Office of the Victorian Information Commissioner

# Preparing for the 2026 Protective Data Security Plan

Victorian Information Security Network (**VISN**)

February 2026

A reminder – Today's session is being recorded.

# Acknowledgment of Country

**Laurencia Dimelow**

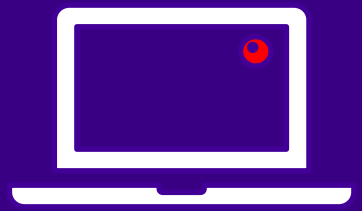
Acting Assistant Commissioner – Information Security

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

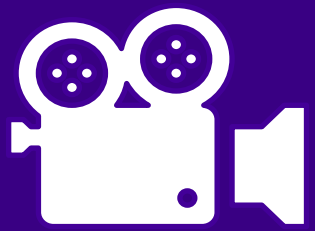
We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

# Housekeeping - What to be aware of

**Cameras and mics** have been **muted** for attendees.

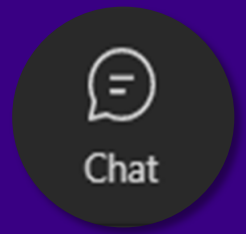


Today's session is **being recorded.**

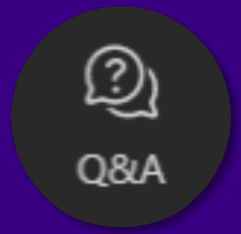


A copy of OVIC's **slides** and the **recording** will be made available in the coming days on our website.

# Housekeeping – How to engage



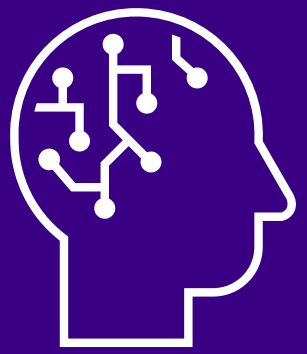

Regular **chat functionality** in Teams is **enabled** in this forum. Your name will be displayed against any questions you post.




If you want to ask an **anonymous question**, type your question into the **Teams Q&A channel**.


Each speaker will answer questions following the presentation. If you prefer to ask your question verbally, **raise your hand and come off mute when called upon.**

# Housekeeping – Use of AI tools



Slides and a recording of this session will be made available in the coming days.

As such, we ask for that no Generative AI tools are used to take notes or record this event. We will remove users/tools who do so.

## OVIC's position on the use of generative AI in meetings with OVIC

A PDF document of this information is available to view and download **here**.

This article outlines the Office of the Victorian Information Commissioner's (**OVIC**) position on the use of generative AI tools including AI notetakers, in meetings between OVIC's staff and OVIC's stakeholders.

OVIC's stakeholders may include Victorian public sector organisations, local councils, contracted service providers, consultants, Members of Parliament, interstate and international colleagues, and members of the public.

OVIC's staff includes OVIC employees and statutory office holders.

https://go.vic.gov.au/4fM3O3t

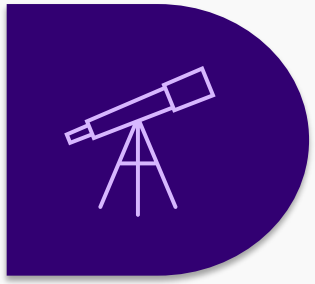
**Sean Morrison**

*Information Commissioner*

# Information Commissioner's highlights

### Thank you for your continued engagement

OVIC appreciates that organisations invest time and effort in complying and engaging with the Victorian Protective Data Security Standards (**VPDSS**).



### What we're seeing

The Information Security Unit understand that agencies and bodies are operating in dynamic risk environments.

### OVIC's forward focus

In 2026 OVIC will focus its efforts on strengthening its monitoring and assurance program, particularly centring on non-compliance.

### PDSP Validation

OVIC encourages organisations to critically consider and validate the responses offered on their PDSP.

# Today's agenda

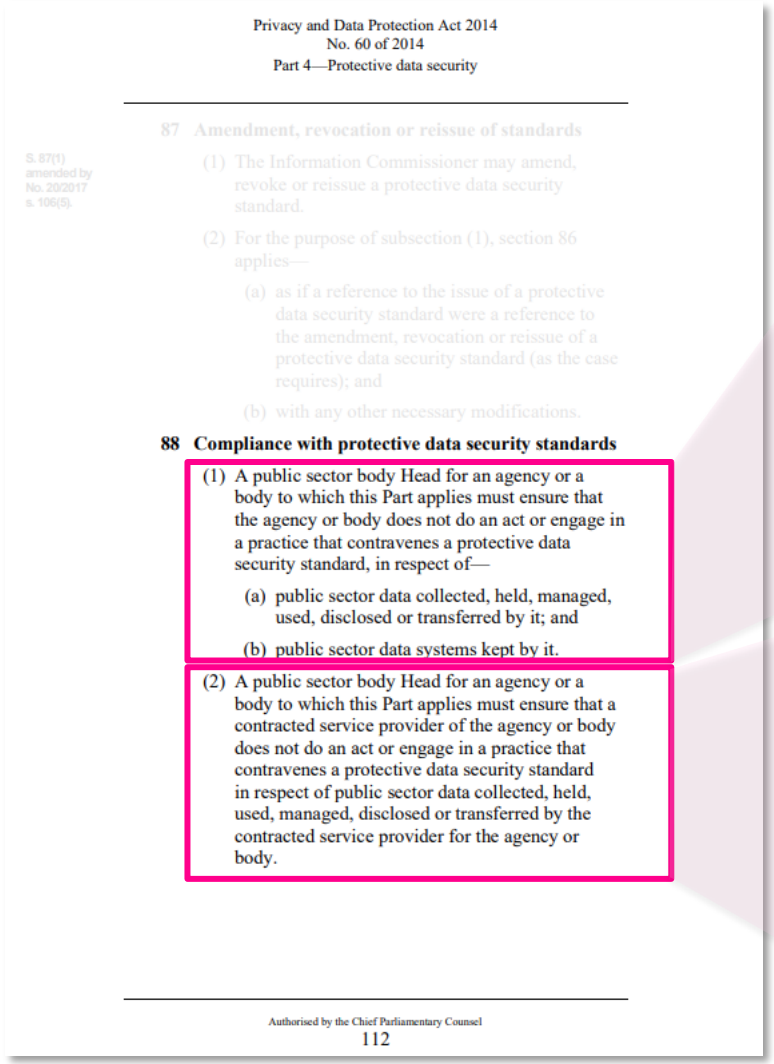
# What we'll explore today

- Legislative obligations
- Resources to support 2026 PDSP submissions
- Changes and updates to the PDSP forms
- Preparing for the 2026 PDSP
- Implications of non-compliance
- VPDSS 3.0 update
- Questions
- Resources and more

# Legislative obligations

Part 4 of the *Privacy and Data Protection Act 2014* (Vic)

# A regulated organisation must ensure that



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

87 Amendment, revocation or reissue of standards

S. 87(1) amended by No. 20/2017 s. 106(5).

(1) The Information Commissioner may amend, revoke or reissue a protective data security standard.

(2) For the purpose of subsection (1), section 86 applies—

(a) as if a reference to the issue of a protective data security standard were a reference to the amendment, revocation or reissue of a protective data security standard (as the case requires); and

(b) with any other necessary modifications.

**88 Compliance with protective data security standards**

(1) A public sector body Head for an agency or a body to which this Part applies must ensure that the agency or body 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.

(2) A public sector body Head for an agency or a body to which this Part applies must ensure that a 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.

