

# **2024 - How-to: A guide to completing the Protective Data Security Plan (PDSP)**

## Document Details

How-to: A guide to completing the Protective Data Security Plan (PDSP)		
Protective Marking		OFFICIAL
Approved for unlimited public release		Yes – Authorised for release
Release Date		February 2024
Review Date		January 2026
Document Version		1.3
Authority		Office of the Victorian Information Commissioner (OVIC)
Author		Information Security Unit - OVIC
Version Control		
Version	Date	Key Changes
1.0	January 2022	Original version
1.1	June 2022	Corrected Maturity assessment example error
1.2	February 2023	<ul style="list-style-type: none"><li>Removed references to ‘2022’ to make document date agnostic</li><li>Added description for ‘Planned’ implementation status</li></ul>
1.3	February 2024	<ul style="list-style-type: none"><li>Updated screenshots to reflect 2024 PDSP form</li><li>Refer to <a href="#">What has changed in the 2024 PDSP form</a> section of this guide</li></ul>

## Contents

Introduction .....	7
How to use this guide .....	7
Where to start.....	7
Completing and filling in the PDSP form.....	8
Breakdown of the PDSP form .....	8
Field character limits within the PDSP form .....	8
Frequently Asked Questions .....	9
What has changed in the 2024 PDSP form? .....	9
Where can an organisation access a copy of the PDSP form? .....	10
What is a PDSP? .....	10
Why is need a PDSP needed? .....	10
When does an organisation have to submit a PDSP? .....	11
What should an organisation do before it starts a PDSP? .....	11
Who should complete the PDSP? .....	12
Who is responsible for the PDSP?.....	12
What should be captured in the PDSP? .....	13
How will the information in the PDSP be used and managed? .....	13
Who can attest and submit the PDSP? .....	14
What protective marking should an organisation label the PDSP with? .....	14
Why does a protective marking need to be assigned to the PDSP? .....	15
How does an organisation submit a copy of the PDSP to OVIC? .....	15
What happens if an organisation doesn't submit a PDSP? .....	15

Part A - Information security self-assessment and implementation plan .....	16
Element Assessment .....	16
Maturity Assessment .....	16
VPDSS Elements .....	18
How to read an element .....	18
Example .....	18
Industrial Automation and Control Systems (IACS) Elements .....	19
Entity Risk Reference .....	19
How to fill in the entity risk reference field .....	20
Example .....	20
Supporting Control Library .....	21
How to select the most appropriate supporting control library .....	21
Example .....	21
Status .....	23
How to select the most appropriate status .....	23
E.g. If an organisation has implemented some components of an element (not all), the status of <i>Partial (some)</i> , or <i>Partial (most)</i> may be appropriate.	
Example .....	24
Proposed Completion Date .....	26
How to select the most appropriate completion date .....	26
Maturity Assessment .....	27
How to conduct a maturity assessment at a whole of Standard level .....	27
Example .....	30
Optional Field .....	31

Part B – Agency Head Executive Summary .....	32
Name of public sector agency or body .....	32
Name of public sector body Head.....	32
In which part of the organisation does the ongoing management of the information security program reside? .....	33
Name of the Victorian government portfolio in which the organisation operates .....	33
Security program executive summary from the past 24 months .....	34
Challenges or barriers .....	34
<b>Organisational Profile Assessment (OPA) .....</b>	<b>35</b>
Number of employees within the organisation .....	35
Does the organisation have Industrial Automation and Control Systems (IACS)? .....	35
Does the organisation obtain, generate, receive, or hold information at Business Impact Level 3 (BIL 3) or higher? .....	36
Provide an approximate protective marking breakdown of the organisation's information assets.....	37
Percentage of information not assessed .....	37
Percentage of information marked using a former scheme or different scheme .....	37
How many information security incidents were recorded in the organisation's internal incident register over the last 24 months? .....	38
Of these incidents, how many affected information assets of a BIL 2 or higher? .....	39
How many third-party arrangements currently have direct access to the organisation's information and information systems? .....	40
What is the highest protective marking that third parties are accessing? .....	41
How did the organisation validate the PDSP prior to submission to OVIC? .....	41
Does your organisation use Generative Artificial Intelligence (Gen AI)?.....	42
Nominate which tools are proposed or in use.....	42
Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation .....	43
Select the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.....	43

Do any of your contracted service providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed, or transferred on behalf of the organisation? .....	44
Nominate the Gen AI tools being proposed or in use by CSPs: .....	44
Select the types of public sector information proposed or in use as inputs into LLMs by CSPs .....	45
Select the BIL rating of public sector information proposed or in use as inputs into LLMs by CSPs.....	45
Part C – Attestation.....	46
Incorporation of Standard 9 elements into Attestation .....	46
Completing the Attestation .....	47
Signing the Attestation/PDSP.....	47
Submission, Next Steps, and Useful Links.....	48
Options for submission .....	48
Next steps .....	49
Useful links .....	50

# Introduction

## How to use this guide

This guide is designed to assist applicable Victorian public sector (**VPS**) agencies and bodies (**organisations**) in completing the Protective Data Security Plan (**PDSP**) form.

This guide is separated into six sections, each represented by a different colour as shown in the table below:

	<a href="#"><u>INTRODUCTION</u></a>
	<a href="#"><u>FREQUENTLY ASKED QUESTIONS</u></a>
	<a href="#"><u>PART A OF THE PDSP FORM</u></a> Information security self-assessment and implementation plan
	<a href="#"><u>PART B OF THE PDSP FORM</u></a> Agency Head executive summary (including the Organisation Profile Assessment)
	<a href="#"><u>PART C OF THE PDSP FORM</u></a> Attestation
	<a href="#"><u>SUBMISSION, NEXT STEPS, AND USEFUL LINKS</u></a>

This guide sets out each field contained in the PDSP form and provides an accompanying explanation and/or description to enable organisations to complete the submission.

## Where to start

If the organisation is familiar with the process for completing a PDSP then it may wish to jump ahead in this guide to [PART A OF THE PDSP FORM](#).

If the organisation is new to the process or would like to gain further insights into the intent of the PDSP form, we suggest starting with the [FAQs](#) section of this guide as these may provide useful context and background.

There may be some unfamiliar terms in this guide. Refer to our [VPDSS Glossary](#) for definitions.

## Completing and filling in the PDSP form

The PDSP form was developed using Acrobat 2020 (20.005.30467). Some functionality of the PDSP form may be impaired or lost if opened with an incompatible PDF reader. For best results when completing this form, use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro. Alternatively users can use Microsoft Edge to edit or complete the PDSP form.

## Breakdown of the PDSP form

The PDSP is a single PDF form comprised of three mandatory parts:

Part		Description
<b>A</b>	Information security self-assessment and implementation plan	<ul style="list-style-type: none"> <li>• Outlines the organisation's self-assessed implementation of the elements under each Standard; and</li> <li>• Outlines the organisation's self-assessed maturity level for each Standard.</li> </ul>
<b>B</b>	Agency Head executive summary (including the Organisation Profile Assessment)	<ul style="list-style-type: none"> <li>• Provides contact information of the public sector body Head and Information Security Lead;</li> <li>• Provides an opportunity for organisations to highlight achievements across the past 24 months and describe any challenges or barriers to the security program; and</li> <li>• Poses a series of questions that form the Organisation Profile Assessment (<b>OPA</b>).</li> </ul>
<b>C</b>	Attestation	<ul style="list-style-type: none"> <li>• Attests that the PDSP reflects the current information security operating environment and ongoing program of work.</li> </ul>

## Field character limits within the PDSP form

The PDSP form is predominantly made up of drop-down fields with some free-text field options. Where there are free-text fields, character limits apply. The limits will differ throughout the form. Character limits are noted against relevant fields.

If the organisation intends to print the PDSP form, be aware that some of the responses may be cut off when printed due to space restrictions. Where the PDSP form is electronically submitted (unscanned) to OVIC, full responses will be captured, character limits permitting.



## Frequently Asked Questions

### What has changed in the 2024 PDSP form?

#### Overall

- Functionality provided by JavaScript has been removed.

#### About the Protective Data Security Plan

- The FAQ section has been removed and incorporated into this 'How to Guide'.

