Office of the Victorian Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

How-to Guide: Completing the Protective Data Security Plan (PDSP)

2026

Freedom of Information | Privacy | Data Protection

Document Details

How-to Guide: Completing the Protective Data Security Plan (PDSP) 2026		
Protective Marking		OFFICIAL
Approved for unlimited public release		Yes – Authorised for release
Release Date		January 2026
Review Date		January 2028
Document Version		1.4
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	• Removed references to ‘2022’ to make document date agnostic • Added description for ‘Planned’ implementation status
1.3	February 2024	• Updated screenshots to reflect 2024 PDSP form
1.4	January 2026	• Updated to reflect the 2026 PDSP form • Added guidance on new PDSP form fields under the organisation summary • Incorporated multi-organisation guide as appendix Refer to What has changed in the 2026 PDSP form section of this guide

Contents

Introduction 5

How to use this guide 5

Where to start 5

Completing and filling in the PDSP form 6

Breakdown of the PDSP form 6

Field character limits within the PDSP form 6

Frequently Asked Questions 7

Part A - Information security self-assessment and implementation plan 14

Element assessment 14

Maturity assessment 14

VPDSS Elements 15

Industrial Automation and Control Systems elements 15

How to read an element 15

Entity Risk Reference 16

How to fill in the entity risk reference field 16

Supporting Control Library 17

How to select the most appropriate supporting control library 18

Implementation status 19

How to select the most appropriate implementation status 19

If an organisation has implemented some components of an element (not all), the status of *Partial (some)*, or *Partial (most)* may be appropriate. 19

Proposed completion date 21

How to select the most appropriate completion date 21

Maturity Assessment 22

How to conduct a maturity assessment at a whole of Standard level 23

Part B – Organisation summary ... 25

Organisation profile assessment ... 28

Part C – Attestation ... 39

Signing the Attestation ... 39

Submission, Next Steps, and Useful Links ... 40

Options for submission ... 40

Next steps ... 41

Useful links ... 41

Appendix – Multi-organisation reporting model ... 42

What is the multi-organisation reporting model? ... 42

What is a primary organisation and a subsidiary organisation? ... 42

Overview of multi-organisation reporting model process ... 43

Participating in the multi-organisation reporting model ... 44

How to complete the multi-organisation PDSP forms ... 45

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**). 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.

This guide is separated into 7 sections, each represented by a different colour as shown in the table below:

◼	Introduction
🟪	Frequently asked questions
🟦	Part A of the PDSP Form Information security self-assessment and implementation plan
🟥	Part B of the PDSP Form Agency Head executive summary (including the Organisation Profile Assessment)
🟩	Part C of the PDSP Form Attestation
🟦	Submission, next steps, and useful links
🟪	Appendix

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.
- new to the process or would like to gain further insights into the intent of the PDSP, 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 Adobe 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, use a compatible version of Acrobat Reader or Acrobat Pro. Alternatively, use Microsoft Edge to complete the PDSP form.

Breakdown of the PDSP form

Part		Description
A	Information security self-assessment and implementation plan	• Outlines the organisation's self-assessed implementation of the elements under each Victorian Protective Data Security Standard (**VPDSS** or **Standard**) and • Outlines the organisation's self-assessed maturity level for each Standard.
B	Organisation summary (including the Organisation Profile Assessment)	• Provides contact information of the public sector body Head and Information Security Lead • Provides an opportunity for the organisation to highlight its security program 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 (**OPA**).
C	Attestation	• Confirms the public sector body Head compliance with Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**), and • Confirms that the PDSP reflects the current information security operating environment and ongoing program of work.
D	Multi-organisation subsidiary list	*Only found in the primary organisation PDSP form.* • Provides a list of subsidiary organisations attested for using the multi-organisation reporting model. For more information see page 11 and the appendix.

Field character limits within the PDSP form

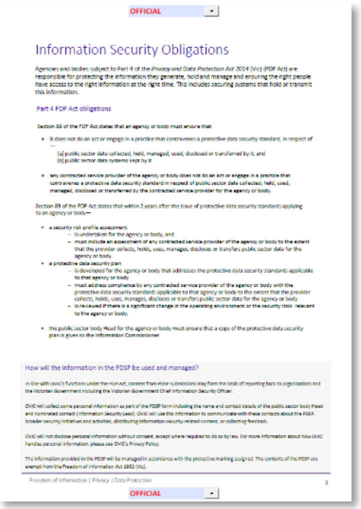
The PDSP form is predominantly made up of drop-down fields with some free-text field options. Where there are free-text fields, character limits apply. The limits will differ throughout the form. Character limits are noted against relevant fields. If the organisation intends to print the PDSP form, be 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 2026 PDSP form?

Information Security obligations

Added information regarding organisations' obligations under Part 4 of the PDP Act.



OFFICIAL

Information Security Obligations

Agencies and bodies subject to Part 4 of the *Privacy and Data Protection Act 2014* (Vic) (PDP Act) are responsible for protecting the information they generate, hold and manage and ensuring the right people have access to the right information at the right time. This includes securing systems that hold or transmit this information.

Part 4 PDP Act obligations

Section 88 of the PDP Act states that an agency or body must ensure that:

- it does not do an act or engage in a practice that contravenes a protective data security standard, in respect of —
  (a) public sector data collected, held, managed, used, disclosed or transferred by it; and
  (b) public sector data systems kept by it.
- any contracted service provider of the agency or body does not do an act or engage in a practice that contravenes a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.

Section 89 of the PDP Act states that within 2 years after the issue of protective data security standards applying to an agency or body—

- a security risk profile assessment
  - is undertaken for the agency or body, and
  - must include an assessment of any contracted service provider of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body.
- a protective data security plan
  - is developed for the agency or body that addresses the protective data security standards applicable to that agency or body
  - must address compliance by any contracted service provider of the agency or body with the protective data security standards applicable to that agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body
  - is reviewed if there is a significant change in the operating environment or the security risks relevant to the agency or body.
- the public sector body Head for the agency or body must ensure that a copy of the protective data security plan is given to the Information Commissioner.

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

In-line with OVIC's functions under the PDP Act, content from PDSP submissions may form the basis of reporting back to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

OVIC will collect some personal information as part of the PDSP form including the name and contact details of the public sector body Head and nominated contact (Information Security Lead). OVIC will use this information to communicate 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.

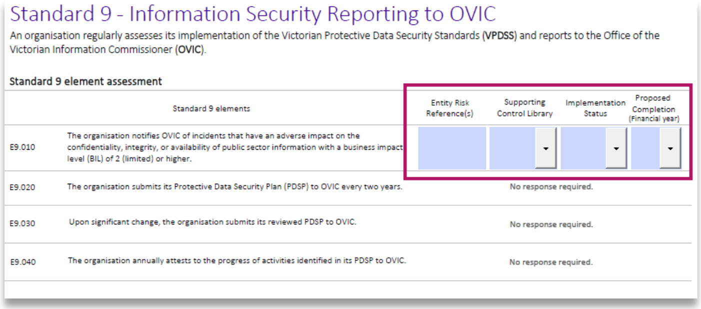
The information provided in the PDSP will be managed in accordance with the protective marking assigned. The contents of the PDSP are exempt from the Freedom of Information Act 1982 (Vic).

Freedom of Information | Privacy | Data Protection 3

OFFICIAL

Part A
Standard 9

In 2024, organisations were not required to provide responses to any elements in Standard 9 in the PDSP form, as these elements were captured by way of completion of the Attestation. The 2026 PDSP form now requires the organisation to complete the required fields for element 1 of Standard 9 (E9.010).



Standard 9 - Information Security Reporting to OVIC

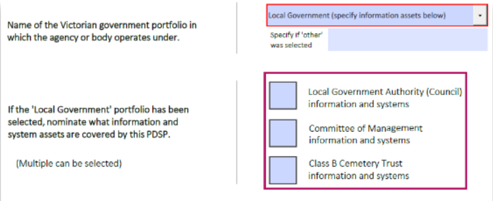
An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (**VPDSS**) and reports to the Office of the Victorian Information Commissioner (**OVIC**).

Standard 9 element assessment

	Standard 9 elements	Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E9.010	The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (BIL) of 2 (limited) or higher.		▾	▾	▾
E9.020	The organisation submits its Protective Data Security Plan (PDSP) to OVIC every two years.	No response required.			
E9.030	Upon significant change, the organisation submits its reviewed PDSP to OVIC.	No response required.			
E9.040	The organisation annually attests to the progress of activities identified in its PDSP to OVIC.	No response required.			

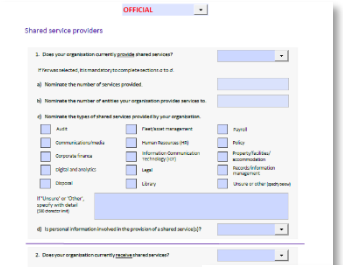
Part B
Organisation executive summary

Added an optional field for the organisation's preferred abbreviation.



Name of the Victorian government portfolio in which the agency or body operates under.	Local Government (specify information assets below) ▾ Specify if 'other' was selected
If the 'Local Government' portfolio has been selected, nominate what information and system assets are covered by this PDSP. (Multiple can be selected)	☐ Local Government Authority (Council) information and systems ☐ Committee of Management information and systems ☐ Class B Cemetery Trust information and systems

Added a required field for Local Government Authorities, outlining the types of information and system assets covered by the PDSP.



OFFICIAL

Shared service providers

1. Does your organisation currently <u>provide</u> shared services? ▾

If Yes was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services provided.

b) Nominate the number of entities your organisation provides services to.

c) Nominate the types of shared services provided by your organisation.

☐ Audit	☐ Fleet/asset management	☐ Payroll
☐ Communications/media	☐ Human Resources (HR)	☐ Policy
☐ Corporate finance	☐ Information Communication Technology (ICT)	☐ Property/facilities/ accommodation
☐ Digital and analytics	☐ Legal	☐ Records/information management
☐ Disposal	☐ Library	☐ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail (500 character limit)

d) Is personal information involved in the provision of a shared service(s)? ▾

2. Does your organisation currently <u>receive</u> shared services? ▾

If Yes was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services received.

b) Nominate the number of entities your organisation receives services f

c) Nominate the types of shared services received by your organisation.

☐ Audit	☐ Fleet/asset management
☐ Communications/media	☐ Human Resources (HR)
☐ Corporate finance	☐ Information Communication Technology (ICT)
☐ Digital and analytics	☐ Legal
☐ Disposal	☐ Library

If 'Unsure' or 'Other', specify with detail (500 character limit)

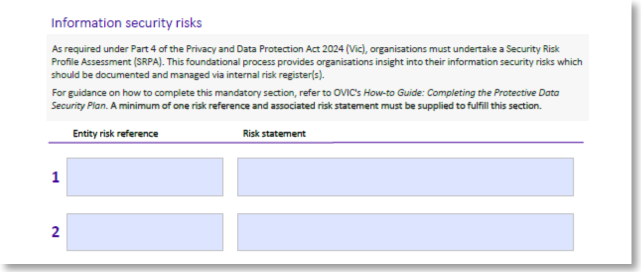
d) Is personal information involved in the provision of a shared service(s)

Freedom of Information | Privacy | Data Protection

OFFICIAL

Added a section addressing any shared service(s) provided to, and received by, organisations.

Added an additional section requesting the organisation provide further insight into its information security risks.



Information security risks

As required under Part 4 of the Privacy and Data Protection Act 2024 (Vic), organisations must undertake a Security Risk Profile Assessment (SRPA). This foundational process provides organisations insight into their information security risks which should be documented and managed via internal risk register(s).

For guidance on how to complete this mandatory section, refer to OVIC's *How-to Guide: Completing the Protective Data Security Plan*. A minimum of one risk reference and associated risk statement must be supplied to fulfill this section.

	Entity risk reference	Risk statement
1		
2		

Part C
Attestation

Attestation wording updated to more closely reflect the public sector body Head's obligations under Part 4 of the PDP Act.

What are the VPDSS?

The VPDSS are designed to help Victorian public sector organisations:

- manage public sector information throughout its lifecycle
- manage public sector information across all the security areas
- manage security risks to the confidentiality, integrity, and availability of public sector information
- manage external parties with access to public sector information
- share public sector information with other organisations with confidence, and
- minimise security incidents.

The VPDSS are consistent with national and international standards and describe the Victorian Government's approach to protecting public sector information. They focus on the outcomes required to enable efficient, effective and economic investment in security measures through a risk-managed approach.

Why is a PDSP required?

Section 89 of the 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 documents the organisation's self-assessed information security capability at a point in time. It 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.

What purposes does a PDSP serve?

A PDSP serves several purposes. It is designed to:

- fulfil your organisation's obligation to OVIC as outlined under section 89 of the PDP Act
- summarise your organisation's progress implementing the VPDSS and elements, and
- help an organisation assess and uplift its information security capability.

Information captured in a PDSP presents a helpful summary of information security arrangements for key stakeholders and provides a level of confidence in how the organisation is progressing against the implementation of the Standards.

The *single organisation PDSP form* consists of 3 parts:

Part A	Information security self-assessment and implementation plan
Part B	Organisation summary (including the Organisation Profile Assessment)
Part C	Attestation

The *primary organisation PDSP form* consists of the above 3 parts and additionally contains the below:

Part D	Multi-organisation subsidiary list

Where can you access a copy of the PDSP form?

The *single organisation PDSP form* is available on the OVIC website under the VPS Agency Reporting Obligations webpage.

Organisations intending to use the multi-organisation reporting model can request forms by contacting the Information Security Unit via security@ovic.vic.gov.au. Further information can be found in the Appendix.

What type of PDSP form should an organisation use?

The majority of organisations are expected to use a single organisation *PDSP form*.

Where organisations have equivalent risk profiles (including appetite and tolerance), risk references, control environments, implementation statuses, completion dates for the VPDSS elements, and maturity levels to those of a primary organisation, a multi-organisation reporting model may be appropriate. This is explained in detail in the Appendix.

Single organisation model

OFFICIAL

OVIC
Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)
Single organisation PDSP form
Version 3.7

Information Security
Victorian Protective Data Security Standards (VPDSS)
Reporting information security capability and implementation progress

Single

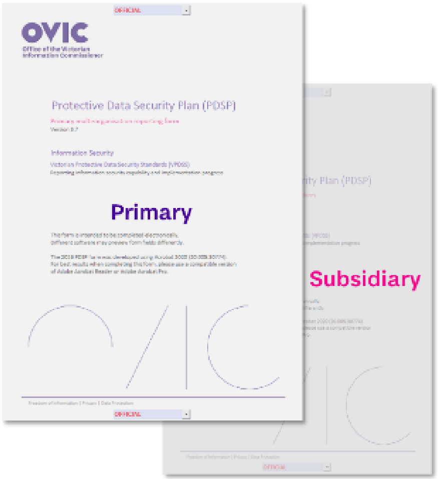
This form is intended to be completed electronically.
Different software may preview form fields differently.

The 2026 PDSP form was developed using Acrobat 2020 (20.005.30774).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Multi-organisation model



OFFICIAL

OVIC
Office of the Victorian Information Commissioner

Protective Data Security Plan (PDSP)
Primary multi-organisation reporting form
Version 3.7

Information Security
Victorian Protective Data Security Standards (VPDSS)
Reporting information security capability and implementation progress

Primary

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

The 2026 PDSP form was developed using Acrobat 2020 (20.005.30774).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Subsidiary

What should an organisation do before it starts a PDSP?

Before developing a PDSP, the organisation should have:

- an understanding of its information assets and systems
- undertaken a security value assessment for these information assets and systems
- an understanding of who should be engaged to assist in assessing security risks and develop associated treatment plans
- undertaken a SRPA (information security risk assessment) for its information assets and systems, and
- an understanding of the security controls already implemented to protect its information assets and systems to develop a risk treatment plan.

What should be captured in the PDSP?

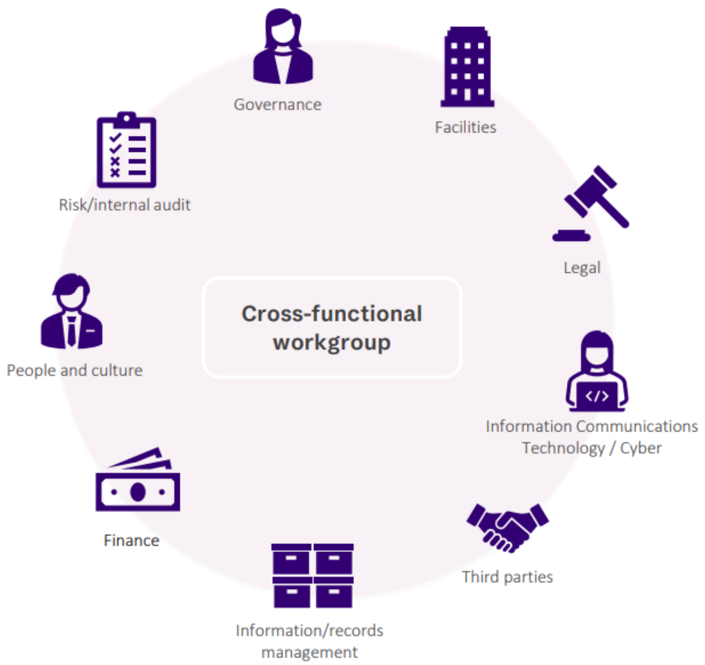
Copies of PDSPs submitted to OVIC should cover security activities spanning a 24-month period as well as any planned activities. Incomplete PDSPs will not be accepted by OVIC. Please ensure all mandatory fields are completed before submitting, including the signed and dated Attestation.

Who should complete and submit the PDSP?

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

Who should be consulted for PDSP responses?

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, as well as external bodies and third parties. Subject matter experts across different workgroups help provide important inputs into PDSP responses for the various Standards.


Governance
Facilities
Risk/internal audit
Legal
People and culture
Cross-functional workgroup
Information Communications Technology / Cyber
Finance
Third parties
Information/records management

Internal organisational groups

OVIC encourages organisations to utilise internal workgroups with representatives from across the business who contribute subject-matter expertise unique to their security domain or functional work area to include specialist knowledge and capabilities. For example, input could be from:

- Risk
- Information/Records Management
- Information Technology
- People and Culture
- Legal
- Corporate
- Finance
- Facilities

Relevant portfolio/department

Where shared support arrangements are offered by portfolio departments, and your organisation utilises their infrastructure, personnel, or other relevant services, the responsibility remains with your organisation to ensure its information and systems are protected throughout the lifecycle of the arrangement. In understanding the risks to your information/systems, you should ask your organisation's portfolio/department about:

- resources
- services
- policies
- infrastructure

Third parties

Under the VPDSS, a third-party provider can be any person/entity outside an organisation that accesses, handles, stores or manages any information or systems on the organisation's behalf.

Third-party arrangements can take many forms, for example:

- state contracts (e.g. with storage facilities for hard-copy and soft-copy records, digitisation services, software vendors, transport companies)
- consultancies brought on to deliver a particular project or task
- information sharing arrangements where those external to the organisation have direct access to information and/or systems.

Public sector body Head

It is also important to engage the public sector body Head early and update them as needed, prior to their signing of the Attestation. Under the PDP Act, the public sector body Head is responsible for providing a copy of the organisation's PDSP to OVIC.

When does an organisation have to submit a PDSP?

There are 2 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	Regular biennial reporting cycle	The submission of a PDSP is due between **1 July and 31 August** of the reporting year. The reporting cycle for PDSPs falls on even-numbered years (e.g., 2024, 2026, 2028). **Please note:** Organisations are still required to submit an **annual** Attestation to OVIC. For more information on the annual reporting obligations, please visit our webpage here.
Scenario 2	Significant change	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. In the event of significant change, contact the Information Security Unit at OVIC to discuss the reporting options. For more information on what constitutes a significant change please visit OVIC's website. **Please note:** Organisations that undergo significant change must still report in the next regular reporting cycle (scenario 1).

Who should sign the Attestation in the PDSP?

The PDSP must be signed by the public sector body Head in acknowledgment of their statutory obligations.[1]

The attestation is set out under Part C of the PDSP form. For more information, see Part C of this guide.