Authorised by the Chief Parliamentary Counsel
112

- it does not do an act or engage in a practice that contravenes a [Victorian] protective data security standard (**VPDSS or Standard**), in respect of:

(a) public sector data collected, held, managed, used, disclosed or transferred by it, and

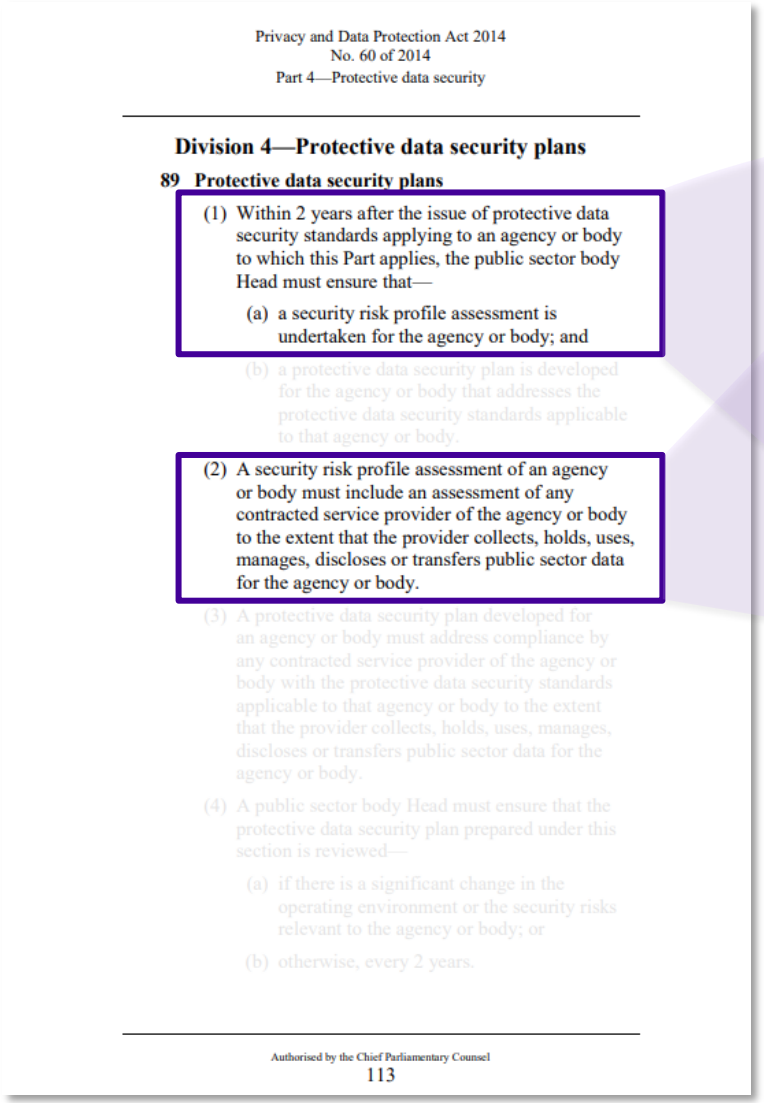
(b) public sector data systems kept by it.

Section 88(1)

- 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 88(2)

# A regulated organisation must ensure that



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

**Division 4—Protective data security plans**

**89 Protective data security plans**

(1) Within 2 years after the issue of protective data security standards applying to an agency or body to which this Part applies, the public sector body Head must ensure that—

(a) a security risk profile assessment is undertaken for the agency or body; and

(b) 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.

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

(3) A protective data security plan developed for an 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.

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

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

(b) otherwise, every 2 years.

Authorised by the Chief Parliamentary Counsel
113

**a security risk profile assessment (SRPA)**

- is undertaken for the agency or body, and

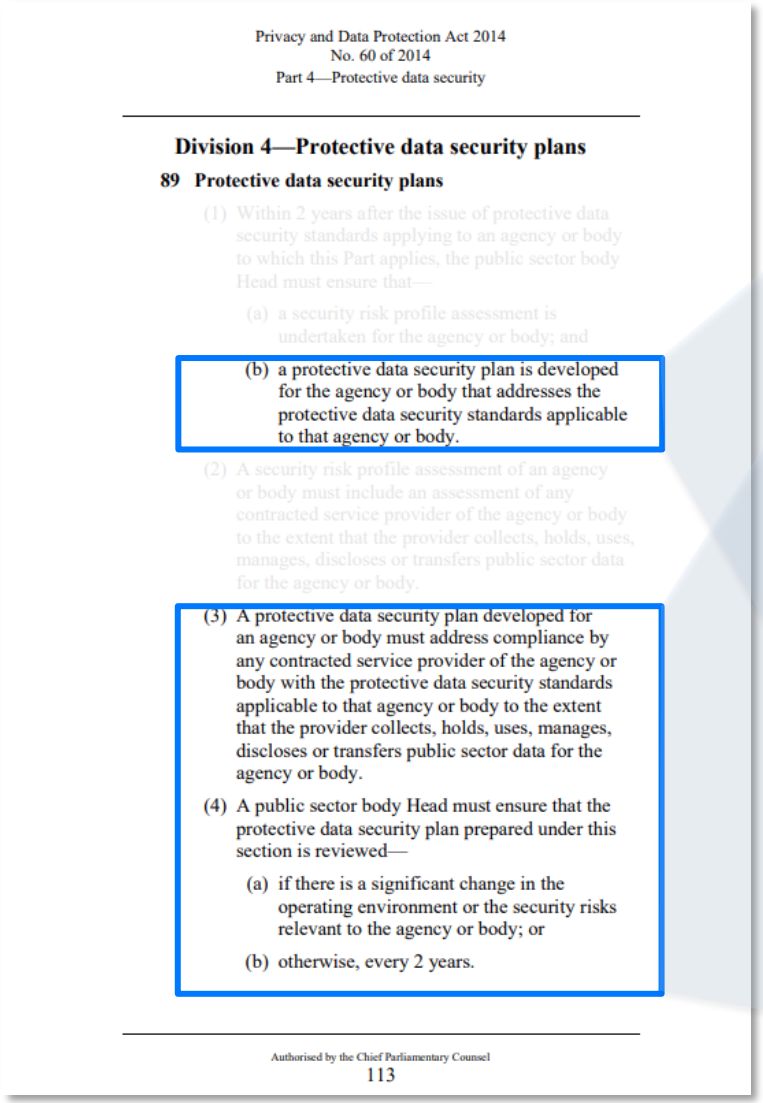
Section 89(1)

- 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

Section 89(2)

**Remember:** The SRPA refers to a process, not a product.

# A regulated organisation must ensure that



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

**Division 4—Protective data security plans**

**89 Protective data security plans**

(1) Within 2 years after the issue of protective data security standards applying to an agency or body to which this Part applies, the public sector body Head must ensure that—

(a) a security risk profile assessment is undertaken for the agency or body; and

(b) 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.

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

(3) A protective data security plan developed for an 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.

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

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

(b) otherwise, every 2 years.

Authorised by the Chief Parliamentary Counsel
113

**a protective data security plan (PDSP)**

- is developed for the agency or body that addresses the protective data security standards applicable to that agency or body

Section 89(1)(b)

- 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

Section 89(3)

- is reviewed if there is a significant change in the operating environment or the security risks relevant to the agency or body, or
- otherwise, every 2 years.

Section 89(4)

# Undertaking the Security Risk Profile Assessment process

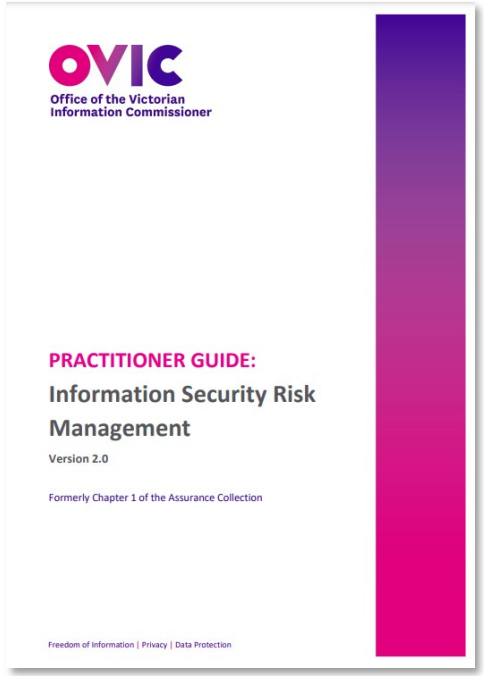
Organisations deal with many categories of risk (financial, safety, people, operational, etc.). Information security risk is just another category.