#### Part A – Information Security self-assessment and implementation plan

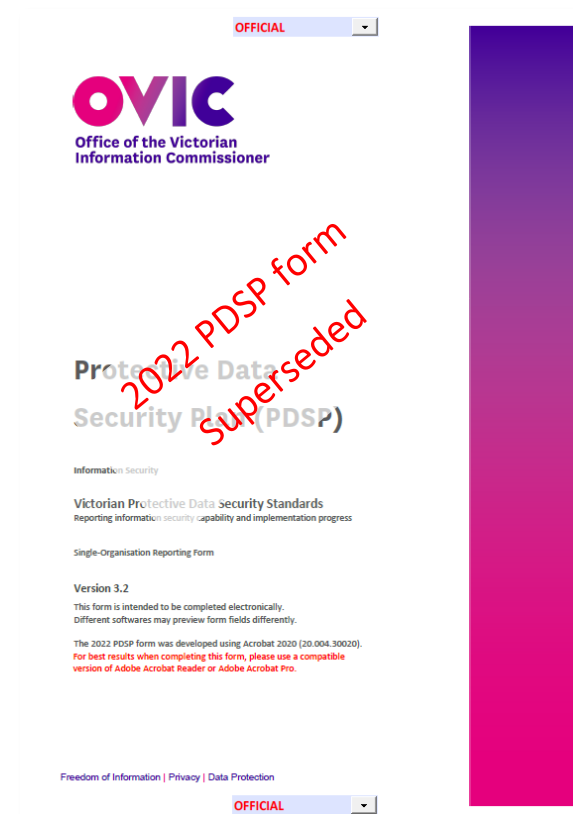
- In previous iterations of the PDSP form, JavaScript supported automated functionality for some features. To cater for this a new field has been added at the end of each Standard which allows for the manual capture of both mandatory and supplementary content. For more information see:
  - [Supporting control library - Other](#)
  - Implementation Status – Not Applicable
  - Additional commentary regarding implementation of the Standard
- [Industrial Automation and Control Systems \(IACS\)](#) elements have been added to VPDSS 1 and 2.
  - Note: Only organisations that operate IACS in their environments need to consider these elements.
  - For more information, see [page 19](#)
- Edits to how Standard 9 responses are captured. See [Incorporation of Standard 9 elements into Attestation section](#).

#### Part B – Agency Head Executive Summary

- OPA - Approximate protective marking breakdown does not automatically calculate information asset percentages. For more information, see [Provide an approximate protective marking breakdown of the organisation's information assets](#)
- Additional Generative Artificial Intelligence (AI) questions. See [Generative AI](#) for more information.

#### Part C – Attestation

- Attestation wording has been amended.



## Where can an organisation access a copy of the PDSP form?

A PDSP form is available on the OVIC website under the [VPS Agency Reporting Obligations webpage](#) or available upon request by contacting the Information Security Unit via [security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)

## What is a PDSP?

A PDSP serves several purposes. It is designed to:

- help an organisation assess its information security capability;
- summarise the organisation's progress towards implementation of the Victorian Protective Data Security Standards (**VPDSS** or **Standards**) and elements; and
- provide assurance to OVIC that the organisation is making progress to improving information security.

The PDSP form provided by OVIC consists of three parts:

1. Part A – Information security self-assessment and implementation plan;
2. Part B – Agency Head executive summary (including the Organisation Profile Assessment); and
3. Part C – Attestation.

## Why is need a PDSP needed?

Section 89 of the *Privacy and Data Protection Act 2014* (**PDP Act**) requires VPS organisations to:

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

A PDSP is a point in time snapshot that documents the organisation's self-assessed information security capability. The PDSP relies upon an organisation having undertaken the SRPA process, which helps identify and prioritise information security risks to provide efficient, effective, and economic investment in security controls.

Information captured in a PDSP may present a helpful summary to key stakeholders and provides a level of confidence in how the organisation is progressing against the implementation of the Standards.

When does an organisation have to submit a PDSP?

There are two scenarios in which organisations must submit a PDSP as outlined in the PDP Act and Victorian Protective Data Security Framework (VPDSF). Each scenario is outlined in the table below:

Scenario 1	Standard reporting cycle	<p>PDSPs are submitted to OVIC on a biennial reporting cycle.</p> <ul style="list-style-type: none"><li>• The submission of a PDSP is due between <b>1 July and 31 August</b> of the reporting year.</li><li>• The standard reporting cycle for PDSPs falls on even-numbered years (e.g., 2024, 2026, 2028).</li></ul> <p><b>Please note:</b> Organisations are still required to submit an annual Attestation to OVIC.</p>
Scenario 2	<a href="#">Significant change</a> (non-standard reporting cycle)	<p>If the organisation has undergone or expects to undergo a ‘significant change’ to its operating environment or its security risks, the organisation may be required to submit an out-of-cycle PDSP. For more information on what constitutes a significant change review the following <a href="#">information sheet</a>.</p> <p>In the event of significant change, contact the Information Security Unit (ISU) at OVIC to discuss the reporting options.</p> <p><b>Please note:</b> Organisations that undergo significant change must still report in the next standard reporting cycle (Scenario 1). These scenarios are not mutually exclusive.</p>

What should an organisation do before it starts a PDSP?

Before developing a PDSP, the organisation needs to have:

- an understanding of the organisation’s information assets and systems;
- undertaken a security value assessment for these information assets and systems;
- undertaken a SRPA (information security risk assessment) for these information assets and systems; and

- understand the security controls already in place to protect the organisation's information assets and systems to develop a risk treatment plan. This might involve talking to the relevant Portfolio/Department, and/or any other third parties if the organisation are utilising:
  - resources,
  - services,
  - infrastructure; or,
  - policies from them.

Additionally, given the broad nature of the Standards, it is likely that the person coordinating the development of a PDSP will need input and assistance from a wide variety of stakeholders from within the business. Subject matter experts across different workgroups will provide important inputs into PDSP responses for the various Standards. Draw inputs from work units such as:

- Risk,
- Legal, Information/Records Management,
- Information Technology,
- Human Resources/People and Culture,
- Corporate,
- Finance,
- Facilities, etc.

It is also important to engage the public sector body Head early and update them as needed, prior to their signing of the Attestation.

## Who should complete the PDSP?

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

## Who is responsible for the PDSP?

Under the PDP Act, the public sector body Head must ensure that a PDSP is developed, and a copy is submitted for the organisation.

A public sector body Head is defined as the head of any Victorian Government department, authority, agency, or body identified as an applicable organisation under Part 4 of the PDP Act.

## What should be captured in the PDSP?

Copies of PDSPs submitted to OVIC should cover security activities spanning a 24-month period as well as any planned activities. Incomplete PDSPs will not be accepted by OVIC. Please ensure all mandatory fields are completed before submitting, including the signed and dated Attestation.

## How will the information in the PDSP be used and managed?

OVIC has a responsibility to provide assurance to Ministers and the Victorian public regarding the information security capabilities of the VPS. The information provided in the PDSP will be used by the ISU to monitor an organisation's information security progress.

Insights and select content drawn from PDSP submissions may form the basis of reporting back to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

Additionally, the ISU will:

- use the PDSP to help plan engagement and support activities for VPS organisations;
- use information to inform assurance activities; and
- provide feedback to VPS organisations based on their submissions.

OVIC will collect some personal information as part of the PDSP submission including name and contact details of the public sector body Head and nominated contact (Information Security Lead). We use this information for the purposes of communicating with these contacts about the PDSP, broader security initiatives and activities, distributing information security related content, or collecting feedback.

OVIC will not disclose personal information without consent, except where required to do so by law. For more information about how OVIC handles personal information, please see [OVIC's Privacy Policy](#).

The information provided in the PDSP will be managed in accordance with the protective marking assigned. The contents of the PDSP are exempt from the *Freedom of Information Act 1982*.

## Who can attest and submit the PDSP?

The PDSP must be signed by the public sector body Head in acknowledgment of their statutory obligations. The attestation is set out under Part C of the PDSP form.