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

VPS organisations regulated by Part 4 of the PDP Act that fail to submit a PDSP to OVIC will be in breach of section 89 of the PDP Act. To find out more about OVIC's regulatory approach refer to the OVIC Regulatory Action Policy.

[1] Under the PDP Act, the public sector body Head must ensure that a PDSP is developed, and a copy is submitted to OVIC.

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 security of public sector data across the VPS.

The information provided in the PDSP will be used by the ISU to

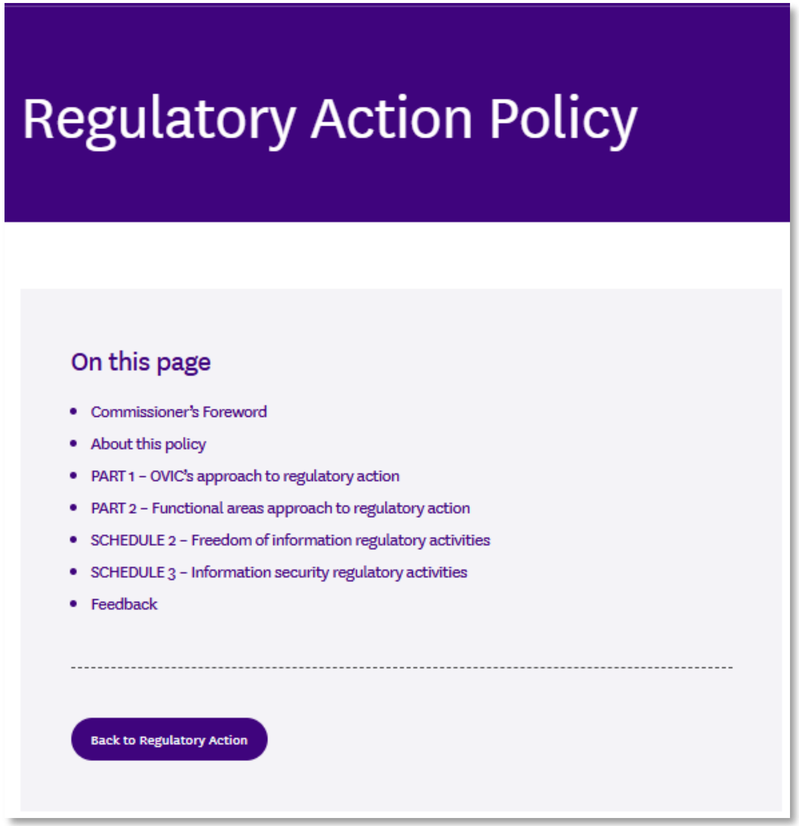
- monitor an organisation's information security risks
- gain insight into organisations' current and future information security programs
- inform and direct OVIC's assurance activities

In-line with OVIC's functions under the PDP Act, content from PDSP submissions may form the basis of reporting back to organisations and the Victorian Government including the Victorian Government Chief Information Security Officer.

OVIC will collect some personal information as part of the PDSP form including the name and contact details of the public sector body Head and nominated contact (Information Security Lead). OVIC will use this information to communicate 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* (Vic).



Regulatory Action Policy

On this page

- Commissioner's Foreword
- About this policy
- PART 1 – OVIC's approach to regulatory action
- PART 2 – Functional areas approach to regulatory action
- SCHEDULE 2 – Freedom of information regulatory activities
- SCHEDULE 3 – Information security regulatory activities
- Feedback

What protective marking should an organisation label the PDSP with?

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

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

Initial Assessment

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

Reassessment

Once the PDSP is complete, organisations should conduct a reassessment of the confidentiality to confirm/update the protective marking based on the finalised content. This should be done before sending a copy of the PDSP to OVIC.

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

(see the VPDSF BIL table for more information).

Part A - Information security self-assessment and implementation plan

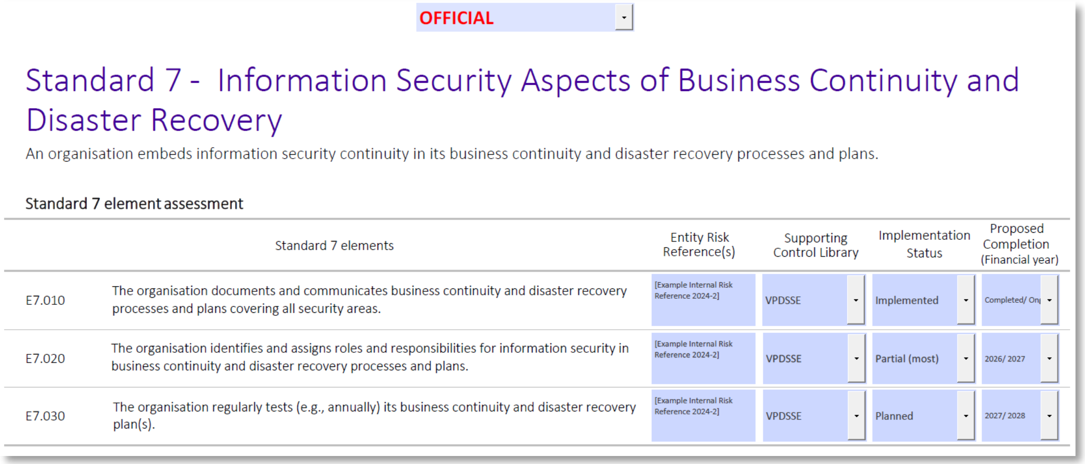
In **Part A** of the PDSP form, organisations must self-assess the implementation of each Standard and supporting elements.

Organisations are required to assess the implementation status of each element considering all the required components of the element.

Element assessment

Organisations must (mandatory) provide a response for the following fields:

- **Entity Risk Reference** for each element, including elements that are considered '*Implemented*'
- **Supporting Control Library** reference used for each element
- **Implementation 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.

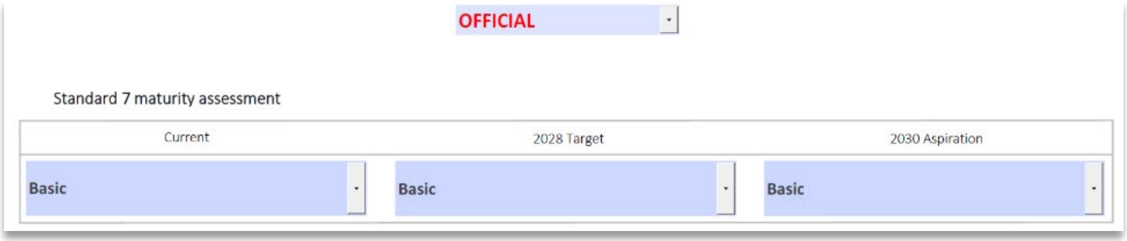
Standard 7 element assessment

Standard 7 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E7.010	The organisation documents and communicates business continuity and disaster recovery processes and plans covering all security areas.	[Example Internal Risk Reference 2024-2]	VPDSSE	Implemented	Completed/ On
E7.020	The organisation identifies and assigns roles and responsibilities for information security in business continuity and disaster recovery processes and plans.	[Example Internal Risk Reference 2024-2]	VPDSSE	Partial (most)	2026/ 2027
E7.030	The organisation regularly tests (e.g., annually) its business continuity and disaster recovery plan(s).	[Example Internal Risk Reference 2024-2]	VPDSSE	Planned	2027/ 2028

Maturity assessment

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

- **Current** maturity assessment
- **Target** maturity assessment
- **Aspiration** maturity assessment

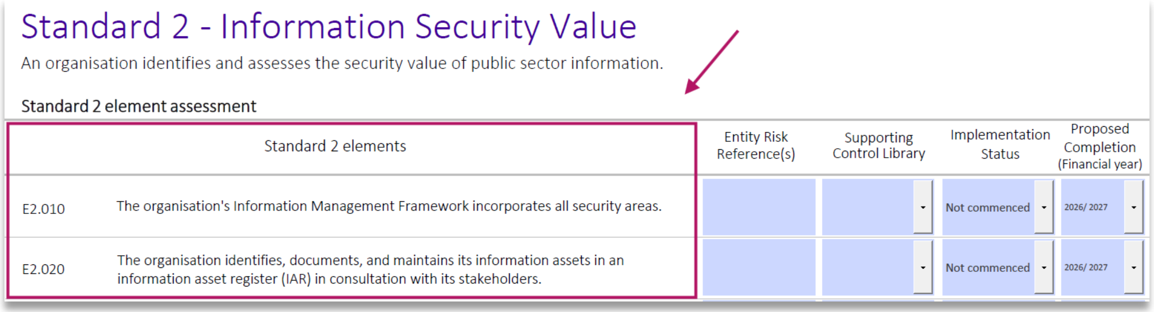


OFFICIAL

Standard 7 maturity assessment

Current	2028 Target	2030 Aspiration
Basic	Basic	Basic

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



Standard 2 - Information Security Value

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

Standard 2 element assessment

Standard 2 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E2.010	The organisation's Information Management Framework incorporates all security areas.			Not commenced	2026/ 2027
E2.020	The organisation identifies, documents, and maintains its information assets in an information asset register (IAR) in consultation with its stakeholders.			Not commenced	2026/ 2027

VPDSS Elements

A VPDSS 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 elements and associated primary sources, please see the VPDSS Implementation Guidance V2.4 on OVIC's website.

Industrial Automation and Control Systems elements

Organisations that operate Industrial Automation and Control Systems (**IACS**) should consider the specific elements applicable to their environments.
Only a small portion of Victorian government organisations operate IACS, this typically includes the water and some transport sectors.
For more information, see OVIC's IACS Implementation Guidance.

The specific IACS elements are:

E1.120 E1.130 E2.100

How to read an element

Some elements contain multiple activities/requirements, so consider all aspects of the element, as this may influence the selection of an implementation status.

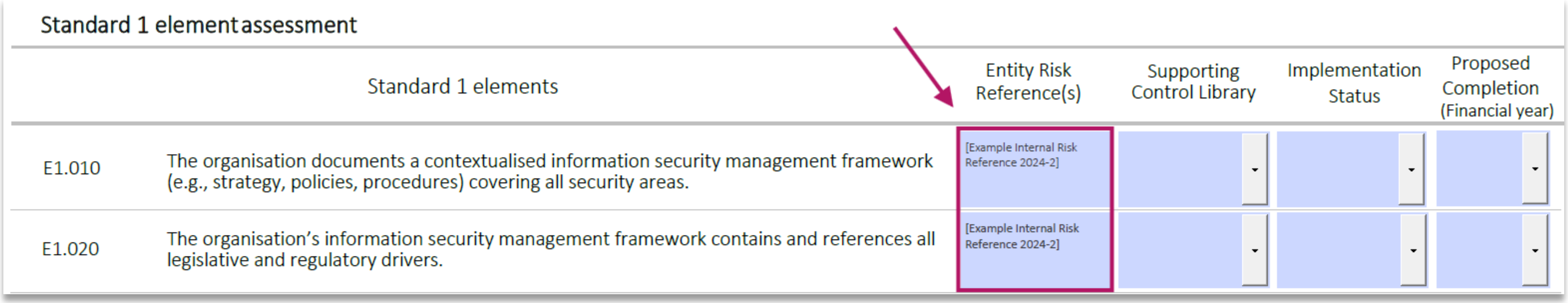
Example

VPDSS Element
E2.020

Descriptor
*The organisation identifies, documents, and maintains its information assets in an information asset register (**IAR**) in consultation with its stakeholders.*

Activities contained in the descriptor
For this element to be implemented an organisation should have:

- 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).



Standard 1 elementassessment

Standard 1 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.	[Example Internal Risk Reference 2024-2]			
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.	[Example Internal Risk Reference 2024-2]			

Entity Risk Reference

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

Registers should 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.[2]

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.

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.

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 internal 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 some or all elements throughout the PDSP (e.g., broad strategic or enterprise risk reference).

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

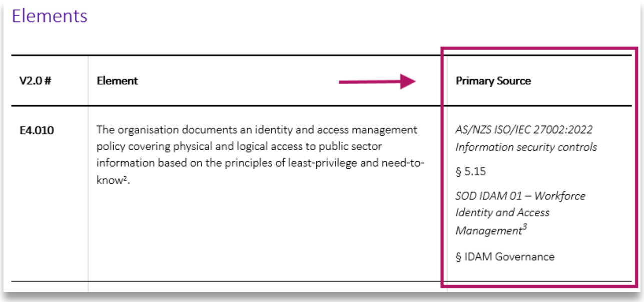
Supporting Control Library

A 'control' is defined as a measure that maintains and/or modifies risk.[3] Controls may include specific policies, procedures, processes and technologies. In an information security context, a supporting *control library* refers to a central repository or catalogue of selected controls that an organisation uses, or intends to use, to protect information and systems.

On the PDSP form, organisations are required to nominate a supporting control library for each element.

The elements described in the VPDSS include both controls that directly modify risk and essential supportive controls. Elements often depend on a supportive control environment to be effective. A control environment can be a set of standards, processes and structures that provide the basis for applying controls across the organisation. The control environment therefore contributes to modifying risk indirectly.

Organisations should refer to the primary sources outlined in the Implementation Guidance for a reference point of the element and for further guidance to assist in the implementation of elements.[4]



Elements

V2.0 #	Element	Primary Source
E4.010	The organisation documents an identity and access management policy covering physical and logical access to public sector information based on the principles of least-privilege and need-to-know².	*AS/NZS ISO/IEC 27002:2022 Information security controls* § 5.15 *SOD IDAM 01 – Workforce Identity and Access Management³* § IDAM Governance

Control Library	Description
ISO 27000 series	The ISO 27000 comprises of mutually supporting information security standards that together provide a globally recognised framework for best-practice information security management.
ISM Australian Government Information Security Manual	The ISM is a suite of controls designed to help government agencies apply a risk-based approach to protecting their information and ICT systems.
PSPF Protective Security Policy Framework	The PSPF sets out Australian Government policy across 6 security domains (governance, risk, information, technology, personnel, physical) and informs how organisations can protect their people, information and resources. Application of the PSPF assures government that organisations are implementing sound and responsible protective security practices and identifying and mitigating security risks and vulnerabilities.
NIST National Institute of Standards and Technology Cybersecurity Framework	This framework consists of standards, guidelines, and best practices to manage security-related risks.
VPDSSE Victorian Protective Data Security Standards Element	For organisations that determine the VPDSS element is descriptive and inclusive enough to be used as a control.
Other	This field can be used to denote an alternative control reference from those offered in the pre-populated drop-down list.

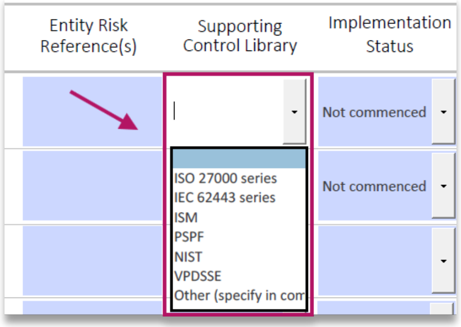
[3] Drawn from ISO 31000:2018, 3.8 and referenced in the VPDSS Glossary V2.1.

[4] See OVIC's VPDSS Implementation Guidance: https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-implementation-guidance/

Part A of the PDSP form

How to select the most appropriate supporting control library

The organisation should have its own documented internal control library.[5] This will assist in selecting one control library reference per applicable element. The above table lists the supporting control libraries available in the dropdown menu in the PDSP.

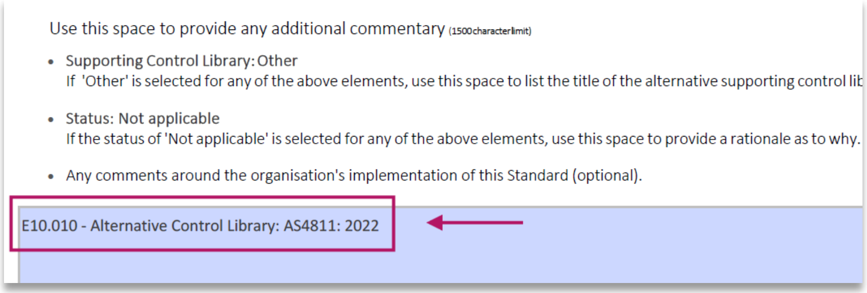


Entity Risk Reference(s)	Supporting Control Library	Implementation Status
		Not commenced
	ISO 27000 series IEC 62443 series ISM PSPF NIST VPDSSE Other (specify in com	Not commenced

Selection of 'Other': As the VPDSS promote a risk-based approach, OVIC recognises alternative control libraries that support the intent of each element and modify organisational risks. Where an organisation uses a supporting control library beyond the ones listed as a primary source of the VPDSS, the organisation must be confident that the control source provides (at a minimum) functional equivalency to what the VPDSS primary source (control reference) describes.

Additional commentary: Where an organisation uses a control library that:

- is not listed, select 'Other' and detail in the *Additional commentary* field at the end of the Standard.
- is listed, and wish to provide additional context regarding its selection, this can be described in this field.



Use this space to provide any additional commentary (1500characterlimit)

- 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 lib
- 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 - Alternative Control Library: AS4811: 2022

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 in *Additional commentary* field at the end of the Standard to list the element and the name of the alternative supporting control library reference.

Note:
Organisations should be careful when selecting alternative control libraries beyond those offered as the primary source material for the elements. Anecdotally, the ISU has identified some instances where the business area responsible for the drafting of the PDSP form influences the nomination of primary source material which may not necessarily provide the coverage intended by the element.

[5] E1.100 - *The organisation documents its internal control library that addresses its information security risks.*

Implementation status

The status field reflects how the organisation is tracking against the implementation of each element at the time of PDSP form. The statuses and their associated descriptors are outlined below.

Organisations must assess the implementation status of each element, considering all components. Some elements contain multiple activities and / or components.
The implementation status should reflect the degree to which an organisation has successfully addressed each aspect of an element.

Status	Description
Not commenced	The organisation has not yet defined or planned the work needed to meet the element.
Planned	The organisation has a program of work in place that includes work to meet the element, and the program is appropriately planned and resourced.
Partial (some)	The organisation has 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	The organisation currently meets all aspects of the element, and this has shifted to a BAU activity.
Not applicable	There is no related information security risk that needs to be managed.

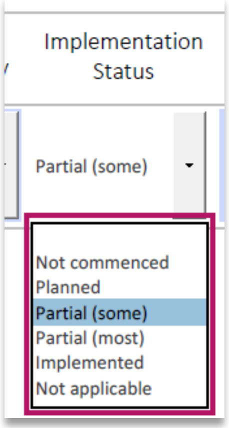
How to select the most appropriate implementation status

To determine an element's applicability, the organisation must first assess whether the element 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.

Deciding which elements apply, depends upon the organisation's criteria for risk acceptance and risk treatment options. Determining applicable elements also depends on the way in which elements interact with one another to provide 'defence-in-depth.'[6]



Example

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

If the element is deemed **Applicable**, select from the available drop-down implementation status options and fill out the *Entity Risk Reference*, *Supporting Control Library* and *Proposed Completion Date* fields.

[6] For further information refer to the VPDSS glossary https://ovic.vic.gov.au/wp-content/uploads/2022/01/VPDSS-Glossary-V2.1.docx.pdf.

When is *Not applicable* appropriate to select as an implementation status?

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

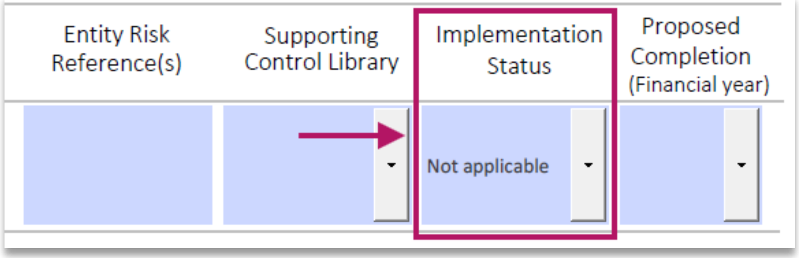
If an element is deemed to be *Not applicable* (i.e., there is no related information security risk that needs to be managed), supporting justification should be documented in the PDSP.

When is *Not applicable* not appropriate to select as an implementation status?

