

How-to: A guide to completing the 2022 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		January 2022
Review Date		January 2024
Document Version		1.0
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	June 2022	Added definition of ‘Planned’ implementation status

Contents

Introduction	6
How to use this guide	6
Where to start	6
Completing and filling in the 2022 PDSP form.....	7
Breakdown of the 2022 PDSP form	7
Field character limits within the PDSP form	7
Frequently Asked Questions	8
Where can I access a copy of the 2022 PDSP form?.....	8
What is a PDSP?	8
Why do I need a PDSP?	8
When do I have to submit a PDSP?	9
What should I do before I start a PDSP?.....	9
Who should complete the PDSP?	10
Who is responsible for the PDSP?	10
What should I capture in the PDSP?.....	10
How will the information in the PDSP be used and managed?	11
Who can attest and submit the PDSP?	11
What protective marking should I label the PDSP with?.....	12
Why does a protective marking need to be assigned to the PDSP?.....	12
How do I submit a copy of the PDSP to OVIC?	13
What happens if I don't submit a PDSP?	13
Part A - Information security self-assessment and implementation plan	14
VPDSS Elements.....	15

How to read an element.....	15
Example	15
Entity Risk Reference	16
How to provide an entity risk reference.....	16
Example	16
Supporting Control Library	17
How to select the most appropriate supporting control library	17
Example	17
Status	19
How to select the most appropriate status.....	19
Example	19
Proposed Completion Date	21
How to select the most appropriate completion date	21
Examples.....	21
Maturity Assessment	22
How to conduct a maturity assessment at a whole of Standard level	22
Example	24
Optional Field	25
Part B – Agency Head Executive Summary	26
Name of public sector agency or body.....	26
Name of public sector body Head	26
Information Security Lead	26
In which part of your organisation does the ongoing management of your information security program reside?	27
Name of the Victorian government portfolio in which the organisation operates.....	27

Security program executive summary from the past 24 months.....	28
Challenges or barriers.....	28
Organisational Profile Assessment (OPA).....	29
Number of employees within the organisation.....	29
Does the organisation have Industrial Automation and Control System (IACS)?.....	29
Does the organisation obtain, generate, receive, or hold information at Business Impact Level 3 (BIL of 3) or higher?.....	30
Provide an approximate protective marking breakdown of the organisation's information assets.....	31
Percentage of information not assessed	31
Percentage of information marked using a former scheme or different scheme.....	31
Total information assets	32
How many information security incidents were recorded in the organisation's internal incident register over the last 24 months?	32
Of these incidents, how many affected information assets of a BIL 2 or higher?.....	33
How many third-party arrangements currently have direct access to the organisation's information and information systems?	34
What is the highest protective marking that third-parties are accessing?	35
How did the organisation validate the PDSP prior to submission to OVIC?.....	35
Part C – Attestation.....	36
Completing the Attestation	36
Signing the Attestation/PDSP	37
Submission, Next Steps, and Useful Links.....	38
Options for submission	38
Next steps	39
Useful links.....	40

Introduction

How to use this guide

This guide is designed to assist applicable Victorian public sector (**VPS**) agencies in completing the 2022 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:

	INTRODUCTION
	FREQUENTLY ASKED QUESTIONS
	PART A OF THE PDSP FORM
	PART B OF THE PDSP FORM
	PART C OF THE PDSP FORM
	SUBMISSION, NEXT STEPS, AND USEFUL LINKS

This guide sets out each field contained in the 2022 PDSP form and provides an accompanying explanation and/or description.

Where to start

If you are familiar with the process for completing a PDSP you may wish to jump ahead to [PART A OF THE PDSP FORM](#).

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

You may come across some terms in this document that you may be unfamiliar with. Refer to our [VPDSS Glossary](#) for definitions.

Completing and filling in the 2022 PDSP form

The 2022 PDSP form was developed using Acrobat 2020 (20.004.30020). Some functionality of the 2022 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. Avoid using Microsoft Edge to edit or complete the 2022 PDSP form as we have identified compatibility issues with this software and the PDSP form.