The SRPA process prompts organisations to identify, assess and prioritise risks relating to information and system assets, across all security domains. These domains include governance, **information** security, **physical** security, **personnel** security and **ICT** security.

The SRPA process consists of 4 steps:

1. risk identification
2. risk analysis
3. risk evaluation
4. risk treatment.

When undertaking the SRPA process, organisations must consult with both internal and external stakeholders at each step in the process. This includes engaging contracted service providers, as these types of engagements may introduce or vary risks, and is requirement under Part 4 of the PDP Act.




The activities set out in this document help organisations identify, analyse and evaluate their information security risks more effectively, and then manage these with their existing risk management frameworks or by referencing established risk management material.

For more info on how to approach the SRPA process navigate to -

https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/

# Developing a Protective Data Security Plan

A PDSP is used by a regulated organisation to report to OVIC on the progress of its information security program.

In preparation for the development of your 2026 PDSP, organisations should:

- reflect on former PDSP responses from previous reporting cycles
- consider any updates to internal planning which may influence a change to proposed work programs or business priorities
- review information asset registers to account for any new or changed assets (including changes to security value of those assets)
- review internal risk registers to identify any new or updated risks
- consider incidents registers to help identify situations where security measures may not be operating effectively.

**Remember:** OVIC encourages organisations to critically consider former PDSP responses and recalibrate these if circumstances have changed.

# SRPA process underpins the development of a PDSP

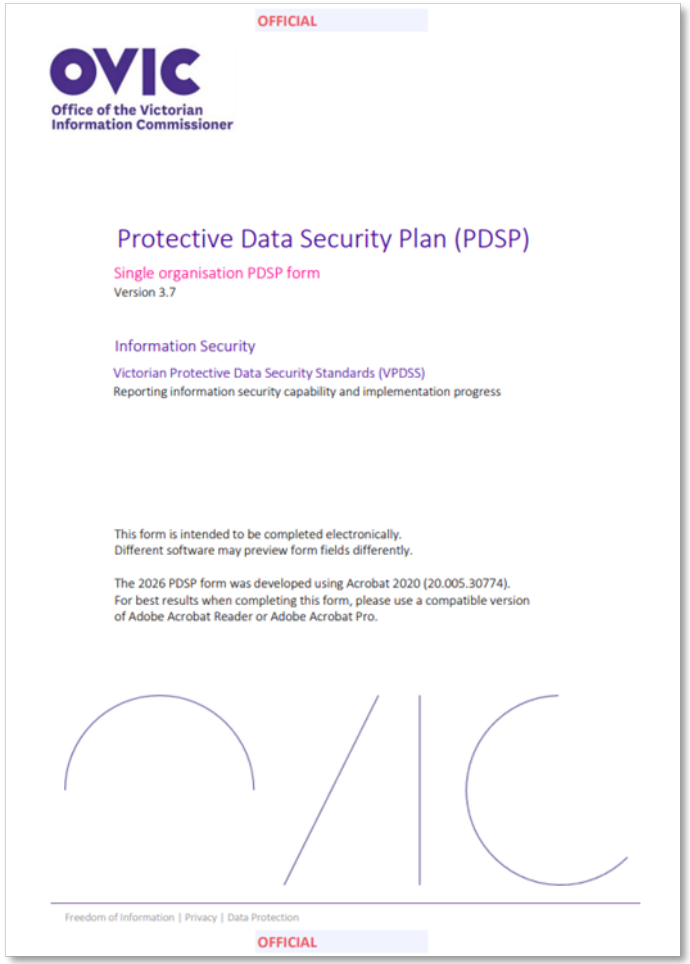
## Security Risk Profile Assessment (SRPA)

| Risk Identification | Risk Analysis | Risk Evaluation | Risk Treatment |
|---|---|---|---|
| Select information asset(s) | Evaluate existing controls | Consider risk treatment options | Identify possible security measures |
| Identify:<br>• Events<br>• Causes (threats)<br>• impacts<br>• risks | Rate:<br>• business impacts (consequences)<br>• likelihood<br>• risks | Risk tolerance | Evaluate security measures |
| | | Prioritise treatment of risks | Endorse security measures |
| | | | Assess target risk |

**Review** – At least annually or when operating environment changes

**Consultation**

**Track in risk register**


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

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

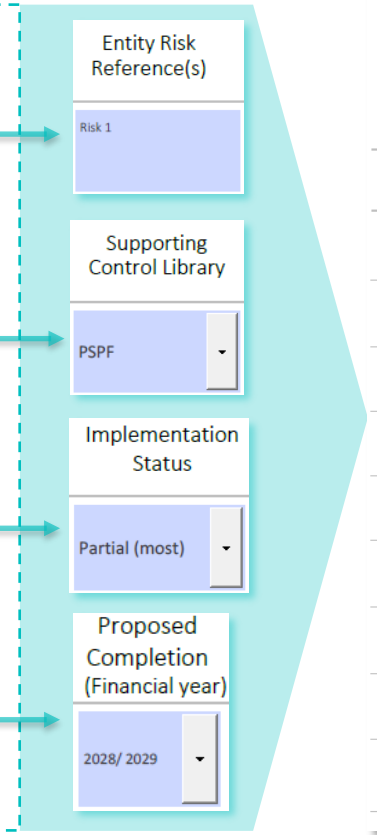
OFFICIAL

# Suggested approach 1: SRPA informing PDSP

**SRPA process**

**KEEP NOTE OF:**

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




## 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. | | | | |

# Suggested approach 2: SRPA informing PDSP

**Consider each of the VPDSS elements and assess its applicability**

**Consider the organisation's current control environment and assess whether there are any gaps**

**Record outcomes from the SRPA process in internal risk registers and relevant PDSP fields**

Standard 1 element assessment

| | Standard 1 elements |
|---|---|
| E1.010 | The organisation documents a contextualised information security manage (e.g., strategy, policies, procedures) covering all security areas. |
| E1.020 | The organisation's information security management framework contains legislative and regulatory drivers. |
| E1.030 | The organisation's information security management framework aligns wit management framework. |
| E1.040 | Executive management defines information security functions, roles, resp competencies and authorities. |
| E1.050 | Executive management nominates an information security lead and notifie changes to this point of contact. |
| E1.060 | Executive management owns, endorses and sponsors the organisation's o information security program(s) including the implementation plan. |
| E1.070 | The organisation identifies information security performance indicators an information security obligations against these. |
| E1.080 | Executive management commits to providing sufficient resources to suppo organisation's ongoing information security program(s). |
| E1.090 | The organisation sufficiently communicates its information security manag and ensures it is accessible. |

**Security Risk Profile Assessment (SRPA)**

| Risk Identification | Risk Analysis | Risk Evaluation | Risk Treatment |
|---|---|---|---|
| Select information asset(s) | Evaluate existing controls | Consider risk treatment options | Identify possible security measures |
| Identify:<br>• Events<br>• Causes (threats)<br>• impacts<br>• risks | Rate:<br>• business impacts (consequences)<br>• likelihood<br>• risks | Risk tolerance | Evaluate security measures |
| | | Prioritise treatment of risks | Endorse security measures |
| | | | Assess target risk |

**Review** – At least annually or when operating environment changes

**Consultation**

**Track in risk register**

| Entity Risk Reference(s) | Supporting Control Library | Implementation Status | Proposed Completion (Financial year) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# Resources to support 2026 PDSP submissions

# Navigating OVIC's website

## 2026 VPS reporting page

1

### Information security

For guidance and resources on how to protect public sector information including how to implement the Victorian Protective Data Security Framework and Standards and more visit **Information security resources.**

### Popular information security links

Victorian Protective Data Security Framework

Victorian Protective Data Security Standards

Agency reporting obligations

Notify OVIC of an information security incident

Victorian Information Security Network

2

**Contents**

- Reporting deliverables and timeframes
  - What is required this year?
- \+ Protective Data Security Plan
- · Attestation

**What is required this year?**

For tailored guidance on what is required this year, select from the options below.