Where a third party (e.g. contracted service provider or departmental portfolio agency) is performing an activity or function on behalf of the organisation, this does not mean there is no related information security risk that needs to be managed.[7] If certain activities are managed outside of your organisation, you must consult with these third parties as outlined above on the page titled "*Who should be consulted for PDSP responses?*"

In these scenarios, the element remains applicable, even if your organisation is not directly performing the associated activities or components outlined in the element description. Despite the third party performing these activities on an organisation's behalf, the element highlights security components that need to be managed **by the reporting organisation.**

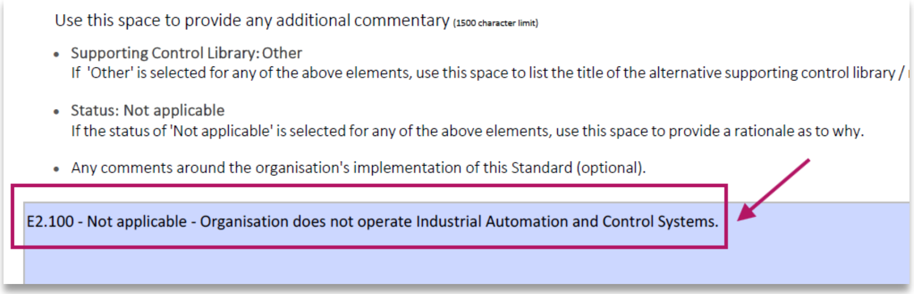
Responsibility for the management and oversight of these risks remains with the reporting organisation and accountability ultimately rests with the public sector body Head of the organisation, not the third party.



Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
		Not applicable	

Example: if the element is *Not applicable* to your organisation, leave the remaining fields of the element blank as seen above.

However, justification of the *Not applicable* element is required and can be provided using the free text fields in the *Additional commentary* field at the end of the Standard, as seen below.



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 /
- 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).

E2.100 - Not applicable - Organisation does not operate Industrial Automation and Control Systems.

[7] For example, departmental bodies, ICT services or facility management.

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 should be used to outline a prioritised list of activities by financial year.

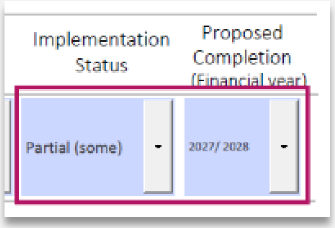
The table below depicts the:

- 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.

Implementation 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. If the organisation has several programs or activities that address different aspects/components of the element spanning multiple years, select the last completion date available.
Planned	
Partial (some)	
Partial (most)	
Implemented	If all activities/components of the element have been completed, select '**Completed/Ongoing**'.
Not applicable	If the element is not applicable to the organisation, leave the completion date field blank.

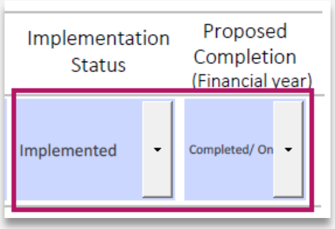
How to select the most appropriate completion date

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



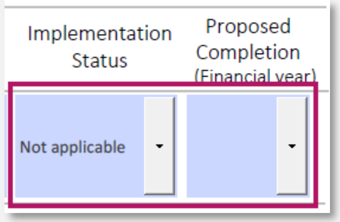
Implementation Status	Proposed Completion (Financial year)
Partial (some)	2027/ 2028

Where organisations **have not implemented all activities** associated with an element, a date must be nominated by which the organisation expects to have activities completed by.



Implementation Status	Proposed Completion (Financial year)
Implemented	Completed/ On

Where organisations **have implemented all activities** associated with an element, the appropriate response is that the activity is 'Completed/Ongoing'.



Implementation Status	Proposed Completion (Financial year)
Not applicable	

Where the organisation has deemed the element is **not applicable** to its environment, no response is required, and the field should be left blank.

Maturity Assessment

Organisations are required to conduct a maturity assessment at a whole of Standard level. The maturity assessment process prompts organisations to engage in critical discussions on perceived areas of strength and opportunities for improvement. Maturity ratings can be used as a guide to help direct information security investment to enhance the organisation's information security capability.

An organisation's maturity level will be influenced by its risk appetite and tolerance, and the economic, efficient, and effective use of resources available to it. Assessing maturity helps an organisation to adopt a structured approach for improvement by providing:

- descriptions that inform organisations of their current status in relation to each Standard, and
- an opportunity to plan for future improvement.

To align with the VPDSS risk-based approach organisations should define what maturity level is suitable for their program, noting that not every organisation needs to achieve the highest maturity level (*Optimised*) for each Standard.

To help organisations contextualise these maturity levels, corresponding maturity descriptions are provided in the following table.

Informal	Processes are usually ad-hoc and undocumented. Some base practices may be performed within the organisation, however there is a lack of consistent planning and tracking. Most improvement activity occurs in reaction to incidents rather than proactively. Where practice is good, it reflects the expertise and effort of individuals rather than institutional knowledge. There may be some confidence that security-related activities are performed adequately, however this performance is variable, and the loss of key staff may significantly impact capability and practice.
Basic	The importance of security is recognised, and key responsibilities are explicitly assigned to positions. At least a base set of protective security measures are planned and tracked. Activities are more repeatable and results more consistent compared to the '**informal**' level, at least within individual business units. Policies are probably well documented, but processes and procedures may not be. Security risks and requirements are occasionally reviewed. Corrective action is usually taken when significant problems are found.
Core	Policies, processes, and standards are well defined and are actively and consistently followed across the organisation. Governance and management structures are in place. Risk assessment and management activities are regularly scheduled and completed. Historic performance information is periodically assessed and used to determine where improvements should be made.
Managed	Day-to-day activity adapts dynamically and automatically in response to situational changes. Quantitative performance measures are defined, baselined, and applied to ensure security performance is analysed objectively and can be accurately predicted in advance. In addition to meeting VPDSS requirements, the organisation also implements many optional 'better practice' requirements in response to its risk assessment.
Optimised	Security is a strategic issue for the organisation. Long-term planning is in place and integrated with business planning to predict and prepare for protective security challenges. Effective continuous process improvement is operating, supported by real-time, metrics-based performance data. Mechanisms are also in place to encourage, develop and test innovations.

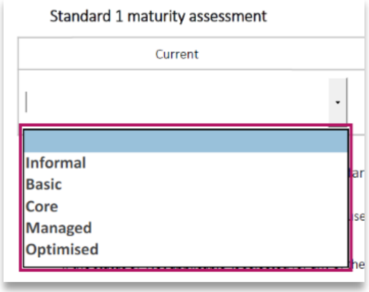
How to conduct a maturity assessment at a whole of Standard level

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

Calculating current maturity

In some instances, a Standard's 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 and systems. Similarly, areas of the organisation may operate at a higher maturity level, while other areas in the organisation may require uplift.

These factors should be taken into consideration when an organisation is assessing its maturity against each Standard.



Sequencing of elements

For some Standards, the elements are sequenced in a particular order of which implementation would inherently influence the selection of the organisation's maturity rating for each Standard (i.e. the implementation of certain elements is necessary for the successful implementation of later elements). Applying this principle, where an organisation assesses earlier the elements' implementation status in a Standard as *not commenced* or *planned*, it is unlikely that the organisation's maturity rating can be assessed as *core*, given the foundational aspects of a Standard have not been met. For example, the description for the maturity level *core* is as follows:

> *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.*
> *(emphasis added)*

In short, an organisation must be able to demonstrate features of the corresponding nominated maturity level. Organisations should document the method used throughout the assessment to provide a level of consistency and continuity on future PDSPs.

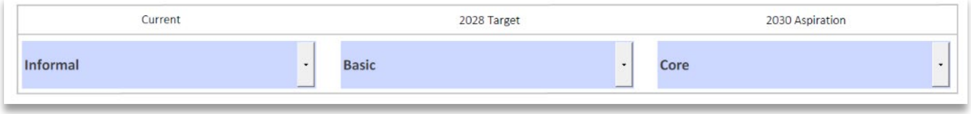
How to fill in the maturity assessment

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).

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.



Current	2028 Target	2030 Aspiration
Informal	Basic	Core

Example

The following is a working example of how to assess an element, (e.g., E1.010) to inform an assessment of the whole Standard (Standard 1).

Step 1 Assess the implementation status of each element that falls under the Standard

VPDSS Element
E1.010

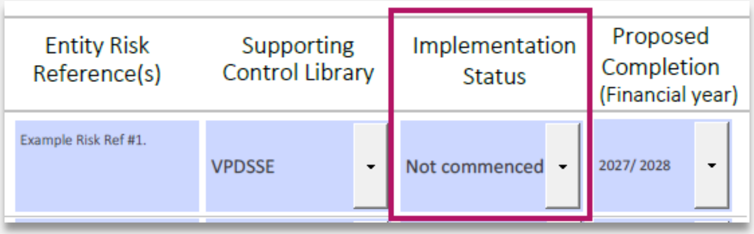
Element descriptor
The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.

Assessment
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, the organisation assesses its implementation status to be *Not commenced*.

This means that the organisation has 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.



Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
Example Risk Ref #1.	VPDSSE	Not commenced	2027/ 2028

Step 2 Conduct a whole of Standard maturity assessment

Standard
1

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

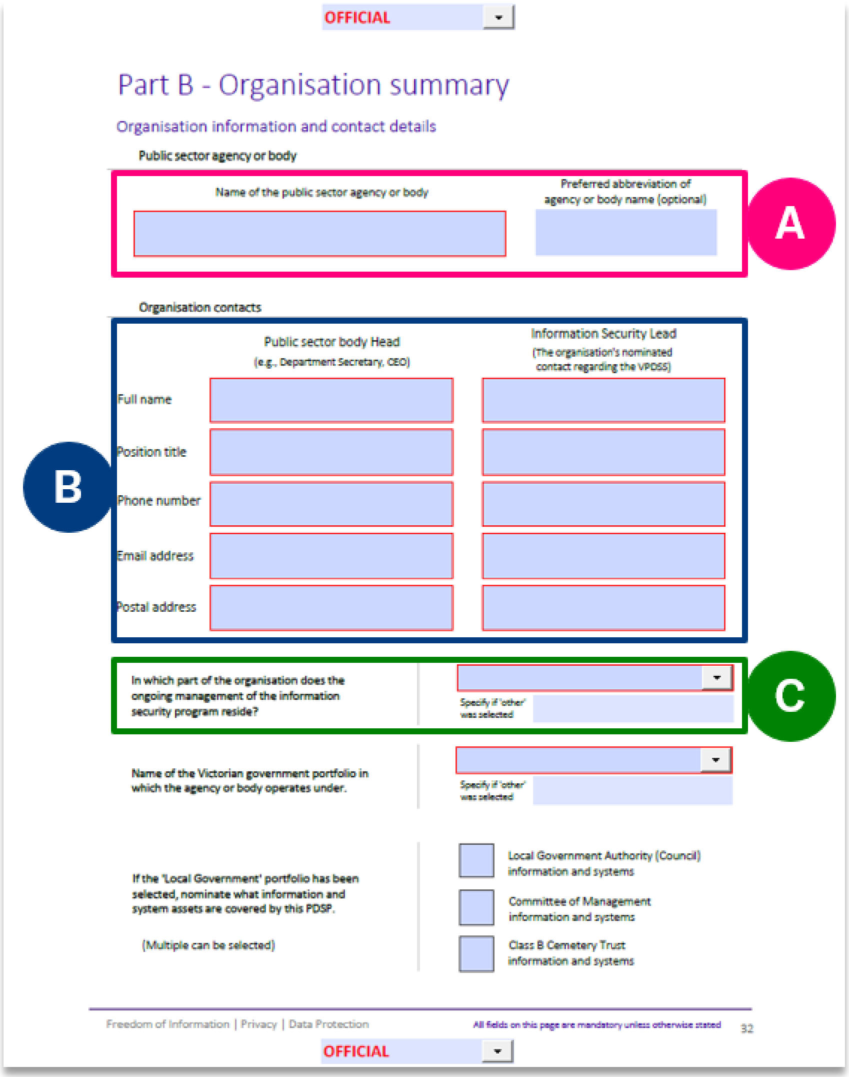
Assessment
The organisation has nominated an implementation status for each element under Standard 1 and can now assess its maturity of the Standard as a whole.
Next, the organisation critically evaluates the aspects of each element within the Standard to assess that Standard's overall alignment to a maturity descriptor.

Given the organisation reported E1.010 implementation status as *Not commenced*, and E1.010 calls for organisations to formalise foundational requirements, an *informal* maturity rating may be appropriate for this Standard, even if other elements in the Standard are implemented.
Consider the 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*".

Part B – Organisation summary

Organisation information and contact details: 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.



OFFICIAL

Part B - Organisation summary

Organisation information and contact details

Public sector agency or body

Name of the public sector agency or body	Preferred abbreviation of agency or body name (optional)

Organisation contacts

	Public sector body Head (e.g., Department Secretary, CEO)	Information Security Lead (The organisation's nominated contact regarding the VPDSS)
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?	▾ Specify if 'other' was selected
Name of the Victorian government portfolio in which the agency or body operates under.	▾ Specify if 'other' was selected
If the 'Local Government' portfolio has been selected, nominate what information and system assets are covered by this PDSP. (Multiple can be selected)	□ Local Government Authority (Council) information and systems □ Committee of Management information and systems □ Class B Cemetery Trust information and systems

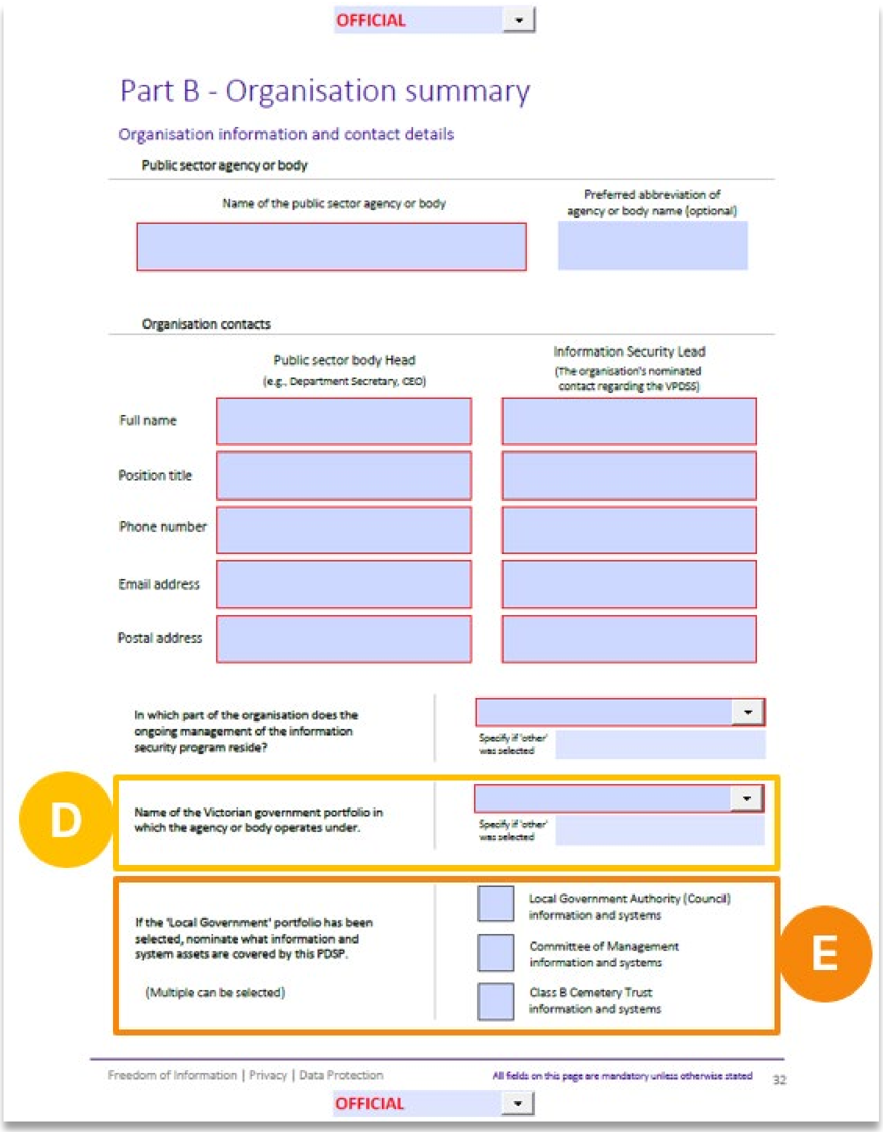
Freedom of Information | Privacy | Data Protection   All fields on this page are mandatory unless otherwise stated   32

OFFICIAL

Description	Field Type	Image ref.
Type the organisation's name, and optionally, any preferred abbreviation of the organisation's name.	Free text	A
Type the name and contact details of the public sector body Head of the Victorian government organisation (e.g., Department Secretary, CEO). Type the name and contact details of the Information Security Lead for the organisation.	Free text	B
While the completion of an organisation's PDSP will likely require input from all areas, this field refers to the area of the organisation responsible for coordinating this program of work. If the responsible area for the ongoing management of the information security program is not among the available drop-down options, please select '**Other**' and briefly elaborate in the associated free text field offered.	Dropdown menu and optional free text	C

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. They can also help coordinate the implementation of the Standards. The ISL should be someone who can influence good information security outcomes for the organisation. For more information visit our webpage.



OFFICIAL

Part B - Organisation summary

Organisation information and contact details

Public sector agency or body

Name of the public sector agency or body

Preferred abbreviation of agency or body name (optional)

Organisation contacts

	Public sector body Head (e.g., Department Secretary, CEO)	Information Security Lead (The organisation's nominated contact regarding the VPDSS)
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?

Specify if 'other' was selected

Name of the Victorian government portfolio in which the agency or body operates under.

Specify if 'other' was selected

If the 'Local Government' portfolio has been selected, nominate what information and system assets are covered by this PDSP.