Breakdown of the 2022 PDSP form

The 2022 PDSP is a single PDF form comprised of three mandatory parts:

Part		Description
A	Information security self-assessment and implementation plan	<ul style="list-style-type: none">• Outlines the organisation's self-assessed implementation of the elements under each Standard; and• Outlines the organisation's self-assessed maturity level for each Standard.
B	Agency Head executive summary	<ul style="list-style-type: none">• Provides contact information of the public sector body Head and Information Security Lead;• Provides an opportunity for organisations to highlight achievements across the past 24 months and describe any challenges or barriers to the security program; and• Poses a series of questions that form the Organisation Profile Assessment.
C	Attestation	<ul style="list-style-type: none">• Confirms/attests that the organisation is continuing information security activities outlined in their previous Protective Data Security Plan.

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 depending on where you are in the form. Character limits are noted against relevant fields.

If you intend to print the 2022 PDSP, be aware that some of the responses may be cut off when printed due to space restrictions. Where the 2022 PDSP is electronically submitted (unscanned) to OVIC, full responses will be captured, character limits permitting.

Frequently Asked Questions

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

The 2022 PDSP form is available on the [Agency Reporting Obligations](#) webpage on OVIC's website.

What is a PDSP?

A PDSP serves several purposes. It is designed to:

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

The PDSP template provided by OVIC consists of three parts:

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

Why do I need a PDSP?

Section 88 and Section 89 of the *Privacy and Data Protection Act 2014* (**PDP Act**) outline the compliance obligations of VPS organisations with respect to the Standards and require VPS organisations to:

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

A PDSP is useful in validating the organisation's information security capability and confirming that activities are in place to achieve the organisation's desired level of information security maturity.

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

When do I 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">• The deadline for submitting a PDSP is 31 August of the reporting year.• The standard reporting cycle for PDSPs falls on even-numbered years (e.g., 2022, 2024, 2026). <p>Please note: Organisations are still required to submit an annual Attestation to OVIC.</p>
Scenario 2	Out of reporting cycle due to significant change	<p>If your organisation has undergone a ‘significant change’ to its operating environment or its security risks, you may be required to submit an out-of-cycle PDSP.</p> <p>In the event of significant change, contact OVIC to discuss your reporting options.</p> <p>Please note: 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 I do before I start a PDSP?

Before developing a PDSP, you need 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 (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 your Portfolio/Department if you 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 across the business.

The public sector body Head should be engaged early and updated as needed. Subject matter experts across different workgroups (e.g., Risk, Legal, Information/Records Management, Information Technology, Human Resources/People and Culture, Corporate, Finance, Facilities, etc.) will provide important inputs into PDSP responses for the various Standards.

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. The person completing the PDSP will require input from subject matter experts across the business.

Who is responsible for the PDSP?

Under the PDP Act, a public sector body Head must ensure that a PDSP is developed 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 I capture in the PDSP?

PDSPs submitted to OVIC should cover security activities across 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.

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

OVIC has a responsibility to provide Ministers and the public with assurance regarding information security capabilities across the Victorian public sector. The information provided in the 2022 PDSP will be used as an input in determining an organisation's progress towards meeting its information security objectives.

Insights and select content drawn from 2022 PDSP submissions will form the basis of reporting to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

Additionally, the OVIC Information Security Unit will:

- use the self-assessed report to help plan engagement and support activities;
- use information to inform assurance activities; and
- provide feedback to 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, distributing 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 2022 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 in Part C of the 2022 PDSP form. Under the PDP Act, the public sector body Head is responsible for providing a copy of the organisation's PDSP to OVIC.

What protective marking should I label the PDSP with?

When drafting PDSP responses, conduct an initial confidentiality assessment to apply an interim protective marking. This will inform handling protections on the 2022 PDSP while responses are being collated and finalised.

Once the 2022 PDSP is complete, conduct an updated final confidentiality assessment to inform the most appropriate protective marking for the 2022 PDSP before sending a copy to OVIC.

When conducting your 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. 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 your organisation's contextualised Business Impact Level (BIL) table or the [VPDSF BIL table](#) and/or [VPDSF BIL App](#).

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

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

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

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

How do I 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 I don't submit a PDSP?

In-scope public sector agencies or bodies 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 2022 PDSP, organisations must self-assess the implementation of each Standard and supporting elements.