Victorian public sector stakeholder

Class B cemetery trust stakeholder

Committee of Management of Crown Land Reserves stakeholder

3

**Download**

VPS PDSP form 2026 | OVIC Single Organisation Protective Data Security Plan V3.7 - PDF
**Size 7.10 MB**
Download

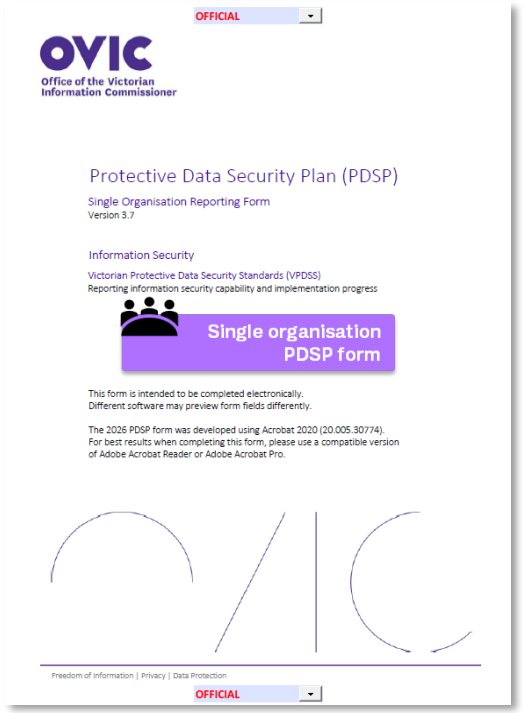
VPS How-To Guide: Completing the Protective Data Security Plan 2026 - PDF
**Size 4.15 MB**
Download

### Victorian public sector stakeholders

Victorian public sector (**VPS**) 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.

Visit the VPS Stakeholder page here - https://ovic.vic.gov.au/information-security/agency-reporting-obligations/vps-stakeholders/

# 2026 PDSP form: VPS organisations




The standard **2026 PDSP form** for VPS organisations has been released and is now available for download.

Ensure you download **V3.7** of this form from the OVIC website.

https://go.vic.gov.au/3O2iKRa

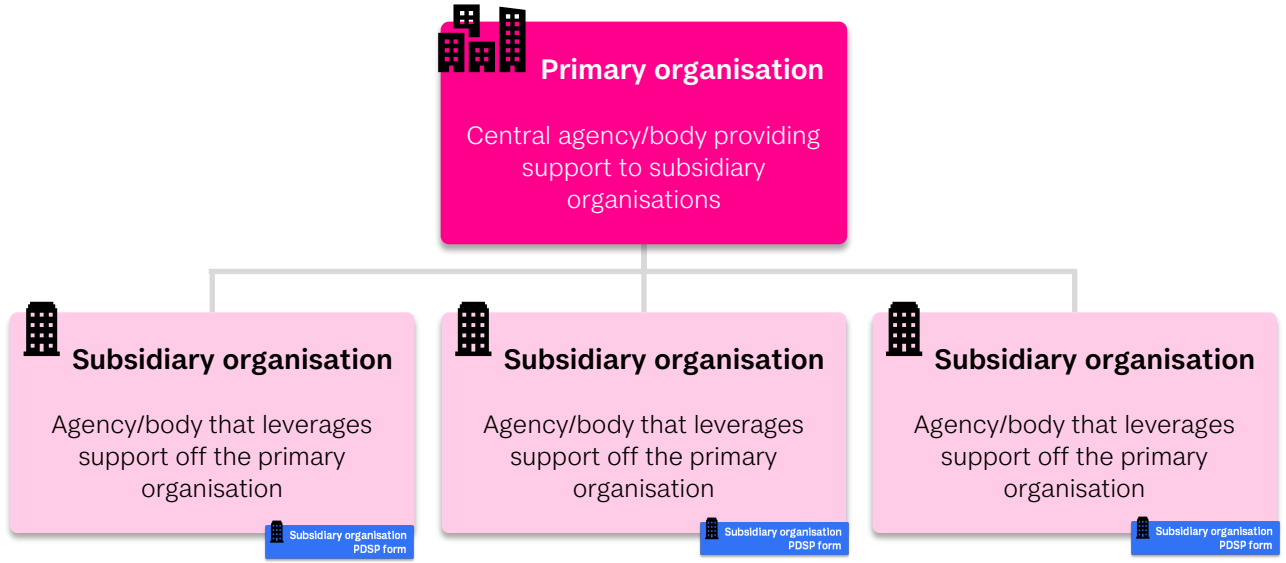

Organisation's intending to use the multi-organisation reporting model to report on behalf of organisations with the same reporting criteria, must request a tailored **multi-organisation PDSP form** from the ISU.

security@ovic.vic.gov.au

# Multi-organisation reporting model

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

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




If, after reading the *How-To Guide*, your organisation intends to use the multi-organisation reporting model, please reach out to security@ovic.vic.gov.au to discuss your 2026 submission.

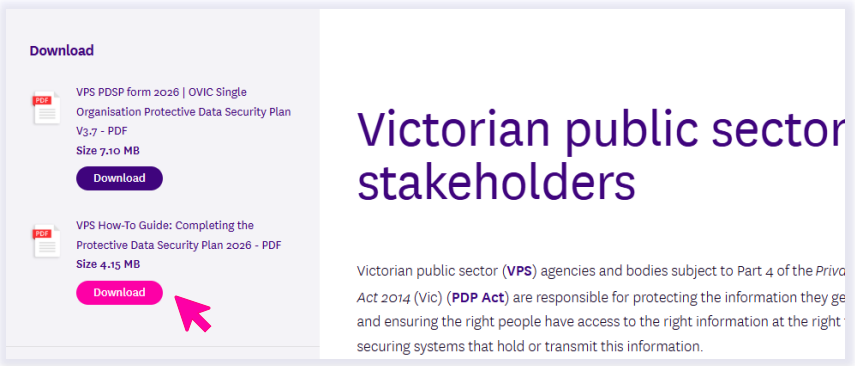
This includes organisations that have previously participated in the multi-organisation process as bespoke PDSP forms need to be generated for you.