(Multiple can be selected)

□ Local Government Authority (Council) information and systems

□ Committee of Management information and systems

□ Class B Cemetery Trust information and systems

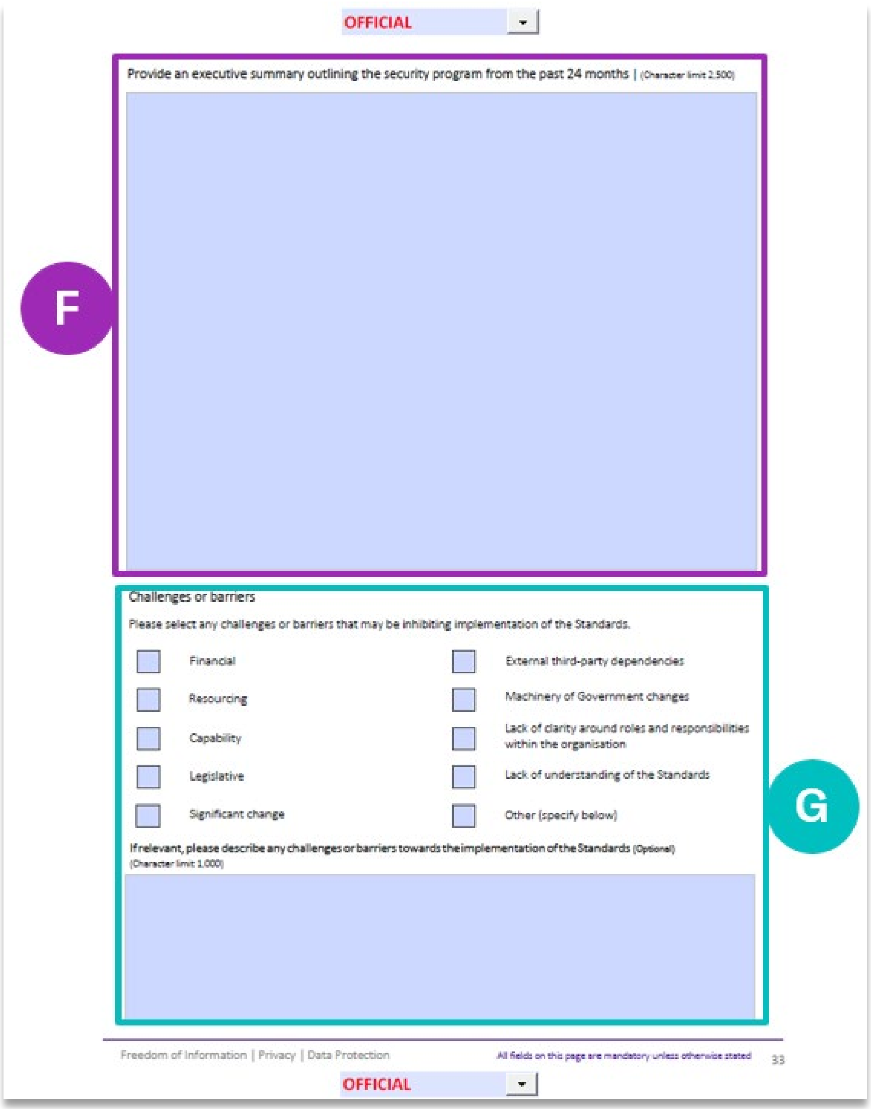
Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

32

OFFICIAL

Description	Field Type	Image ref.
Select the related portfolio/department that the organisation falls under from the drop-down menu. If the Victorian government portfolio is not among the available drop-down options, please select '**Other**' and briefly elaborate in the associated free text field offered. If you have selected *Local Government* from the dropdown, please proceed to field E below.	Dropdown menu with optional free text	D
Field E is only for organisations that have selected *Local Government* as its portfolio in field D above.		
Some LGAs support/manage a Committee of Management and/or a Class B Cemetery Trust. If your organisation is categorised as Local Government in the field above, these checkboxes should be selected to inform OVIC of what type of information and systems are covered by this PDSP. Multiple boxes may be selected as needed. For more information about Local Government information security obligations, please see OVIC's LGA Guide.	Checkbox(es)	E



OFFICIAL

Provide an executive summary outlining the security program from the past 24 months | (Character limit 2,500)

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 changes
□ Capability	□ Lack of clarity around roles and responsibilities within the organisation
□ Legislative	□ Lack of understanding of the Standards
□ Significant change	□ Other (specify below)

If relevant, please describe any challenges or barriers towards the implementation of the Standards (Optional) (Character limit 1,000)

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

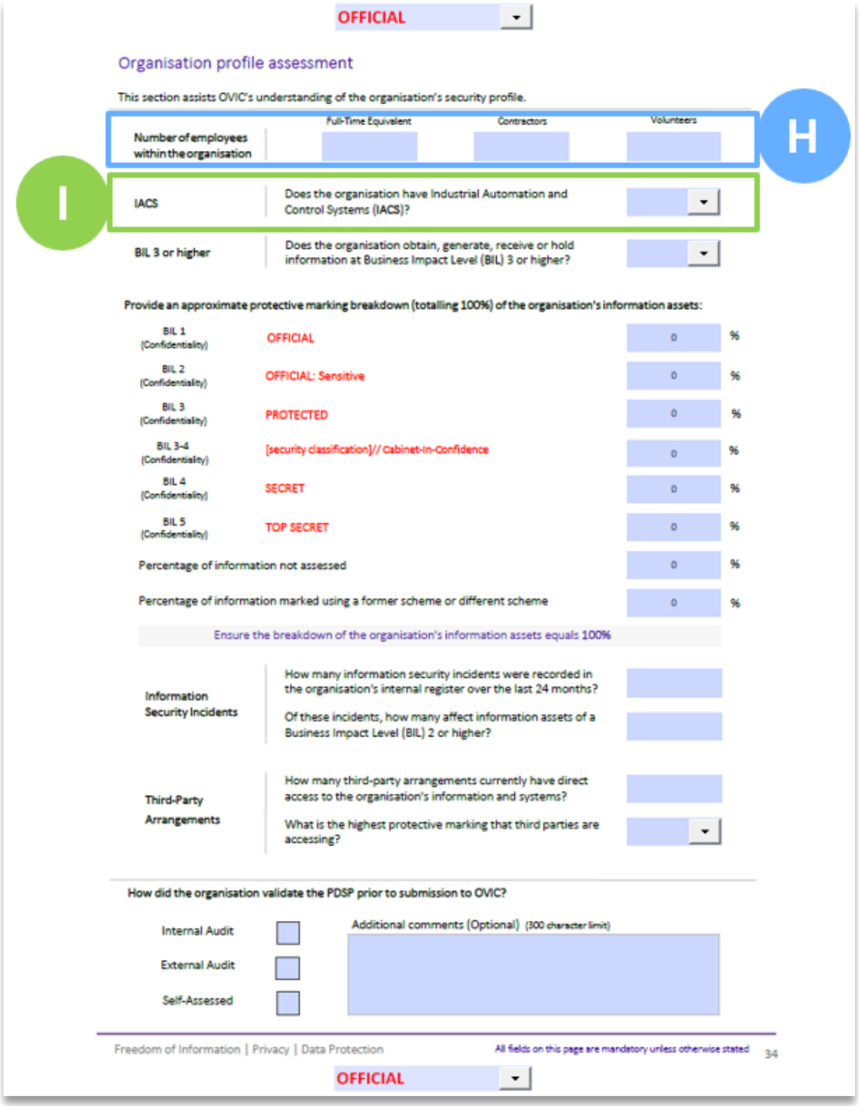
33

OFFICIAL

Description	Field Type	Image ref.
Use this free text field to highlight a summary of key information security activities from the past 24 months. These activities are a good way to highlight items of interest to the public sector body Head and to OVIC. While there is no set way to complete this section, include enough detail for OVIC to gain sufficient insight into the information security program of the organisation and understand the progress that has been made in your organisation's information security capability. Topics could include, but are not limited to: • major projects that the organisation has undertaken • high-level summaries of the organisation's incidents • changes to the organisation's risk profile, and • significant events for the organisation	Free text	F
Further information regarding the implementation of the VPDSS can be provided in the free text fields under each Standard.		
Use this section to highlight relevant challenges or barriers that the public sector body Head and/or OVIC should be aware of that have inhibited the organisation's implementation of the Standards. If there are additional challenges and barriers to be added (beyond the available check boxes), check 'Other' and note these in the free text field below.	Checkbox(es) and optional free text	G

Organisation profile assessment

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



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			

IACS	Does the organisation have Industrial Automation and Control Systems (IACS)?	▾
BIL 3 or higher	Does the organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3 or higher?	▾

Provide an approximate protective marking breakdown (totalling 100%) 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	%

Ensure the breakdown of the organisation's information assets equals 100%

Information Security Incidents	How many information security incidents were recorded in the organisation's internal register over the last 24 months?	
	Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and 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) (300 character limit)

Freedom of Information | Privacy | Data Protection   All fields on this page are mandatory unless otherwise stated   34

OFFICIAL ▾

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

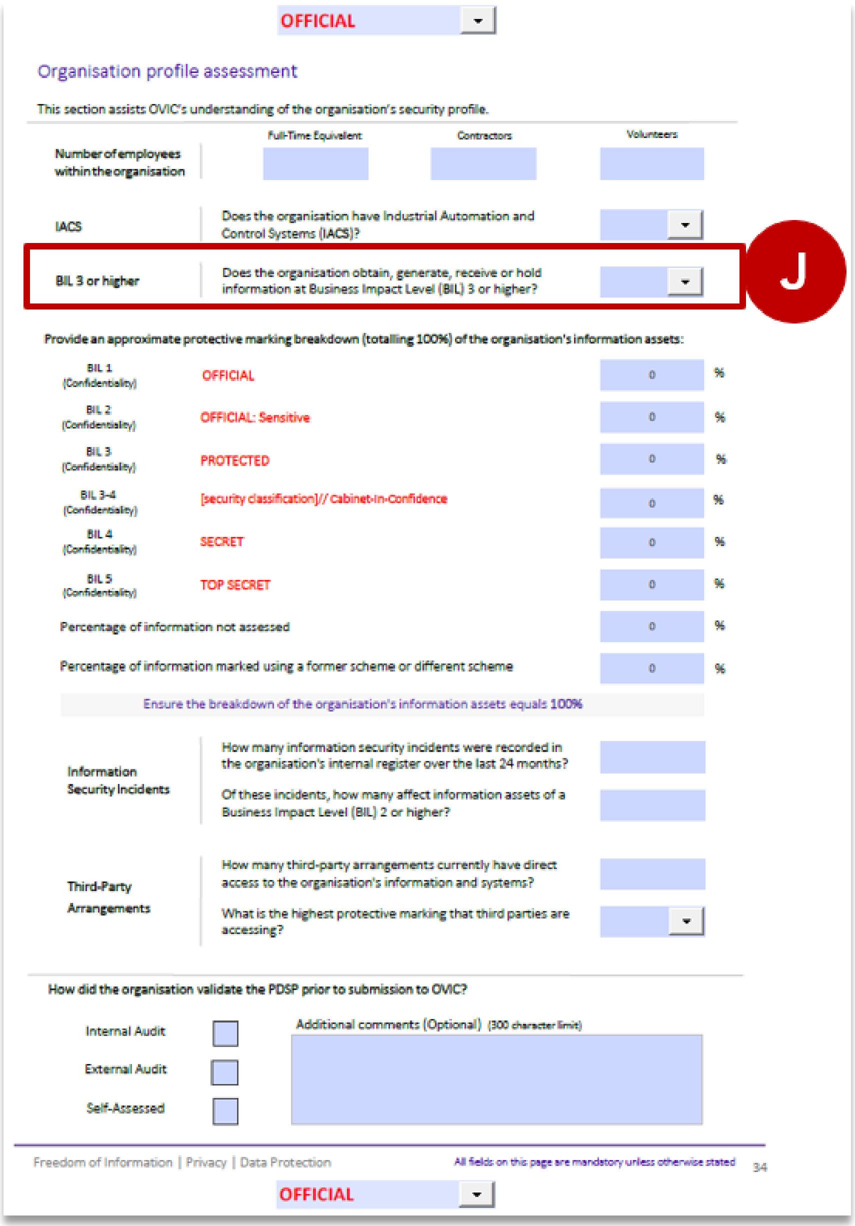
Note: this also includes Board members.

What is meant by Industrial Automation and Control Systems (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
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Select the most appropriate *IACS* response based on the organisation's systems.	Dropdown menu	I



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			

IACS	Does the organisation have Industrial Automation and Control Systems (IACS)?	▾
BIL 3 or higher	Does the organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3 or higher?	▾

Provide an approximate protective marking breakdown (totalling 100%) 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	%

Ensure the breakdown of the organisation's information assets equals 100%

Information Security Incidents	How many information security incidents were recorded in the organisation's internal register over the last 24 months?	
	Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and 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) (300 character limit)

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

34

OFFICIAL ▾

Description	Field Type	Image ref.
Select the most appropriate *BIL 3 or higher* response based on the organisation's information. This is not an average, but the highest level of information that your organisation obtains, generates, receives, or holds. To assist in answering this section, refer to the organisation's Information Asset Register outlined under elements **E2.020** and **E2.040**.	Dropdown menu	J

What is meant by a BIL 3?

Business Impact Levels (**BILs**) are quantitative measures that describe the potential impact arising from a compromise of the -

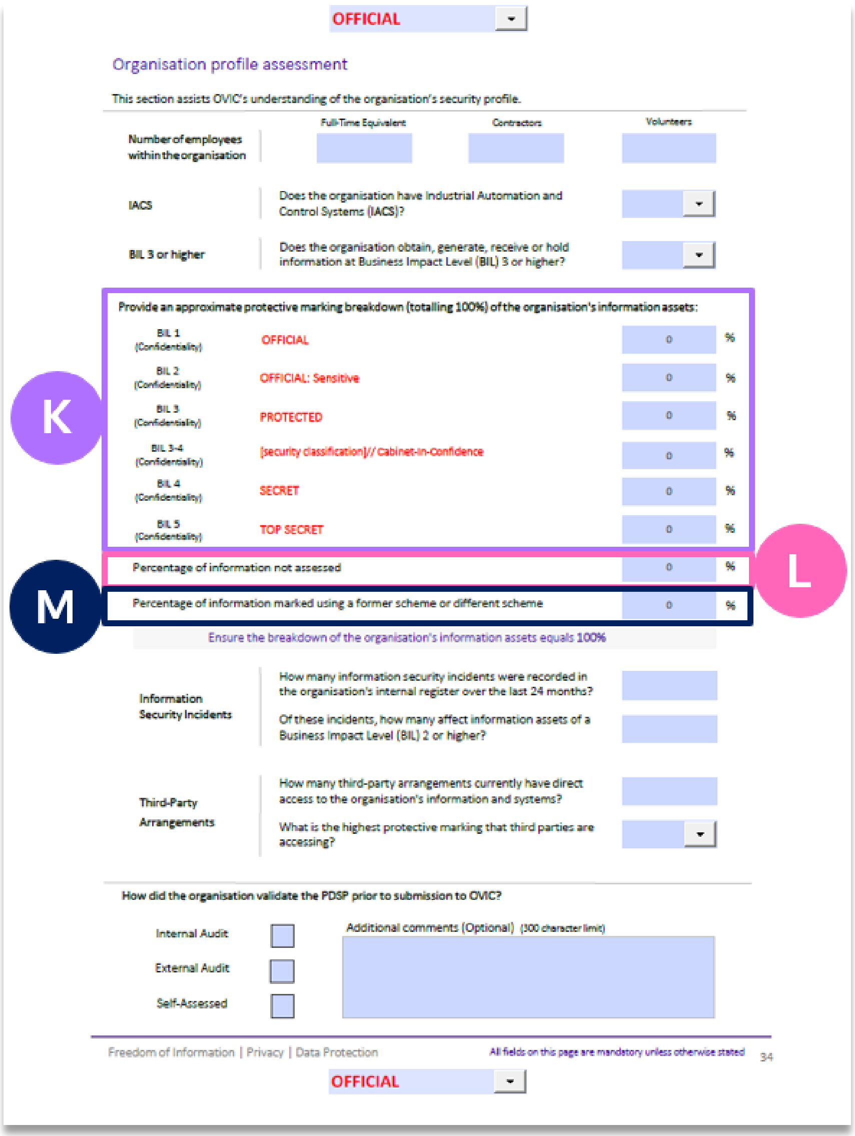
- Confidentiality
- Integrity and / or
- Availability

of public sector information.

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 organisation.



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			

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

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

Provide an approximate protective marking breakdown (totalling 100%) 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	%

Ensure the breakdown of the organisation's information assets equals 100%

Information Security Incidents
- How many information security incidents were recorded in the organisation's internal register over the last 24 months?
- Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?

Third-Party Arrangements
- How many third-party arrangements currently have direct access to the organisation's information and 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) (300 character limit)

Freedom of Information | Privacy | Data Protection All fields on this page are mandatory unless otherwise stated 34

OFFICIAL

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

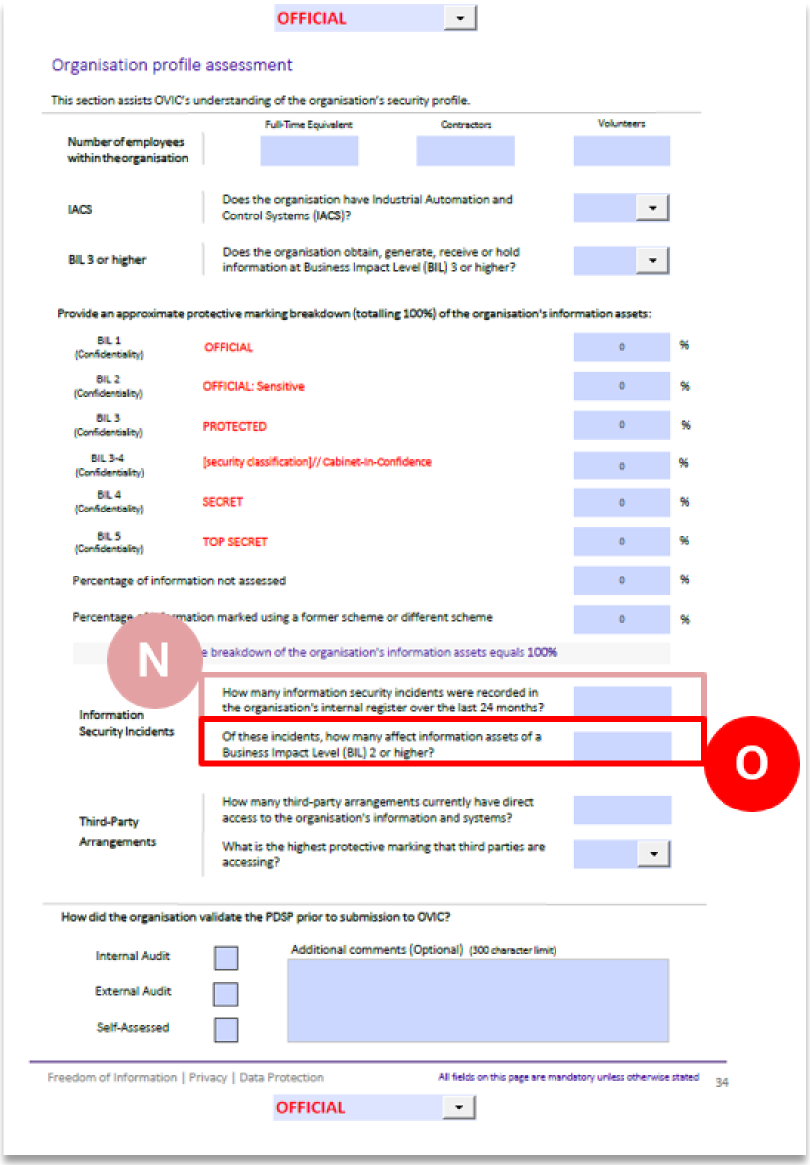
What are protective markings?

Protective markings are security labels assigned to public sector information and directly correspond to outcomes of a confidentiality assessment.

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.

If the organisation is yet to undertake an information security value assessment for all **active** information assets, provide an indicative percentage of the information assets that are yet to be assessed.	Numerical free text	L
If the organisation has **active** information assets marked under a **former or different scheme** (i.e. those that are yet to be reassessed and re-labelled under the current protective marking scheme), provide an indicative percentage in this field.	Numerical free text	M

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



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			

IACS	Does the organisation have Industrial Automation and Control Systems (IACS)?	▾
BIL 3 or higher	Does the organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3 or higher?	▾

Provide an approximate protective marking breakdown (totalling 100%) 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	%

e breakdown of the organisation's information assets equals 100%

Information Security Incidents	How many information security incidents were recorded in the organisation's internal register over the last 24 months?	
	Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and 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) (300 character limit)

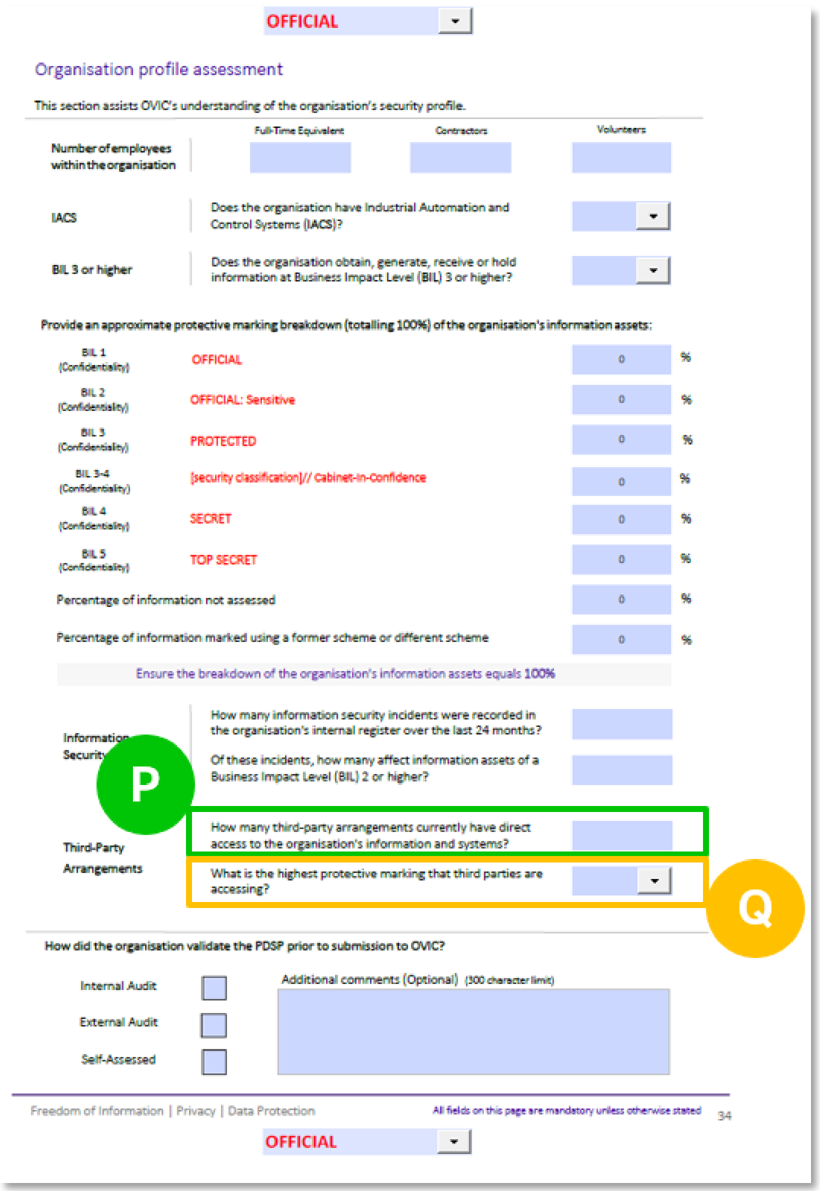
Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

34

OFFICIAL ▾

Description	Field Type	Image ref.
The organisation should indicate the number of information security incidents that occurred in the last **24 months** and were **recorded** (documented) in its internal incident register.	Numerical free text	N
What qualifies as an information security incident? An information security incident refers to one or multiple 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 information or verbal discussions.		
Note: Under E6.040 the organisation records information security incidents in a register.		
To complete the follow up incident question, the organisation should have an understanding of the security value of the information (expressed as a BIL) impacted by the incident. List the total number of incidents where the information affected was assessed as BIL 2 or higher.	Numerical free text	O
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.		
Note: Under element E9.010 information security incidents that have resulted in a compromise of information assessed at a BIL 2 or higher, should be reported to OVIC.		