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

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

At a whole of Standard level, you must indicate:

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

An optional 'additional commentary' field is also provided at the end of each Standard. This space can be used by organisations to provide any additional commentary around the organisation's implementation of the Standard.

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

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 Commenced	
E7.020 The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.			Not Commenced	
E7.030 The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).			Not Commenced	

VPDSS Standard 7 Maturity Assessment

Current	2024 Target	2026 Aspiration
Informal	Informal	Informal

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

Freedom of Information | Privacy | Data Protection

OFFICIAL

17

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 V2.1](#) 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 Commence	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commence	

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 (IAR) 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"> • Identified the organisation's information assets; • Documented its information assets in an IAR; • Actively maintained the IAR; and • Consulted with the organisation's stakeholders throughout this process (this includes internal and external stakeholders).

Entity Risk Reference

An Entity Risk Reference refers to an internal reference used by an organisation to track specific information security risks. It can be expressed in whatever form, format, or way that makes sense to the organisation. The purpose of this field is to identify the internal organisational risk reference(s) that the elements (supporting control(s)) address or relate to, and to demonstrate the risks identified through the SRPA process.

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 Commence ▼	▼
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.		▼	Not Commence ▼	▼

Depending on different organisations' risk management framework and processes, information security risks should be recorded and managed via an organisational risk register. It is expected that an organisation has at least one information security risk recorded in its risk register, helping track and manage information security risks on an ongoing basis. For further guidance on risk management please refer to the [Practitioner Guide: Information Security Risk Management](#).

How to provide an entity risk reference

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

Example

Entity Risk Reference(s)
RISK 123

Refer to your organisation's risk register and copy the relevant risk reference documented within it.

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

Supporting Control Library

Each element has been derived from control references and provides guidance on security controls 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.

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 Commence	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commence	

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. Your organisation may have your own documented internal control library. If so, or if you are 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' above a drop-down menu. The menu is open, displaying a list of options: 'ISO 27000 series', 'ISM', 'PSPF', 'NIST', 'VPDSS', and 'Other'. The 'Other' option is highlighted at the bottom of the list.

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
ISO 27000 series	The ISO 27000 series comprises mutually supporting information security standards that together provide a globally recognised framework for best-practice information security management.
ISM Australian Government Information Security Manual (ISM)	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.
PSPF Protective Security Policy Framework (PSPF)	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.
NIST National Institute of Standards and Technology Cybersecurity Framework (NIST)	This Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risks.
VPDSSE Victorian Protective Data Security Standards Element (VPDSSE)	For organisations that determine the VPDSS Element (element) is descriptive and inclusive enough to be used as a control.
Other	This field can be used to enter an alternative control reference from those offered in the pre-populated drop-down list.

Please note: When you select ‘**Other**’, a new field will appear to the left when you click elsewhere on the page or hit the tab button (as shown in the image to the right).

You will be prompted to enter an alternative control reference in this new field. Type in the title of this reference and press ‘**Add**’ to add this response to the list of available drop-down options and ensure this is selected before continuing to the next element.

The screenshot shows a form titled "VPDSS Standard 2 Elements". It has three main sections: "Entity Risk Reference(s)", "Supporting Control Library", and "Other". The "Supporting Control Library" section contains a dropdown menu with "Other" selected. The "Other" section is a text input field with "E2.010" entered. An "Add" button is located between the "Supporting Control Library" and "Other" sections.

Status

Status reflects how the organisation is progressing or tracking against the implementation of a particular element at the time of PDSP submission.

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 select the most appropriate status

To complete this section of the 2022 PDSP organisations need to consider each element outlined under the Standard.

As a rule, most elements will apply to majority of Victorian government organisations, however there will be some scenarios where an organisation may assess an element as not applicable.

1. Make sure all components of the element are read and understood. Some elements contain multiple activities/requirements, so it's important to critically consider all aspects of the element, as this may influence the selection of an implementation status. Whether your organisation has implemented some but not all these activities will inform the status selected for this element.
2. Assess whether implementing this element (control) is addressing an identified risk. These risks should have been identified and considered under the SRPA process and documented in your organisation's risk register.

