk profile assessment process is a foundational activity that needs to be undertaken prior to developing a PDSP.

Download

2022-Single-Organisation-Protective-Data-Security-Plan-PDSP-form-V3.1.pdf
Size 6.86 MB
Download

How-to-A-guide-to-completing-the-2022-Protective-Data-Security-Plan-PDSP-form-V1.0.docx
Size 746.98 KB
Download

How-to-A-guide-to-completing-the-2022-Protective-Data-Security-Plan-PDSP-form-V1.0.pdf
Size 817.20 KB
Download

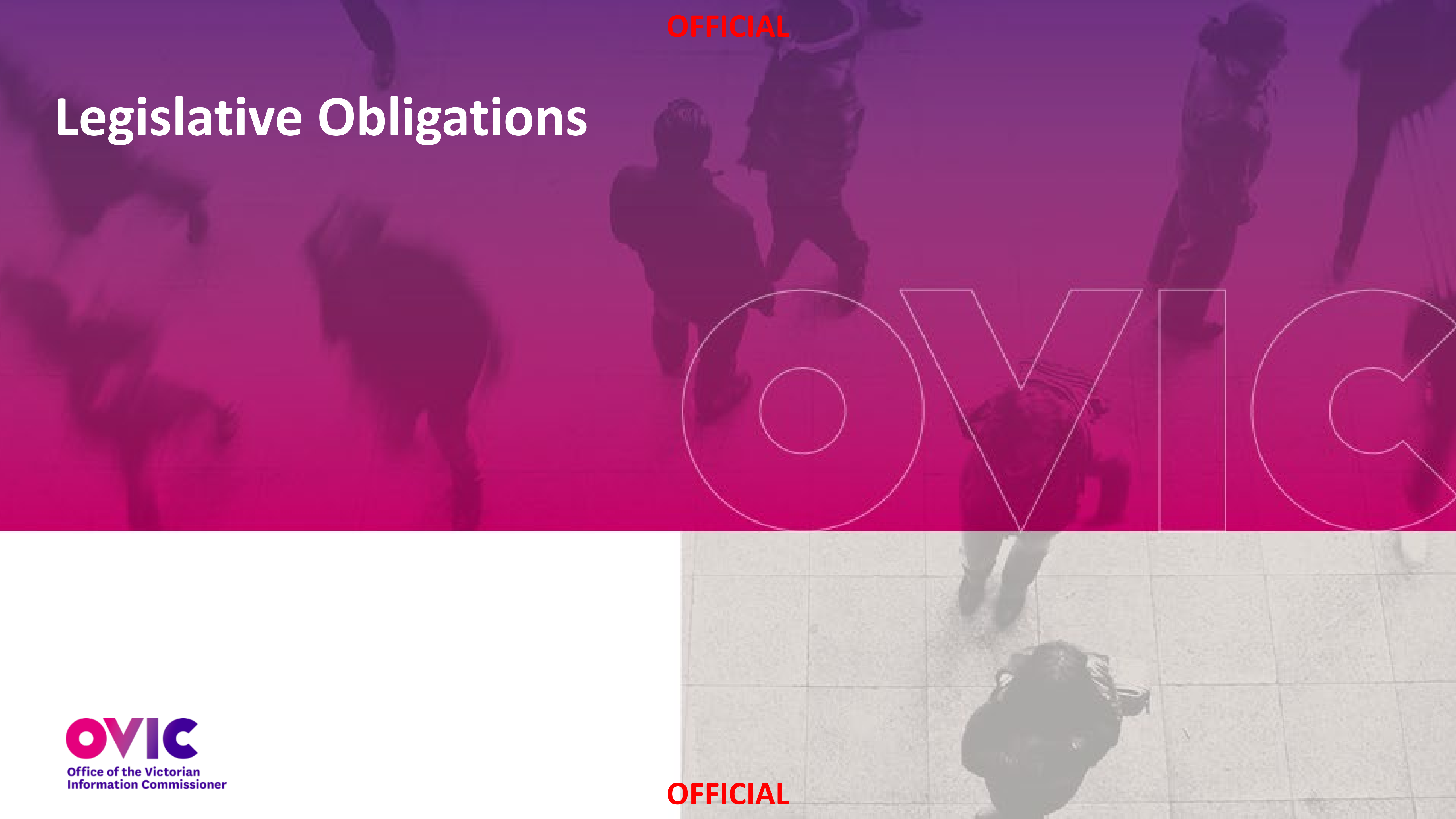
Contents

- ATTESTATION
- PROTECTIVE DATA SECURITY PLAN
- SIGNIFICANT CHANGE
- INCIDENT NOTIFICATION
- INFORMATION SECURITY RESOURCES
- CONTACT US

Back To Index

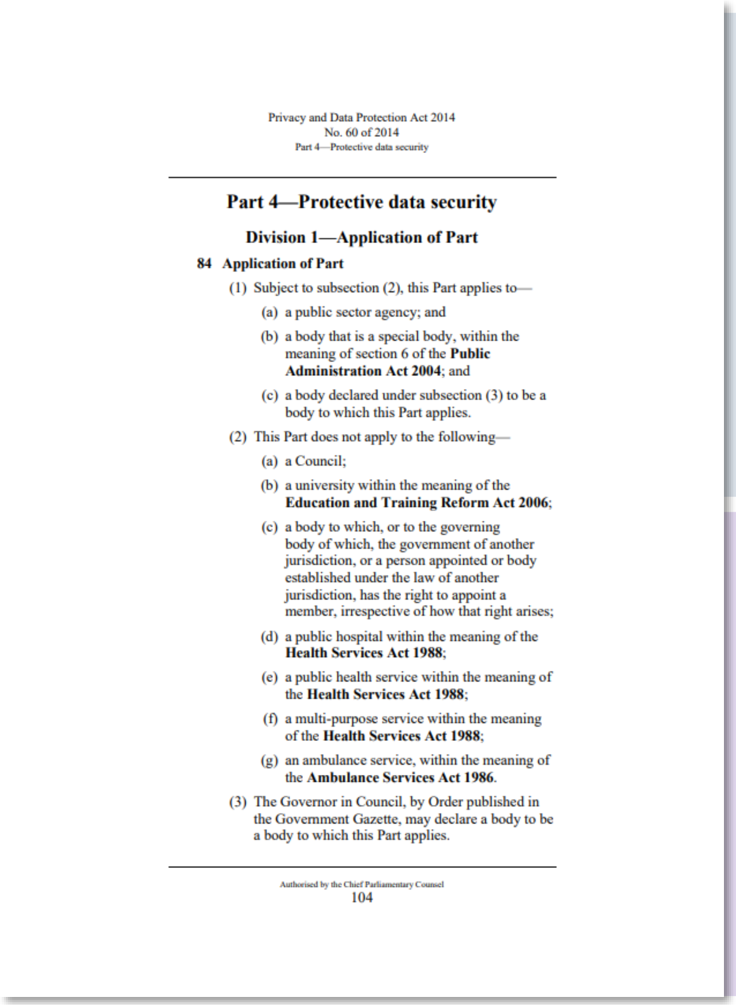
Here VPS stakeholders will find everything they need for this year’s reporting cycle.

Legislative Obligations



Office of the Victorian Information Commissioner

Part 4 of the PDP Act



Privacy and Data Protection Act 2014
No. 60 of 2014
Part 4—Protective data security

Part 4—Protective data security

Division 1—Application of Part

84 Application of Part

(1) Subject to subsection (2), this Part applies to—

(a) a public sector agency; and

(b) a body that is a special body, within the meaning of section 6 of the **Public Administration Act 2004**; and

(c) a body declared under subsection (3) to be a body to which this Part applies.

(2) This Part does not apply to the following—

(a) a Council;

(b) a university within the meaning of the **Education and Training Reform Act 2006**;

(c) a body to which, or to the governing body of which, the government of another jurisdiction, or a person appointed or body established under the law of another jurisdiction, has the right to appoint a member, irrespective of how that right arises;

(d) a public hospital within the meaning of the **Health Services Act 1988**;

(e) a public health service within the meaning of the **Health Services Act 1988**;

(f) a multi-purpose service within the meaning of the **Health Services Act 1988**;

(g) an ambulance service, within the meaning of the **Ambulance Services Act 1986**.

(3) The Governor in Council, by Order published in the Government Gazette, may declare a body to be a body to which this Part applies.

Authorised by the Chief Parliamentary Counsel
104

Security Risk Profile Assessment (SRPA)

Section 89(1)(a) The public sector body Head must ensure that a security risk profile assessment is undertaken for the agency or body

Section 89(2) A security risk profile assessment of an agency or body **must include an assessment of any contracted service provider** of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.

Protective Data Security Plan (PDSP)

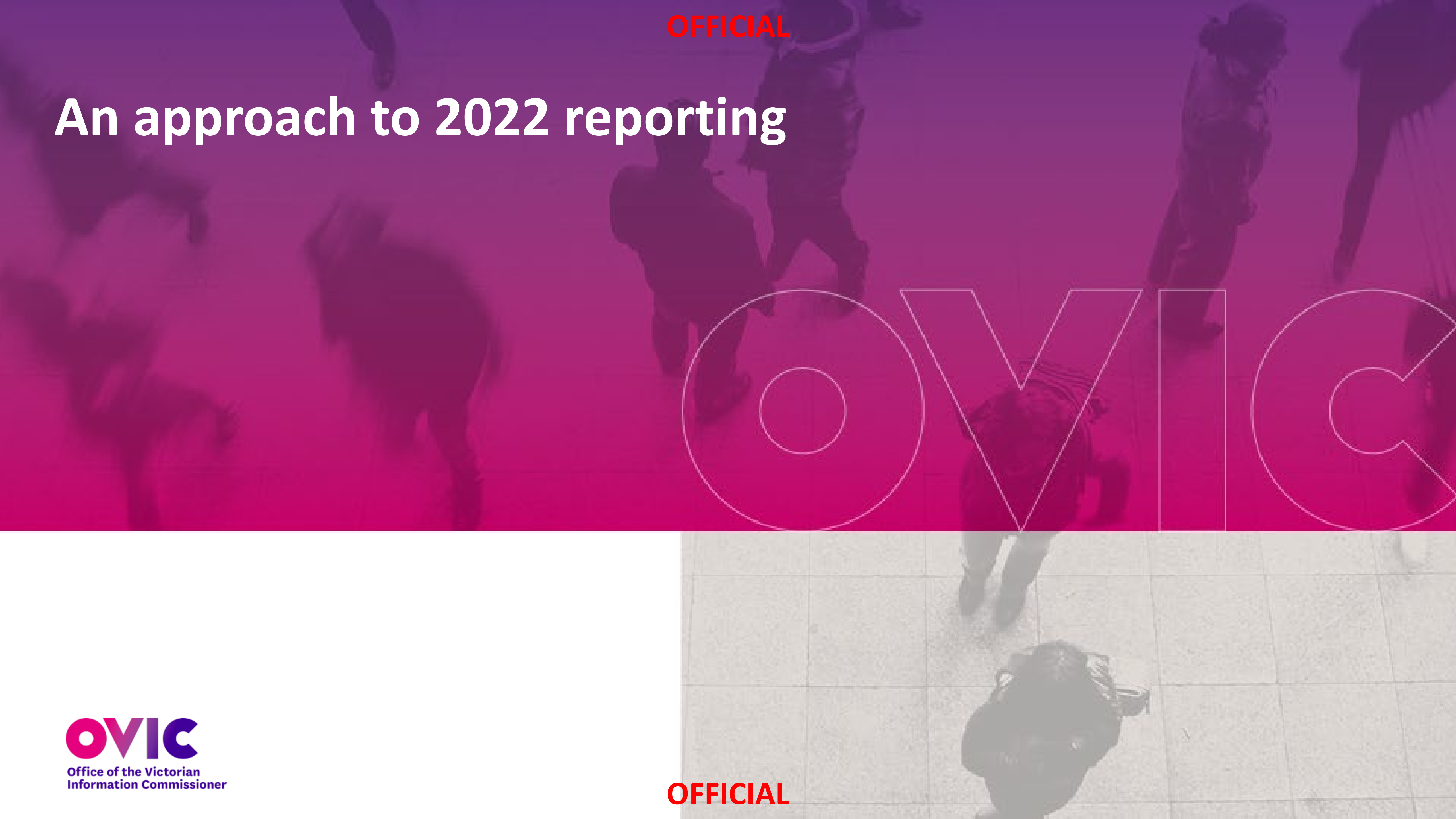
Section 89(4) A public sector body Head must ensure that the protective data security plan prepared under this section is reviewed--

(a) if there is a **significant change** in the operating environment or the security risks relevant to the agency or body; or

(b) otherwise, **every 2 years**.