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			

IACS	Does the organisation have Industrial Automation and Control Systems (IACS)?	
BIL 3 or higher	Does the organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3 or higher?	

Provide an approximate protective marking breakdown (totalling 100%) 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	%

Ensure the breakdown of the organisation's information assets equals 100%

Information Security	How many information security incidents were recorded in the organisation's internal register over the last 24 months?	
	Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and 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) (300 character limit)

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

34

OFFICIAL

Description	Field Type	Image ref.
List the number of third-party arrangements where the third party currently has direct access to the organisation's information and information systems. If the organisation has a register of third-party arrangements (e.g., contracts, MOUs, and information sharing agreements), this can be helpful in identifying which third parties may have direct access to public sector information. Refer to your third-party arrangements register as outlined under element **E8.050**.	Numerical free text	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 2 parts of the State is also an arrangement because it is not possible to make a legally binding contract between 2 parts of the same legal entity – the State of Victoria.

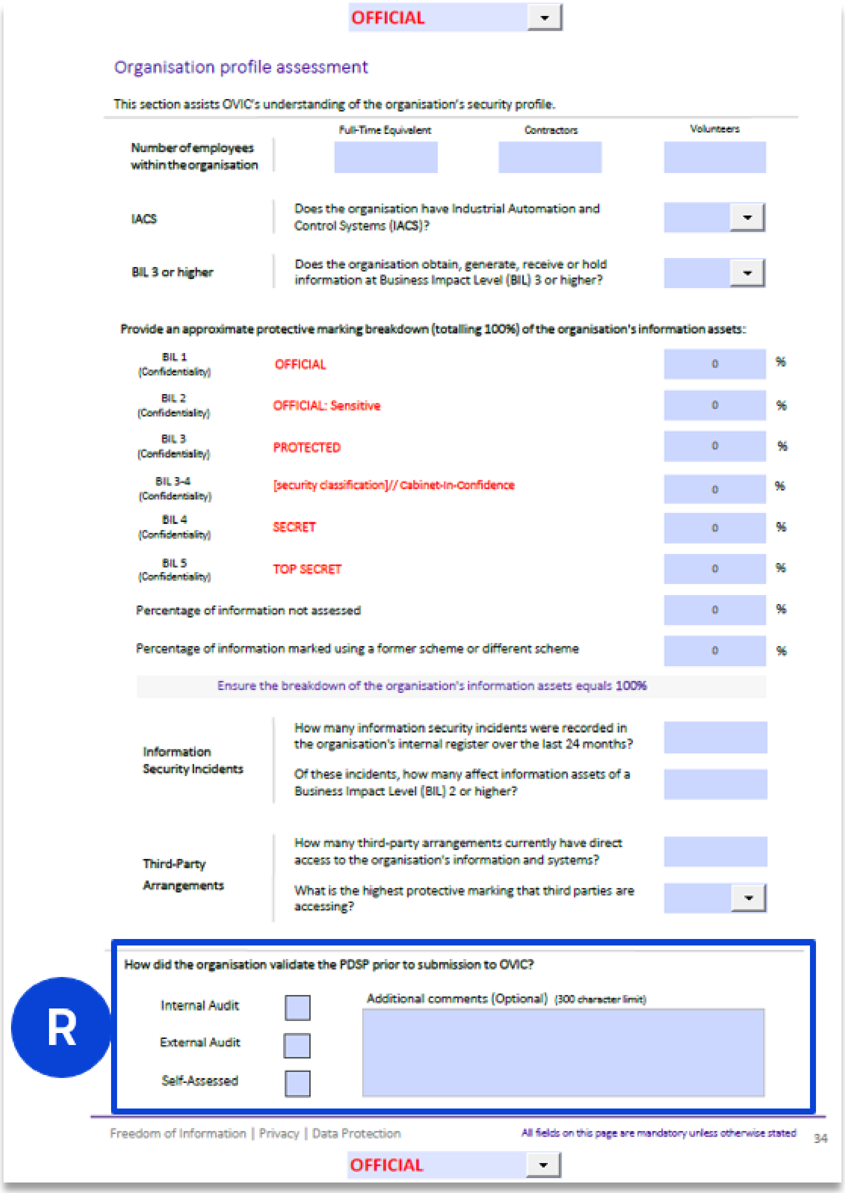
What is meant by third party?

Any person or entity external to the organisation. This can include another public or private organisation, 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. Viewing information / systems that has been released in an authorised manner is not considered direct access.

Choose the most appropriate *protective marking* response from the drop-down selections. If the organisation has a register of third-party arrangements, this can be helpful in identifying what type of information third parties are accessing and the highest security value accessed by them.	Dropdown menu	Q



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			

IACS	Does the organisation have Industrial Automation and Control Systems (IACS)?	
BIL 3 or higher	Does the organisation obtain, generate, receive or hold information at Business Impact Level (BIL) 3 or higher?	

Provide an approximate protective marking breakdown (totalling 100%) 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	%

Ensure the breakdown of the organisation's information assets equals 100%

Information Security Incidents	How many information security incidents were recorded in the organisation's internal register over the last 24 months?	
	Of these incidents, how many affect information assets of a Business Impact Level (BIL) 2 or higher?	
Third-Party Arrangements	How many third-party arrangements currently have direct access to the organisation's information and systems?	
	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 □

Additional comments (Optional) (300 character limit)

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

34

OFFICIAL

Description	Field Type	Image ref.
Check the most appropriate *PDSP validation* box or note the method used in the '**Additional comments**' field. When answering this section consider how the responses provided on the PDSP were verified and confirmed prior to the submission to OVIC. The drop-down options are: **Internal Audit** – the organisation conducted an internal security audit to validate PDSP responses. **External Audit**– the organisation contracted a third party to validate PDSP responses. **Self-assessed –** no formal audit or review was undertaken of the PDSP responses. **Additional comments** – If the organisation verified the PDSP prior to submission in another way, or wants to provide more information about this, note this in the '*Additional comments*' free text field.	Checkboxes with optional free text field (300-character limit)	R

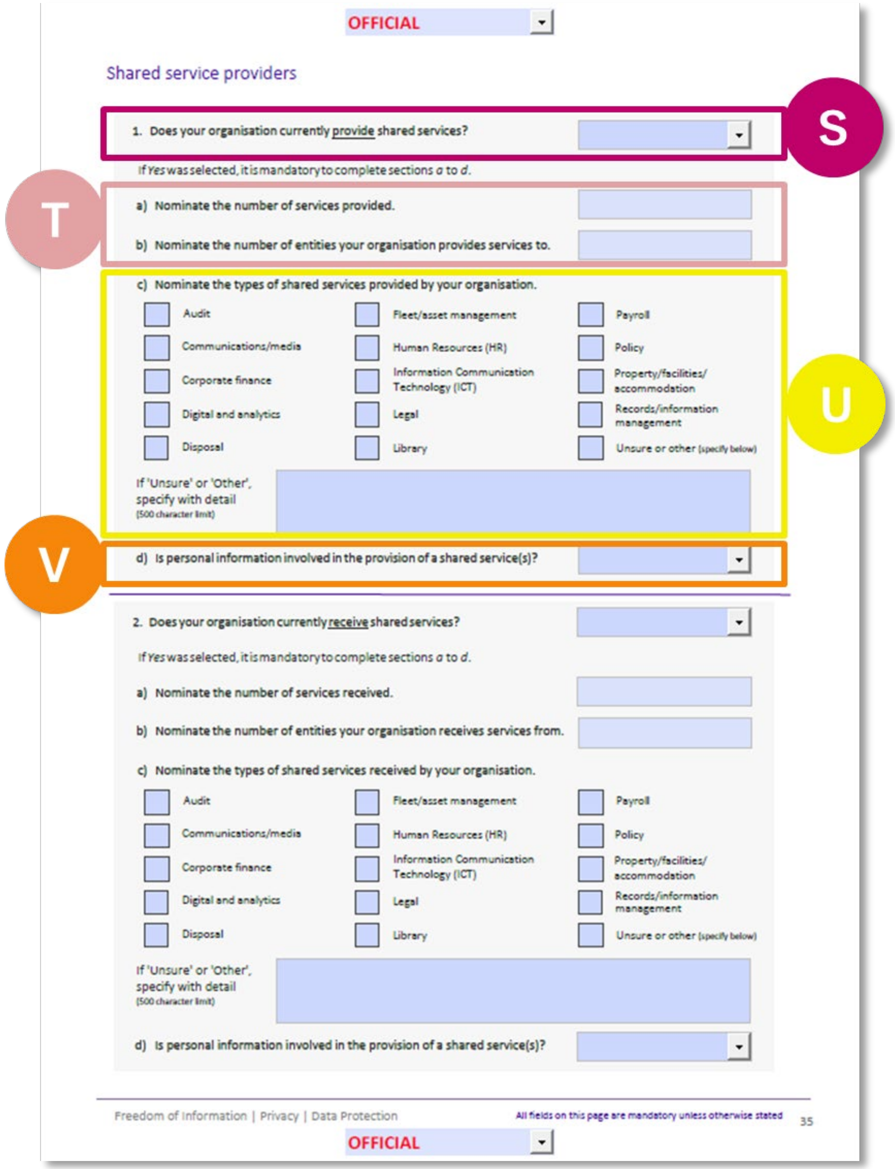
Note to auditors

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

When auditing against a PDSP, auditors should consider how specific controls are implemented with regard to the organisation's own internal and external context, the security value of its information, and any associated risks.

Auditors should avoid viewing implementation of the elements as a compliance activity and instead focus on the risk management aspects.

Shared Service Providers: OVIC has added questions around the provision or receipt of shared services. Responses to this section of the PDSP form should reflect arrangements that are in place at the time of submission, noting that these arrangements may be subject to change.



OFFICIAL

Shared service providers

1. Does your organisation currently provide shared services?

If *Yes* was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services provided.

b) Nominate the number of entities your organisation provides services to.

c) Nominate the types of shared services provided by your organisation.

□ Audit	□ Fleet/asset management	□ Payroll
□ Communications/media	□ Human Resources (HR)	□ Policy
□ Corporate finance	□ Information Communication Technology (ICT)	□ Property/facilities/ accommodation
□ Digital and analytics	□ Legal	□ Records/information management
□ Disposal	□ Library	□ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail (500 character limit)

d) Is personal information involved in the provision of a shared service(s)?

2. Does your organisation currently receive shared services?

If *Yes* was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services received.

b) Nominate the number of entities your organisation receives services from.

c) Nominate the types of shared services received by your organisation.

□ Audit	□ Fleet/asset management	□ Payroll
□ Communications/media	□ Human Resources (HR)	□ Policy
□ Corporate finance	□ Information Communication Technology (ICT)	□ Property/facilities/ accommodation
□ Digital and analytics	□ Legal	□ Records/information management
□ Disposal	□ Library	□ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail (500 character limit)

d) Is personal information involved in the provision of a shared service(s)?

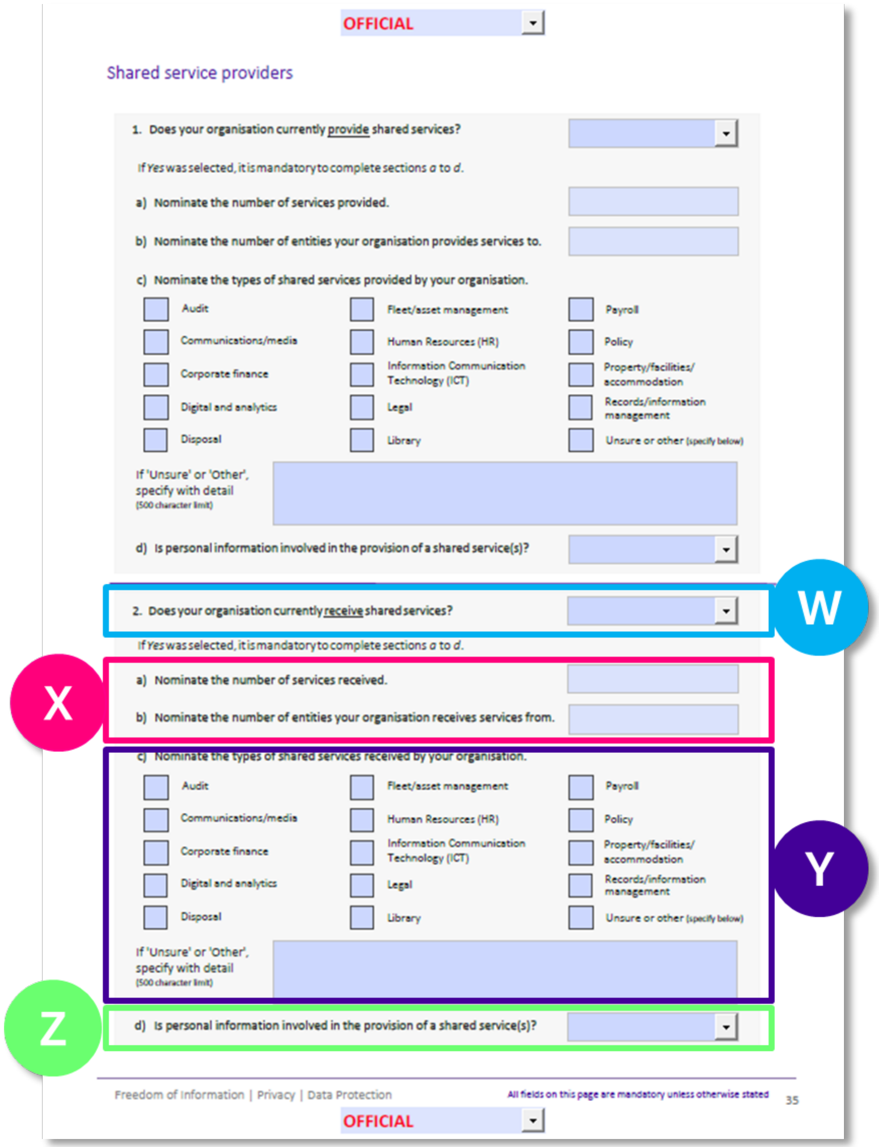
Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

35

OFFICIAL

Description	Field Type	Image ref.
Choose the most appropriate *shared service provider* response from the drop-down selections. If either *No* or *Unsure* are selected, no further response is required (proceed to Question 2).	Dropdown menu	S
A **shared service provider** is a government agency/body that delivers support functions to other government agencies/bodies, acting like an internal business unit. Services may include but are not limited to HR, finance, IT, property, payroll, legal, libraries, and waste collection.		
Input the number of shared services provided and to how many organisations. The organisation should indicate the number of: a) **shared services provided** by your organisation, and b) the **number of entities** that your organisation provides shared services to.	Numerical free text	T
Check the corresponding boxes noting the type(s) of shared services provided by your organisation. If the service type is not listed or unknown, select *Unsure or other* and specify any additional type(s) in the space provided.	Checkboxes with accompanying free text field (500-character limit)	U
Choose the most appropriate *personal information* response from the drop-down selections.	Dropdown menu	V
Under section 3 of the PDP Act, **personal information** means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* applies.		



OFFICIAL

Shared service providers

1. Does your organisation currently provide shared services?

If *Yes* was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services provided.

b) Nominate the number of entities your organisation provides services to.

c) Nominate the types of shared services provided by your organisation.

- □ Audit
- □ Communications/media
- □ Corporate finance
- □ Digital and analytics
- □ Disposal
- □ Fleet/asset management
- □ Human Resources (HR)
- □ Information Communication Technology (ICT)
- □ Legal
- □ Library
- □ Payroll
- □ Policy
- □ Property/facilities/ accommodation
- □ Records/information management
- □ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail (500 character limit)

d) Is personal information involved in the provision of a shared service(s)?

2. Does your organisation currently receive shared services?

If *Yes* was selected, it is mandatory to complete sections *a* to *d*.

a) Nominate the number of services received.

b) Nominate the number of entities your organisation receives services from.

c) Nominate the types of shared services received by your organisation.

- □ Audit
- □ Communications/media
- □ Corporate finance
- □ Digital and analytics
- □ Disposal
- □ Fleet/asset management
- □ Human Resources (HR)
- □ Information Communication Technology (ICT)
- □ Legal
- □ Library
- □ Payroll
- □ Policy
- □ Property/facilities/ accommodation
- □ Records/information management
- □ Unsure or other (specify below)

If 'Unsure' or 'Other', specify with detail (500 character limit)

d) Is personal information involved in the provision of a shared service(s)?