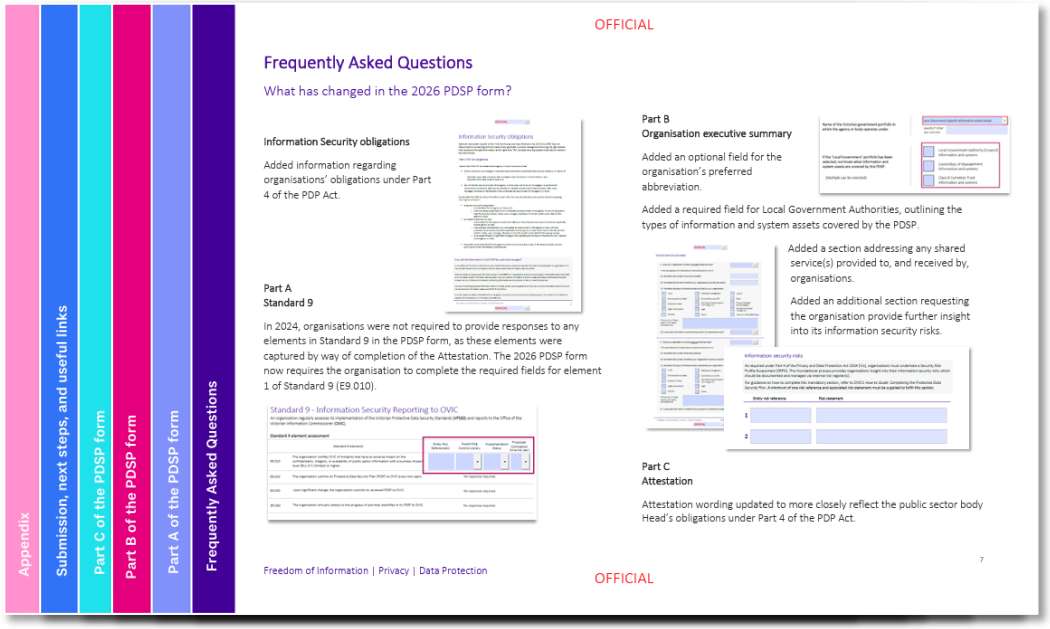
# Updated VPS How-to Guide

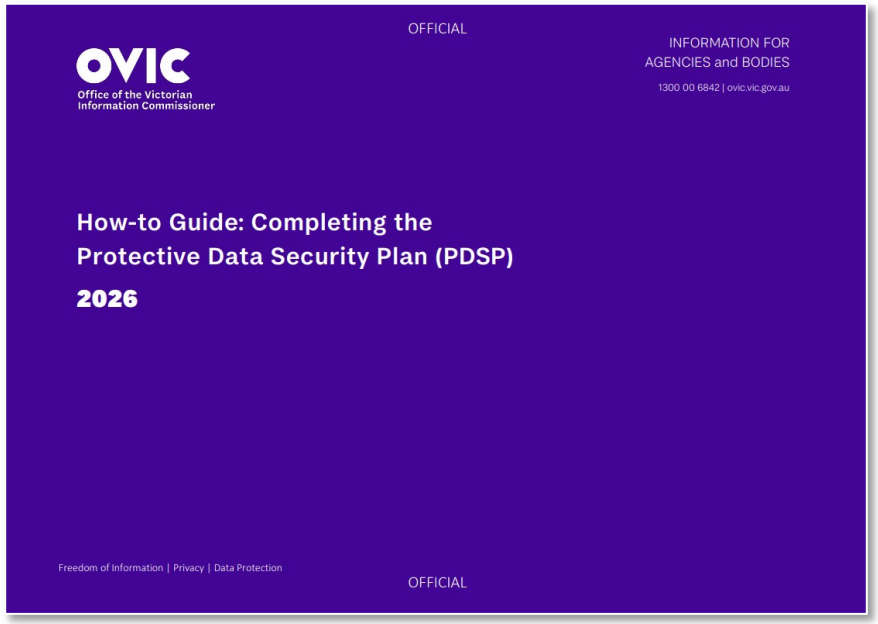
The VPS **How-to Guide** has been updated to reflect the changes to the standard VPS 2026 PDSP form and is now available for download.

The How-To Guide provides:

- Explanations of terms
- Step-by-step guidance for each field on the PDSP form (Parts A – C)
- Answers to frequently asked questions
- Instructions for submission of the PDSP
- Multi-organisation reporting model criteria and steps



# Navigating OVIC's website

## 2026 Class B CT and CoM PDSPs and How-To Guides

1

### Information security

For guidance and resources on how to protect public sector information including how to implement the Victorian Protective Data Security Framework and Standards and more visit **Information security resources.**

### Popular information security links

Victorian Protective Data Security Framework

Victorian Protective Data Security Standards

Agency reporting obligations

Notify OVIC of an information security incident

Victorian Information Security Network

2

**Contents**

- Reporting deliverables and timeframes
  - What is required this year?
+ Protective Data Security Plan
- Attestation

**What is required this year?**

For tailored guidance on what is required this year, select from the options below.

Victorian public sector stakeholder

Class B cemetery trust stakeholder

Committee of Management of Crown Land Reserves stakeholder

3

**Download**

2026 | Class B Cemetery Trust Protective Data Security Plan (PDSP) - DOCX
Size 215.92 KB
Download

2026 | Class B Cemetery Trust Protective Data Security Plan (PDSP) - PDF
Size 428.32 KB
Download

https://go.vic.gov.au/3VFX4KD

### Class B Cemetery Trust stakeholders

In Victoria there are over 400 Class B Cemetery Trusts (**Class B CTs**) managed by community members, often in a voluntary capacity. These Class B CTs are public boards that manage public cemeteries and

4

**Download**

2026-Committee-of-Management-of-Crown-land-reserves-Protective-Data-Security-Plan-V1.0.docx
Size 215.77 KB
Download

2026-Committee-of-Management-of-Crown-land-reserves-Protective-Data-Security-Plan-V1.0.pdf
Size 424.26 KB

https://go.vic.gov.au/4bRLupH

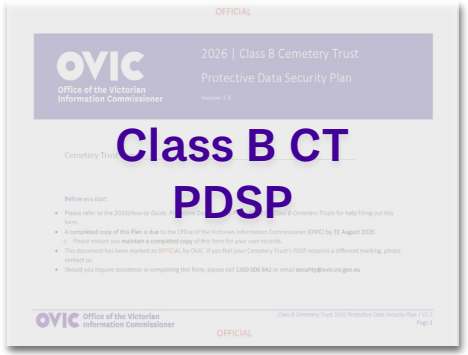
### Committees of Management of Crown Land Reserve stakeholders

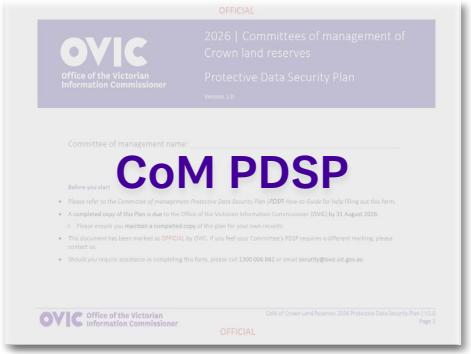
# 2026 PDSP form: Class B CTs and CoMs

To address the unique governance arrangements and challenges of Class B CTs and CoMs, OVIC has published tailored PDSP templates and associated requirements for these entities. These PDSP templates are supported by customised resources, designed to assist Class B CTs and CoMs meet their reporting obligations in 2026. Some larger organisations such as LGAs may appointed to manage these bodies.