Under the PDP Act, the public sector body Head is responsible for providing a copy of the organisation's PDSP to OVIC. Once signed by the public sector body Head, the submission can be actioned by any member of the organisation.

## What protective marking should an organisation label the PDSP with?

When drafting PDSP responses, organisations should conduct an initial confidentiality assessment and apply an interim protective marking based on the draft content. This will inform handling protections on the PDSP while responses are being collated and finalised.

Once the PDSP is complete, organisations should conduct an updated confidentiality assessment to inform the most appropriate protective marking for the PDSP based on the finalised content. This should be done before sending a copy of the PDSP to OVIC.

When conducting an assessment, consider the responses/information provided by the organisation and the potential harm/damage that could result from a compromise of the confidentiality of the information captured on the PDSP. Keep in mind that a protective marking of:

- **OFFICIAL** means compromise of the *confidentiality* of information would be expected to cause minor harm/damage to government operations, organisations, or individuals.
- **OFFICIAL: Sensitive** means compromise of the *confidentiality* of information would be expected to cause limited harm/damage to government operations, organisations, or individuals.
- **PROTECTED** means compromise of the *confidentiality* of information would be expected to cause major harm/damage to government operations, organisations, or individuals.

For more information on what these impact descriptors mean (minor, limited, major), reference the organisation's contextualised Business Impact Level (BIL) table or the [VPDSF BIL table](#).

## Why does a protective marking need to be assigned to the PDSP?

Protective markings are security labels assigned to public sector information that signal the confidentiality requirements of the information, and visually highlight to the user that particular security controls are needed to manage the material. It is important that the organisation label its PDSP with an appropriate protective marking as it:

- guides OVIC on the expected controls to maintain the confidentiality of the responses captured in the organisation's PDSP; and
- informs the most appropriate submission method to OVIC.

Where a marking is not provided, OVIC will handle the PDSP at the **OFFICIAL**/BIL 1 level.

## How does an organisation submit a copy of the PDSP to OVIC?

Submission options will vary depending on the protective marking of the PDSP. Refer to [SUBMISSION AND NEXT STEPS](#) for detail.

## What happens if an organisation doesn't submit a PDSP?

In-scope VPS organisations that fail to submit a PDSP to OVIC will be in breach of the PDP Act. To find out more about OVIC's regulatory approach refer to the [OVIC Regulatory Action Policy](#).

## Part A - Information security self-assessment and implementation plan

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

### Element Assessment

For each element, organisations must (mandatory) provide a response 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.

OFFICIAL

### Standard 7 – Information Security Aspects of Business Continuity and Disaster Recovery

An organisation embeds information security continuity in its business continuity and disaster recovery processes and plans. VPDSS

Standard 7 Element Assessment

	VPDSS Standard 7 Elements	Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.			Not Commence	
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.			Not Commence	
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).			Not Commence	

### Maturity Assessment

At a whole of Standard level, the organisation must indicate:

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

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

OFFICIAL

### VPDSS Standard 7 Maturity Assessment

Current	2026 Target	2028 Aspiration



## Additional Commentary

In previous iterations of the PDSP form, JavaScript supported automated functionality for some features.

To cater for the removal of JavaScript, a new field has been added at the end of each Standard. This field allows for the manual capture of both mandatory and supplementary content relating to the Standard.

This free-text field **must** be used where:

1. [Supporting control library – ‘Other’ is selected](#)
2. [Implementation Status – Not Applicable is selected](#)

This free-text field can be used to provide optional:

3. [Additional commentary regarding implementation of the Standard](#)

Use this space to provide any additional commentary 1500 character limit

- **Supporting Control Library: Other**  
If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- **Status: Not Applicable**  
If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

## VPDSS Elements

A VPDSS element (**element**) refers to security measure(s) that modify risk.

These measures are derived from primary source material that provide further guidance on how to meet the objectives of a Standard.

For a full list of the VPDSS elements please refer to the:

- [VPDSS Implementation Guidance V2.3](#) and/or;
- [IACS Implementation Guidance](#).

VPDSS Standard 2 Element Assessment

VPDSS Standard 2 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commenced	

### How to read an element

Some elements contain multiple activities/requirements so it is worth critically considering all aspects of the element, as this may influence the selection of an implementation status. An example is provided below.

### Example

VPDSS Element	Descriptor	Activities
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register ( <b>IAR</b> ) in consultation with its stakeholders.	<p>This element has more than one aspect/activity listed in its description.</p> <p>For this element to be implemented an organisation should have:</p> <ul style="list-style-type: none"> <li>• Identified the organisation's information assets;</li> <li>• Documented its information assets in an IAR;</li> <li>• Actively maintained the IAR; and</li> <li>• Consulted with the organisation's stakeholders throughout this process (this includes internal and external stakeholders).</li> </ul>

## Industrial Automation and Control Systems (IACS) Elements

Organisations that operate IACS should consider the specific elements that are applicable to those environments.

These specific elements are outlined in the [Implementation Guidance for Industrial Automation and Controls Systems – Extension to VPDSS Implementation Guidance](#), and should be considered in addition to the general VPDSS Elements captured in the [VPDSS Implementation Guidance \(V2.3\)](#) document.

The specific IACS elements include:

- E1.120
- E1.130
- E2.100

VPDSS Standard 2 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commenced	

Victorian Government organisations that come from the IACS sector contributed to the development of these elements and are aware of their requirement to report against these. In practical terms, this typically includes the water and transport sectors who are a public sector agency or body and may be operating a critical infrastructure asset.

### Entity Risk Reference

As part of an organisation's risk management framework and supporting processes, risks are recorded and managed via an organisational risk register.

These registers contain risk descriptions that are often given a unique identifier / number providing a way to quickly reference that risk internally. It can be expressed in whatever form, format, or way that makes sense to the organisation.

Depending on different organisations' risk management processes, information security risks should also be recorded and managed via this internal risk register.

It is expected that an organisation has at least one information security risk recorded in its internal risk register, helping track and manage information security risks resulting from the SRPA process. Information security risks should be reviewed and managed on an ongoing basis.

On the PDSP form, organisations are expected to record entity risk reference(s) against corresponding element/s.

This risk reference(s) highlights applicable risks relating to the supporting control(s) that the element intends to address. Risk references are mandatory and must be entered into the PDSP form.

For further guidance on risk management please refer to the [Practitioner Guide: Information Security Risk Management](#).

VPDSS Standard 2 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commenced	

### How to fill in the entity risk reference field

This is a free text field for referencing risk(s) that the element (control) is treating. Refer to the organisation's risk register and copy the relevant risk reference documented within it, into the PDSP form. The organisation may have:

- a separate risk reference for each element;
- multiple risk references for each element; or
- one risk reference repeated for all elements throughout the PDSP (e.g., strategic or enterprise risk reference).

The organisation may have various risk references recorded in the PDSP, or one risk reference repeated throughout the PDSP.

### Example

VPDSS Standard 2 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.	Risk 123		Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.	Risk 123, Risk ABC		Not Commenced	

## Supporting Control Library

Each element has been derived from references and provides further guidance on security controls/measures to assist organisations in implementing the Standards.

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

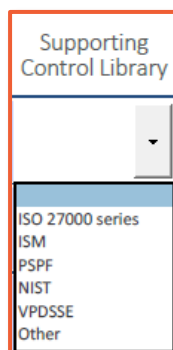
As the VPDSS promotes a risk-based approach, OVIC recognises alternative control libraries that support the intent of each Standard and modify organisational risks. Should organisations wish to use these alternative control libraries, they must provide (at a minimum) functional equivalency to what the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

Alternative control libraries must be documented in the 'Additional Commentary' field at the end of each Standard.

### How to select the most appropriate supporting control library

Organisations need to select at least one control library reference per element. The table below summarises the more common supporting control library selections offered on the PDSP form. The organisation may have its own documented internal control library. If so, or if the organisation is using an alternative control library not on this table, please select '**Other**'.

#### Example



The image shows a screenshot of a web form. At the top, there is a label 'Supporting Control Library' in blue text. Below it is a drop-down menu. The menu is currently open, showing a list of options: 'ISO 27000 series', 'ISM', 'PSPF', 'NIST', 'VPDSS', and 'Other'. The 'Other' option is highlighted in blue.