Section 89(5) A public sector body Head for the agency or body must ensure that a copy of the protective data security plan is given to the Information Commissioner.

An approach to 2022 reporting



Office of the Victorian
Information Commissioner

Single Organisation Sample Approach

ENGAGE

1 Engage your executive and assemble your team*

2 Review your previous PDSP and internal security program

UNDERTAKE

3 Undertake an updated **SRPA** ensuring you capture risks associated with **CSPs** and **third-parties**

4 Review and/or update your risk register

5 Download the 2022 PDSP form and How-to Guide

DEVELOP

6 Develop your 2022 PDSP in consultation with relevant stakeholders

7 Validate your PDSP responses (internally or externally)

8 Brief your executive and seek sign off on the finalised PDSP

SUBMIT

9 Submit PDSP to OVIC by **31 August 2022** --------> OVIC Office of the Victorian Information Commissioner

*we acknowledge that some organisations may not have a team to leverage off.

Engage

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

When engaging executive teams, organisations need to consider what approach will work best for their business.

1 **NOMINATE AN EXECUTIVE SPONSOR**
An important first step includes the nomination of an Executive Sponsor who will champion the significance of information security throughout the business.

2 **ESTABLISH A WORKING GROUP TO COORDINATE EFFORTS**
A working group may help coordinate efforts in implementing the VPDSS and should include representation from all areas of the business.

3 **CONFIRM YOUR ORGANISATION'S INFORMATION SECURITY LEAD**
Your information security lead acts as a central point of contact for OVIC, helping deliver important information security messages and updates relating to the Framework and Standards.

Review PDSP and Internal Security Program

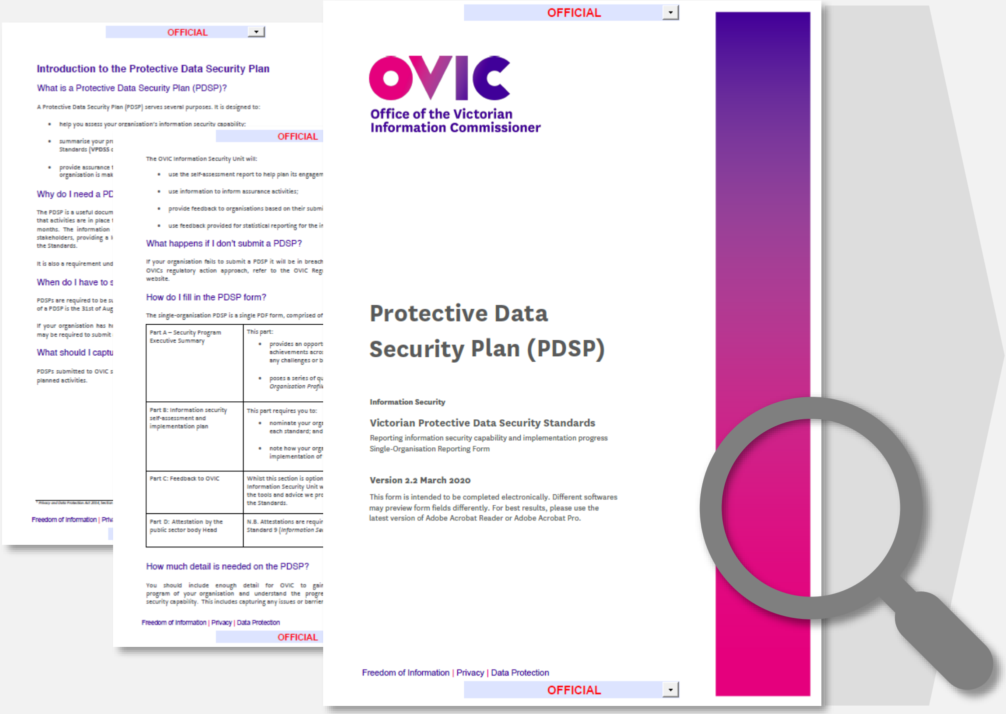
ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

Review your previous PDSP and internal security program


OFFICIAL

Introduction to the Protective Data Security Plan

What is a Protective Data Security Plan (PDSP)?

A Protective Data Security Plan (PDSP) serves several purposes. It is designed to:

- help you assess your organisation's information security capability;
- summarise your pr Standards (VPDSS c
- provide assurance t organisation is mak

Why do I need a PD

The PDSP is a useful docum that activities are in place t months. The information stakeholders, providing a l the Standards.

It is also a requirement und

When do I have to s

PDSPs are required to be su of a PDSP is the 31st of Aug

If your organisation has h may be required to submit

What should I captu

PDSPs submitted to OVIC s planned activities.

Freedom of Information | Priv

OFFICIAL

The OVIC Information Security Unit will:

- use the self-assessment report to help plan its engagem
- use information to inform assurance activities;
- provide feedback to organisations based on their submi
- use feedback provided for statistical reporting for the in

What happens if I don't submit a PDSP?

If your organisation fails to submit a PDSP it will be in breach OVICs regulatory action approach, refer to the OVIC Reg website.

How do I fill in the PDSP form?

The single-organisation PDSP is a single PDF form, comprised of

Part A – Security Program Executive Summary	This part: • provides an opport achievements acros any challenges or b • poses a series of qu *Organisation Profil*
Part B: Information security self-assessment and implementation plan	This part requires you to: • nominate your org each standard; and • note how your orga implementation of
Part C: Feedback to OVIC	Whilst this section is option Information Security Unit w the tools and advice we pro the Standards.
Part D: Attestation by the public sector body Head	N.B. Attestations are requir Standard 9 (*Information Se*

How much detail is needed on the PDSP?

You should include enough detail for OVIC to gain program of your organisation and understand the progre security capability. This includes capturing any issues or barrier

Freedom of Information | Privacy | Data Protection

OFFICIAL

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 2.2 March 2020

This form is intended to be completed electronically. Different softwares may preview form fields differently. For best results, please use the latest version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Not met
On track
Complete

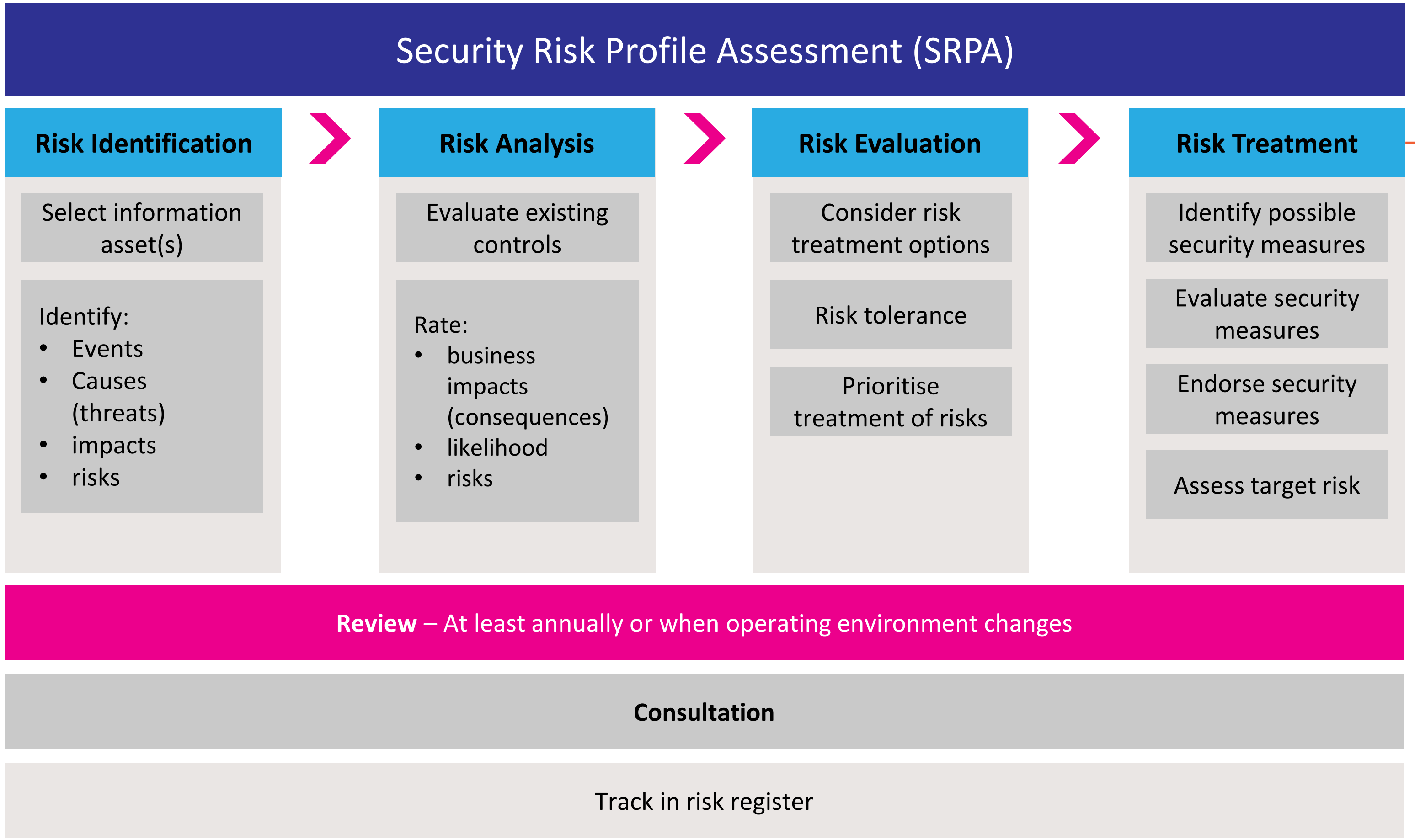
Undertake a SRPA

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT



Security Risk Profile Assessment (SRPA)

Risk Identification

Select information asset(s)

Identify:
- Events
- Causes (threats)
- impacts
- risks

Risk Analysis

Evaluate existing controls

Rate:
- business impacts (consequences)
- likelihood
- risks

Risk Evaluation

Consider risk treatment options

Risk tolerance

Prioritise treatment of risks

Risk Treatment

Identify possible security measures

Evaluate security measures

Endorse security measures

Assess target risk

Review – At least annually or when operating environment changes

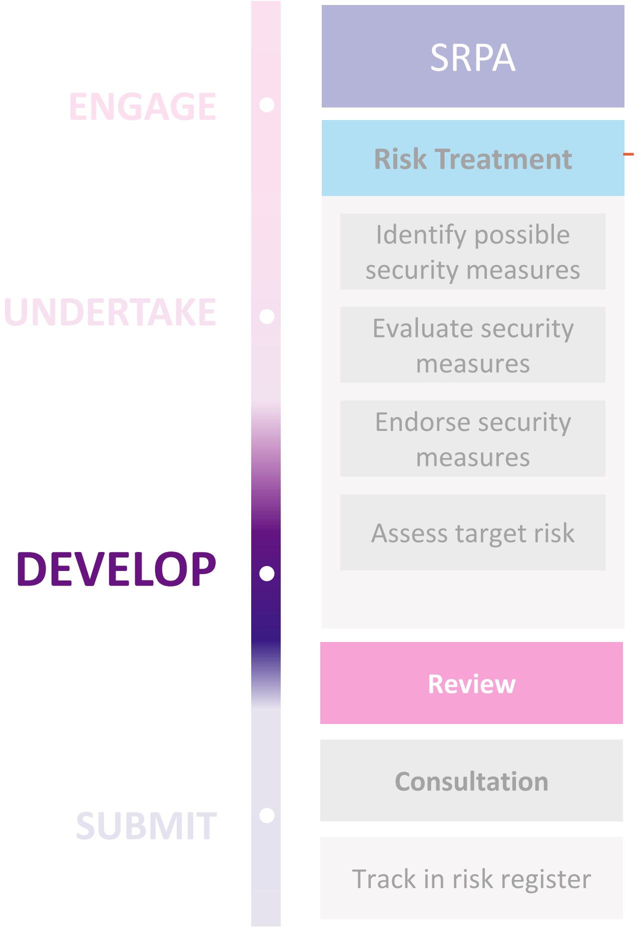
Consultation

Track in risk register

FOR YOUR PDSP, KEEP NOTE OF:

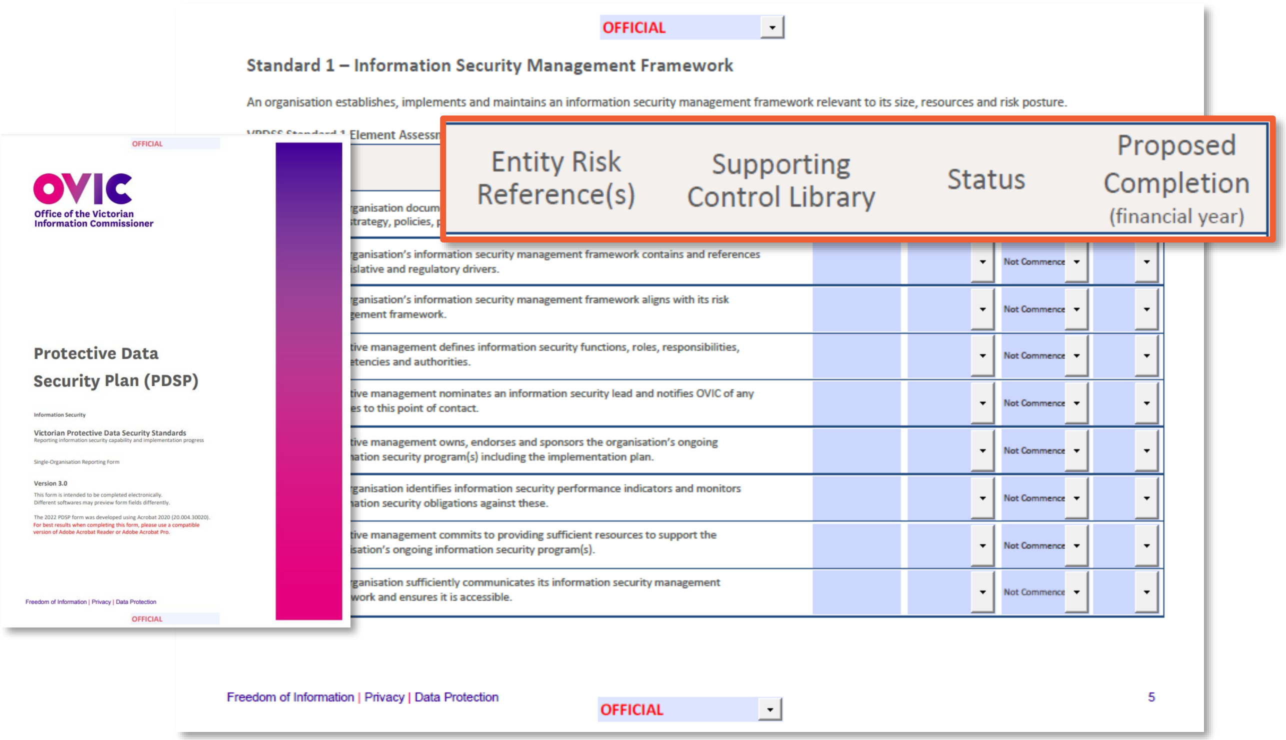
- relevant **risk reference** for your agency/entity
- the **supporting control library** from which the security measure was selected
- **implementation status** of various security measures
- **proposed completion date** for implementation of these security measures

Develop – Approach 1: SRPA informing PDSP



FOR YOUR PDSP, KEEP NOTE OF:

- relevant **risk reference** for your agency/entity
- the **supporting control library** from which the security measure was selected
- **implementation status** of various security measures
- **proposed completion date** for implementation of these security measures



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 3.0

This form is intended to be completed electronically.
Different softwares may preview form fields differently.

The 2022 PDSP form was developed using Acrobat 2020 (20.004.30020).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

OFFICIAL

Standard 1 – Information Security Management Framework

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

VPDSS Standard 1 Element Assessm

	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
ganisation docum strategy, policies, p				
ganisation's information security management framework contains and references islative and regulatory drivers.			Not Commence	
ganisation's information security management framework aligns with its risk gement framework.			Not Commence	
tive management defines information security functions, roles, responsibilities, etencies and authorities.			Not Commence	
tive management nominates an information security lead and notifies OVIC of any es to this point of contact.			Not Commence	
tive management owns, endorses and sponsors the organisation's ongoing nation security program(s) including the implementation plan.			Not Commence	
ganisation identifies information security performance indicators and monitors nation security obligations against these.			Not Commence	
tive management commits to providing sufficient resources to support the isation's ongoing information security program(s).			Not Commence	
ganisation sufficiently communicates its information security management work and ensures it is accessible.			Not Commence	

Freedom of Information | Privacy | Data Protection

OFFICIAL

5

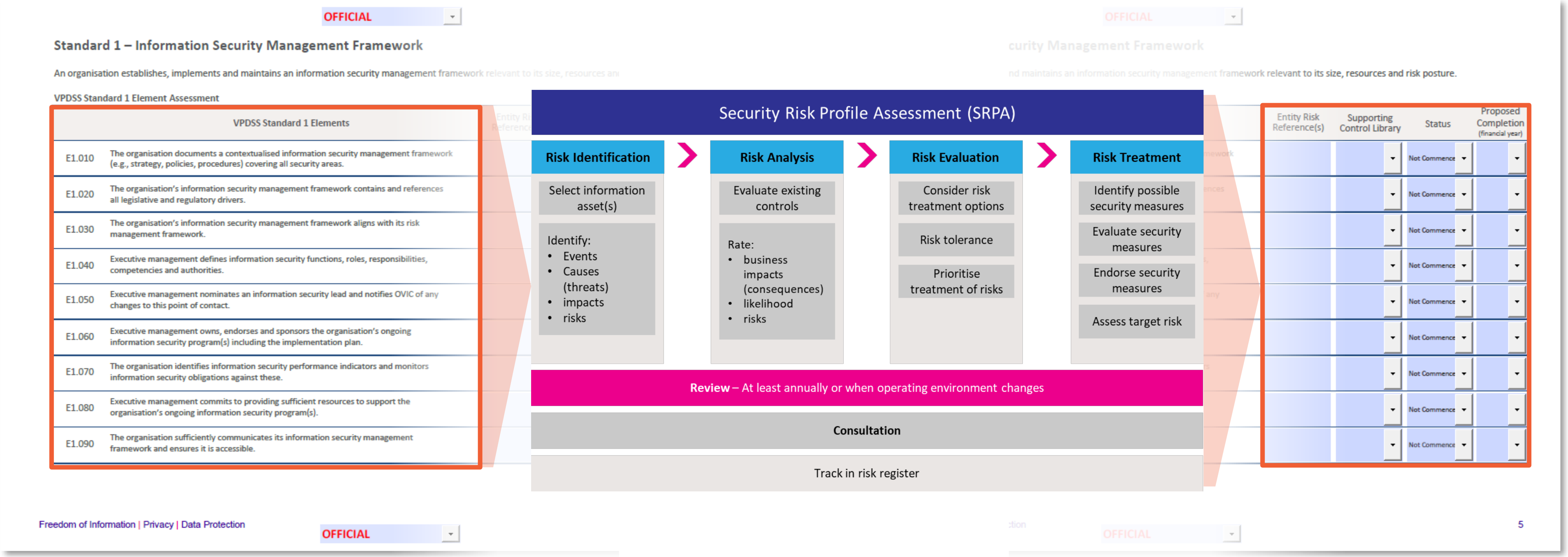
Develop - Approach 2: PDSP informing SRPA

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT



OFFICIAL

Standard 1 – Information Security Management Framework

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

VPDSS Standard 1 Element Assessment

VPDSS Standard 1 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.			Not Commence	
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.			Not Commence	
E1.030	The organisation's information security management framework aligns with its risk management framework.			Not Commence	
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.			Not Commence	
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.			Not Commence	
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.			Not Commence	
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.			Not Commence	
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).			Not Commence	
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.			Not Commence	

Security Risk Profile Assessment (SRPA)

Risk Identification
- Select information asset(s)
- Identify:
  - Events
  - Causes (threats)
  - impacts
  - risks

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

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

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

Review – At least annually or when operating environment changes

Consultation

Track in risk register

Freedom of Information | Privacy | Data Protection

OFFICIAL

5

Consider each element and its applicability to your environment

Review your risk register to identify applicable risks and identify gaps, anomalies and discrepancies

Record SRPA outcomes in PDSP

The 2022 PDSP form – hot off the press!

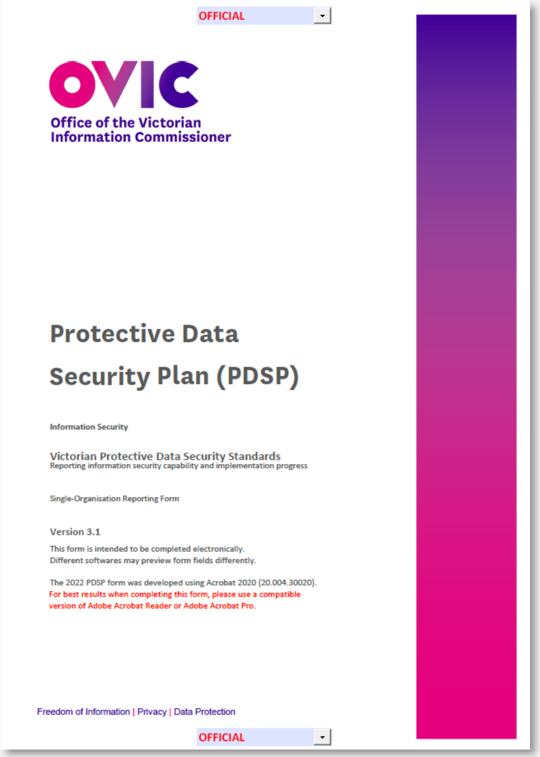
ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

VERSION 3.1



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 3.1

This form is intended to be completed electronically.
Different softwares may preview form fields differently.

The 2022 PDSP form was developed using Acrobat 2020 (20.004.30020).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Some of you may have accessed an earlier version of the form (V3.0), however as of **9 February 2022 V3.1** has been published and supersedes V3.0.