## Option 1

**Tailored PDSP templates for Class B CTs and CoMs (for one or more CT or CoM)**



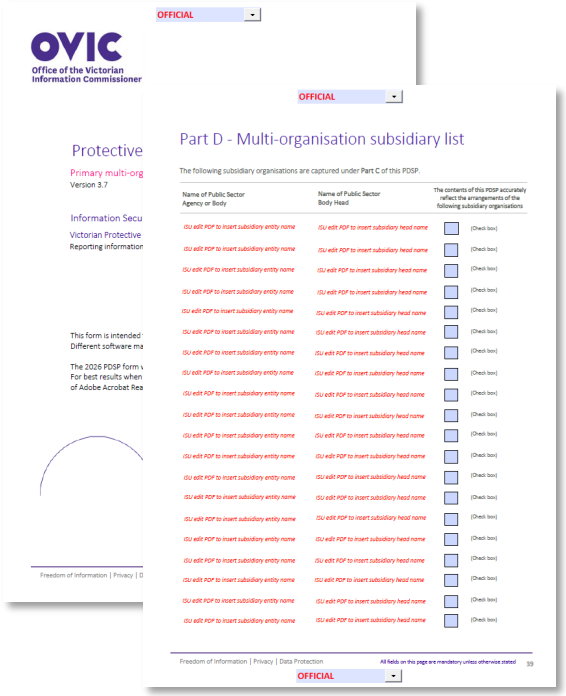




## Option 2

**Standard single organisation 2026 PDSP template per body**

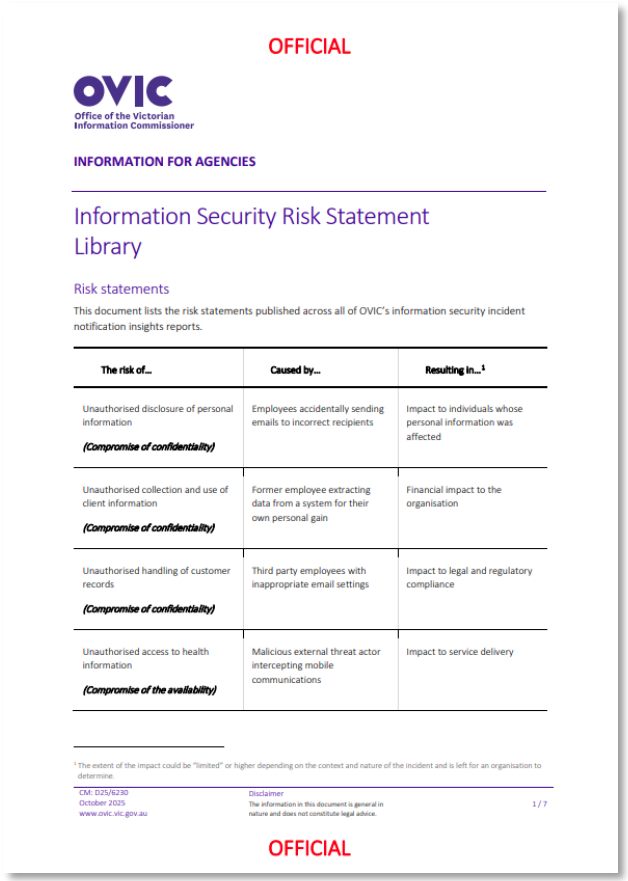

## Option 3

**Standard multi-organisation 2026 PDSP template**



# Other recently refreshed resources

## Information Security Risk Statement Library


OFFICIAL

OVIC
Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Information Security Risk Statement Library

Risk statements

This document lists the risk statements published across all of OVIC's information security incident notification insights reports.

| The risk of... | Caused by... | Resulting in...[1] |
|---|---|---|
| Unauthorised disclosure of personal information *(Compromise of confidentiality)* | Employees accidentally sending emails to incorrect recipients | Impact to individuals whose personal information was affected |
| Unauthorised collection and use of client information *(Compromise of confidentiality)* | Former employee extracting data from a system for their own personal gain | Financial impact to the organisation |
| Unauthorised handling of customer records *(Compromise of confidentiality)* | Third party employees with inappropriate email settings | Impact to legal and regulatory compliance |
| Unauthorised access to health information *(Compromise of the availability)* | Malicious external threat actor intercepting mobile communications | Impact to service delivery |

[1] The extent of the impact could be "limited" or higher depending on the context and nature of the incident and is left for an organisation to determine.

CM: D25/6230
October 2025
www.ovic.vic.gov.au

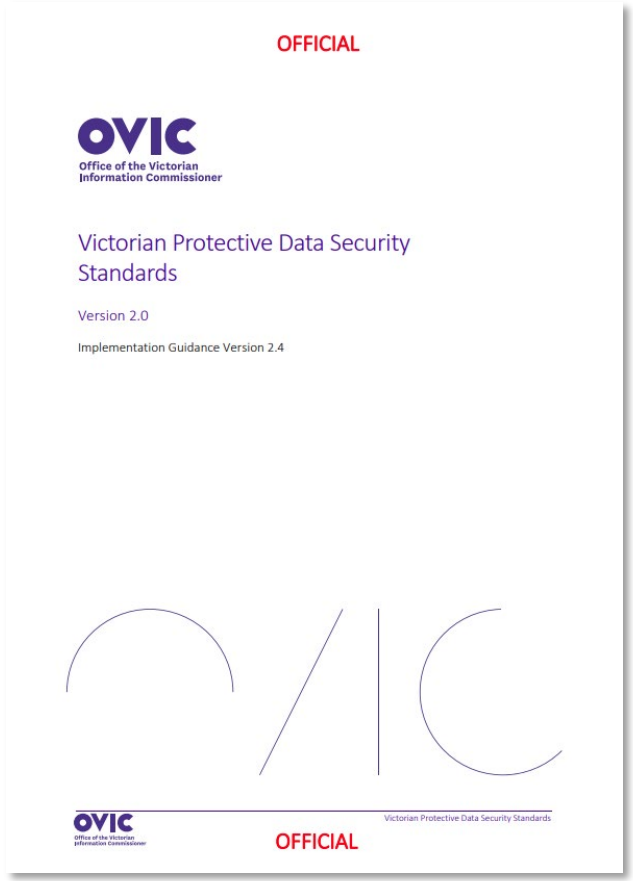
Disclaimer
The information in this document is general in nature and does not constitute legal advice.

1 / 7

OFFICIAL

https://go.vic.gov.au/49lgICG

## VPDSS Implementation Guidance V2.4


OFFICIAL

OVIC
Office of the Victorian Information Commissioner

Victorian Protective Data Security Standards

Version 2.0

Implementation Guidance Version 2.4

OVIC
Office of the Victorian Information Commissioner

Victorian Protective Data Security Standards

OFFICIAL

https://go.vic.gov.au/4bkRoPN

## Victorian Public Sector Insights - Information Security Monitoring and Assurance Report 2025


OVIC
Office of the Victorian Information Commissioner

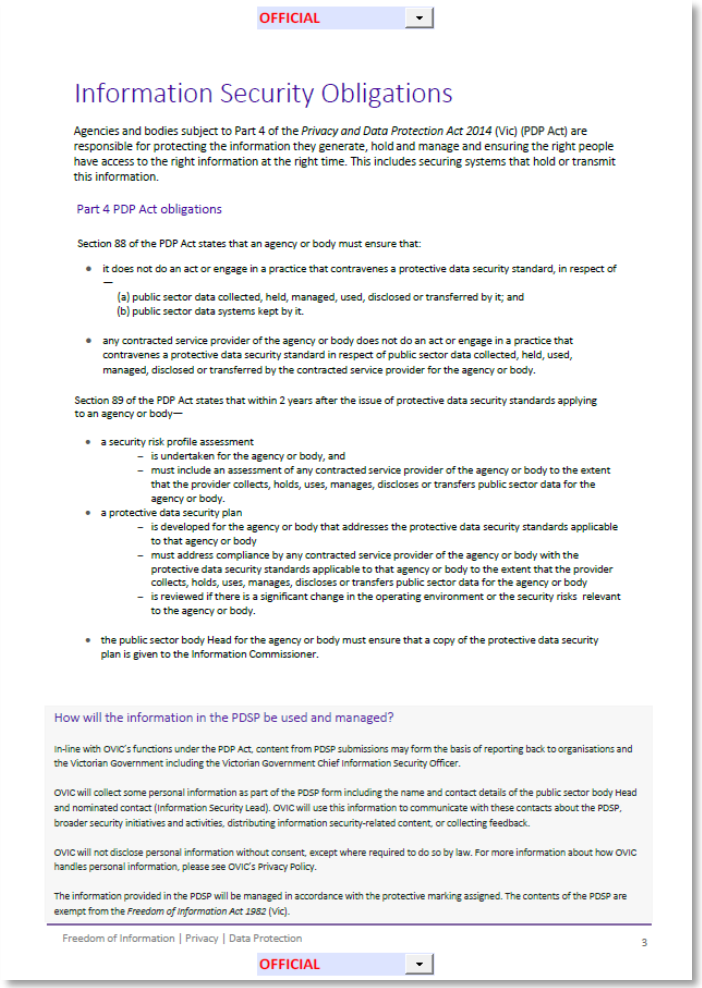
VICTORIAN PUBLIC SECTOR INSIGHTS
INFORMATION SECURITY MONITORING AND ASSURANCE

2025

https://go.vic.gov.au/4mtDSMr

# What has changed on the 2026 PDSP?

# New page: Highlighting Information Security Obligations



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

**This new page:**

- provides organisations a snapshot of the obligations outlined under Part 4 of the PDP Act
- provides organisations an easy reference of what is required when briefing the public sector body Head
- highlights how OVIC will use and manage the information provided in this PDSP

# Updated section: Standard 9 response

On the 2024 PDSP form, organisations were not required to provide responses to any elements in Standard 9. These were captured by way of completion of the Attestation.