Example

A screenshot of a web form showing a dropdown menu for the 'Status' field. The dropdown is open, displaying six options: 'Not Applicable', 'Not Commenced', 'Planned', 'Partial (some)', 'Partial (most)', and 'Implemented'. The option 'Partial (most)' is currently selected and highlighted with a blue background.

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

If the element is deemed Not Applicable (i.e., you determine 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.

A description of the Not Applicable status option is provided in the table below.

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

Please note: When you select the status of '**Not Applicable**' a new field will appear when you click elsewhere on the page or hit the tab button.

You must provide a rationale explaining why the element was assessed as being not applicable as shown in the image to the right.



For the three supporting Elements under Standard 9 (**E9.010**, **E9.020** and **E9.030**) the implementation status of the '**Not Applicable**' and '**Not Commenced**' are invalid responses (as these are mandatory elements) and are not available in the drop-down options for this Standard.

Proposed Completion Date

Proposed completion date refers to the estimated date that the organisation believes all activities/aspects 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 Commence	
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not Commence	

How to select the most appropriate completion date

Proposed Completion (financial year)

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

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

The table below depicts the relationship between the implementation status of an element and the degree to which the activities/aspects 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/aspects of the element are expected to be implemented.
Planned	
Partial (some)	If the organisation has several programs or activities that address the element, spanning multiple years, please select the latest completion date available.
Partial (most)	
Implemented	If all activities / aspects of the element have been completed, select ' Completed/ BAU ' in this field.

Examples

Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
Risk 123	VPDSSE	Not Commenced	2022/ 2023

Entity Risk Reference(s)	Supporting Control Library	Status	Proposed Completion (financial year)
Risk 123	VPDSSE	Implemented	Completed/ BAU

Maturity Assessment

A maturity assessment is conducted at a whole of Standard level, indicating the maturity level of certain aspects 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.

VPDSS Standard 2 Maturity Assessment

Current	2024 Target	2026 Aspiration
Informal	Informal	Informal

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

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

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

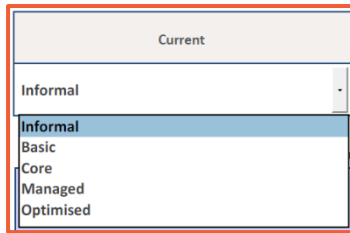
To complete this section of the 2022 PDSP the organisation needs to have first assessed the implementation status of each element under the Standard.

Some areas of your 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.

Organisations should be mindful of the sequencing of the elements (especially some of the earlier or foundational 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.

You must select a maturity rating for:

- Current;
- 2024 Target; and
- 2026 Aspiration.

To help organisations contextualise these maturity levels, the maturity descriptions are provided¹ in the table below. Organisations must finalise all aspects of the prior maturity level before reporting advancement to the next. 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.



Maturity Level	Description
Informal	<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>
Basic	<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 'informal' 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>

¹ adapted from New Zealand Protective Security Requirements (PSR).

Core	Policies, processes, and standards are well defined and are actively and consistently followed across the organisation. Governance and management structures are in place. Risk assessment and management activities are regularly scheduled and completed. Historic performance information is periodically assessed and used to determine where improvements should be made.
Managed	<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>
Optimised	<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 for Standard 1.

Step 1 Assess implementation status of each element in the Standard

Example element: VPDSS E1.010

The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.

- 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).
- In this example *Organisation X* assesses their implementation status to be '**Not Commenced**'.
- This means that *Organisation X* is yet to define or plan the work needed to meet the requirement of this element.
- The organisation continues to assess the implementation status of the other elements under Standard 1.

Step 2 Conduct a whole of Standard maturity assessment

Critically consider aspects of each element and the organisation's alignment to the maturity descriptors

- After nominating an implementation status for all of the elements under Standard 1, *Organisation X* can now assess their maturity at a whole of Standard level.
- *Organisation X* considers some key words from the maturity descriptors to see if they align with the requirements set out in E1.010.
- 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 no character limit.

VPDSS Standard 2 Maturity Assessment		
Current	2024 Target	2026 Aspiration
Informal	Informal	Informal

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

Part B – Agency Head Executive Summary

Under this section of the 2022 PDSP 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
A	Free text	Enter the organisation's name here.