Visit our website to access the latest version:
https://ovic.vic.gov.au/agency-reporting-obligations-hub/vps-stakeholders/

The 2022 PDSP form – what's new, what's changed

ENGAGE

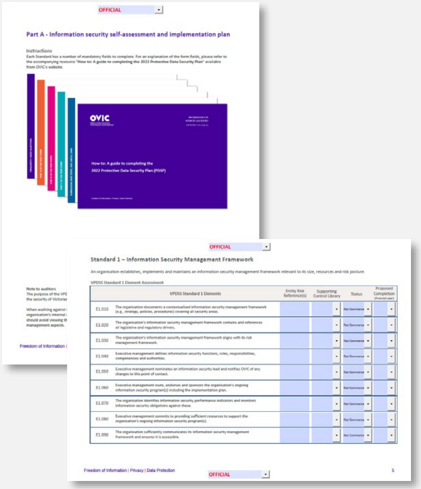
UNDERTAKE

DEVELOP

SUBMIT

OVERALL FORM STRUCTURE

PART A

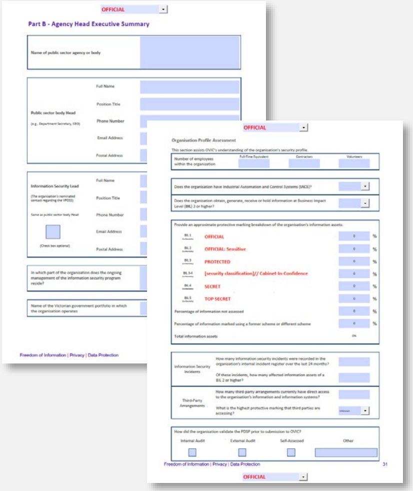


Part A - Information security self-assessment and implementation plan

Standard 1 – Information Security Management Framework

Introductory notes and all 12 Standards and associated Elements

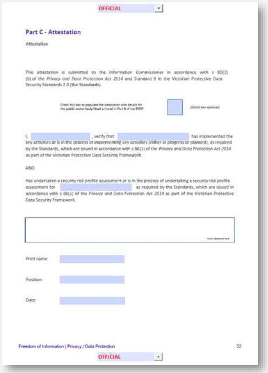
PART B



Part B - Agency Head Executive Summary

Contact details and Organisational Profile Assessment (OPA)

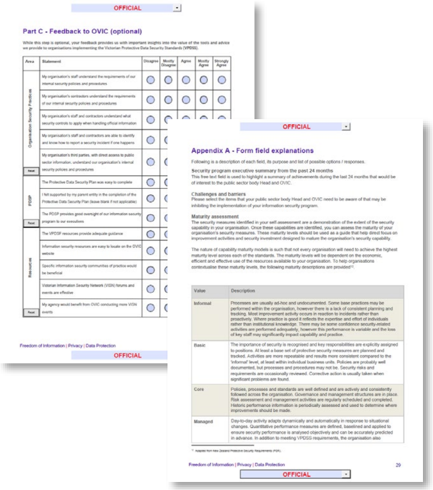
PART C



Part C - Attestation

Attestation

Removed



Part C - Feedback to OVIC (optional)

Appendix A - Form field explanations

Feedback to OVIC and Appendix

Office of the Victorian Information Commissioner

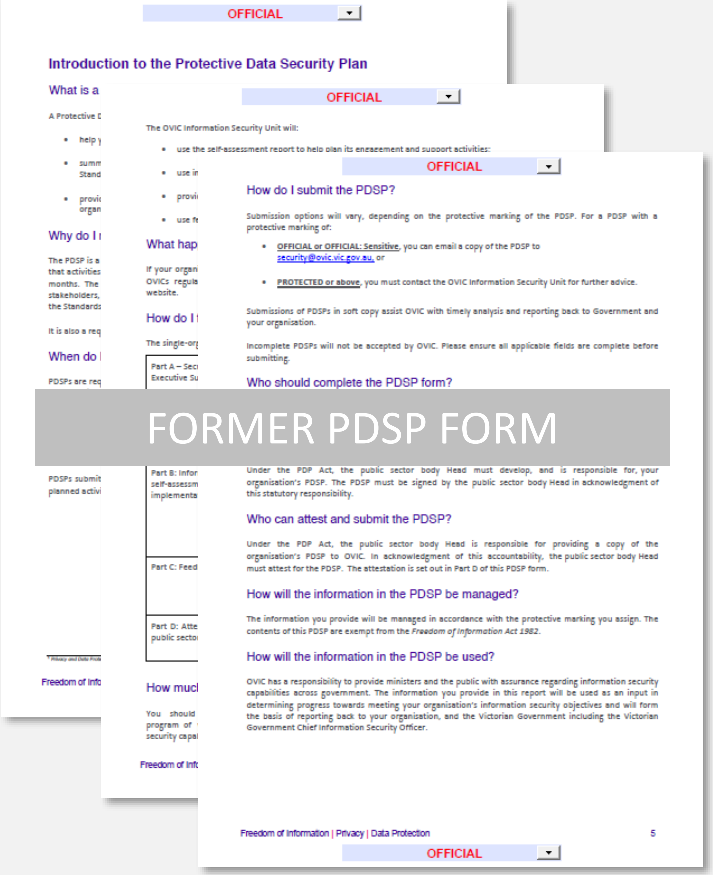
The 2022 PDSP form – what's new, what's changed

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT



OFFICIAL

Introduction to the Protective Data Security Plan

OFFICIAL

The OVIC Information Security Unit will:

- use the self-assessment report to help plan its engagement and support activities;

OFFICIAL

How do I submit the PDSP?

Submission options will vary, depending on the protective marking of the PDSP. For a PDSP with a protective marking of:

- **OFFICIAL or OFFICIAL: Sensitive**, you can email a copy of the PDSP to security@ovic.vic.gov.au, or
- **PROTECTED or above**, you must contact the OVIC Information Security Unit for further advice.

Submissions of PDSPs in soft copy assist OVIC with timely analysis and reporting back to Government and your organisation.

Incomplete PDSPs will not be accepted by OVIC. Please ensure all applicable fields are complete before submitting.

Who should complete the PDSP form?

FORMER PDSP FORM

Under the PDP Act, the public sector body Head must develop, and is responsible for, your organisation's PDSP. The PDSP must be signed by the public sector body Head in acknowledgment of this statutory responsibility.

Who can attest and submit the PDSP?

Under the PDP Act, the public sector body Head is responsible for providing a copy of the organisation's PDSP to OVIC. In acknowledgment of this accountability, the public sector body Head must attest for the PDSP. The attestation is set out in Part D of this PDSP form.

How will the information in the PDSP be managed?

The information you provide will be managed in accordance with the protective marking you assign. The contents of this PDSP are exempt from the *Freedom of Information Act 1982*.

How will the information in the PDSP be used?

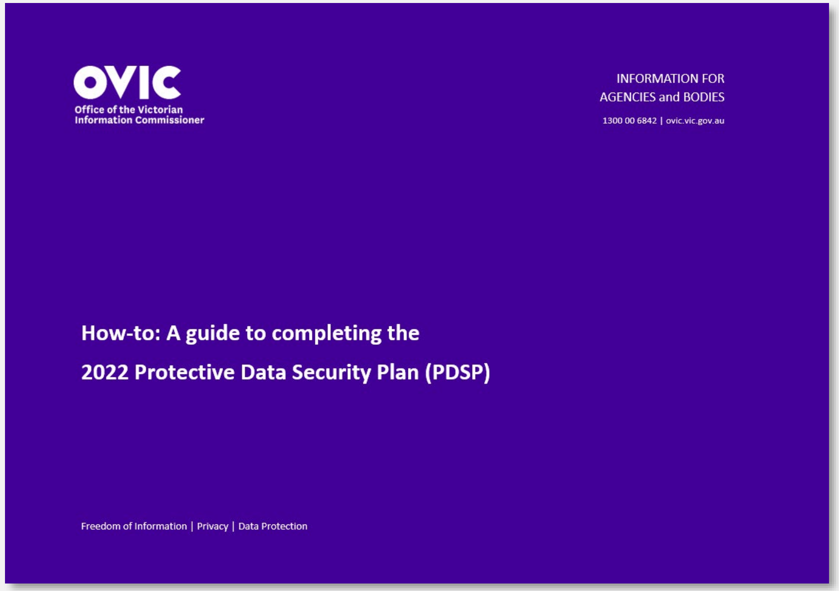
OVIC has a responsibility to provide ministers and the public with assurance regarding information security capabilities across government. The information you provide in this report will be used as an input in determining progress towards meeting your organisation's information security objectives and will form the basis of reporting back to your organisation, and the Victorian Government including the Victorian Government Chief Information Security Officer.

Freedom of Information | Privacy | Data Protection 5

OFFICIAL

Cut down explanatory and introductory notes from the 2020 PDSP form

These are now in the How-to Guide



OVIC
Office of the Victorian Information Commissioner

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

How-to: A guide to completing the 2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

The 2022 PDSP form – what's new, what's changed

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

PART A

OFFICIAL

Part A - Information security self-assessment and implementation plan

Instructions
Each Standard has a number of mandatory fields to complete. For an explanation of the form fields, please refer to the accompanying resource **"How to: A guide to completing the 2022 Protective Data Security Plan"** available from OVIC's website.

FREQUENTLY ASKED QUESTIONS
PART A OF THE PDSP FORM
PART B OF THE PDSP FORM
PART C OF THE PDSP FORM
SUBMISSION, NEXT STEPS, AND USEFUL LINKS
OVIC
Office of the Victorian Information Commissioner
INFORMATION FOR AGENCIES and BODIES
How-to: A guide to completing the 2022 Protective Data Security Plan (PDSP)
Freedom of Information | Privacy | Data Protection

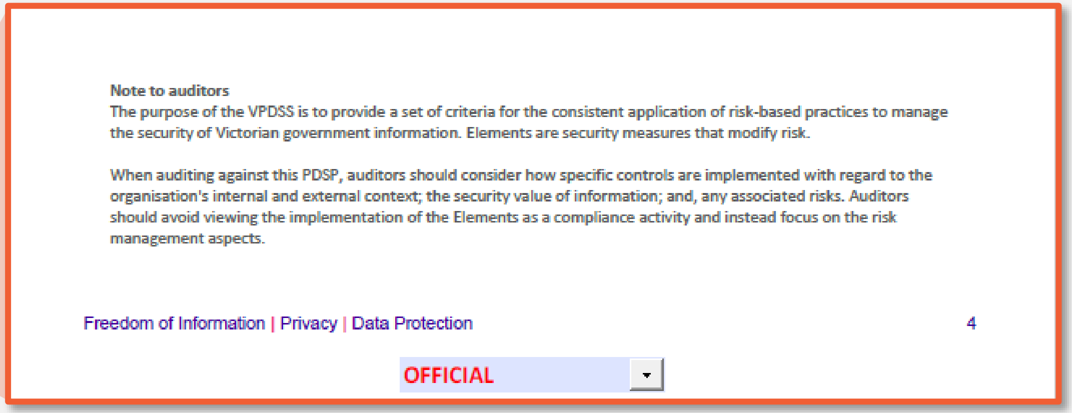
Note to auditors
The purpose of the VPDSS is to provide a set of criteria for the consistent application of risk-based practices to manage the security of Victorian government information. Elements are security measures that modify risk.

When auditing against this PDSP, auditors should consider how specific controls are implemented with regard to the organisation's internal and external context; the security value of information; and, any associated risks. Auditors should avoid viewing the implementation of the Elements as a compliance activity and instead focus on the risk management aspects.

Freedom of Information | Privacy | Data Protection 4

OFFICIAL

Added a note to auditors reiterating the risk-based nature of the Victorian Protective Data Security Standards



Note to auditors
The purpose of the VPDSS is to provide a set of criteria for the consistent application of risk-based practices to manage the security of Victorian government information. Elements are security measures that modify risk.

When auditing against this PDSP, auditors should consider how specific controls are implemented with regard to the organisation's internal and external context; the security value of information; and, any associated risks. Auditors should avoid viewing the implementation of the Elements as a compliance activity and instead focus on the risk management aspects.