On the 2026 PDSP form OVIC had adjusted this reporting requirement. Organisations must complete the required fields associated with E9.010, however subsequent elements under Standard 9 do not require responses (E9.020, E9.030, E9.040).

The wording of the 2026 Attestation has also been adjusted and simplified to reflect this.

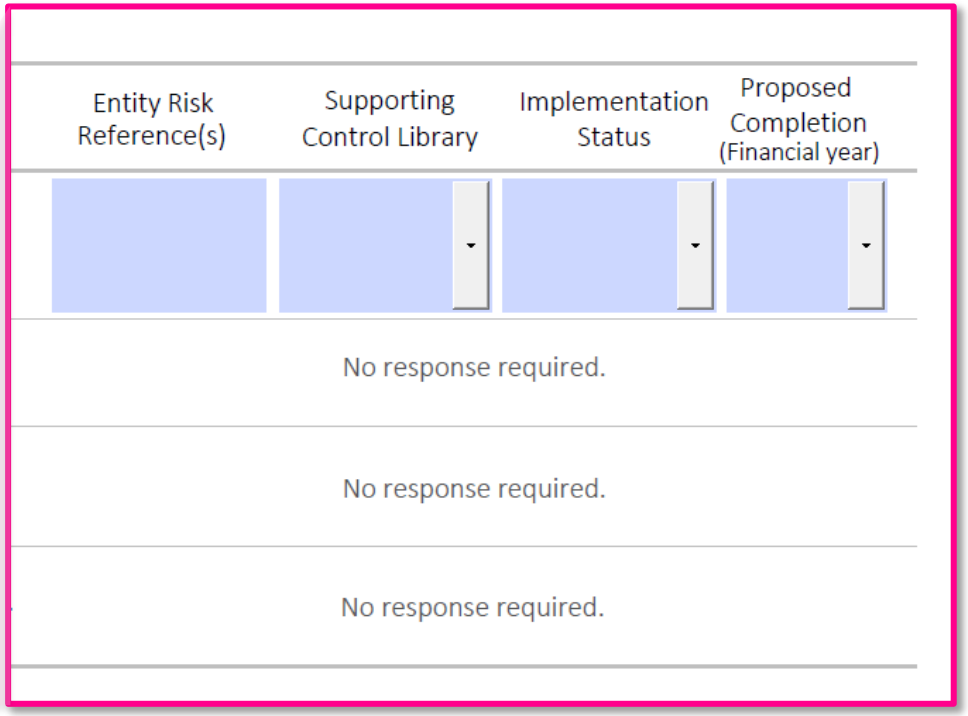
## 2026 PDSP form

### Standard 9 - Information Security Reporting to OVIC

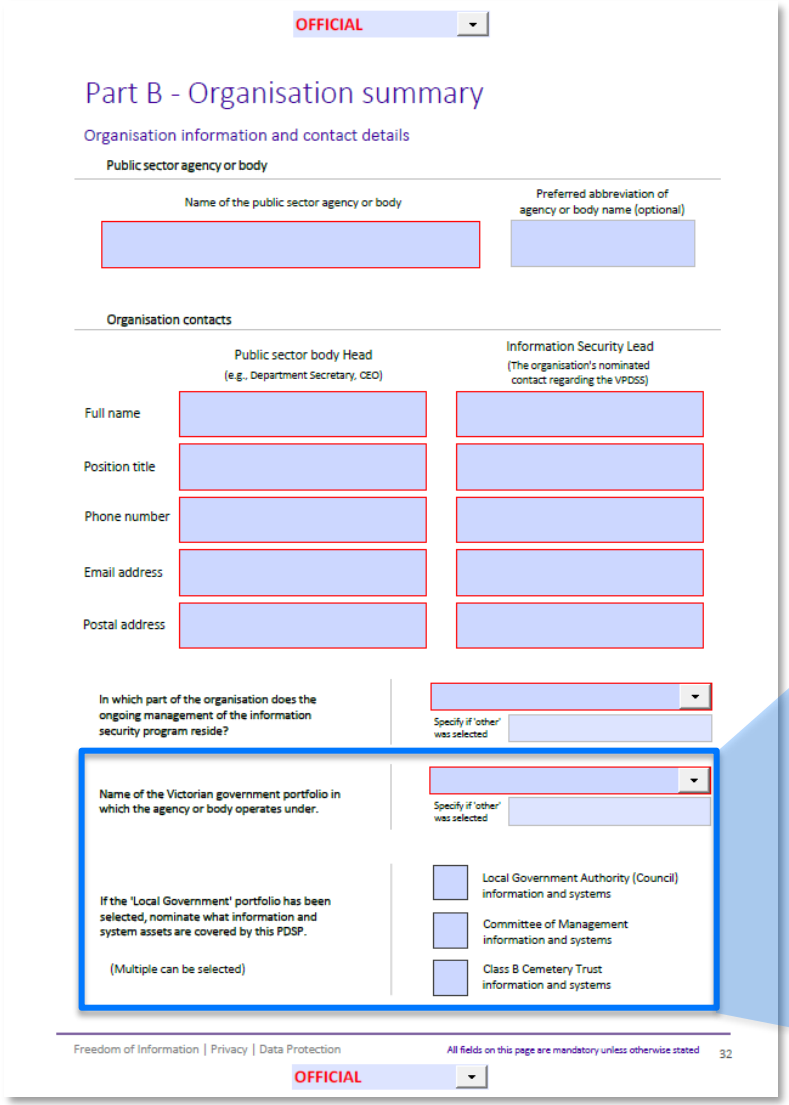
An organisation regularly assesses its implementation of the Victorian Protective Data Security Standards (**VPDSS**) and reports to the Office of the Victorian Information Commissioner (**OVIC**).

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. | | | |



# New section: Local Government Authority information

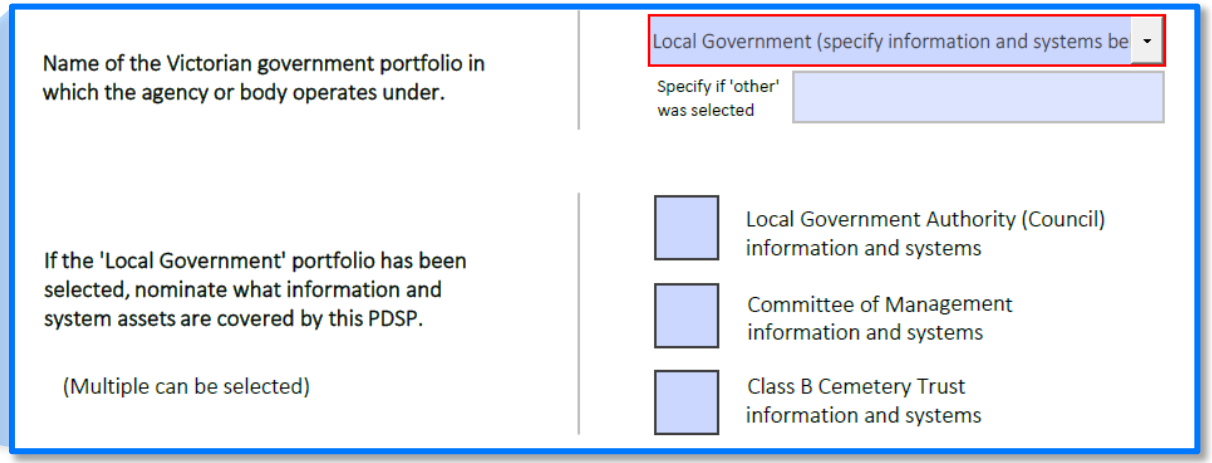



While Local Government Authorities (**LGAs**) are excluded under Part 4 of the PDP Act, there are some scenarios where they develop and submit PDSPs on behalf of organisations they are responsible for.