Name of public sector body Head

Image Ref.	Field Type	Description
B	Free text	Enter the name of the head of your 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
C	Free text	Enter your nominated organisational contact regarding the VPDSS.



What is an Information Security Lead?

An information security lead acts as a central point of contact for OVIC, helping deliver important information security messages and updates relating to the Framework and Standards. 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 but 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

Full Name

Position Title

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

Phone Number

Email Address

Postal Address

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

Same as public sector body Head
☐
(Check box optional)

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

29

OFFICIAL

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

Image Ref.	Field Type	Description
D	Drop-down menu with additional free text field option	<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 ‘Other’.</p> <p>Please note: When you select ‘Other’, a new field will only appear when you click elsewhere on the page or hit the tab button. You will be prompted to enter an alternative section of the business in this new field. Type in the area and press ‘OK’ to add this response to the list of available drop-down options and ensure this is selected before continuing to the next field.</p>

Name of the Victorian government portfolio in which the organisation operates

Image Ref.	Field Type	Description
E	Drop-down menu	<p>Select the related portfolio/department that your organisation falls under from the drop-down menu.</p> <p>Please note: When you select ‘Other’, a new field will only appear when you click elsewhere on the page or hit the tab button. You will be prompted to enter an alternative section of the business in this new field. Type in the area and press ‘OK’ to add this response to the list of available drop-down options and ensure this is selected before continuing to the next field.</p>

OFFICIAL

Security program executive summary from the past 24 months (Maximum: 2500 characters)

F

Challenges or barriers

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

☐ Financial
 ☐ External third-party dependencies
☐ Resourcing
 ☐ Machinery of Government
☐ Capability
 ☐ Lack of clarity around roles and responsibilities within the organisation
☐ Legislative
 ☐ Lack of understanding of the Standards
☐ Significant change
 ☐ Other (please elaborate below)

G

Please describe any challenges or barriers towards the implementation of the Standards (Maximum: 2500 characters)

Freedom of Information | Privacy | Data Protection

OFFICIAL

30

Security program executive summary from the past 24 months

Image Ref.	Field Type	Description
F	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, you should include enough detail for OVIC to gain sufficient insight into the security program of your organisation and understand the progress that you have 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>Note: 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
G	Check box(es) and free text	<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 'Other' and note these in the free text field.</p>

Organisational Profile Assessment (OPA)

Under this section of the 2022 PDSP organisations are asked to answer mandatory questions that provide insights into the profile of your organisation.

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 of the organisation's information assets:

BIL	Protective Marking	Count	Percentage
BIL 1	OFFICIAL	0	0%
BIL 2	OFFICIAL: Sensitive	0	0%
BIL 3	PROTECTED	0	0%
BIL 3.4	[security classification]// Cabinet-In-Confidence	0	0%
BIL 4	SECRET	0	0%
BIL 5	TOP SECRET	0	0%
Percentage of information not assessed		0	0%
Percentage of information marked using a former scheme or different scheme		0	0%
Total information assets		0	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

Other

Freedom of Information | Privacy | Data Protection

OFFICIAL

Number of employees within the organisation

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

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

Image Ref.	Field Type	Description
I	Drop-down menu	Select the most appropriate response (yes , no , or unsure) based on your organisations systems.



What is meant by an Industrial Automation and Control System?

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 Equivalents, 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? **J**

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

BIL	Protective Marking	Count	Percentage
BIL 1	OFFICIAL	0	0%
BIL 2	OFFICIAL: Sensitive	0	0%
BIL 3	PROTECTED	0	0%
BIL 3.4	[security classification]// Cabinet-in-Confidence	0	0%
BIL 4	SECRET	0	0%
BIL 5	TOP SECRET	0	0%
Percentage of information not assessed		0	0%
Percentage of information marked using a former scheme or different scheme		0	0%
Total information assets		0	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, Other

Freedom of Information | Privacy | Data Protection

OFFICIAL

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

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



What is meant by a BIL of 3?

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 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 your organisation does obtain, generate, receive, or hold information at Business Impact Level 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.