Freedom of Information | Privacy | Data Protection 4

OFFICIAL

Office of the Victorian Information Commissioner

The 2022 PDSP form – what's new, what's changed

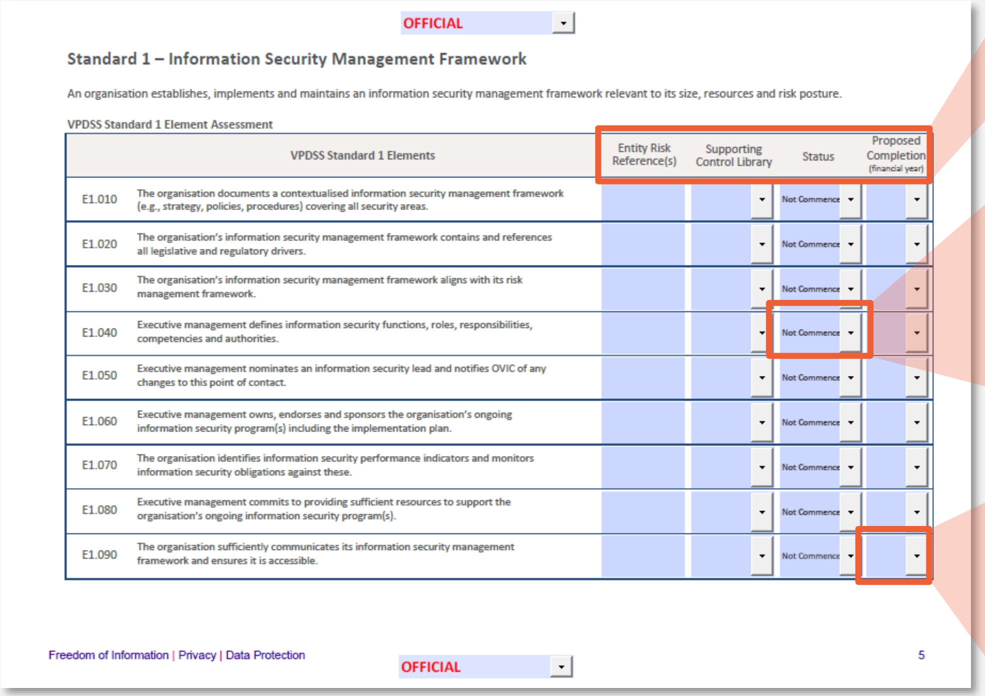
ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

PART A



OFFICIAL

Standard 1 – Information Security Management Framework

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

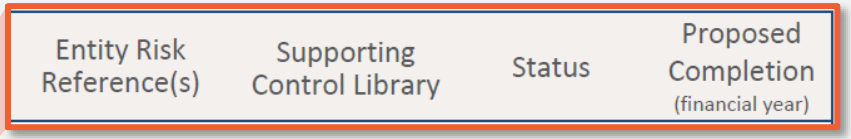
VPDSS Standard 1 Element Assessment

	VPDSS Standard 1 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.			Not Commence	
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.			Not Commence	
E1.030	The organisation's information security management framework aligns with its risk management framework.			Not Commence	
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.			Not Commence	
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.			Not Commence	
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.			Not Commence	
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.			Not Commence	
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).			Not Commence	
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.			Not Commence	

Freedom of Information | Privacy | Data Protection

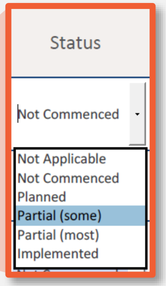
OFFICIAL

5



Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)

Column order has shifted

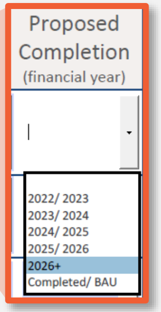


Status

Not Commenced

- Not Applicable
- Not Commenced
- Planned
- Partial (some)
- Partial (most)
- Implemented

'Partial' option allows for greater granularity with 'some' or 'most'



Proposed Completion (financial year)

- 2022/ 2023
- 2023/ 2024
- 2024/ 2025
- 2025/ 2026
- 2026+
- Completed/ BAU

Completion dates updated

Office of the Victorian Information Commissioner

The 2022 PDSP form – what's new, what's changed

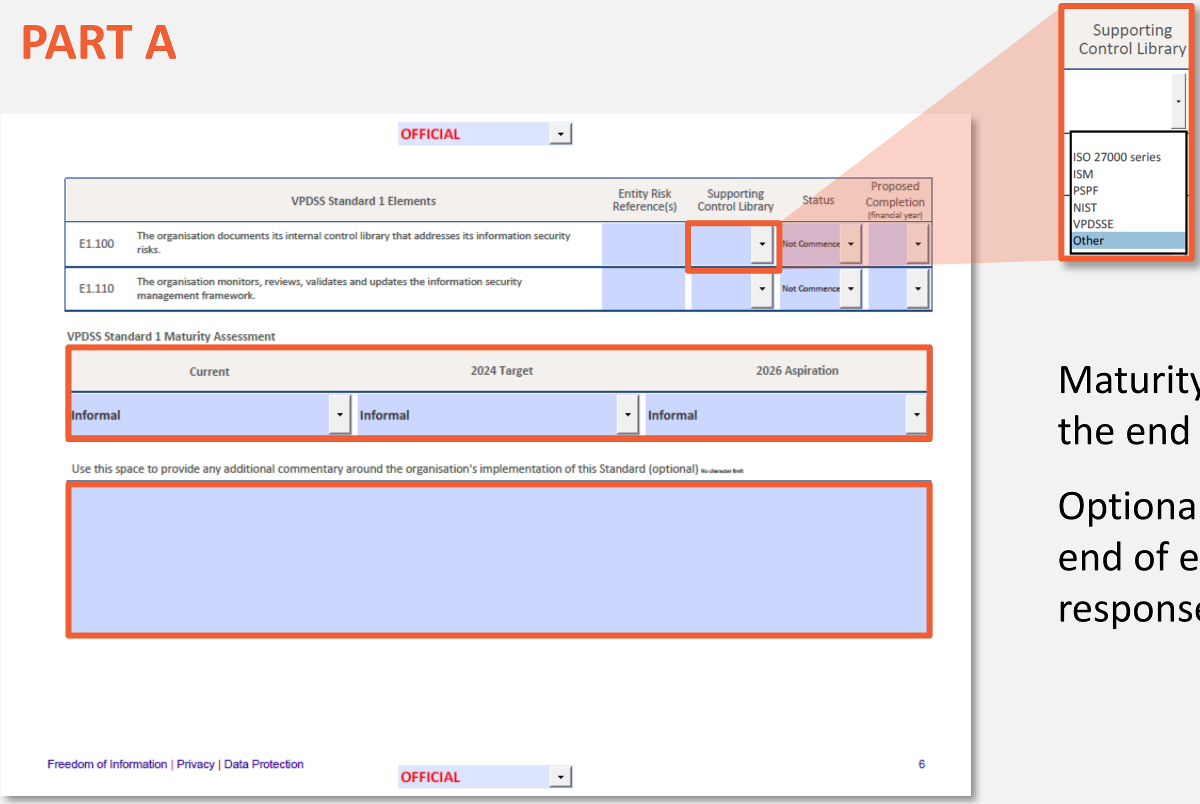
ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

PART A



OFFICIAL

VPDSS Standard 1 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E1.100	The organisation documents its internal control library that addresses its information security risks.			Not Commence	
E1.110	The organisation monitors, reviews, validates and updates the information security management framework.			Not Commence	

VPDSS Standard 1 Maturity Assessment

Current	2024 Target	2026 Aspiration
Informal	Informal	Informal

Use this space to provide any additional commentary around the organisation's implementation of this Standard (optional) No character limit

Freedom of Information | Privacy | Data Protection

OFFICIAL

6

Supporting Control Library

- ISO 27000 series
- ISM
- PSPF
- NIST
- VPDSSE
- Other

Added 'Other' option for supporting control libraries

Maturity assessment moved towards the end of the Standard

Optional free text field provided at the end of each Standard to contextualise responses

The 2022 PDSP form – what’s new, what’s changed

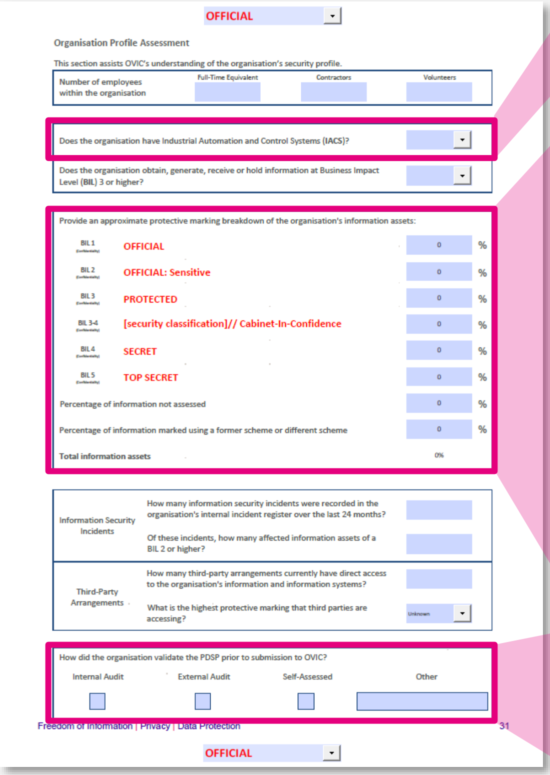
ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

PART B – Organisational Profile Assessment



OFFICIAL

Organisation Profile Assessment

This section assists OVIC’s understanding of the organisation’s security profile.

	Full-Time Equivalent	Contractors	Volunteers
Number of employees within the organisation			

Does the organisation have Industrial Automation and Control Systems (IACS)?

Does the organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3 or higher?

Provide an approximate protective marking breakdown of the organisation's information assets:

BIL 1 (Confidentiality)	OFFICIAL	0	%
BIL 2 (Confidentiality)	OFFICIAL: Sensitive	0	%
BIL 3 (Confidentiality)	PROTECTED	0	%
BIL 3-4 (Confidentiality)	[security classification]// Cabinet-In-Confidence	0	%
BIL 4 (Confidentiality)	SECRET	0	%
BIL 5 (Confidentiality)	TOP SECRET	0	%
Percentage of information not assessed		0	%
Percentage of information marked using a former scheme or different scheme		0	%
Total information assets		0%	

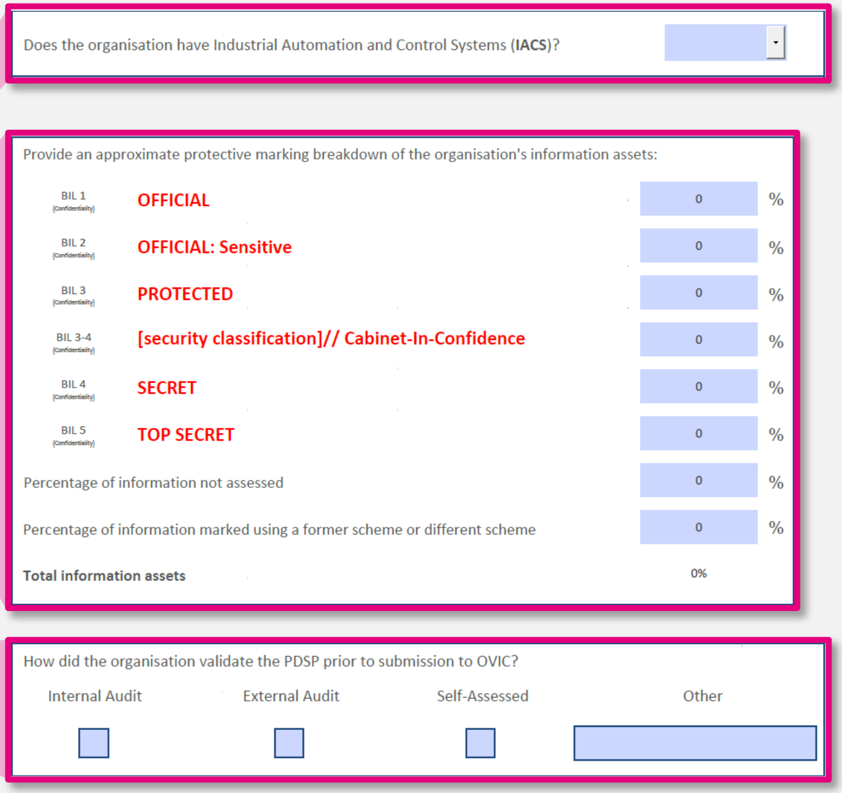
Information Security Incidents	How many information security incidents were recorded in the organisation's internal incident register over the last 24 months?	
	Of these incidents, how many affected information assets of a BIL 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and information systems?	
	What is the highest protective marking that third parties are accessing?	Unknown

How did the organisation validate the PDSP prior to submission to OVIC?

Internal Audit	External Audit	Self-Assessed	Other
□	□	□	

Freedom of Information | Privacy | Data Protection 31

OFFICIAL



Does the organisation have Industrial Automation and Control Systems (IACS)?

Provide an approximate protective marking breakdown of the organisation's information assets:

BIL 1 (Confidentiality)	OFFICIAL	0	%
BIL 2 (Confidentiality)	OFFICIAL: Sensitive	0	%
BIL 3 (Confidentiality)	PROTECTED	0	%
BIL 3-4 (Confidentiality)	[security classification]// Cabinet-In-Confidence	0	%
BIL 4 (Confidentiality)	SECRET	0	%
BIL 5 (Confidentiality)	TOP SECRET	0	%
Percentage of information not assessed		0	%
Percentage of information marked using a former scheme or different scheme		0	%
Total information assets		0%	

How did the organisation validate the PDSP prior to submission to OVIC?