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

35

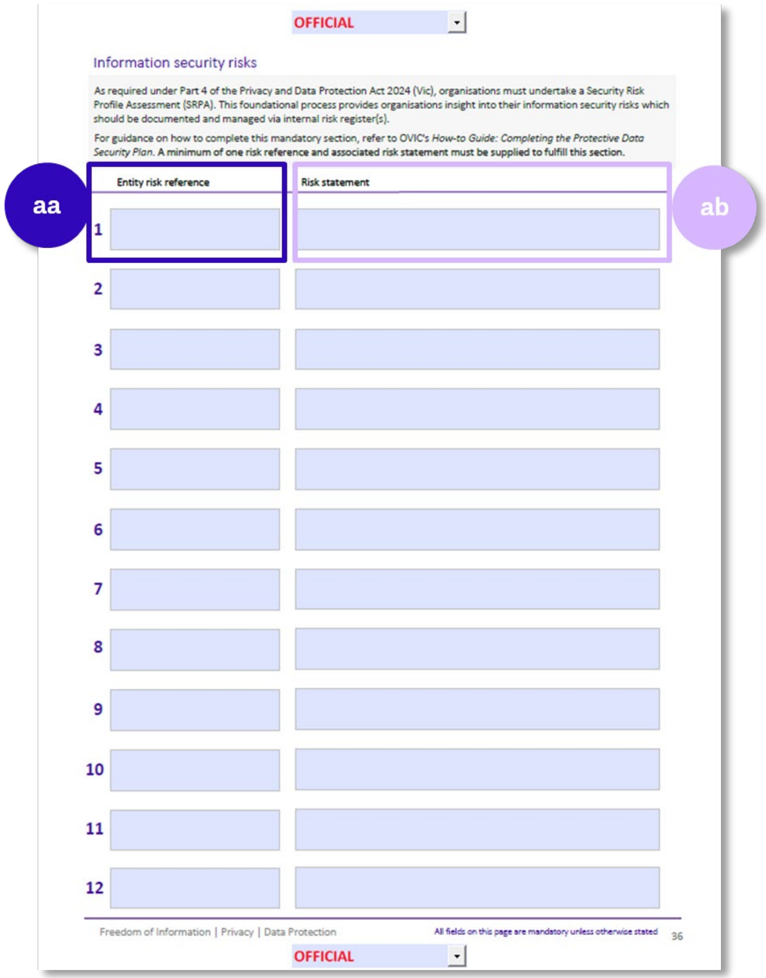
OFFICIAL

Description	Field Type	Image ref.
Choose the most appropriate *shared service receiver* response from the drop-down selections. If either *No* or *Unsure* are selected, no further responses are required, proceed to the next page.	Dropdown menu	W
A **shared service receiver** is a government agency/body that uses support functions delivered by another department or agency. These services can include HR, finance, IT, property, payroll, legal, libraries and waste collection.		
Input the number of shared services received and from how many organisations. The organisation should indicate the number of: a) **shared services received** by your organisation, and b) the **number of entities** that provide services to your organisation.	Numerical free text	X
Check the corresponding boxes noting the type(s) of shared services received by your organisation. If the service type is not listed or unknown, select *Unsure or other* and specify any additional type(s) in the space provided.	Checkboxes with accompanying free text field (500-character limit)	Y
Choose the most appropriate *personal information* response from the drop-down selections.	Dropdown menu	Z

Information Security Risks: OVIC has added questions regarding organisations' information security risks. When responding to this section of the PDSP, consider the key information security risks of your organisation.

Organisations will have assessed information security risks and developed risk treatment strategies as part of the Security Risk Profile Assessment process, recording outcomes in an internal risk register.

Organisations may have a single enterprise-level information security risk addressing the 12 VPDSS. If so, note the single *entity risk reference* and associated *risk statement* in the first line. Where an organisation has multiple information security risk references and statements, use the additional fields to record these (max of 12).



OFFICIAL

Information security risks

As required under Part 4 of the Privacy and Data Protection Act 2024 (Vic), organisations must undertake a Security Risk Profile Assessment (SRPA). This foundational process provides organisations insight into their information security risks which should be documented and managed via internal risk register(s).

For guidance on how to complete this mandatory section, refer to OVIC's *How-to Guide: Completing the Protective Data Security Plan*. A minimum of one risk reference and associated risk statement must be supplied to fulfill this section.

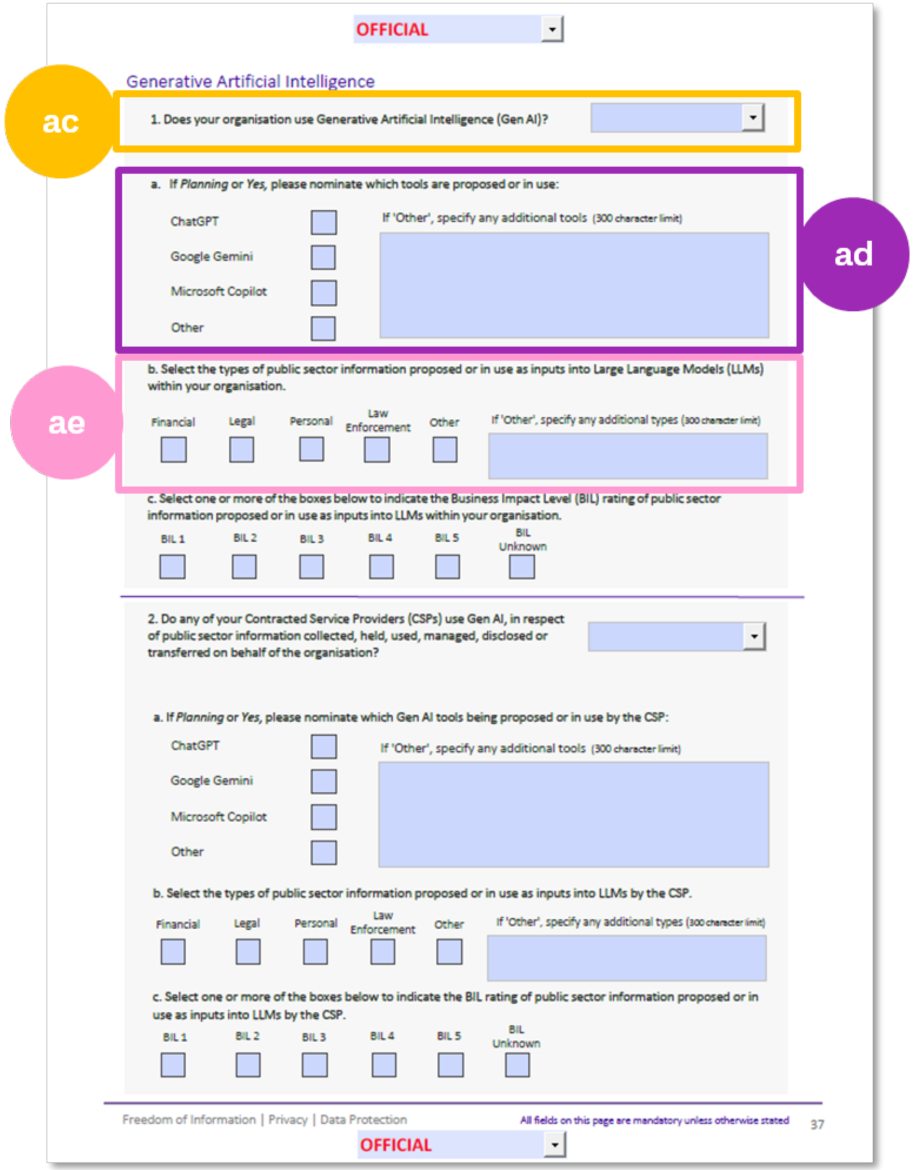
	Entity risk reference	Risk statement
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated 36

OFFICIAL

Description	Field Type	Image ref.
Note: The information security risks do not need to be listed in a particular order.		
Note: If your organisation has more than 12 information security risks and would like more space, contact the ISU to discuss your options.		
Input the **entity risk reference** in the associated field. Entity risk reference(s) recorded in Part A of the PDSP form will assist you in completing this section.	Free text field	aa
What is meant by information security risk? In the context of information security, information security risks can be expressed as events that can negatively influence the achievement of information security objectives in the organisation. Information security risks can be associated with the potential that threats will exploit vulnerabilities of an information asset(s) and thereby cause harm to an organisation. For more information, read OVIC's Practitioner Guide – Information Security Risk Management.		
Input the associated **risk statement** into the corresponding field. To complete this field, refer to your internal risk register and copy the relevant contents that correlates to the entity risk reference. Refer to your risk register as outlined under element E3.020.	Free text field	ab



OFFICIAL

Generative Artificial Intelligence

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

a. If *Planning* or *Yes*, please nominate which tools are proposed or in use:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools (300 character limit)

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 (300 character limit)

c. Select one or more of the boxes below to indicate the Business Impact Level (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 □ BIL 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?

a. If *Planning* or *Yes*, please nominate which Gen AI tools being proposed or in use by the CSP:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools (300 character limit)

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 (300 character limit)

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 □ BIL Unknown □

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

37

OFFICIAL

Description	Field Type	Image ref.
Choose the most appropriate *Generative Artificial Intelligence* (**Gen AI**) response from the drop-down selections. If either *No* or *Unsure* are selected, no further responses are required, proceed to Question 2.	Dropdown menu	ac

What is Gen AI?

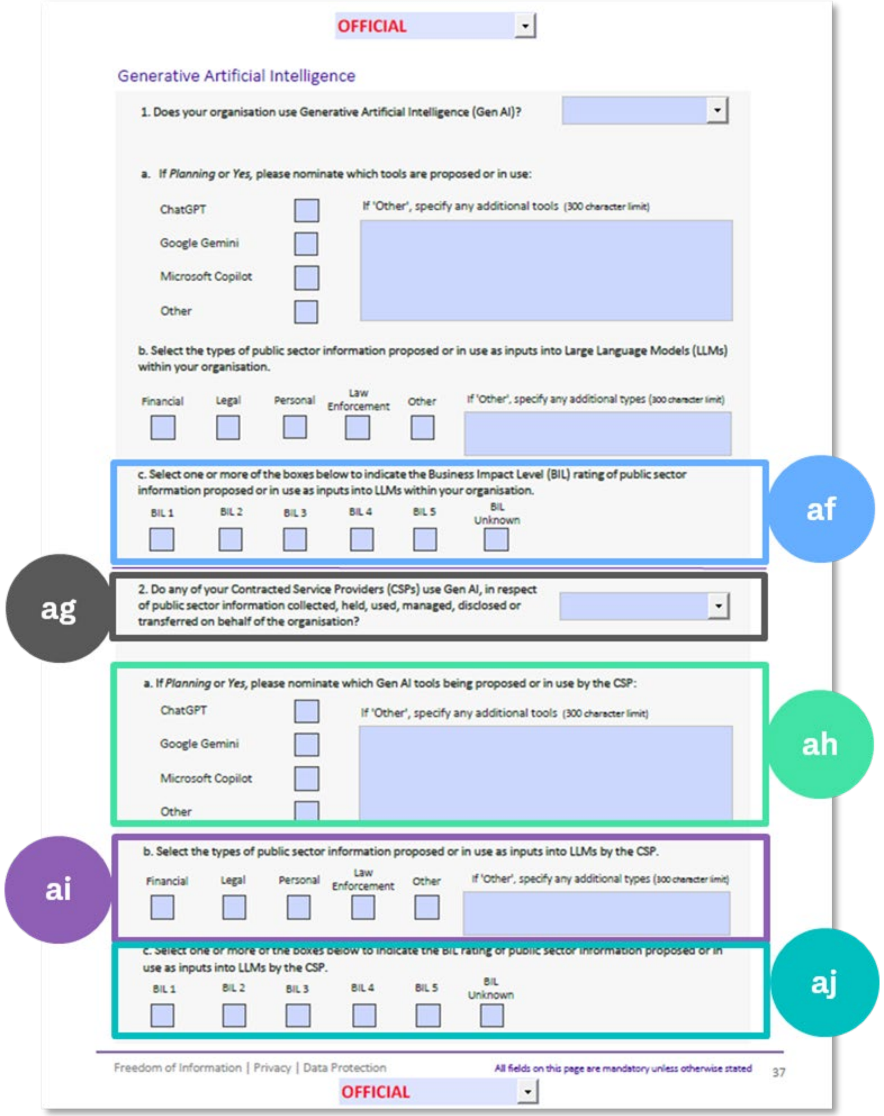
Algorithms, derived from machine learning, that learn from training data and can be used to create content with similar characteristics.

If either *Yes* or *Planning* were selected above, check the corresponding boxes against the relevant tool(s) proposed or in use. If the tool is: • not listed, select *Other* and specify any additional tool(s) in the free text field. • unknown at this stage, select *Other* and note this in the free text field. Multiple tools can be selected.	Checkboxes with accompanying free text field (300-character limit)	ad
Check the corresponding boxes noting the information type(s) that are proposed, or in use, as inputs into LLMs within your organisation. If the information type is not listed, select *Other* and specify any additional type(s) in the space provided. If the information type is unknown at this stage, select *Other* and note this in the free text field. Multiple information types can be selected.	Checkboxes with accompanying free text field (300-character limit)	ae

What are Large Language Models (LLMs)?

A subset of generative AI based on transformer networks. A transformer is a type of AI model that learns to understand and generate human-like text by analysing patterns in large amounts of text data.

Part B of the PDSP form



OFFICIAL

Generative Artificial Intelligence

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

a. If *Planning* or *Yes*, please nominate which tools are proposed or in use:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools (300 character limit)

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 (300 character limit)
□	□	□	□	□	

c. Select one or more of the boxes below to indicate the Business Impact Level (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	BIL 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?

a. If *Planning* or *Yes*, please nominate which Gen AI tools being proposed or in use by the CSP:

ChatGPT □
Google Gemini □
Microsoft Copilot □
Other □

If 'Other', specify any additional tools (300 character limit)

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 (300 character limit)
□	□	□	□	□	

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	BIL Unknown
□	□	□	□	□	□

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

37

OFFICIAL

Description	Field Type	Image ref.
Nominate the assessed BIL rating(s) of public sector information used as an input into the LLM. Select all BIL ratings that apply.	Checkbox(es)	af
Choose the most appropriate *Gen AI* response from the dropdown selection. If either *No* or *Unsure* are selected, no further responses are required for this page.	Dropdown menu	ag
Note: The below questions relate only to the use of Gen AI by Contracted Service Providers (CSP) for public sector information collected, held, used, managed, disclosed, or transferred on behalf of the organisation.		
If either *Yes* or *Planning* were selected, check the corresponding boxes against the relevant tool(s) proposed or in use by the CSP. If the tool is: • not listed, select *Other* and specify any additional tool(s) in the free text field. • unknown at this stage, select *Other* and note in the free text field. Multiple tools can be selected.	Checkboxes with accompanying free text field (300-character limit)	ah
Check the corresponding boxes noting the information type(s) that are proposed, or in use, as inputs into LLMs by CSPs. • If the information type is not listed, select *Other* and specify in the free text field. • If the information type is unknown at this stage, select *Other* and note in the free text field. Multiple information types can be selected.	Checkboxes with accompanying free text field (300-character limit)	ai
Nominate the assessed BIL rating(s) of public sector information used as an input into the LLM by CSPs. Select all BIL ratings that apply	Checkboxes	aj

Part C – Attestation

Annual submission of an Attestation to OVIC is set out under element **E9.040**.

The purpose of the Attestation is to:

- confirm the organisation is continuing its program of information security activities per the VPDSS, as outlined in the PDSP,
- confirm the contents of the PDSP are accurate, and
- acknowledge the public sector body Head's obligations under Part 4 of the PDP Act.

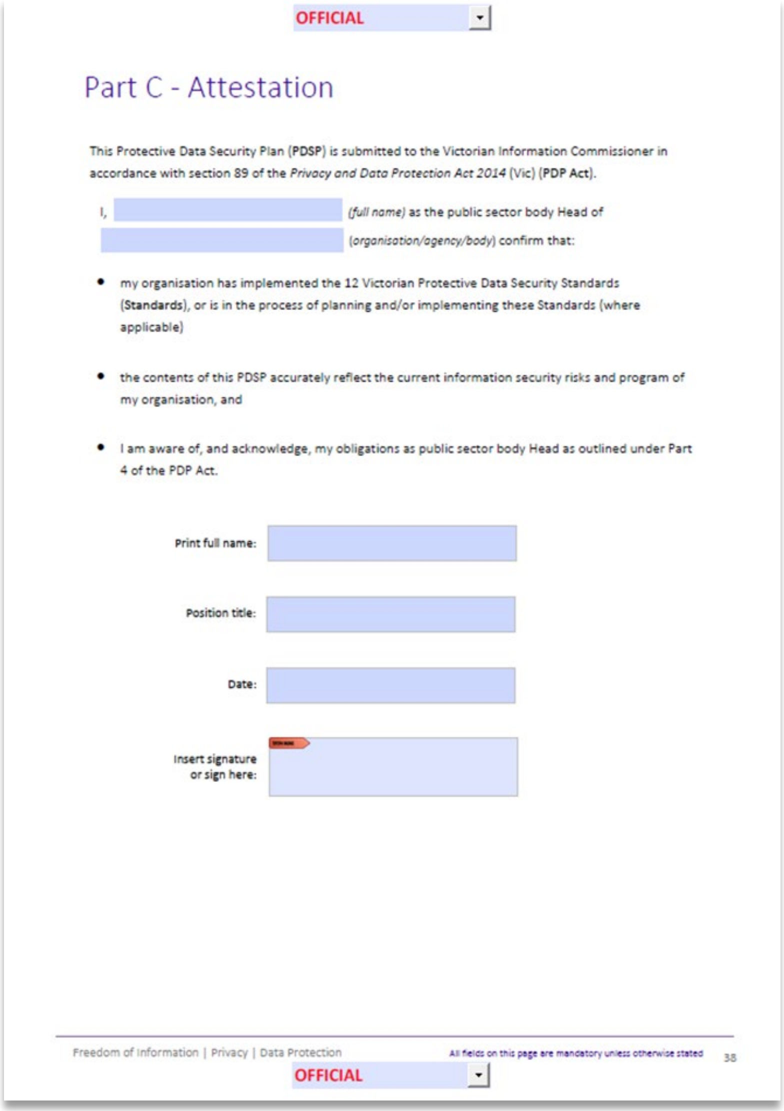
The Attestation must be signed by the public sector body Head and cannot be delegated to another person.

Signing the Attestation

Data entry	Description
Soft copy / electronic	• Use the Adobe Acrobat Reader *Fill & Sign* feature to add the public sector body Head's signature into the box provided • Insert an image file (e.g. jpg, tiff, bmp) of the public sector body Head's signature into the box provided, or • Type the name of the public sector body Head's signature into the box provided.
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 page may be combined with the remainder of the PDSP.

Note: OVIC uses the data extracted from the PDSPs to develop insights to provide back to Victorian government on the VPS's compliance with the Standards over time.

If, by signing the PDSP, the document locks, our team is unable to extract data for review. In order to extract the data, we require an unlocked/unsigned version of the PDSP, to analyse data and trends.



OFFICIAL

Part C - Attestation

This Protective Data Security Plan (**PDSP**) is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

I, ______ *(full name)* as the public sector body Head of

______ (*organisation/agency/body*) confirm that:

- my organisation has implemented the 12 Victorian Protective Data Security Standards (**Standards**), or is in the process of planning and/or implementing these Standards (where applicable)
- the contents of this PDSP accurately reflect the current information security risks and program of my organisation, and
- I am aware of, and acknowledge, my obligations as public sector body Head as outlined under Part 4 of the PDP Act.

Print full name:

Position title:

Date:

Insert signature or sign here:

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated 38

OFFICIAL

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.