Select the most relevant supporting control library from the drop-down menu.

For more information on each of the control libraries, refer to the table below.

Control Library	Description
<b>ISO 27000</b> series	The ISO 27000 series comprises mutually supporting information security standards that together provide a globally recognised framework for best-practice information security management.
<b>ISM</b> Australian Government Information Security Manual ( <b>ISM</b> )	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. The ISM helps organisations use their risk management framework to protect information and systems from cyber threats.
<b>PSPF</b> Protective Security Policy Framework ( <b>PSPF</b> )	The PSPF is the Australian Government framework for protective security policy. It provides guidance to support the effective implementation of policies across the areas of security governance, personnel security, physical security, and information security.
<b>NIST</b> National Institute of Standards and Technology Cybersecurity Framework ( <b>NIST</b> )	This Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risks.
<b>VPDSSE</b> Victorian Protective Data Security Standards Element ( <b>VPDSSE</b> )	For organisations that determine the VPDSS Element (element) is descriptive and inclusive enough to be used as a control.
<b>Other</b>	<p>This field can be used to denote an alternative control reference (i.e. select the drop-down 'Other') from those offered in the pre-populated drop-down list.</p> <p><b>Please note:</b> If 'Other' is selected, the organisation will be required to use the text box below the corresponding Standard. If 'Other' is selected for multiple elements, please ensure the organisation describe the alternative control reference and the element it applies to.</p>

### Example of 'Other' and mandatory commentary

An organisation has selected an alternative supporting control library reference for E10.010.

Given that this supporting control library is not listed in the drop down options on the PDSP form, they must select 'Other' and then use the free text field at the end of the Standard to list the element (E10.010) and the title of the alternative supporting control library / reference material (in this case AS4811: 2022).

Use this space to provide any additional commentary (500 character limit)

- Supporting Control Library: Other**  
If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- Status: Not Applicable**  
If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

E10.010 - AS 4811:2022

E10.010 - AS 4811:2022

### Status

The status field reflects how the organisation is tracking against the implementation of a particular element, at the time of PDSP submission.

### How to select the most appropriate status

Organisations must assess the status of each element, critically considering all components.

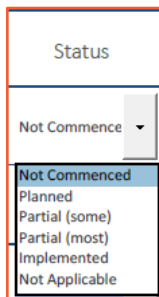
Some elements contain multiple activities and / or components.

VPDSS Standard 2 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commenced	

The implementation status should reflect the degree to which an organisation has successfully addressed each aspect of an element.

E.g. If an organisation has implemented some components of an element (not all), the status of *Partial (some)*, or *Partial (most)* may be appropriate.

#### Example



A screenshot of a web form showing a 'Status' drop-down menu. The menu is open, displaying the following options: 'Not Commenced', 'Not Commenced Planned', 'Partial (some)', 'Partial (most)', 'Implemented', and 'Not Applicable'. The 'Not Commenced' option is currently selected.

If the element is deemed **Applicable**, select from the available drop-down implementation status options.

A description of each of the status options is provided in the following table.

Status	Description
<b>Not Commenced</b>	The organisation has not yet defined or planned the work needed to meet the element.
<b>Planned</b>	The organisation has a program of work in place that includes work to meet the requirement; and the program is appropriately planned and resourced.
<b>Partial (some)</b>	The organisation has commenced aspects of this element with some activities finalised, but additional work needs to be undertaken.
<b>Partial (most)</b>	Most aspects of this element have been implemented. However, activities are not fully completed or have not been fully shifted to business-as-usual ( <b>BAU</b> ).
<b>Implemented</b>	The organisation currently meets all aspects of the element, and this has shifted to a BAU activity.

#### How to determine if an element is *Not Applicable*

As a rule, most elements will apply to most Victorian government organisations, however there will be some scenarios where an organisation may assess an element as *Not Applicable*.

To determine whether an element is applicable, the organisation must first assess if by implementing this particular element (control) helps addresses an identified risk.



Note: These risks should have been:

- identified and considered under the SRPA process; and
- documented in the organisation's risk register.

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

If the element is deemed *Not Applicable* (i.e., the organisation determines that there is no related information security risk that needs to be managed), select the implementation status of 'Not Applicable' from the drop-down list.

Status	Description
Not Applicable	There is no related information security risk that needs to be managed.

### Example of 'Not Applicable' and mandatory commentary

**Please note:** If the status of 'Not Applicable' is selected for any of the elements, organisations **must** use this field to provide a rationale as to why this is so.

Use this space to provide any additional commentary (500 character limit)

- **Supporting Control Library: Other**  
If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- **Status: Not Applicable**  
If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

E1.120 - Organisation does not operate Industrial Automation and Control Systems (IACS).  
E1.130 - Organisation does not operate Industrial Automation and Control Systems (IACS).

E1.120 - Organisation does not operate Industrial Automation and Control Systems (IACS).  
E1.130 - Organisation does not operate Industrial Automation and Control Systems (IACS).

## Proposed Completion Date

Proposed completion date refers to the estimated date that the organisation believes all activities/components of the element will be finalised. This column is used to prioritise the list of activities by financial year.

VPDSS Standard 2 Elements		Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not Commenced	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commenced	

Proposed Completion (financial year)

▼

2024/ 2025  
2025/ 2026  
2026/ 2027  
2027/ 2028  
2028+  
Completed/ Ongoing

### How to select the most appropriate completion date

Select the appropriate completion date from the drop-down list.

The table below depicts the:

- relationship between the implementation status of an element,
- the degree to which all the activities/components of the element will be implemented; and
- by when.

Status	Proposed completion date
Not Commenced	If the activities are yet to be completed, select the financial year all activities/components of the element are expected to be implemented.
Planned	
Partial (some)	
Partial (most)	If the organisation has several programs or activities that address different aspects/components of the element spanning multiple years, please select the latest completion date available.
Implemented	If all activities/components of the element have been completed, select ' <b>Completed/Ongoing</b> ' in this field.

## Maturity Assessment

A maturity assessment is conducted at a whole of Standard level, indicating the maturity level of the organisation's security practices that support the Standard.

The maturity assessment process prompts organisations to engage in critical discussions around perceived areas of strength and opportunities for improvement. Maturity ratings can be used as a guide to help direct information security investment to mature the organisation's security capability.

The nature of capability maturity models means that not every organisation will need to achieve the highest maturity level for each of the Standards. Maturity levels will be influenced by economic, efficient, and effective use of the resources available to the organisation, along with their risk appetite and tolerance.

VPDSS Standard 1 Maturity Assessment

Current	2026 Target	2028 Aspiration
<div></div>	<div></div>	<div></div>

### How to conduct a maturity assessment at a whole of Standard level

To complete this section of the PDSP form, the organisation needs to have first assessed the implementation status of each element under the Standard.

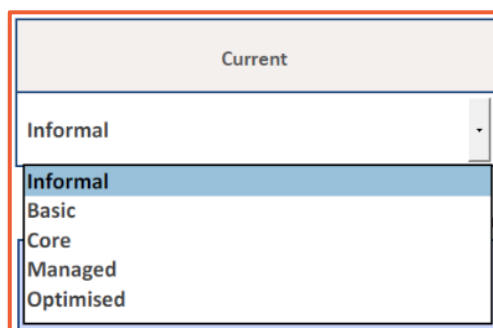
Some areas of the organisation may be operating at a higher maturity level, whereas other areas may require significant uplift. These variances in maturity should be considered when assessing the overall maturity level of the entire organisation against the Standard.

In some instances, this maturity rating may be determined by a simple average. In other instances, a weighted average may be more appropriate, accounting for the sensitivity and/or significance of the information asset and/or information system. Ultimately, the overall maturity rating should be something that best represents the maturity rating of that Standard for the organisation. OVIC recommends documenting the method used throughout the maturity rating assessment to provide a level of consistency and continuity on future PDSPs.

Organisations should be mindful of the sequencing of the elements (especially some of the earlier elements) as the implementation status of some of these will influence the selection of the organisation's maturity rating for each Standard.

In addition to providing a maturity assessment for the '**Current**' year, organisations are also asked to estimate a state of maturity for two- and four-years' time (e.g., a '**Target**' state and an '**Aspiration**' rating).