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

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

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

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

BIL	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
Total information assets		0%

Information Security Incidents

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

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

Third-Party Arrangements

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

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


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

Internal Audit External Audit Self-Assessed Other

Freedom of Information | Privacy | Data Protection

OFFICIAL

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

Image Ref.	Field Type	Description
	Numerical free-text	<p>Insert an approximate percentage breakdown in the respective fields. These figures will automatically tally as you complete the fields and click or tab away from them totalling 100%.</p> <p>To assist in answering this section, refer to your organisation's Information Asset Register (IAR) required under VPDSS E2.020 and E2.040.</p>




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
	Numerical free text	If your organisation is yet to undertake an information security value assessment for all active information assets, provide an indicative percentage in this field.

Percentage of information marked using a former scheme or different scheme

Image Ref.	Field Type	Description
	Numerical free text	If your organisation has active information assets marked under a former or different scheme that are yet to be reassessed and re-marked under the current protective marking scheme, provide an indicative percentage in this field.

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 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 %
Total information assets		0%

Information Security

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

Incidents

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	Other
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


Freedom of Information | Privacy | Data Protection

OFFICIAL

Total information assets

Image Ref.	Field Type	Description
	Numerical (automatic)	This field will automatically calculate based on the entries you have made above. When completed this field should total 100%.

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

Image Ref.	Field Type	Description
	Numerical free text	To complete this field, the organisation needs to understand the number of information security incidents that were: <ol style="list-style-type: none"> recorded (documented) in its internal incident register; and occurred in the last 24 months. If you are unsure leave this field blank.



What qualifies as an information security incident?

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

Information security incidents may take many forms, such as compromises of electronic information held on government systems and services and include information in physical formats (e.g., printed, photographs, recorded information either audio or video) and 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 of the organisation's information assets:

BIL	Protective Marking	Count	Percentage
BIL 1	OFFICIAL	0	0%
BIL 2	OFFICIAL: Sensitive	0	0%
BIL 3	PROTECTED	0	0%
BIL 3.4	[security classification]// Cabinet-In-Confidence	0	0%
BIL 4	SECRET	0	0%
BIL 5	TOP SECRET	0	0%
Percentage of information not assessed		0	0%
Percentage of information marked using a former scheme or different scheme		0	0%
Total information assets		0	0%

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

Incidents: 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, Other

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 impacted by the incident. In response to this question list the total number of incidents where the affected information was assessed as BIL 2 or higher. This number can be approximate.



What is meant by a BIL of 2?

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 meet the threshold of BIL 2 or higher must be reported to OVIC.

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 of the organisation's information assets:

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

Information Security Incidents

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

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

Third-Party Arrangements

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

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	Other
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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 ((MOUs)), and information sharing agreements), this can be helpful in identifying which third parties may have direct access to public sector information.</p>



What is meant by arrangement?

An informal and non-legally binding understanding between the State and a third party. An 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.

Note: Under **E8.050**, the organisation needs to establish, maintain, and review a register of third-party arrangements/agreements (e.g., contracts, MOUs and information sharing agreements).

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 of the organisation's information assets:

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

Information Security Incidents

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

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

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

Arrangements - What is the highest protective marking that third parties are accessing? **R**

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

Internal Audit	External Audit	Self-Assessed	Other
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Freedom of Information | Privacy | Data Protection

OFFICIAL

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

Image Ref.	Field Type	Description
R	Drop-down menu	<p>Choose the most appropriate response from the drop-down selections.</p> <p>If your 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.</p>

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

Image Ref.	Field Type	Description
S	Check boxes with free text field option	<p>Check the most appropriate box or note the method used in the 'Other' field.</p> <p>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:</p> <p>Internal Audit – the organisation conducted an internal security audit to validate PDSP responses.</p> <p>External Audit/Review - the organisation contracted a third party to validate PDSP responses.</p> <p>Self-Assessed - no formal audit or review was undertaken of the PDSP responses.</p> <p>Other - If the organisation checked the PDSP prior to submission in another way, note what method was use in the 'Other' field.</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 and that the organisation has undertaken the SRPA process.

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

In acknowledgement of their obligations under Part 4 of PDP Act the Attestation must be signed by the public sector body Head and cannot be delegated to another person.