PDSPs marked as **OFFICIAL** **and** **OFFICIAL: Sensitive**	Option 1	Soft copy / electronic	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 a copy of the PDSP in a single opaque envelope with no protective marking label on the outside to: PO Box 24274 Melbourne VIC 3001	
	Option 3	Hard copy	Hand-deliver a copy of the PDSP to: Attention: OVIC Level 34/121 Exhibition Street Melbourne	**Please note:** Please ensure you contact the ISU prior to submitting via options 3, 4, 5 and 6.
PDSPs marked as **PROTECTED**	Option 4	Soft copy / electronic	Speak to the ISU requesting to send a copy of the completed, signed and dated PDSP via OVIC's authorised secure file transfer platform	
	Option 5	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	
	Option 6	Hard copy	Deliver a copy of the PDSP by SCEC-endorsed courier to: Attention: OVIC Level 34/121 Exhibition Street Melbourne	

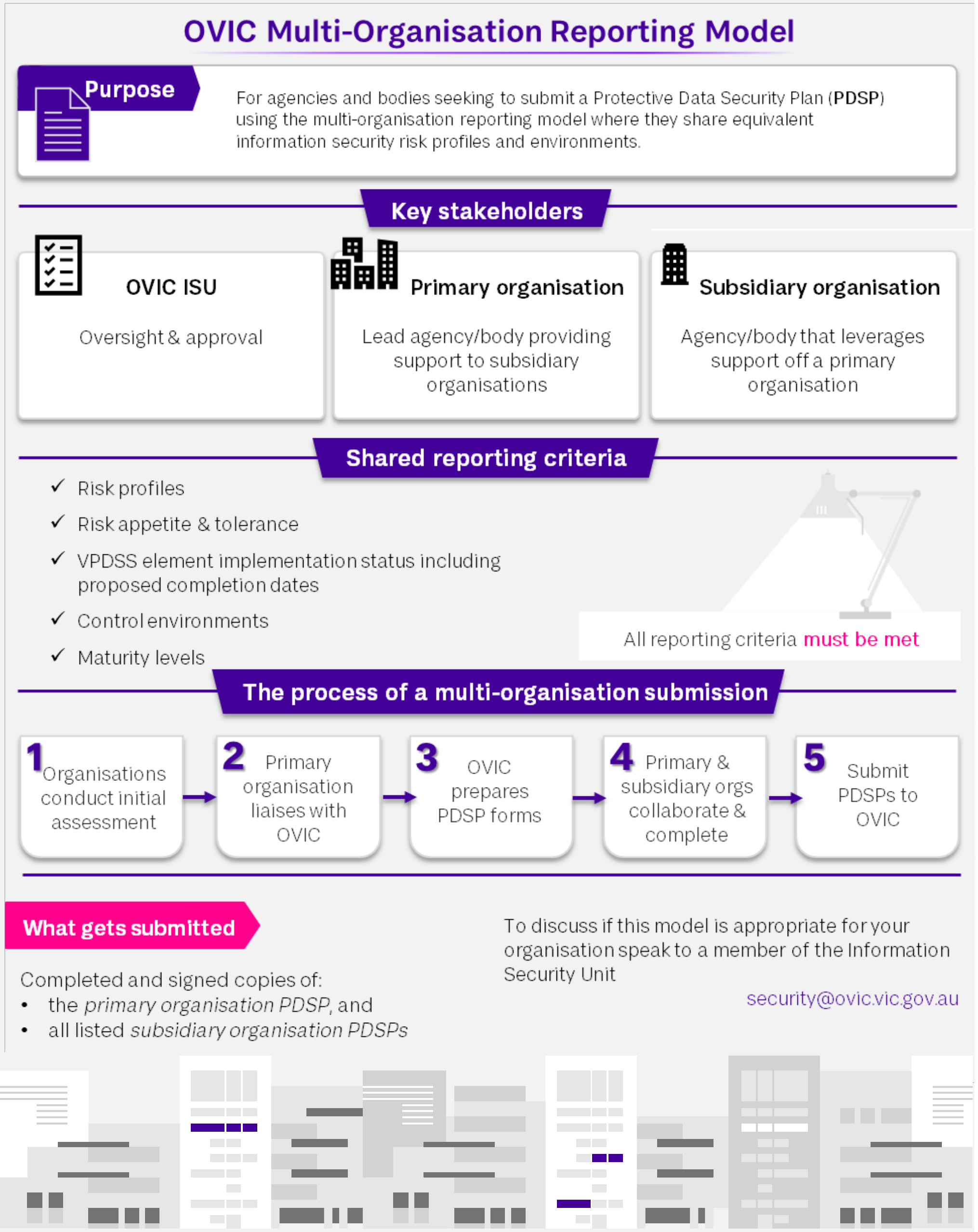
Next steps

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 and document 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

VPDSS Glossary	https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-glossary-v2-1/
Agency Reporting Obligations	https://ovic.vic.gov.au/information-security/agency-reporting-obligations/
Victorian public sector stakeholders	https://ovic.vic.gov.au/information-security/agency-reporting-obligations/vps-stakeholders/
VPDSF BIL Table	https://ovic.vic.gov.au/information-security/victorian-protective-data-security-framework-business-impact-level-table-v2-1/
OVIC Regulatory Action Policy	https://ovic.vic.gov.au/regulatory-action/regulatory-action-policy/
VPDSS Implementation Guidance v2.4	https://ovic.vic.gov.au/information-security/victorian-protective-data-security-standards-implementation-guidance/
Implementation Guidance for IACS	https://ovic.vic.gov.au/information-security/information-security-resources/implementation-guidance-for-industrial-automation-and-control-systems/
Information Security Risk Management	https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/
Assessing the Security Value of Public Sector Information	https://ovic.vic.gov.au/information-security/practitioner-guide-assessing-the-security-value-of-public-sector-information-v2-0/
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/



OVIC Multi-Organisation Reporting Model

Purpose

For agencies and bodies seeking to submit a Protective Data Security Plan (**PDSP**) using the multi-organisation reporting model where they share equivalent information security risk profiles and environments.

Key stakeholders

OVIC ISU

Oversight & approval

Primary organisation

Lead agency/body providing support to subsidiary organisations

Subsidiary organisation

Agency/body that leverages support off a primary organisation

Shared reporting criteria

✓ Risk profiles

✓ Risk appetite & tolerance

✓ VPDSS element implementation status including proposed completion dates

✓ Control environments

✓ Maturity levels

All reporting criteria **must be met**

The process of a multi-organisation submission

1 Organisations conduct initial assessment →

2 Primary organisation liaises with OVIC →

3 OVIC prepares PDSP forms →

4 Primary & subsidiary orgs collaborate & complete →

5 Submit PDSPs to OVIC

What gets submitted

Completed and signed copies of:

- the *primary organisation PDSP*, and
- all listed *subsidiary organisation PDSPs*

To discuss if this model is appropriate for your organisation speak to a member of the Information Security Unit

security@ovic.vic.gov.au

Appendix – Multi-organisation reporting model

What is the multi-organisation reporting model?

This model is designed to help organisations submit a consolidated PDSP where organisations have equivalent:

- risk profiles (including appetite and tolerance)
- risk references
- control environments
- implementation statuses
- completion dates for the VPDSSE, and
- maturity levels

Where this shared reporting criteria:

- **can be** met by all parties, contact the ISU to discuss your requirements and request a copy of the tailored PDSP forms.
- **cannot be** met by all parties, the multi-organisation PDSP reporting model is deemed unsuitable. In this scenario a *single organisation PDSP form* must be submitted by each agency or body.

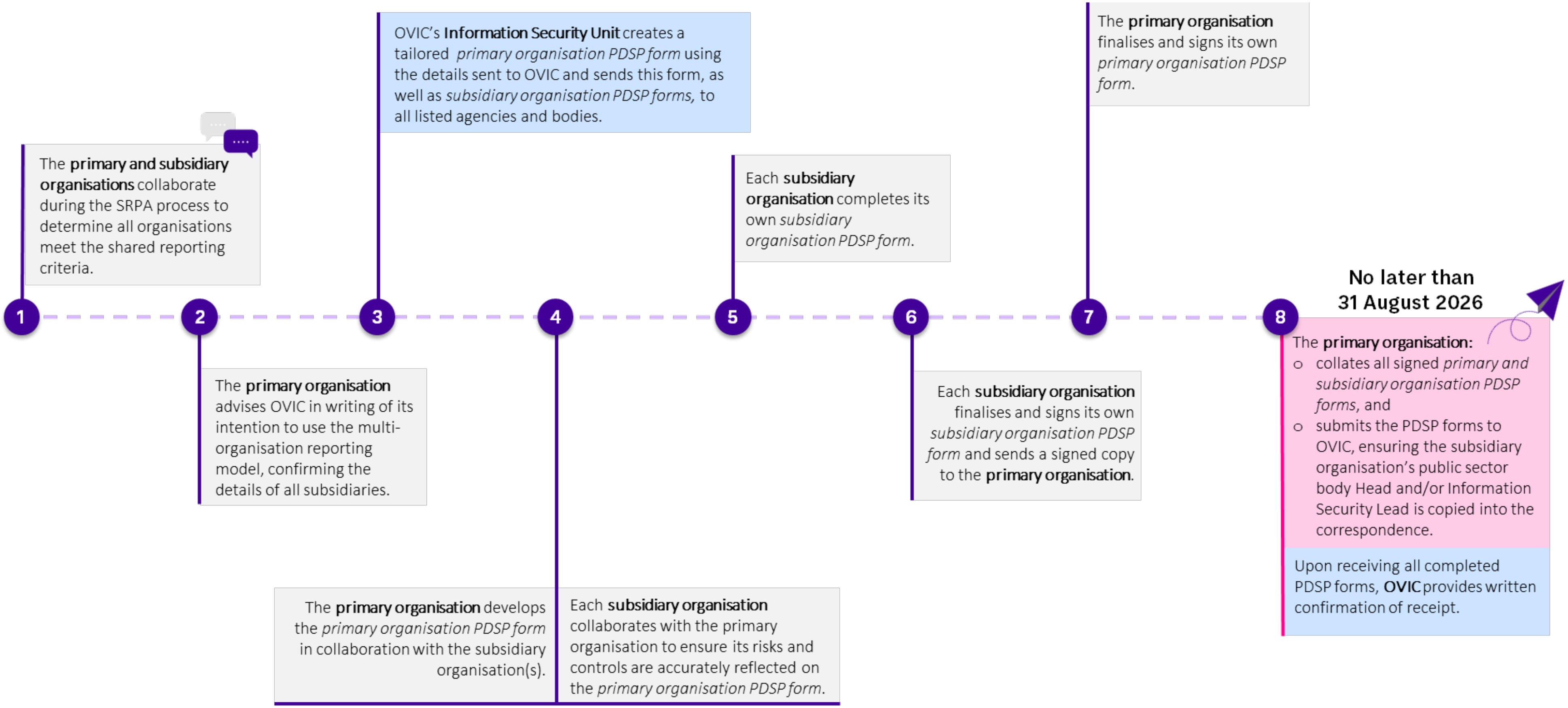
What is a primary organisation and a subsidiary organisation?

The *primary organisation* refers to the agency or body that leads/supports the information security program for itself and other organisations. Support arrangements may entail providing guidance on information security risk, helping implement the Standards, and submitting a PDSP to OVIC.

A *subsidiary organisation* effectively operates as a business unit of the *primary organisation*, that leverages support off a primary organisation to help manage its information security program.

Overview of multi-organisation reporting model process

Organisations intending to use the multi-organisation reporting model should refer to the below to help navigate the process.



The **primary and subsidiary organisations** collaborate during the SRPA process to determine all organisations meet the shared reporting criteria.

The **primary organisation** advises OVIC in writing of its intention to use the multi-organisation reporting model, confirming the details of all subsidiaries.

OVIC's **Information Security Unit** creates a tailored *primary organisation PDSP form* using the details sent to OVIC and sends this form, as well as *subsidiary organisation PDSP forms*, to all listed agencies and bodies.

The **primary organisation** develops the *primary organisation PDSP form* in collaboration with the subsidiary organisation(s).

Each **subsidiary organisation** collaborates with the primary organisation to ensure its risks and controls are accurately reflected on the *primary organisation PDSP form*.

Each **subsidiary organisation** completes its own *subsidiary organisation PDSP form*.

Each **subsidiary organisation** finalises and signs its own *subsidiary organisation PDSP form* and sends a signed copy to the **primary organisation**.

The **primary organisation** finalises and signs its own *primary organisation PDSP form*.

No later than 31 August 2026

The **primary organisation:**

- collates all signed *primary and subsidiary organisation PDSP forms*, and
- submits the PDSP forms to OVIC, ensuring the subsidiary organisation's public sector body Head and/or Information Security Lead is copied into the correspondence.

Upon receiving all completed PDSP forms, **OVIC** provides written confirmation of receipt.

Participating in the multi-organisation reporting model

All organisations that intend to utilise the multi-organisation reporting model must collaborate with one another, confirming that all agencies and bodies meet the same shared reporting criteria. Once established, the *primary organisation* must contact OVIC to confirm in writing their intention to participate in the multi-organisation reporting model.

OVIC suggests primary organisations use the following email template when liaising with the ISU.

To:	security@ovic.vic.gov.au	
cc:	*[include any relevant contacts from within the primary organisation and the subsidiary organisation]*	
Subject:	*[primary organisation name]* - intention to use multi-organisation PDSP reporting model in 2026	
Content:	I write to confirm that *[primary organisation name]* intends to use the multi-organisation reporting model in 2026, and the subsidiaries listed below meet the shared criteria outlined below: a. risk profiles (including appetite and tolerance) b. control environments c. implementation statuses for the elements (including completion dates for VPDSSE) d. risk references, and e. maturity levels Subsidiaries: 1. Subsidiary organisation name: *[subsidiary organisation name]* Public sector body Head's name: *[public sector body Head of the subsidiary organisation]* Public sector body Head's position title: *[title of public sector body Head of the subsidiary organisation]* Public sector body Head's email address: *[email address of public sector body Head of the subsidiary organisation]* 2. Subsidiary organisation name: *[Insert subsidiary organisation name #2]* …	If you need to add additional subsidiaries, please copy and paste item 1 and complete the corresponding details. Please include your email signature with your contact details and role title, should the ISU have any follow-up questions.

How to complete the multi-organisation PDSP forms

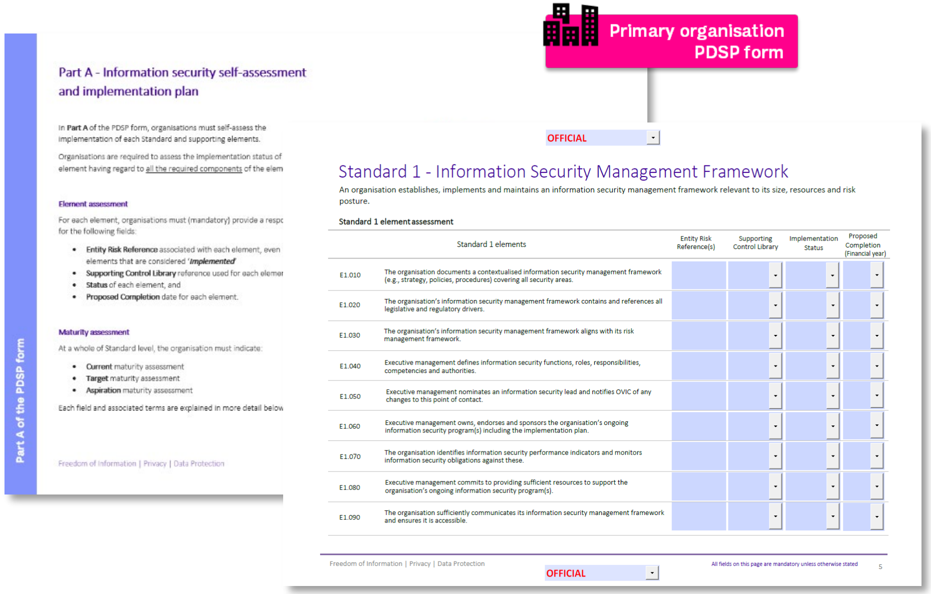
Part A – Information security self-assessment and implementation plan

Primary organisation PDSP form

The primary organisation develops Part A of the *primary organisation PDSP form* in collaboration with the subsidiary organisation(s) listed in Part D of the PDSP form.

Part A of the *primary organisation PDSP form* must accurately represent the information security program for **all** the subsidiary agencies and bodies, as well as the primary organisation.

For further guidance on how to complete this section, refer to Part A of the PDSP form in this guide.



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.

Organisations are required to assess the implementation status of element having regard to all the required components of the elem

Element assessment

For each element, organisations must (mandatory) provide a respo for the following fields:

- **Entity Risk Reference** associated with each element, even elements that are considered '***Implemented***'
- **Supporting Control Library** reference used for each elemer
- **Status** of each element, and
- **Proposed Completion** date for each element.

Maturity assessment

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

- **Current** maturity assessment
- **Target** maturity assessment
- **Aspiration** maturity assessment

Each field and associated terms are explained in more detail below

Freedom of Information | Privacy | Data Protection

OFFICIAL

Standard 1 - Information Security Management Framework

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

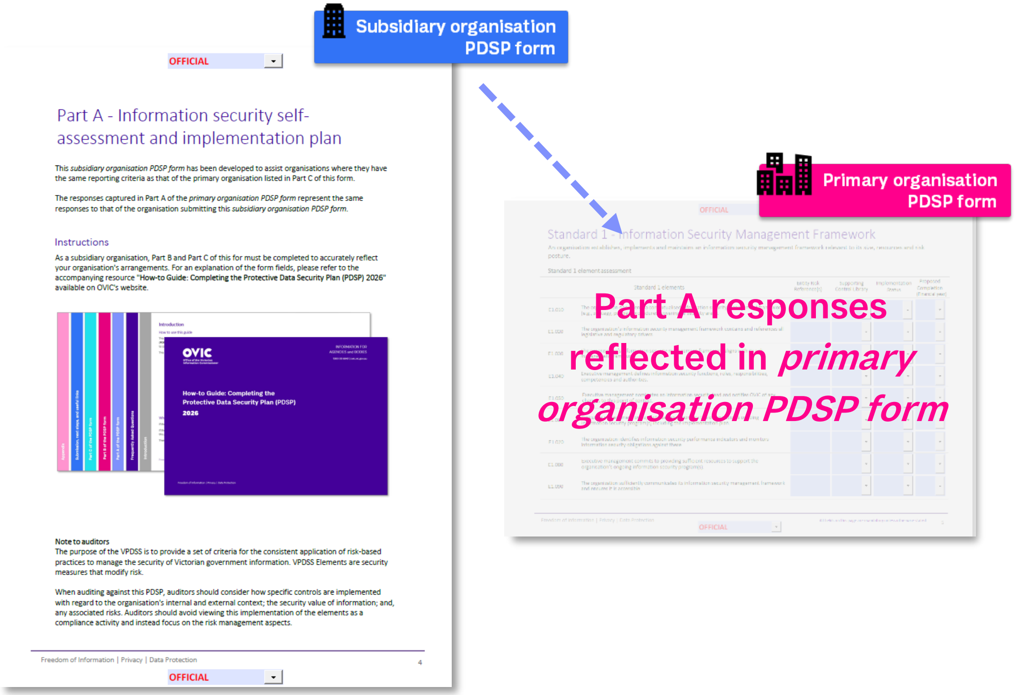
Standard 1 element assessment

Standard 1 elements		Entity Risk Reference(s)	Supporting Control Library	Implementation Status	Proposed Completion (Financial year)
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.				
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.				
E1.030	The organisation's information security management framework aligns with its risk management framework.				
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.				
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.				
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.				
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.				
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).				
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.				

Freedom of Information | Privacy | Data Protection OFFICIAL All fields on this page are mandatory unless otherwise stated 5

Subsidiary organisation PDSP form

The PDSP form for subsidiary organisations does not include a section for the subsidiary agency or body to record responses in Part A of their PDSP form. Instead, the information security self-assessment and implementation responses for the subsidiary agency or body are reflected on the primary organisation's PDSP submission.


Subsidiary organisation PDSP form
Primary organisation PDSP form
Part A responses reflected in *primary organisation PDSP form*
OVIC
How to Guide: Completing the Protective Data Security Plan (PDSP) 2026
Standard 1 - Information Security Management Framework
OFFICIAL

OFFICIAL

Part A - Information security self-assessment and implementation plan

This *subsidiary organisation PDSP form* has been developed to assist organisations where they have the same reporting criteria as that of the primary organisation listed in Part C of this form.

The responses captured in Part A of the *primary organisation PDSP form* represent the same responses to that of the organisation submitting this *subsidiary organisation PDSP form*.

Instructions

As a subsidiary organisation, Part B and Part C of this for must be completed to accurately reflect your organisation's arrangements. For an explanation of the form fields, please refer to the accompanying resource "**How-to Guide: Completing the Protective Data Security Plan (PDSP) 2026**" available on OVIC's website.

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

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

Freedom of Information | Privacy | Data Protection 4

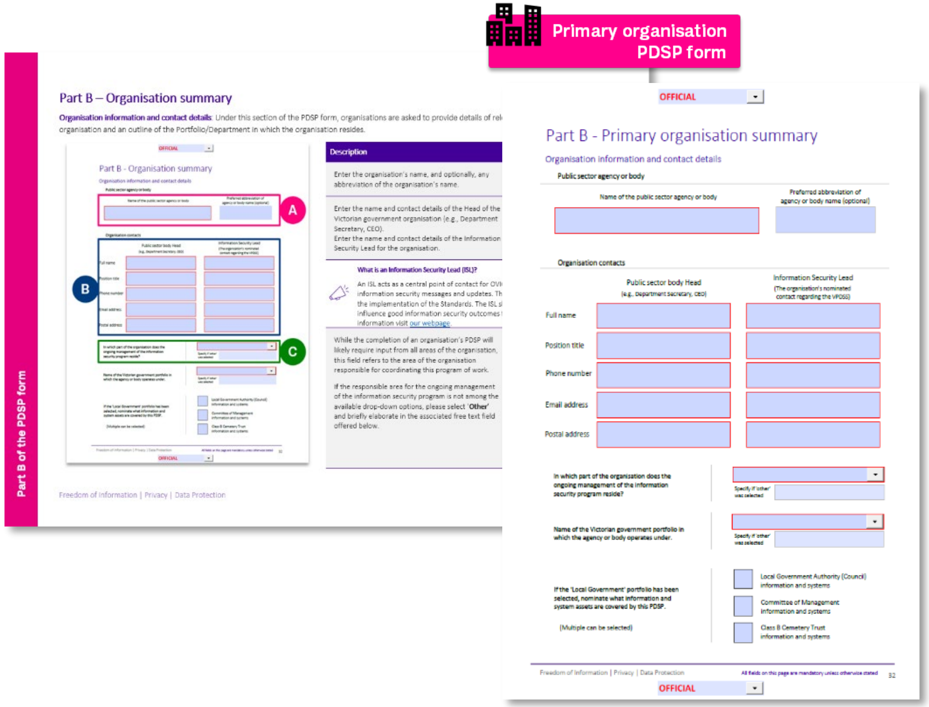
OFFICIAL

If the responses captured in the *primary organisation PDSP form* do not accurately represent the subsidiary organisation's implementation of the Standards, the multi-organisation reporting model should not be used.