Internal Audit	External Audit	Self-Assessed	Other
□	□	□	

Reframed Critical Infrastructure question (now IACS)

Reference to former protective marking scheme removed

Added field for indicating how the PDSP was validated

The 2022 PDSP form – what's new, what's changed

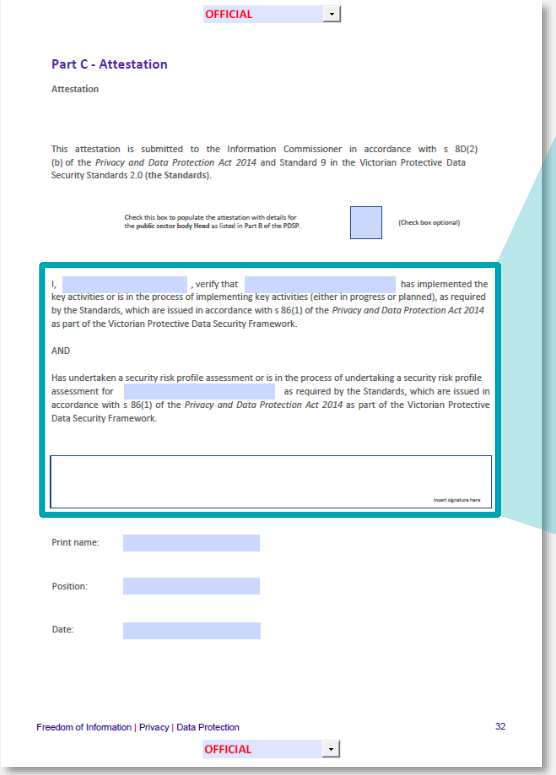
ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

PART C – Attestation



OFFICIAL

Part C - 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).

Check this box to populate the attestation with details for the **public sector body Head** as listed in Part B of the PDSP. □ (Check box optional)

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.

AND

Has undertaken a security risk profile assessment or is in the process of undertaking a security risk profile assessment for 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.

Insert signature here

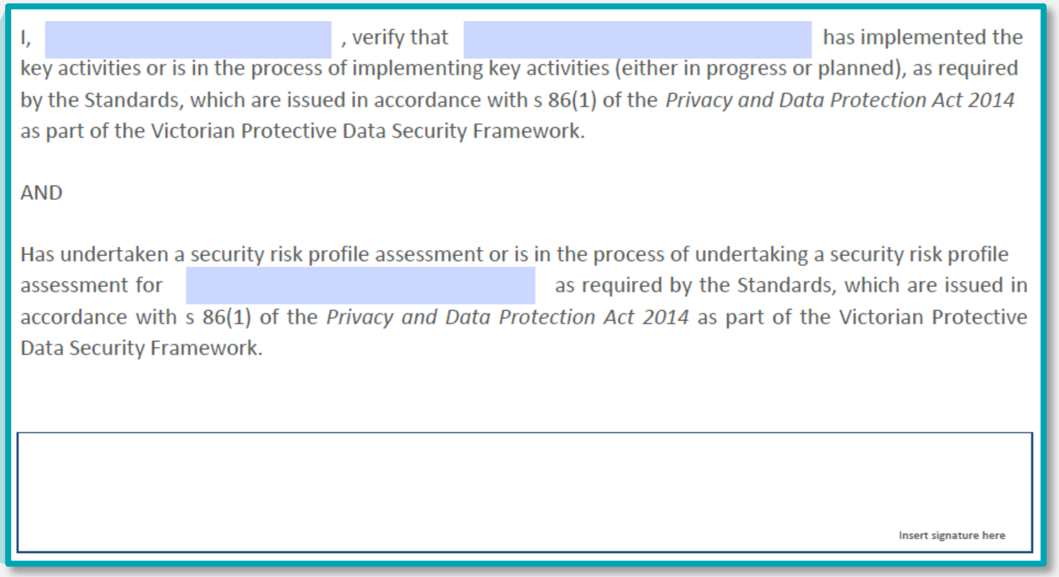
Print name:

Position:

Date:

Freedom of Information | Privacy | Data Protection 32

OFFICIAL



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.

AND

Has undertaken a security risk profile assessment or is in the process of undertaking a security risk profile assessment for 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.

Insert signature here

Attestation **must be signed by the public sector body Head**, not a delegate

New guidance: How-to Guide

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT

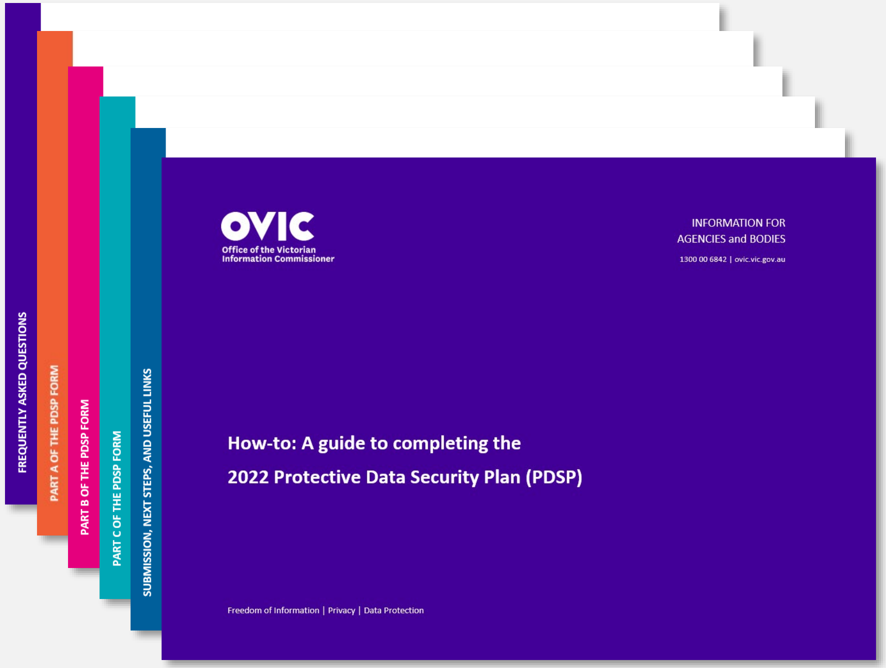
What is it?

A detailed guide designed to assist you in completing the 2022 PDSP form.

How do I use it?

You can work your way through the guide from start to finish, or jump ahead to Part A.

The How-to Guide sets out each field contained in the 2022 PDSP form and provides an accompanying explanation and/or description. Includes screenshots for visual references.



FREQUENTLY ASKED QUESTIONS

PART A OF THE PDSP FORM

PART B OF THE PDSP FORM

PART C OF THE PDSP FORM

SUBMISSION, NEXT STEPS, AND USEFUL LINKS

OVIC
Office of the Victorian
Information Commissioner

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

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

Where do I find it?

Download a copy from our website: https://ovic.vic.gov.au/agency-reporting-obligations-hub/vps-stakeholders/

What’s inside?

ENGAGE

UNDERTAKE

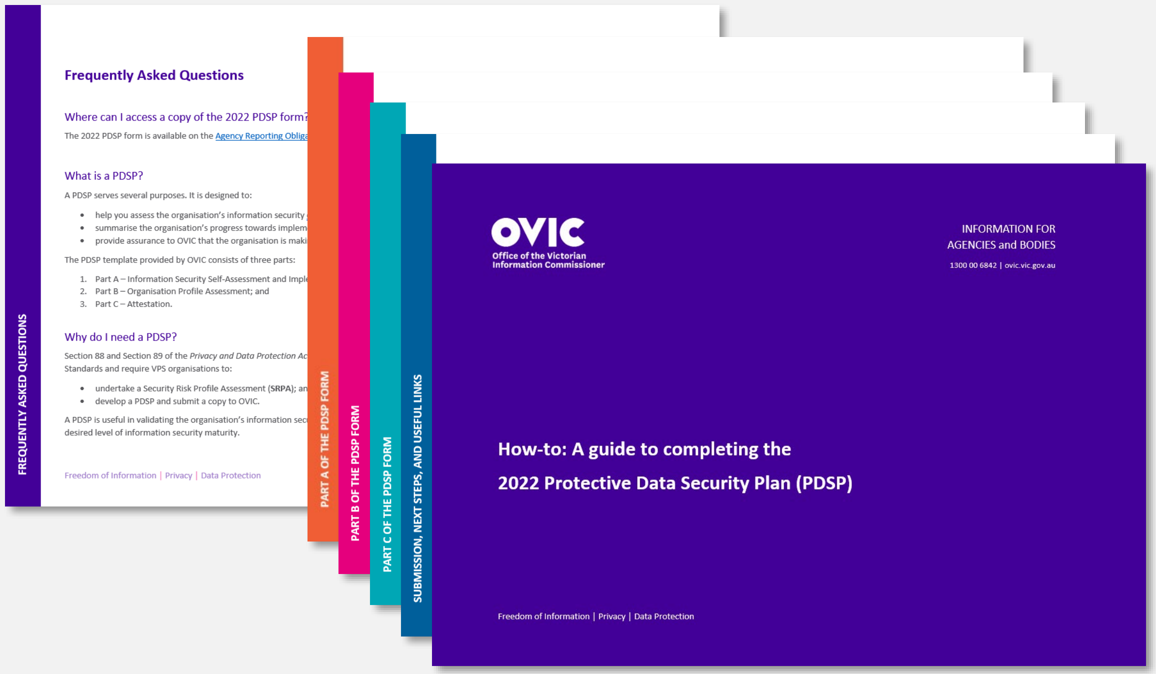
DEVELOP

SUBMIT

Frequently Asked Questions (FAQ)

Frequently asked questions about the PDSP and reporting period.

If you are new to the reporting process or would like to gain further insights into the intent of the PDSP form, we suggest starting with the FAQs as these may provide useful context and background.



Frequently Asked Questions

Where can I access a copy of the 2022 PDSP form?

The 2022 PDSP form is available on the Agency Reporting Obliga

What is a PDSP?

A PDSP serves several purposes. It is designed to:

- help you assess the organisation’s information security
- summarise the organisation’s progress towards implem
- provide assurance to OVIC that the organisation is maki

The PDSP template provided by OVIC consists of three parts:

1. Part A – Information Security Self-Assessment and Imple
2. Part B – Organisation Profile Assessment; and
3. Part C – Attestation.

Why do I need a PDSP?

Section 88 and Section 89 of the *Privacy and Data Protection Ac*
Standards and require VPS organisations to:

- undertake a Security Risk Profile Assessment (**SRPA**); an
- develop a PDSP and submit a copy to OVIC.

A PDSP is useful in validating the organisation’s information sec
desired level of information security maturity.

Freedom of Information | Privacy | Data Protection

OVIC
Office of the Victorian
Information Commissioner

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

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

What’s inside?

ENGAGE

UNDERTAKE

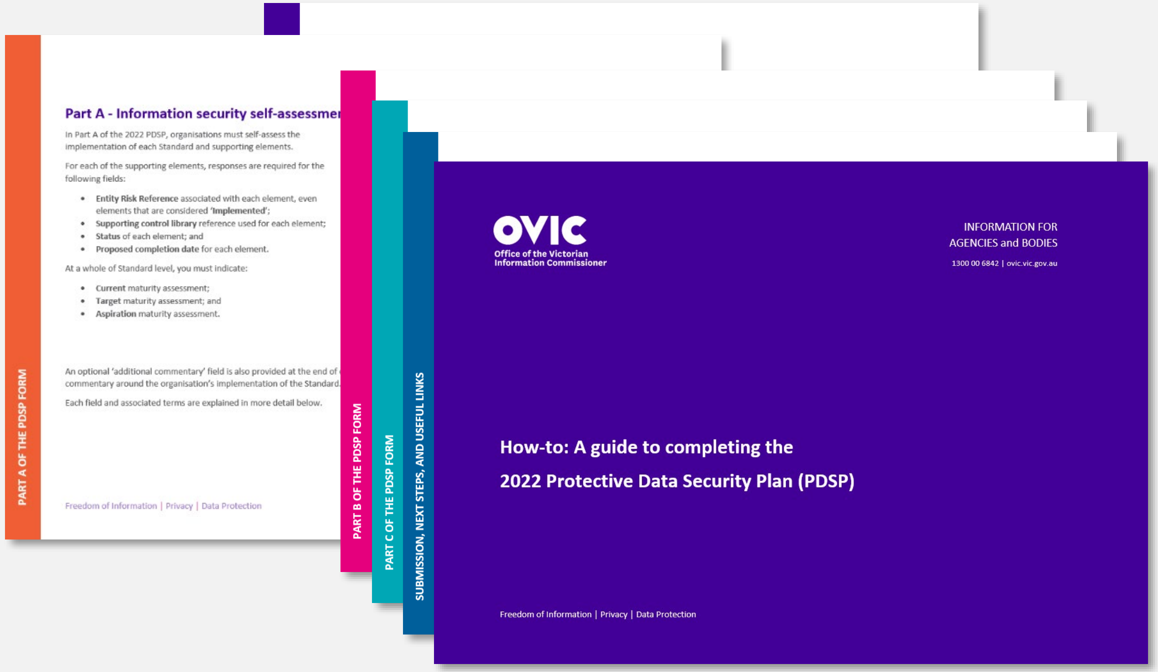
DEVELOP

SUBMIT

Part A of the PDSP form

Provides detailed guidance on each field within Part A of the PDSP form, including:

- Purpose of each field
- Field explanations
- Examples for how to complete each field



PART A OF THE PDSP FORM

Part A - Information security self-assessmen

In Part A of the 2022 PDSP, organisations must self-assess the implementation of each Standard and supporting elements.