Conduct a maturity assessment and select a maturity rating from the available drop-down options.



The organisation must select a maturity rating for:

- Current;
- Target (2-year goal); and
- Aspiration (4-year goal).

To help organisations contextualise these maturity levels, corresponding maturity descriptions are provided<sup>1</sup> in the table below.

As each maturity level builds on the previous (i.e., to move from an INFORMAL maturity level to a BASIC maturity level, all aspects of the INFORMAL maturity description must be met before progressing to BASIC), organisations must finalise all aspects of the prior maturity level before reporting advancement to the next.



<sup>1</sup> adapted from New Zealand Protective Security Requirements (PSR).

Maturity Level	Description
<b>Informal</b>	<p>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.</p> <p>Where practice is good, it reflects the expertise and effort of individuals rather than institutional knowledge. There may be some confidence that security-related activities are performed adequately, however this performance is variable, and the loss of key staff may significantly impact capability and practice.</p>
<b>Basic</b>	<p>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 ‘<b>informal</b>’ level, at least within individual business units.</p> <p>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.</p>
<b>Core</b>	<p>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.</p>
<b>Managed</b>	<p>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.</p> <p>In addition to meeting VPDSS requirements, the organisation also implements many optional ‘better practice’ requirements in response to its risk assessment.</p>
<b>Optimised</b>	<p>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.</p> <p>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.</p>

### Example

The following is a working example of a maturity assessment, at a whole of Standard level.

Step 1	Assess the <u>implementation status of each element</u> that falls under the Standard
	<p><b>Example element:</b> VPDSS E1.010</p> <p>The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.</p> <ul style="list-style-type: none"> <li>VPDSS E1.010 is a foundational element under Standard 1. All subsequent elements build on the foundational aspects of this element (e.g., establishing security documentation).</li> <li>In this example Organisation X assesses their implementation status to be <b>‘Not Commenced’</b>.</li> <li>This means that Organisation X is yet to define or plan the work needed to meet the requirement of this element.</li> <li>The organisation continues to assess the implementation status of the other elements under Standard 1.</li> </ul>
Step 2	Conduct a whole of Standard <u>maturity assessment</u>
	<p>Critically consider aspects of each element and the organisation’s alignment to the maturity descriptors</p> <ul style="list-style-type: none"> <li>After nominating an implementation status for each of the elements under Standard 1, Organisation X can now assess their maturity at a whole of Standard level.</li> <li><i>Organisation X</i> considers some key words from the maturity descriptors to see if they align with the requirements set out in E1.010.</li> </ul>

- The Informal maturity descriptor notes that organisations at this level typically have “ad-hoc and undocumented [processes]”, a “lack of consistent planning”, and “where practice is good it reflects the expertise and effort of individuals rather than institutional knowledge”.
- Given *Organisation X* reported VPDSS E1.010 implementation status as ‘**Not Commenced**’, and VPDSS E1.010 calls for organisations to formalise foundational requirements (including having security documentation), an Informal maturity rating may be an appropriate selection for this Standard, even if Organisation X has successfully implemented other elements for this Standard. This is due to the foundational aspects of the Standard having not been met.

## Optional Field

Use this space to provide any additional commentary around the organisation's implementation of the Standard.

This field is optional and free-text and there is a 1500-character limit.

Use this space to provide any additional commentary 1500 character limit

- **Supporting Control Library: Other**  
If 'Other' is selected for any of the above elements, use this space to list the title of the alternative supporting control library / reference material and the particular element it relates.
- **Status: Not Applicable**  
If the status of 'Not Applicable' is selected for any of the above elements, use this space to provide a rationale as to why.
- Any comments around the organisation's implementation of this Standard (optional).

## Part B – Agency Head Executive Summary

Under this section of the PDSP form, organisations are asked to provide details of relevant contacts within the organisation and an outline of the Portfolio/Department in which the organisation resides.

### Name of public sector agency or body

Image Ref.	Field Type	Description
<b>A</b>	Free text	Enter the organisation's name here.

### Name of public sector body Head

Image Ref.	Field Type	Description
<b>B</b>	Free text	Enter the name and contact details of the Head of the Victorian government department, authority, agency, or body identified as an applicable organisation under Part 4 of the PDP Act (e.g., Department Secretary, CEO).

### Information Security Lead

Image Ref.	Field Type	Description
<b>C</b>	Free text	Enter the name and contact details of the nominated organisational contact for the VPDSS.



#### What is an Information Security Lead (ISL)?

An ISL acts as a central point of contact for OVIC, helping deliver important information security messages and updates relating to the Framework and Standards. They can also help coordinate or guide the implementation of the Standards on behalf of the organisation. There is no set role that this function should be assigned to, however it should be someone who can influence good information security outcomes for the organisation.



OFFICIAL

Part B - Agency Head Executive Summary

Name of public sector agency or body

Public sector body Head  
(e.g., Department Secretary, CEO)

Full Name

Position Title

Phone Number

Email Address

Postal Address

Information Security Lead  
(The organisation's nominated contact regarding the VPDOS)

Full Name

Position Title

Phone Number

Email Address

Postal Address

In which part of the organisation does the ongoing management of the information security program reside?

D

Name of the Victorian government portfolio in which the organisation operates

E

Freedom of Information | Privacy | Data Protection

30

OFFICIAL

In which part of the organisation does the ongoing management of the information security program reside?

Image Ref.	Field Type	Description
<div>D</div>	Drop-down menu	<p>Choose the most appropriate response from the drop-down selections.</p> <p>Whilst the completion of an organisation’s PDSP will likely require input from all areas of the organisation, this field refers to the area of the organisation responsible for coordinating this program of work.</p> <p>If the responsible area for the ongoing management of the information security program is not among the available drop-down options, please select <b>‘Other (please elaborate in executive summary)’</b> and provide a quick description in the executive summary on the next page.</p>

Name of the Victorian government portfolio in which the organisation operates

Image Ref.	Field Type	Description
<div>E</div>	Drop-down menu	<p>Select the related portfolio/department that the organisation falls under from the drop-down menu.</p> <p>If the Victorian government portfolio is not among the available drop-down options, please select <b>‘Other (please elaborate in executive summary)’</b> and provide a quick description in the executive summary on the next page.</p>

Freedom of Information | Privacy | Data Protection

33

### Security program executive summary from the past 24 months

Image Ref.	Field Type	Description
<b>F</b>	Free text (2500-character limit)	<p>Use this free text field to highlight a summary of key information security achievements from the past 24 months. These achievements are a good way to highlight items of interest to the public sector body Head and to OVIC.</p> <p>Whilst there is no set way to complete this section, include enough detail for OVIC to gain sufficient insight into the security program of the organisation and understand the progress has been made in information security capability. Topics could include major projects that the organisation has undertaken, high-level summaries of the organisation's incidents, changes to the organisation's risk profile, significant events for the organisation, etc.</p> <p><b>Note:</b> Further information regarding the implementation of the VPDSS can be provided in the free text fields under each Standard.</p>

### Challenges or barriers

Image Ref.	Field Type	Description
<b>G</b>	Check box(es) and free text (1000-character limit)	<p>Use this section to highlight relevant items that the public sector body Head and/or OVIC should be aware of that have inhibited the organisation's implementation of the Standards.</p> <p>If there are additional items to be added (beyond the available check boxes), check '<b>Other</b>' and note these in the free text field below.</p>

OFFICIAL

Organisation Profile Assessment

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

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

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 (totaling 100%) of the organisation's information assets:

Protective Marking	Percentage
BIL 1 (Official)	0 %
BIL 2 (Official: Sensitive)	0 %
BIL 3 (Protected)	0 %
BIL 3-4 ([security classification]// Cabinet-In-Confidence)	0 %
BIL 4 (Secret)	0 %
BIL 5 (Top Secret)	0 %
Percentage of information not assessed	0 %
Percentage of information marked using a former scheme or different scheme	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?

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

Internal Audit, External Audit, Self-Assessed

Additional comments (Optional)


Freedom of Information | Privacy | Data Protection

OFFICIAL

## Organisational Profile Assessment (OPA)

Under this section of the PDSP, organisations are asked to answer several mandatory questions that provide insights into the profile of the organisation.