Completing the Attestation

Option 1	Optional check box (soft copy)	An optional check box is provided in the Attestation section of the form, which if selected, will populate this section with the public sector body Head as outlined in Part B of the PDSP (Agency Head Executive Summary table). Note: Ensure you click outside the box or tab away from the box to allow the details to populate.
Option 2	Manual data entry (soft copy)	Manually enter the public sector body Head's details in each of the free text fields offered.
Option 3	Manual data entry (hard copy)	Print a copy of the completed PDSP for your public sector body Head to physically sign and date in hard copy form.

OFFICIAL

Part C - Attestation

Attestation

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

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

(Check box optional)

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

AND

Has undertaken a security risk profile assessment or is in the process of undertaking a security risk profile assessment for as required by the Standards, which are issued in accordance with s 86(1) of the *Privacy and Data Protection Act 2014* as part of the Victorian Protective Data Security Framework.

Insert signature here

Print name:

Position:

Date:

Freedom of Information | Privacy | Data Protection

32

OFFICIAL

Signing the Attestation/PDSP

Option 1	Soft copy	<p>Use the Adobe Acrobat Reader Fill & Sign feature to add the public sector body Head’s signature into the box provided.</p> <p>Note: An image file (e.g., soft copy signature) cannot be inserted into the PDSP form as it is locked for editing.</p>
Option 2	Hard copy	<p>Print a copy of the completed PDSP for your public sector body Head to physically sign and date in hard copy form.</p> <p>Note: Scan a copy of the PDSP form and submit to OVIC, retaining a copy for your own records.</p>

Submission, Next Steps, and Useful Links

Options for submission

When all mandatory fields on the PDSP have been completed and your agency's public sector body Head has reviewed and signed off the form you can submit a copy of your PDSP to OVIC via one of the options below.

For PDSPs marked as OFFICIAL and OFFICIAL: Sensitive Please note: A prior appointment must be made with a member of OVIC's Information Security Unit for option 3.	Option 1	Soft copy	Send a copy of the completed, signed and dated PDSP to security@ovic.vic.gov.au (either from the public sector body Head's email address, or the Information Security Lead's email address)
	Option 2	Hard copy	Post your PDSP in a single opaque envelope with no protective marking labelled on the outside to: PO Box 24274 Melbourne VIC 3001
	Option 3	Hard copy	Hand deliver your PDSP to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne VIC 3001
For PDSPs marked as PROTECTED Please note: A prior appointment must be made with a member of OVIC's Information Security Unit for options 4 and 5.	Option 4	Hard copy	Deliver your PDSP by safe-hand (e.g. delivered in person by an authorised messenger) to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne
	Option 5	Hard copy	Deliver your PDSP by SCEC-endorsed courier to: Attention: OVIC, Level 34 121 Exhibition Street Melbourne
For PDSPs marked as SECRET	Option 6		If your PDSP is assessed as containing security classified information as SECRET , please speak to a member of OVIC's Information Security Unit to arrange secure submission.

Next steps

After submitting your PDSP to OVIC you 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 you continue to:

- Monitor your organisation's information security risks;
- Alert OVIC to any [significant changes](#) to your organisation's information security risks and/or operating environment;
- Notify OVIC of any changes to your 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
VPDSS Glossary	https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-glossary/
Agency Reporting Obligations	https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/
Significant Change	https://ovic.vic.gov.au/data-protection/significant-change-and-protective-data-security-obligations/
OVIC Privacy Policy	https://ovic.vic.gov.au/privacy-policy/
VPDSF BIL Table	https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-framework-business-impact-level-table-v2-1/
VPDSF BIL App	https://ovic.vic.gov.au/data-protection/for-agencies/business-impact-level-app/
OVIC Regulatory Action Policy	https://ovic.vic.gov.au/regulatory-approach/regulatory-action-policy/
VPDSS Implementation Guidance v2.1	https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-implementation-guidance/
Practitioner Guide: Information Security Risk Management	https://ovic.vic.gov.au/data-protection/practitioner-guide-information-security-risk-management/
Practitioner Guide: Assessing the Security Value of Public Sector Information	https://ovic.vic.gov.au/data-protection/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/
Practitioner Guide: Protective Markings	https://ovic.vic.gov.au/data-protection/practitioner-guide-protective-markings/
Incident Notification Scheme	https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/