For each of the supporting elements, responses are required for the following fields:

- **Entity Risk Reference** associated with each element, even elements that are considered **‘Implemented’**;
- **Supporting control library** reference used for each element;
- **Status** of each element; and
- **Proposed completion date** for each element.

At a whole of Standard level, you must indicate:

- **Current** maturity assessment;
- **Target** maturity assessment; and
- **Aspiration** maturity assessment.

An optional ‘additional commentary’ field is also provided at the end of
commentary around the organisation’s implementation of the Standard.

Each field and associated terms are explained in more detail below.

Freedom of Information | Privacy | Data Protection

PART B OF THE PDSP FORM

PART C OF THE PDSP FORM

SUBMISSION, NEXT STEPS, AND USEFUL LINKS

OVIC
Office of the Victorian
Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

What’s inside?

ENGAGE

UNDERTAKE

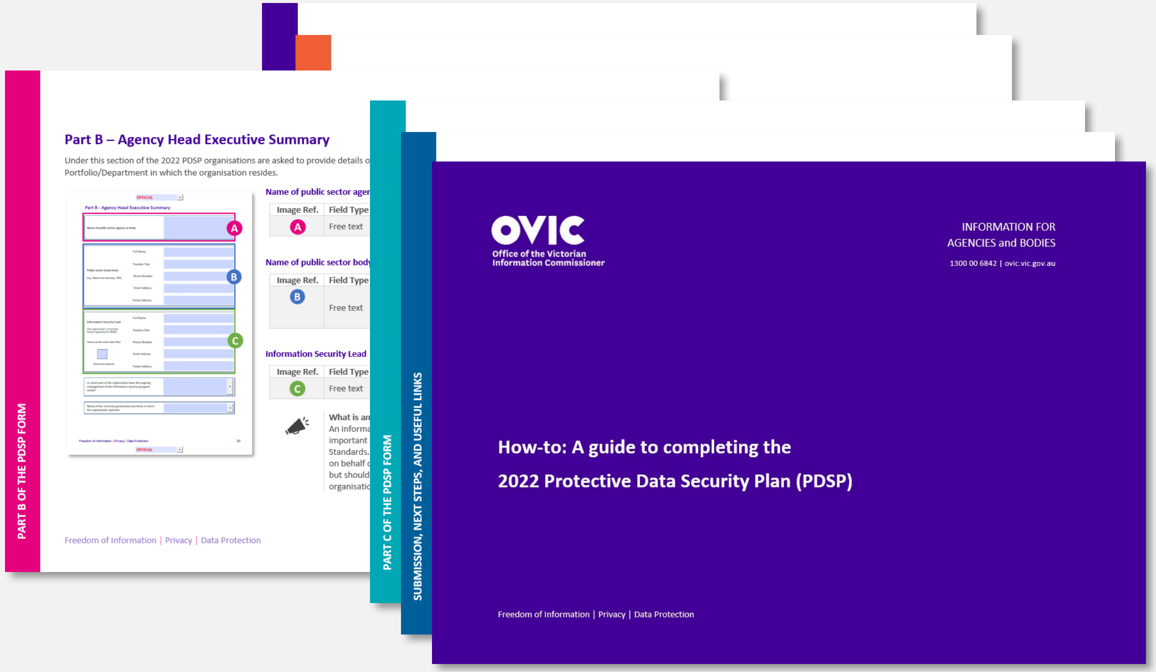
DEVELOP

SUBMIT

Part B of the PDSP form

Provides detailed guidance on each field within Part B PDSP form, including:

- The agency head executive summary
- Questions within the Organisational Profile Assessment (OPA)



Part B – Agency Head Executive Summary

Under this section of the 2022 PDSP organisations are asked to provide details o
Portfolio/Department in which the organisation resides.

Name of public sector ager

Image Ref.	Field Type
A	Free text

Name of public sector body

Image Ref.	Field Type
B	Free text

Information Security Lead

Image Ref.	Field Type
C	Free text

What is an
An informa
important
Standards.
on behalf c
but should
organisatio

Freedom of Information | Privacy | Data Protection

OVIC
Office of the Victorian Information Commissioner

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

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

What’s inside?

ENGAGE

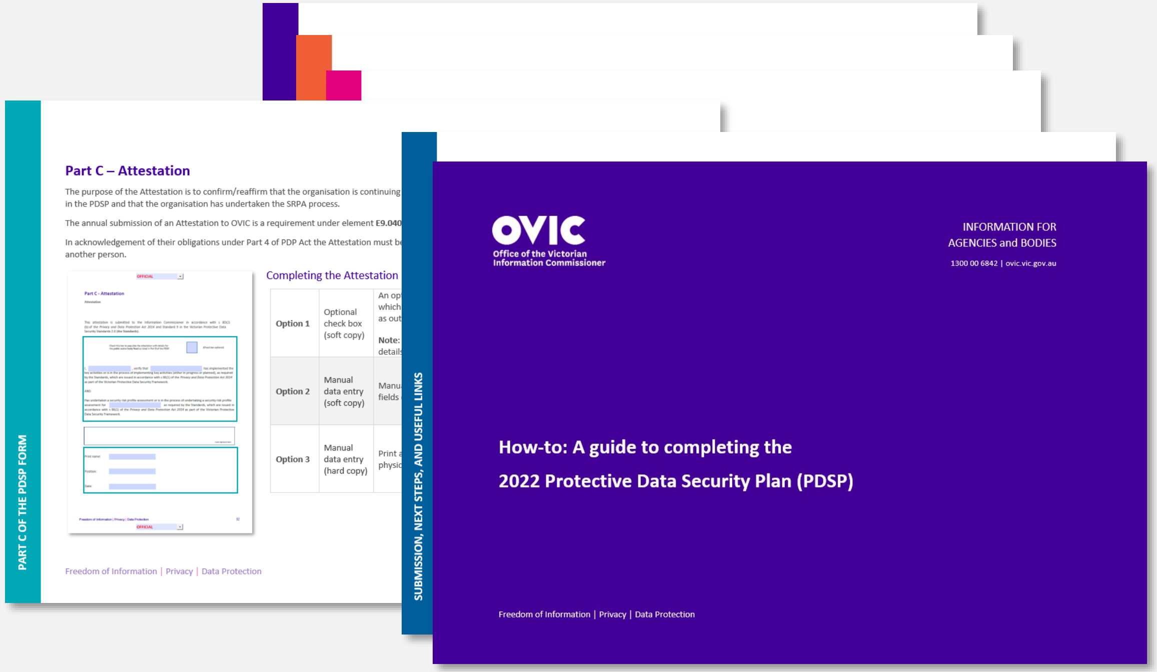
UNDERTAKE

DEVELOP

SUBMIT

Part C of the PDSP form

Provides guidance on the purpose of and options (soft copy vs. hard copy) for completing the Attestation within the PDSP form.



PART C OF THE PDSP FORM

Part C – Attestation

The purpose of the Attestation is to confirm/reaffirm that the organisation is continuing
in the PDSP and that the organisation has undertaken the SRPA process.

The annual submission of an Attestation to OVIC is a requirement under element **E9.040**

In acknowledgement of their obligations under Part 4 of PDP Act the Attestation must be
another person.

OFFICIAL

Part C - Attestation

Attestation

Print name:

Position:

Date:

Freedom of Information | Privacy | Data Protection

OFFICIAL

Completing the Attestation

Option 1	Optional check box (soft copy)	An op which as out **Note:** details
Option 2	Manual data entry (soft copy)	Manu fields
Option 3	Manual data entry (hard copy)	Print a physic

Freedom of Information | Privacy | Data Protection

SUBMISSION, NEXT STEPS, AND USEFUL LINKS

OVIC
Office of the Victorian
Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

How-to: A guide to completing the
2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

What’s inside?

ENGAGE

UNDERTAKE

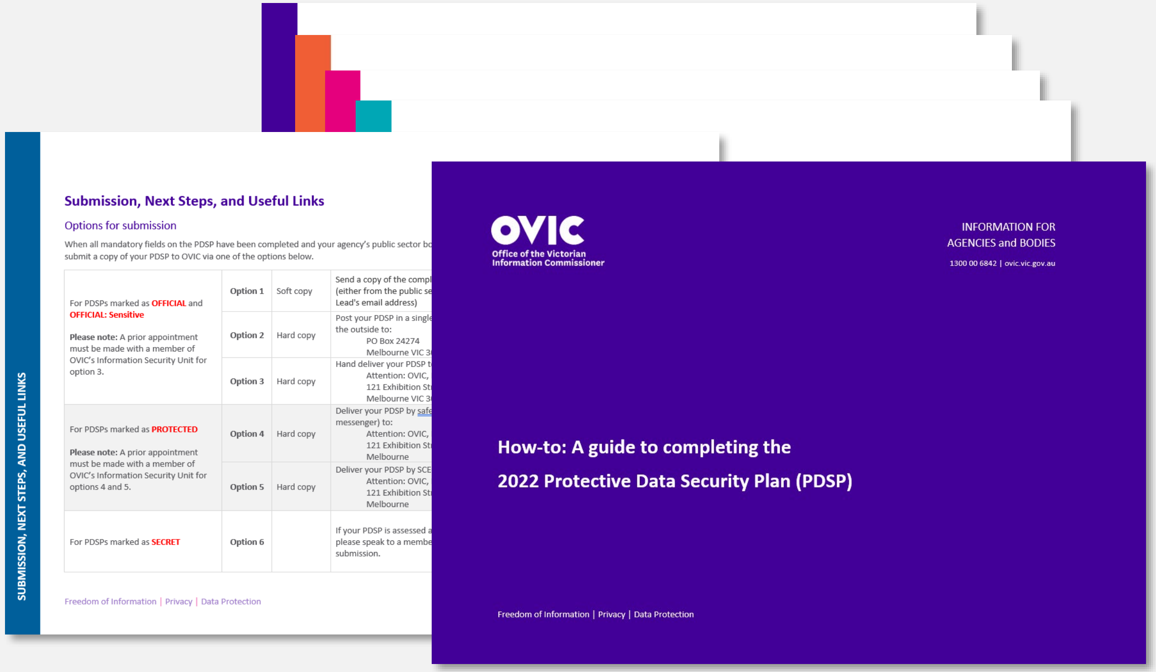
DEVELOP

SUBMIT

Submission, Next Steps, and Useful Links

Provides:

- options for submission based on the protective marking assigned to the PDSP
- next steps to consider following submission, and
- useful links that will help throughout the reporting process.



SUBMISSION, NEXT STEPS, AND USEFUL LINKS

Submission, Next Steps, and Useful Links

Options for submission

When all mandatory fields on the PDSP have been completed and your agency’s public sector bo
submit a copy of your PDSP to OVIC via one of the options below.