### Number of employees within the organisation


Image Ref.	Field Type	Description
	Numerical free text	Record the approximate full-time equivalent staff members, contractors, and volunteers in each of the fields.



### Does the organisation have board members?

Board members should also be recorded in this section of the OPA.

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

Image Ref.	Field Type	Description
	Drop-down menu	Select the most appropriate response ( <b>yes</b> , <b>no</b> , or <b>unsure</b> ) based on the organisation's systems.



### What is meant by IACS?

A collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.

These systems include but are not limited to:

- industrial control systems, including distributed control systems (**DCSs**), programmable logic controllers (**PLCs**), remote terminal units (**RTUs**), intelligent electronic devices, supervisory control and data acquisition (**SCADA**), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system (**SIS**) functions, whether they are physically separate or integrated);
- associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems; and

- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

OFFICIAL

Organisation Profile Assessment

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

Number of employees within the organisation

Full-Time Equivalent

Contractors

Volunteers

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 (totaling 100%) of the organisation's information assets:

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

Additional comments (Optional)

Freedom of Information | Privacy | Data Protection

OFFICIAL

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

Image Ref.	Field Type	Description
J	Drop-down menu	Select the most appropriate response ( <b>yes</b> , <b>no</b> , or <b>unsure</b> ) based on the organisation's information.  To assist in answering this section, refer to the organisation's Information Asset Register which is required under <b>VPDSS E2.020</b> and <b>E2.040</b> .



**What is meant by a BIL 3?**  
BILs present scaled impacts describing the harm or damage to government operations, organisations, or individuals, resulting from a compromise of the confidentiality, integrity and/or availability of public sector information. Information assessed as BIL 3 would be expected to cause *major* harm/damage.

For further information about BIL assessments refer to OVIC's [Practitioner Guide: Assessing the Security Value of Public Sector Information](#) and the [VPDSF BIL Table](#).

**Note:** If the organisation does obtain, generate, receive, or hold information at BIL 3 or higher, heightened security controls must be considered by the business.

OFFICIAL

Organisation Profile Assessment

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

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

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 (totaling 100%) of the organisation's information assets:

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

How did the organisation validate the PDSP prior to submission to OVIC? Internal Audit, External Audit, Self-Assessed. Additional comments (Optional) 800 character limit.

Freedom of Information | Privacy | Data Protection

OFFICIAL

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

Image Ref.	Field Type	Description
 K	Numerical free text	Insert an approximate percentage breakdown in the respective fields. To assist in answering this section, refer to the organisation's Information Asset Register (IAR) required under <b>VPDSS E2.020 and E2.040</b> .




### What are protective markings?


Protective markings are security labels assigned to public sector information and directly correspond to outcomes of a confidentiality assessment. To help populate this section, organisations could refer to their IAR or information/records management systems, offering an approximate breakdown of assets and associated protective markings.

For more information refer to OVIC's [Practitioner Guide: Protective Markings](#)

## Percentage of information not assessed

Image Ref.	Field Type	Description
 L	Numerical free text	If the organisation is yet to undertake an information security value assessment for all <b>active</b> information assets, provide an indicative percentage of the information assets that are yet to be assessed.

## Percentage of information marked using a former scheme or different scheme

Image Ref.	Field Type	Description
 M	Numerical free text	If the organisation has <b>active</b> information assets <b>marked under a former or different scheme</b> (i.e. those that are yet to be reassessed and re-marked under the current protective marking scheme), provide an indicative percentage in this field.



### What is calculated to get the total protective marking breakdown?

The current PDSP form does not automatically calculate the total breakdown. Organisations should manually check over fields K, L and M to ensure they come to a total of 100%.

OFFICIAL

Organisation Profile Assessment

This section assists ONIC's understanding of the organisation's security profile.

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

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 (totaling 100%) of the organisation's information assets:

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

Information Security Incidents: How many information security incidents were recorded in the organisation's internal incident register over the last 24 months? N

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 ONIC?

Internal Audit: External Audit: Self-Assessed:

Additional comments (Optional) 500 character limit

Freedom of Information | Privacy | Data Protection

OFFICIAL

### How many information security incidents were recorded in the organisation's internal incident register over the last 24 months?

Image Ref.	Field Type	Description
N	Numerical free text	<p>To complete this field, the organisation needs to understand the number of information security incidents that were:</p> <ol style="list-style-type: none"><li>1. <b>recorded</b> (documented) in its internal incident register; and</li><li>2. occurred in the last <b>24 months</b>.</li></ol> <p>To assist in answering this section, refer to the organisation's information security incidents register as required under <b>VPDSS E6.040</b>.</p>



#### What qualifies as an information security incident?

An information security incident refers to one, or multiple related, identified information security events that can harm/damage an organisation, its assets, individuals or compromise its operations.

Information security incidents may take many forms. These include but are not limited to compromises of electronic or physical (e.g., printed, photographs, recorded information either audio or video) information or verbal discussions.

**Note:** Under element **E6.040** the organisation records information security incidents in a register.

**OFFICIAL**

**Organisation Profile Assessment**

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

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

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 (totaling 100%) of the organisation's information assets:

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

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?

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?

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

Internal Audit, External Audit, Self-Assessed

Additional comments (Optional)

Freedom of Information | Privacy | Data Protection

**OFFICIAL**

Of these incidents, how many affected information assets of a BIL 2 or higher?

Image Ref.	Field Type	Description
	Numerical free text	To complete this field the organisation needs to understand the security value of the information (expressed as a BIL) impacted by the incident.  List the total number of incidents where the information affected by the incident was assessed as BIL 2 or higher.



#### What is meant by a BIL 2?

BILs present scaled impacts describing the harm or damage to government operations, organisations, or individuals resulting from a compromise of the confidentiality, integrity and/or availability of public sector information. Information assessed as BIL of 2 would be expected to cause limited harm/damage.

For further information about BIL assessments, refer to OVIC's [Practitioner Guide: Assessing the Security Value of Public Sector Information](#) and the [VPDSF BIL Table](#).

**Note:** Under **E9.010** information security incidents that have resulted in a compromise of information assessed at a BIL 2 or higher, must be reported to OVIC.

**OFFICIAL**

Organisation Profile Assessment

This section assists CIVIC's understanding of the organisation's security profile.

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

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 (totaling 100%) of the organisation's information assets:

BIL	Protective Marking	Percentage
BIL 1	OFFICIAL	0 %
BIL 2	OFFICIAL: Sensitive	0 %
BIL 3	PROTECTED	0 %
BIL 3-4	[security classification]// Cabinet-in-Confidence	0 %
BIL 4	SECRET	0 %
BIL 5	TOP SECRET	0 %
Percentage of information not assessed		0 %
Percentage of information marked using a former scheme or different scheme		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?

How did the organisation validate the PDSP prior to submission to CIVIC? Internal Audit, External Audit, Self-Assessed. Additional comments (Optional) 200 character limit.

Freedom of Information | Privacy | Data Protection

**OFFICIAL**

## How many third-party arrangements currently have direct access to the organisation's information and information systems?

Image Ref.	Field Type	Description
	Numerical free text	<p>List the number of third-party arrangements where the third party currently has direct access to the organisation's information and information systems.</p> <p>If the organisation has a register of third-party arrangements (e.g., contracts, memorandums of understanding (<b>MOUs</b>), and information sharing agreements), this can be helpful in identifying which third parties may have direct access to public sector information.</p> <p>To assist in answering this section, refer to the organisation's third-party arrangements register as required under <b>VPDSS E8.050</b>.</p>



### What is meant by 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.



### What is meant by third-party?

Any person or entity external to the organisation. This can include another organisation (public or private), a contracted service provider, or individual.



### What is meant by direct access?

Direct access means the ability, right, or permission to collect (obtain), hold, manage, use (interact with or retrieve), disclose, or transfer public sector information (data) from information holdings or systems. The viewing of information or information systems that has been released in an authorised manner is not considered direct access.