Part B – Primary organisation summary

Primary organisation PDSP form

The primary organisation independently completes Part B of the *primary organisation PDSP form,* reflecting its current arrangements.



Part B – Organisation summary

Organisation information and contact details: Under this section of the PDSP form, organisations are asked to provide details of rel organisation and an outline of the Portfolio/Department in which the organisation resides.

Description
Enter the organisation's name, and optionally, any abbreviation of the organisation's name.
Enter the name and contact details of the Head of the Victorian government organisation (e.g., Department Secretary, CEO). Enter the name and contact details of the Information Security Lead for the organisation.
What is an Information Security Lead (ISL)? An ISL acts as a central point of contact for OVI information security messages and updates. Th the implementation of the Standards. The ISL s influence good information security outcomes information visit our webpage.
While 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. If the responsible area for the ongoing management of the information security program is not among the available drop-down options, please select '**Other**' and briefly elaborate in the associated free text field offered below.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Part B - Primary organisation summary

Organisation information and contact details

Public sector agency or body

Name of the public sector agency or body	Preferred abbreviation of agency or body name (optional)

Organisation contacts

	Public sector body Head (e.g., Department Secretary, CEO)	Information Security Lead (The organisation's nominated contact regarding the VPDSS)
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? — Specify if 'other' was selected

Name of the Victorian government portfolio in which the agency or body operates under. — Specify if 'other' was selected

If the 'Local Government' portfolio has been selected, nominate what information and system assets are covered by this PDSP.

(Multiple can be selected)

□ Local Government Authority (Council) information and systems

□ Committee of Management information and systems

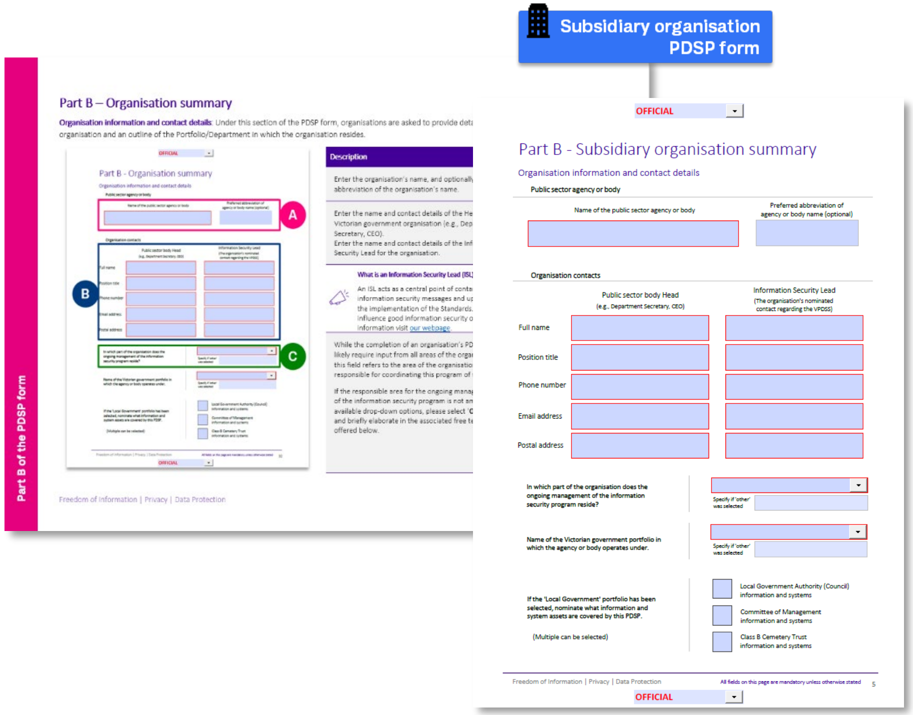
□ Class B Cemetery Trust information and systems

Freedom of Information | Privacy | Data Protection — All fields on this page are mandatory unless otherwise stated — 32

OFFICIAL

Subsidiary organisation PDSP form

The subsidiary organisation independently completes Part B of the *subsidiary organisation PDSP form,* reflecting its current arrangements.



Part B – Organisation summary

Organisation information and contact details: Under this section of the PDSP form, organisations are asked to provide deta organisation and an outline of the Portfolio/Department in which the organisation resides.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Part B - Subsidiary organisation summary

Organisation information and contact details

Public sector agency or body

Name of the public sector agency or body	Preferred abbreviation of agency or body name (optional)

Organisation contacts

	Public sector body Head (e.g., Department Secretary, CEO)	Information Security Lead (The organisation's nominated contact regarding the VPDSS)
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? — Specify if 'other' was selected

Name of the Victorian government portfolio in which the agency or body operates under. — Specify if 'other' was selected

If the 'Local Government' portfolio has been selected, nominate what information and system assets are covered by this PDSP.

(Multiple can be selected)

□ Local Government Authority (Council) information and systems

□ Committee of Management information and systems

□ Class B Cemetery Trust information and systems

Freedom of Information | Privacy | Data Protection — All fields on this page are mandatory unless otherwise stated — 5

OFFICIAL

Note: Primary and subsidiary organisations are not required to collaborate to complete this section.

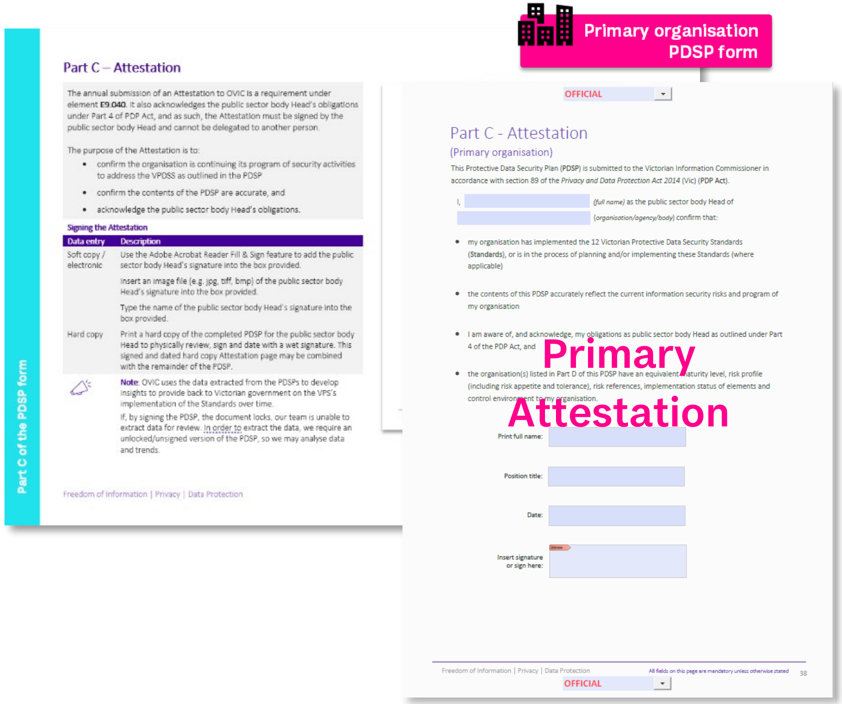
For further guidance on how to complete this section, refer to Part B of the PDSP form in this document.

Part C – Attestation

Primary organisation PDSP form

As part of the multi-organisation reporting model, the Attestation by the primary organisation includes confirmation that the subsidiary organisation(s) listed in Part D of the *primary organisation PDSP form* have an equivalent maturity level, risk profile (including risk appetite and tolerance), risk references, implementation status of elements and control environment.

The public sector body Head of the primary agency or body must complete the Attestation on the *primary organisation PDSP form*.



Part C of the PDSP form

Part C – Attestation

The annual submission of an Attestation to OVIC is a requirement under element **E9.040**. It also acknowledges the public sector body Head's obligations under Part 4 of PDP Act, and as such, the Attestation must be signed by the public sector body Head and cannot be delegated to another person.

The purpose of the Attestation is to:

- confirm the organisation is continuing its program of security activities to address the VPDSS as outlined in the PDSP
- confirm the contents of the PDSP are accurate, and
- acknowledge the public sector body Head's obligations.

Signing the Attestation

Data entry	Description
Soft copy / electronic	Use the Adobe Acrobat Reader Fill & Sign feature to add the public sector body Head's signature into the box provided. Insert an image file (e.g. jpg, tiff, bmp) of the public sector body Head's signature into the box provided. Type the name of the public sector body Head's signature into the box provided.
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 page may be combined with the remainder of the PDSP.

Note: OVIC uses the data extracted from the PDSPs to develop insights to provide back to Victorian government on the VPS's implementation of the Standards over time.

If, by signing the PDSP, the document locks, our team is unable to extract data for review. In order to extract the data, we require an unlocked/unsigned version of the PDSP, so we may analyse data and trends.

Freedom of Information | Privacy | Data Protection

OFFICIAL

Part C - Attestation

(Primary organisation)

This Protective Data Security Plan (**PDSP**) is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

I, ________ *(full name)* as the public sector body Head of ________ (*organisation/agency/body*) confirm that:

- my organisation has implemented the 12 Victorian Protective Data Security Standards (**Standards**), or is in the process of planning and/or implementing these Standards (where applicable)
- the contents of this PDSP accurately reflect the current information security risks and program of my organisation
- I am aware of, and acknowledge, my obligations as public sector body Head as outlined under Part 4 of the PDP Act, and
- the organisation(s) listed in Part D of this PDSP have an equivalent maturity level, risk profile (including risk appetite and tolerance), risk references, implementation status of elements and control environment to my organisation.

Print full name:

Position title:

Date:

Insert signature or sign here:

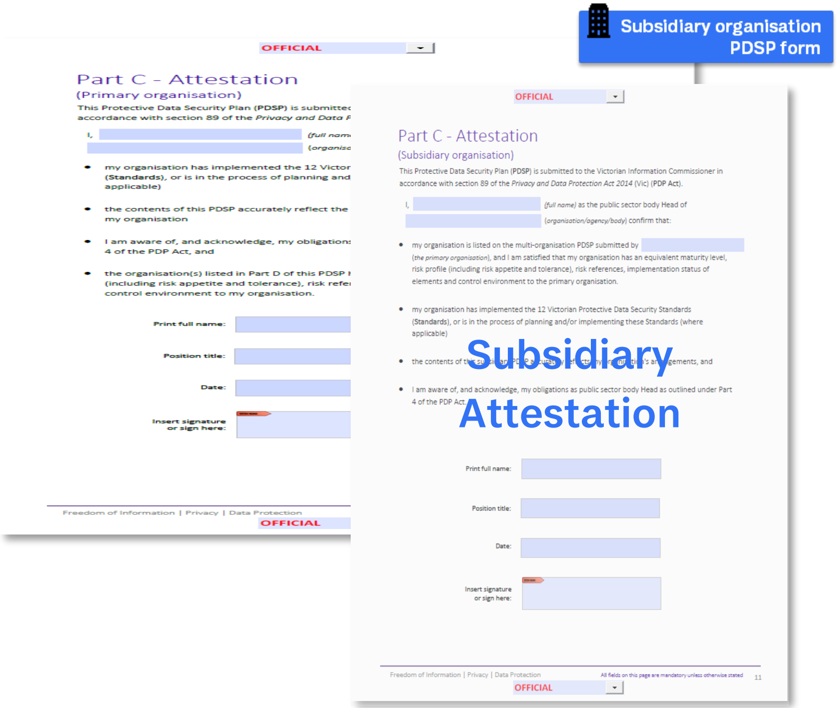
Freedom of Information | Privacy | Data Protection All fields on this page are mandatory unless otherwise stated 38

OFFICIAL

Subsidiary organisation PDSP form

As part of the multi-organisation reporting model, the Attestation by the subsidiary organisation includes confirmation the subsidiary organisation is listed in Part D of the *primary organisation PDSP form*. The public sector body Head of the subsidiary organisation attests that their agency or body has an equivalent maturity level, risk profile (including risk appetite and tolerance), risk references, implementation status of elements and control environment to that of the primary organisation.

The public sector body Head of the subsidiary agency or body must complete the Attestation on the *subsidiary organisation PDSP form*.



OFFICIAL

Part C - Attestation

(Primary organisation)

This Protective Data Security Plan (PDSP) is submitted
accordance with section 89 of the *Privacy and Data P*

I, *(full nam*

(organisa

- my organisation has implemented the 12 Victor (Standards), or is in the process of planning and applicable)
- the contents of this PDSP accurately reflect the my organisation
- I am aware of, and acknowledge, my obligations 4 of the PDP Act, and
- the organisation(s) listed in Part D of this PDSP h (including risk appetite and tolerance), risk refe control environment to my organisation.

Print full name:

Position title:

Date:

Insert signature or sign here:

Freedom of Information | Privacy | Data Protection

OFFICIAL

OFFICIAL

Part C - Attestation

(Subsidiary organisation)

This Protective Data Security Plan (**PDSP**) is submitted to the Victorian Information Commissioner in accordance with section 89 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

I, ________ *(full name)* as the public sector body Head of ________ (*organisation/agency/body*) confirm that:

- my organisation is listed on the multi-organisation PDSP submitted by ________ (*the primary organisation*), and I am satisfied that my organisation has an equivalent maturity level, risk profile (including risk appetite and tolerance), risk references, implementation status of elements and control environment to the primary organisation.
- my organisation has implemented the 12 Victorian Protective Data Security Standards (**Standards**), or is in the process of planning and/or implementing these Standards (where applicable)
- the contents of this subsidiary PDSP accurately reflects my organisation's arrangements, and
- I am aware of, and acknowledge, my obligations as public sector body Head as outlined under Part 4 of the PDP Act.

Print full name:

Position title:

Date:

Insert signature or sign here:

Freedom of Information | Privacy | Data Protection All fields on this page are mandatory unless otherwise stated 11

OFFICIAL

For further guidance on how to complete this section, refer to Part C of the PDSP form in this document.

Part D – Multi-organisation subsidiary list

Primary organisation PDSP form

The *primary organisation PDSP form* contains a section (Part D) listing the subsidiary organisations that meet the shared reporting criteria. By checking each box, the primary organisation confirms that the contents of its PDSP submission accurately reflect the arrangements of:

- itself, and
- each listed subsidiary organisation.

In doing so, OVIC will rely upon the responses offered in Part A of the *primary organisation PDSP form* when considering the information security arrangements of the subsidiary organisation, including the information security self-assessment and associated implementation plans.

Organisations intending to use the multi-organisation reporting model must approach OVIC early as the ISU needs to create customised reporting forms. The ISU will provide a *primary organisation PDSP form* that includes the:

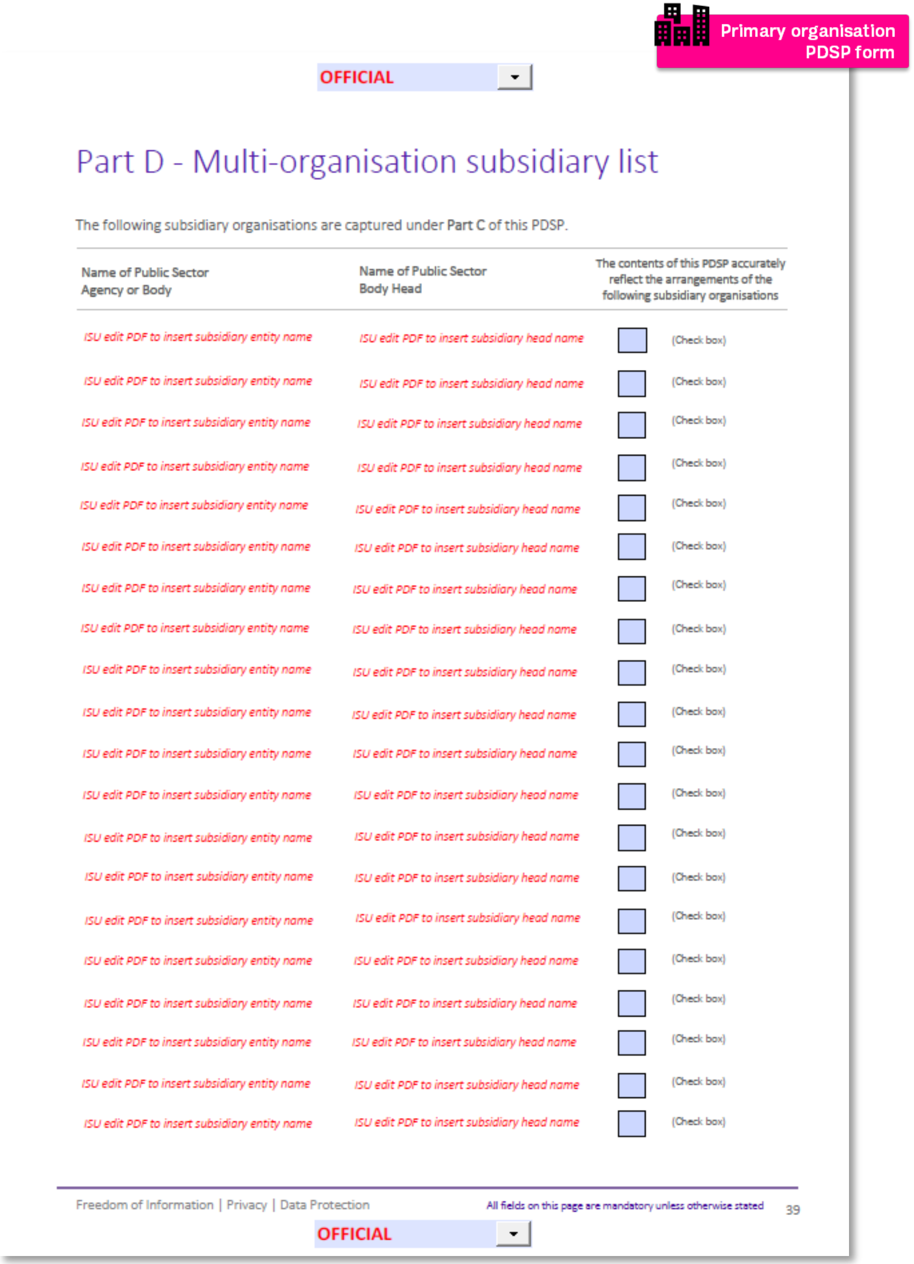
- *Name of Public Sector Agency or Body* and
- *Name of Public Sector Body Head*

of the subsidiary organisations.

If the subsidiary list needs to be amended, contact the ISU to do so.

Subsidiary organisation PDSP form

Part D is not included in the subsidiary organisation PDSP form.



OFFICIAL

Part D - Multi-organisation subsidiary list

The following subsidiary organisations are captured under **Part C** of this PDSP.

Name of Public Sector Agency or Body	Name of Public Sector Body Head	The contents of this PDSP accurately reflect the arrangements of the following subsidiary organisations
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)
ISU edit PDF to insert subsidiary entity name	*ISU edit PDF to insert subsidiary head name*	□ (Check box)

Freedom of Information | Privacy | Data Protection

All fields on this page are mandatory unless otherwise stated

39

OFFICIAL

OVIC

ovic.vic.gov.au