For PDSPs marked as **OFFICIAL** and **OFFICIAL: Sensitive** **Please note:** A prior appointment must be made with a member of OVIC’s Information Security Unit for option 3.	**Option 1**	Soft copy	Send a copy of the compl (either from the public se Lead's email address)
	Option 2	Hard copy	Post your PDSP in a single the outside to: PO Box 24274 Melbourne VIC 3
	Option 3	Hard copy	Hand deliver your PDSP t Attention: OVIC, 121 Exhibition St Melbourne VIC 3
For PDSPs marked as **PROTECTED** **Please note:** A prior appointment must be made with a member of OVIC’s Information Security Unit for options 4 and 5.	**Option 4**	Hard copy	Deliver your PDSP by safe messenger) to: Attention: OVIC, 121 Exhibition St Melbourne
	Option 5	Hard copy	Deliver your PDSP by SCE Attention: OVIC, 121 Exhibition St Melbourne
For PDSPs marked as **SECRET**	**Option 6**		If your PDSP is assessed a please speak to a membe submission.

Freedom of Information | Privacy | Data Protection

OVIC
Office of the Victorian
Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

How-to: A guide to completing the

2022 Protective Data Security Plan (PDSP)

Freedom of Information | Privacy | Data Protection

Single Organisation Sample Approach

ENGAGE

1 Engage your executive and assemble your team*

2 Review your previous PDSP and internal security program

UNDERTAKE

3 Undertake an updated **SRPA** ensuring you capture risks associated with **CSPs** and **third-parties**

4 Review and/or update your risk register

DEVELOP

5 Download the 2022 PDSP form and How-to Guide

6 Develop your 2022 PDSP in consultation with relevant stakeholders

7 Validate your PDSP responses (internally or externally)

SUBMIT

8 Brief your executive and seek sign off on the finalised PDSP

9 Submit PDSP to OVIC by **31 August 2022** --------> OVIC Office of the Victorian Information Commissioner

*we acknowledge that some organisations may not have a team to leverage off.

OFFICIAL

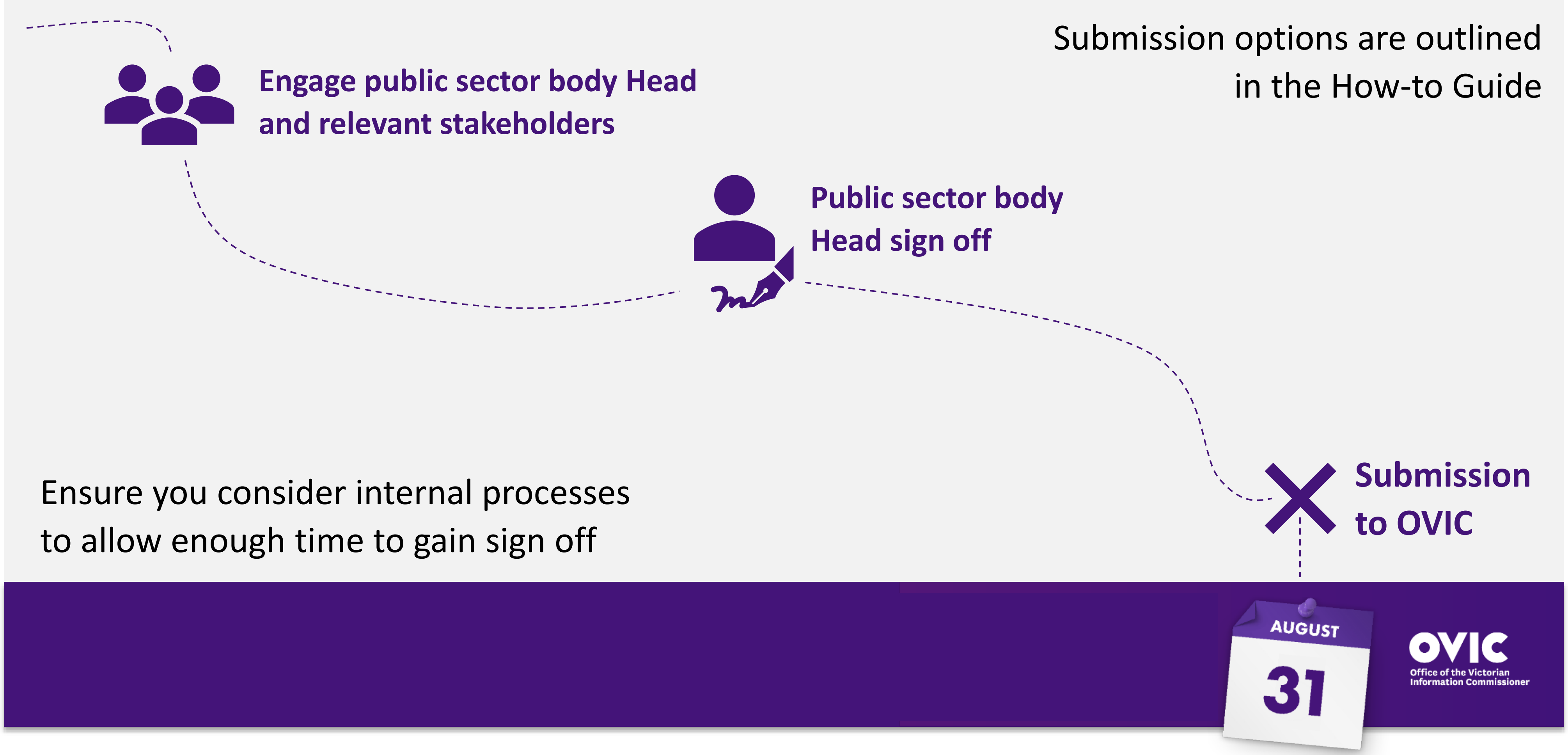
Submit

ENGAGE

UNDERTAKE

DEVELOP

SUBMIT



Submission options are outlined in the How-to Guide

Engage public sector body Head and relevant stakeholders

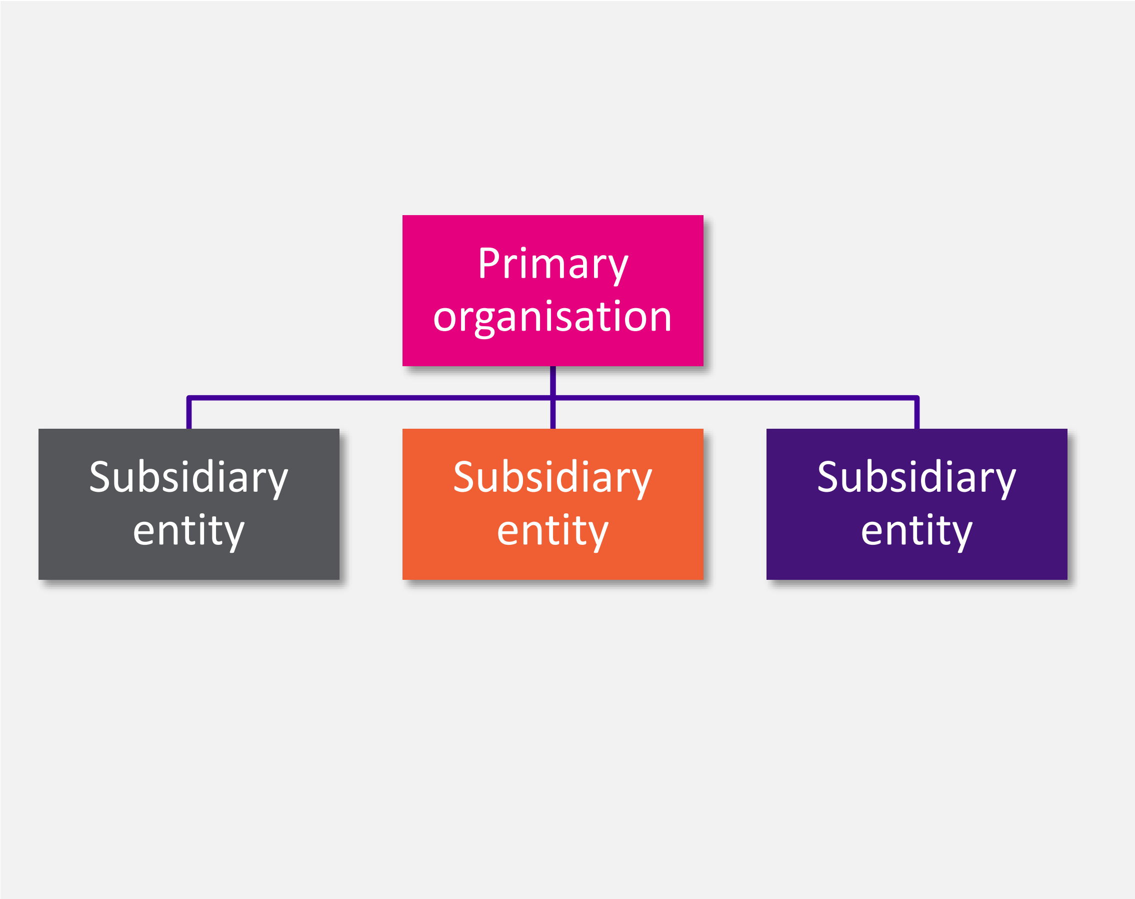
Public sector body Head sign off

Ensure you consider internal processes to allow enough time to gain sign off

Submission to OVIC

OFFICIAL

A word on the Multi-organisation Reporting model



Primary organisation

Subsidiary entity

Subsidiary entity

Subsidiary entity

Where appropriate an organisation (primary organisation) may request a multi-organisation PDSP form to use to report on behalf of itself and its subsidiary entities.

This reporting approach may be based upon a portfolio model where agencies or bodies fall within the portfolio of responsibilities of a department (primary organisation) and have a similar control environment and risk profile to nominated subsidiary entities.

Please contact OVIC's Information Security Unit to discuss your requirements.

Additional Resources: VPDSS Glossary v2.1

Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards – Glossary

Version 2.1 January 2022

Freedom of Information | Privacy | Data Protection

Term	Definition
Active (information)	See 'Current' (information)
Agency	As per *Privacy and Data Protection Act 2014*, a public service body (departments and administrative offices) or a public entity (a body established under an Act, by the Governor in Council or by a Minister) within the meaning of the *Public Administration Act 2004*.
Aggregation	A compilation of information. Compilations of public sector information may require enhanced protection, as the combination of the information assets may be of greater value than any single part.
Agreement	A formal and legally binding contract between the State and a third party or parties. For example, a contract between a VPS organisation, on behalf of the State, and a third-party company delivering IT services. State agreements are usually in writing.
All persons	Employees, volunteers, contractors/sub-contractors, and consultants, whether directly or indirectly engaged by the organisation with access to public sector information. Also referred to as Personnel.
Arrangement	An informal and non-legally binding understanding between the State and a third party. A memorandum of understanding between two parts of the State is also an arrangement because it is not possible to make a legally binding contract between two parts of the same legal entity – the State of Victoria.
Asset	Any item (whether tangible or intangible) that has a useful or valuable quality for an organisation. This includes information, physical, people and/or system-based assets to support that organisation's business functions, services and activities. Value can be subjective or objective.
Assurance	A degree of confidence that an organisation is managing information security risks, in the context of the VPDSF.
Augmented Backus–Naur form	A system of a language used as a bidirectional communications protocol for emails.

Freedom of Information | Privacy | Data Protection 5

Availability	The desired state that allows authorised persons and/or systems to access defined information for authorised purposes at the time they need to do so.

6

In January 2022, we released version 2.1 of the VPDSS Glossary.

This document defines the terms and acronyms used in the VPDSS and VPDSF material, including the Protective Data Security Plan.

With thanks from the Deputy Commissioner

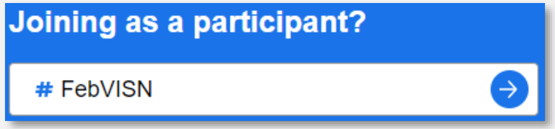
Rachel Dixon
Deputy Commissioner
Privacy and Data Protection

Feedback and Questions

Please provide any **feedback** you have on today's session.

slido

Go to slido.com



Joining as a participant?

FebVISN

For those with **questions** following this forum, please email:

security@ovic.vic.gov.au

Thank you!