**OFFICIAL**

**Organisation Profile Assessment**

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

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

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 (totaling 100%) of the organisation's information assets:

BIL	Protective Marking	Percentage
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 %

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: Additional comments (Optional) 300 character limit


Freedom of Information | Privacy | Data Protection

**OFFICIAL**

### What is the highest protective marking that third parties are accessing?

Image Ref.	Field Type	Description
	Drop-down menu	Choose the most appropriate response from the drop-down selections.  If the organisation has a register of third-party arrangements (e.g., contracts, MOUs, and information sharing agreements), this can be helpful in identifying what type of information third parties are accessing and the highest security value accessed by them.

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

Image Ref.	Field Type	Description
	Check boxes with accompanying free text field option (300-character limit)	Check the most appropriate box or note the method used in the ' <b>Additional Comments</b> ' field.  When answering this section consider how the responses provided on the PDSP were checked and confirmed (e.g., confirming the responses are an accurate reflection of the current status and organisational intent) prior to the submission to OVIC. The drop-down options are:  <b>Internal Audit</b> – the organisation conducted an internal security audit to validate PDSP responses.  <b>External Audit/Review</b> - the organisation contracted a third party to validate PDSP responses.  <b>Self-Assessed</b> - no formal audit or review was undertaken of the PDSP responses.  <b>Additional Comments</b> - If the organisation checked the PDSP prior to submission in another way, or want to provide more information about this, note this in the ' <b>Additional Comments</b> ' free text field.

Generative Artificial Intelligence

1. Does your organisation use Generative Artificial Intelligence (Gen AI)? S

If you have selected *Planning* or *Yes*:

a. Nominate which tools are proposed or in use:

ChatGPT ☐ If 'Other', specify any additional tools:

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation:

Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types:

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation:

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation? T

If you have selected *Planning* or *Yes*:

a. Nominate the Gen AI tools being proposed or in use by the CSP:

ChatGPT ☐ If 'Other', specify any additional tools:

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into LLMs by the CSP:


Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types:

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP:

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

33

## Does your organisation use Generative Artificial Intelligence (Gen AI)?


Image Ref.	Field Type	Description
	Drop-down menu	Choose the most appropriate response from the drop-down selections. If either <i>No</i> or <i>Unsure</i> are selected, no further responses are required, proceed to Question 2 under this section.



### What is Generative AI?

Algorithms, derived from machine learning, that “learn from training data and can be used to create content with similar characteristics.

## Nominate which tools are proposed or in use

Image Ref.	Field Type	Description
	Check boxes with accompanying free text field option (300-character limit)	<p>Check the corresponding boxes against the relevant tool(s) if either <i>Yes</i> or <i>Planning</i> were selected.</p> <ul style="list-style-type: none"> <li>If the tool is not listed, select <i>Other</i> and specify any additional tool(s) in the space provided.</li> <li>If the tool is unknown at this stage, select <i>Other</i> and specify this in the space provided.</li> </ul> <p><b>N.B.</b> Multiple tools can be selected.</p>

Generative Artificial Intelligence

1. Does your organisation use Generative Artificial Intelligence (GenAI)? ☐

If you have selected *Planning* or *Yes*:

a. Nominate which tools are proposed or in use:

ChatGPT ☐ If 'Other', specify any additional tools:

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation.

Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types:

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation? ☐

If you have selected *Planning* or *Yes*:

a. Nominate the GenAI tools being proposed or in use by the CSP:

ChatGPT ☐ If 'Other', specify any additional tools:

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into LLMs by the CSP.


Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types:

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP.

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

33

### Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation

Image Ref.	Field Type	Description
	Check boxes with accompanying free text field option (300-character limit)	<p>Check the corresponding boxes noting the information type(s) that are proposed, or in use, as inputs into LLMs within your organisation.</p> <ul style="list-style-type: none"> <li>If the information type is not listed, select <i>Other</i> and specify any additional type(s) in the space provided.</li> <li>If the information type is unknown at this stage, select <i>Other</i> and specify this in the space provided.</li> </ul> <p>N.B. Multiple information types can be selected.</p>




#### What are Large Language Models?

A subset of generative AI, based on transformer networks.

A transformer is a type of artificial intelligence model that learns to understand and generate human-like text by analysing patterns in large amounts of text data.

### Select the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation

Image Ref.	Field Type	Description
	Check boxes	<p>Nominate the assessed BIL rating(s) of public sector information used as an input into the LLM.</p> <p>N.B. Multiple BIL ratings can be selected.</p>

Generative Artificial Intelligence

1. Does your organisation use Generative Artificial Intelligence (GenAI)? OFFICIAL

If you have selected *Planning* or *Yes*:

a. Nominate which tools are proposed or in use:

ChatGPT ☐ If 'Other', specify any additional tools:

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation.

Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types:

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation? OFFICIAL

If you have selected *Planning* or *Yes*:

a. Nominate the Gen AI tools being proposed or in use by the CSP:

ChatGPT ☐ If 'Other', specify any additional tools:

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into LLMs by the CSP.


Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types:

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP.


BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

33

Do any of your contracted service providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed, or transferred on behalf of the organisation?

Image Ref.	Field Type	Description
	Drop-down menu	Choose the most appropriate response from the drop-down selections. If either <i>No</i> or <i>Unsure</i> are selected, no further responses are required.

Nominate the Gen AI tools being proposed or in use by CSPs:

Image Ref.	Field Type	Description
	Check boxes with accompanying free text field option (300-character limit)	<p>Check the corresponding boxes against the relevant tool(s) if either <i>Yes</i> or <i>Planning</i> were selected.</p> <ul style="list-style-type: none"> <li>If the tool is not listed, select <i>Other</i> and specify any additional tool(s) in the space provided.</li> <li>If the tool is unknown at this stage, select <i>Other</i> and specify this in the space provided.</li> </ul> <p>N.B. Multiple tools can be selected.</p> <p><b>Caveat.</b> This question relates only to the use of Gen AI by CSPs for public sector information collected, held, used, managed, disclosed, or transferred on behalf of the organisation.</p>

OFFICIAL

Generative Artificial Intelligence

1. Does your organisation use Generative Artificial Intelligence (GenAI)? ☐

If you have selected *Planning* or *Yes*:

a. Nominate which tools are proposed or in use:

ChatGPT ☐ If 'Other', specify any additional tools.

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into Large Language Models (LLMs) within your organisation.

Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types.

c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs within your organisation.

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐

2. Do any of your Contracted Service Providers (CSPs) use Gen AI, in respect of public sector information collected, held, used, managed, disclosed or transferred on behalf of the organisation? ☐

If you have selected *Planning* or *Yes*:

a. Nominate the GenAI tools being proposed or in use by the CSP:

ChatGPT ☐ If 'Other', specify any additional tools.

Google Gemini ☐

Microsoft Copilot ☐

Other ☐

b. Select the types of public sector information proposed or in use as inputs into LLMs by the CSP.

Financial ☐ Legal ☐ Personal ☐ Law Enforcement ☐ Other ☐ If 'Other', specify any additional types.


c. Select one or more of the boxes below to indicate the BIL rating of public sector information proposed or in use as inputs into LLMs by the CSP.

BIL 1 ☐ BIL 2 ☐ BIL 3 ☐ BIL 4 ☐ BIL 5 ☐ Unknown ☐


33

OFFICIAL

### Select the types of public sector information proposed or in use as inputs into LLMs by CSPs

Image Ref.	Field Type	Description
	Check boxes with accompanying free text field option (300-character limit)	<p>Check the corresponding boxes noting the information type(s) that are proposed, or in use, as inputs into LLMs by CSPs.</p> <ul style="list-style-type: none"> <li>If the information type is not listed, select <i>Other</i> and specify any additional type(s) in the space provided.</li> <li>If the information type is unknown at this stage, select <i>Other</i> and specify this in the space provided.</li> </ul> <p>N.B. Multiple information types can be selected.</p> <p><b>Caveat.</b> This question relates only to the use of Gen AI by CSPs for public sector information collected, held, used, managed, disclosed, or transferred on behalf of the organisation.</p>

### Select the BIL rating of public sector information proposed or in use as inputs into LLMs by CSPs

Image Ref.	Field Type	Description
	Check boxes	<p>Nominate the assessed BIL rating(s) of public sector information used as an input into the LLM by CSPs.</p> <p>N.B. Multiple BIL ratings can be selected.</p> <p><b>Caveat.</b> This question relates only to the use of Gen AI by CSPs for public sector information collected, held, used, managed, disclosed, or transferred on behalf of the organisation.</p>

## Part C – Attestation

The purpose of the Attestation is to confirm/reaffirm that the organisation is continuing its program of security activities to address the VPDSS as outlined in the PDSP, including confirmation 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 signed by the public sector body Head and cannot be delegated to another person.

### Incorporation of Standard 9 elements into Attestation

Following stakeholder feedback, responses for Standard 9 Elements have been removed from Part B of the PDSP form and incorporated into the Attestation by the public sector body Head (Part C of the PDSP form).

Image Ref.	Element	Description
	<b>E9.040</b>	This is covered in the Attestation. No response required on page 22 of the PDSP form.
	<b>E9.010</b>	This is covered in the Attestation. No response required on page 22 of the PDSP form.
	<b>E9.030</b>	This is covered in the Attestation. No response required on page 22 of the PDSP form.



#### E9.020

##### How to capture E9.020 in the PDSP form?

This element is satisfied via the submission of a current copy of the PDSP form to OVIC. No further response is required for this element (either on page 22 of the PDSP form or in the Attestation).

OFFICIAL

**Part C - Attestation**

Attestation

Under Part 4 of the *Privacy and Data Protection Act 2014* (PDP Act) and Standard 9 of the Victorian Protective Data Security Standards 2.0 (the Standards), I   attest that <sup>(E9.010)</sup> I am the public sector body Head of   and my organisation:

- has undertaken, or is in the process of undertaking a security risk profile assessment (including assessment/s of any contracted service provider of my organisation, to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector information for my organisation) as required under section 89 of the PDP Act;
- ensures that a contracted service provider does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector information collected, held, used, managed, disclosed or transferred by the contracted service provider for my organisation;
- notifies the Office of the Victorian Information Commissioner of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information and systems with a business impact level (BIL) of 2 (limited) or higher <sup>(E9.010)</sup>;
- has implemented the key activities, or is in the process of planning and implementing key activities, as required by the Standards; and
- upon significant change, submits a reviewed PDSP to the Office of the Victorian Information Commissioner <sup>(E9.010)</sup>

Print name:  

Position:  

Date:  

Freedom of Information | Privacy | Data Protection 33

OFFICIAL

## Completing the Attestation

Image ref.	Option	Data entry	Description
D	1	Free text (soft copy / electronic)	Manually enter the public sector body Head's details in each of the free text fields offered.
	2	Free text (hard copy)	Print a hard copy of the completed PDSP for the public sector body Head to physically review, sign and date with a wet signature.

## Signing the Attestation/PDSP

Image ref.	Option	Data entry	Description
E	1	Soft copy / electronic	Use the Adobe Acrobat Reader Fill & Sign feature to add the public sector body Head's signature into the box provided on the Attestation.
	2	Soft copy / electronic	Insert an image file (e.g. jpg, tiff, bmp) of the public sector body Head's signature into the box provided on the Attestation.
	3	Soft copy / electronic	Type the name of the public sector body Head's signature into the box provided on the Attestation.
	4	Hard copy	Print a hard copy of the completed PDSP for the public sector body Head to physically review, sign and date with a wet signature.  This signed and dated hard copy Attestation may be scanned and combined with the remainder of the PDSP.

## Submission, Next Steps, and Useful Links

### Options for submission

When all mandatory fields on the PDSP have been completed and the public sector body Head has reviewed the form, signed and dated the Attestation the organisation can submit a copy of the PDSP to OVIC via one of the options below.

Note: Remember to retain a copy of the completed PDSP for organisational records.

For PDSPs marked as <b>OFFICIAL</b> and <b>OFFICIAL: Sensitive</b>  <b>Please note:</b> A prior appointment must be made with a member of OVIC's Information Security Unit for option 3.	<b>Option 1</b>	Soft copy / electronic	Send a copy of the completed, signed and dated PDSP to <a href="mailto:security@ovic.vic.gov.au">security@ovic.vic.gov.au</a> (either from the public sector body Head's email address, or the Information Security Lead's email address)
	<b>Option 2</b>	Hard copy	Post a copy of the PDSP in a single opaque envelope with no protective marking labelled on the outside to: PO Box 24274 Melbourne VIC 3001
	<b>Option 3</b>	Hard copy	Hand deliver a copy of the PDSP to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne VIC 3001
For PDSPs marked as <b>PROTECTED</b>  <b>Please note:</b> A prior appointment must be made with a member of OVIC's Information Security Unit for options 4 and 5.	<b>Option 4</b>	Hard copy	Deliver a copy of the PDSP by safe-hand (e.g. delivered in person by an authorised messenger) to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne
	<b>Option 5</b>	Hard copy	Deliver a copy of the PDSP by SCEC-endorsed courier to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne



## Next steps

After submitting the PDSP to OVIC the organisation will receive an email confirming receipt by OVIC's Information Security Unit within 1-15 business days.

Between now and the next OVIC reporting period ensure the organisation continues to:

- monitor the organisation's information security risks;
- alert OVIC to any [significant changes](#) to the organisation's information security risks and/or operating environment;
- notify OVIC of any changes to the organisation's Information Security Lead and/or public sector body Head; and
- report information security incidents through the [Incident Notification Scheme](#).

## Useful links

Title	URL
<b>VPDSS Glossary</b>	<a href="https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-glossary-v2-1/">https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-glossary-v2-1/</a>
<b>Agency Reporting Obligations</b>	<a href="https://ovic.vic.gov.au/information-security/agency-reporting-obligations/">https://ovic.vic.gov.au/information-security/agency-reporting-obligations/</a>
<b>Victorian public sector stakeholders</b>	<a href="https://ovic.vic.gov.au/information-security/agency-reporting-obligations/vps-stakeholders/">https://ovic.vic.gov.au/information-security/agency-reporting-obligations/vps-stakeholders/</a>
<b>Significant Change</b>	<a href="https://ovic.vic.gov.au/data-protection/significant-change-and-protective-data-security-obligations/">https://ovic.vic.gov.au/data-protection/significant-change-and-protective-data-security-obligations/</a>
<b>OVIC Privacy Policy</b>	<a href="https://ovic.vic.gov.au/about-us/internal-policies-procedures-and-registers/privacy-policy/">https://ovic.vic.gov.au/about-us/internal-policies-procedures-and-registers/privacy-policy/</a>
<b>VPDSF BIL Table</b>	<a href="https://ovic.vic.gov.au/information-security/victorian-protective-data-security-framework-business-impact-level-table-v2-1/">https://ovic.vic.gov.au/information-security/victorian-protective-data-security-framework-business-impact-level-table-v2-1/</a>
<b>OVIC Regulatory Action Policy</b>	<a href="https://ovic.vic.gov.au/regulatory-action/regulatory-action-policy/">https://ovic.vic.gov.au/regulatory-action/regulatory-action-policy/</a>
<b>VPDSS Implementation Guidance v2.3</b>	<a href="https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-implementation-guidance/">https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-implementation-guidance/</a>
<b>Implementation Guidance for Industrial Automation and Control Systems Guidance</b>	<a href="https://ovic.vic.gov.au/information-security/information-security-resources/implementation-guidance-for-industrial-automation-and-control-systems/">https://ovic.vic.gov.au/information-security/information-security-resources/implementation-guidance-for-industrial-automation-and-control-systems/</a>
<b>Practitioner Guide: Information Security Risk Management</b>	<a href="https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/">https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/</a>
<b>Practitioner Guide: Assessing the Security Value of Public Sector Information</b>	<a href="https://ovic.vic.gov.au/information-security/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/">https://ovic.vic.gov.au/information-security/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/</a>
<b>Practitioner Guide: Protective Markings</b>	<a href="https://ovic.vic.gov.au/data-protection/practitioner-guide-protective-markings/">https://ovic.vic.gov.au/data-protection/practitioner-guide-protective-markings/</a>
<b>Incident Notification Scheme</b>	<a href="https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/">https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/</a>