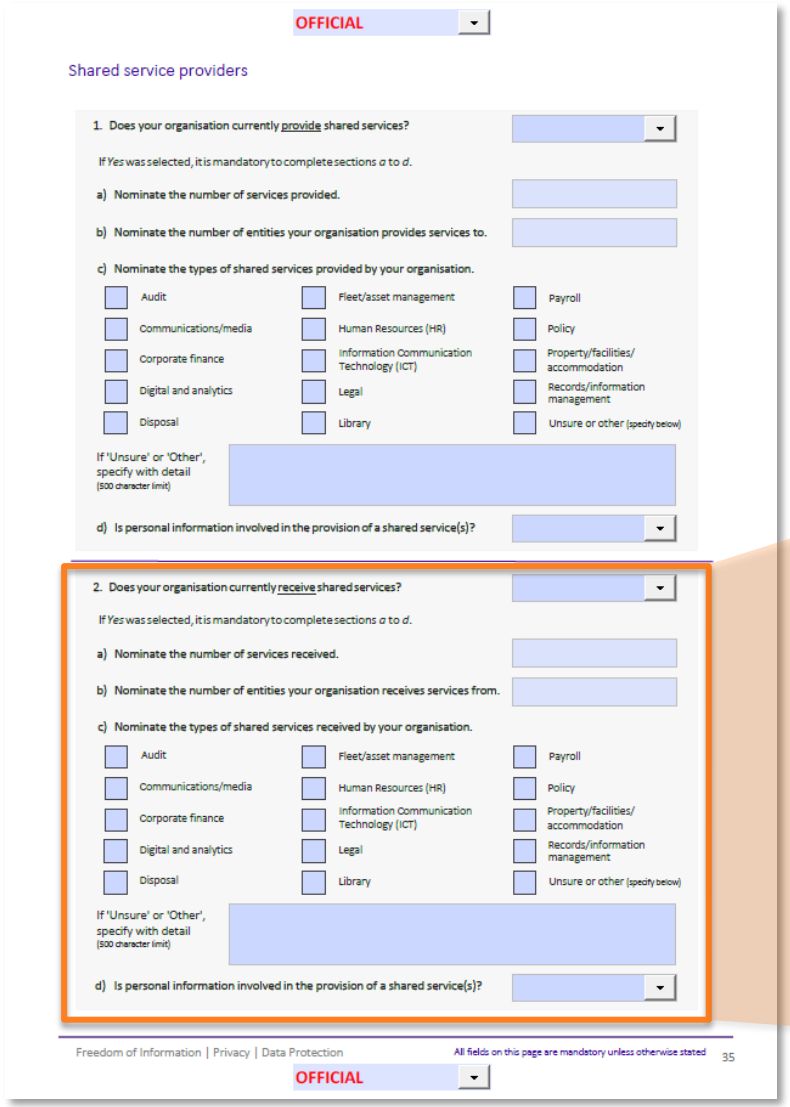
LGAs using the standard 2026 PDSP form must identify the types of organisations (the LGA, a Committee of Management and/or Class B Cemetery Trust) are covered by the PDSP.

As referenced earlier, alternative PDSP forms are available for CoMs and Class B CT reporting.

For more information about Local Government information security considerations, please see OVIC's LGA Guide.



# New page: Shared services


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

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.

2. Does your organisation currently receive shared services? Yes

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

a) Nominate the number of services received. 4

b) Nominate the number of entities your organisation receives services from. 1

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)? Yes

# New page: Information security risks


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

The 2026 standard VPS PDSP form has added questions regarding the organisations' information security risks.

When completing this section of the PDSP, consider the key information security risks identified as part of the SRPA process.

Outcomes of the SRPA process may have been recorded in an internal risk register. Refer to these entries when completing this section of the PDSP.

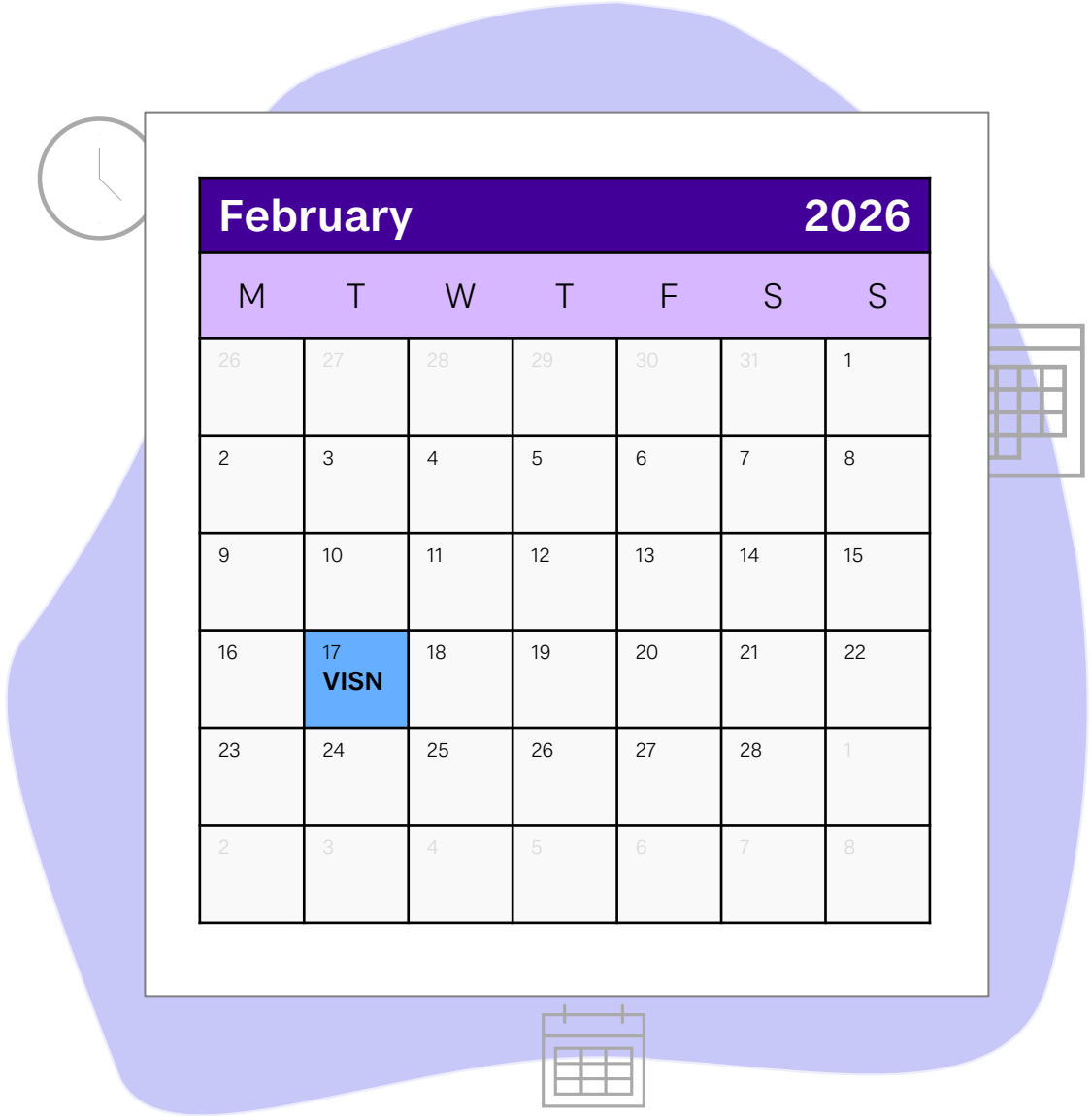
| | Entity risk reference | Risk statement |
|---|---|---|
| 1 | ER 123 | The risk of ... caused by .... resulting in ... |

**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.

# Preparing for the 2026 PDSP

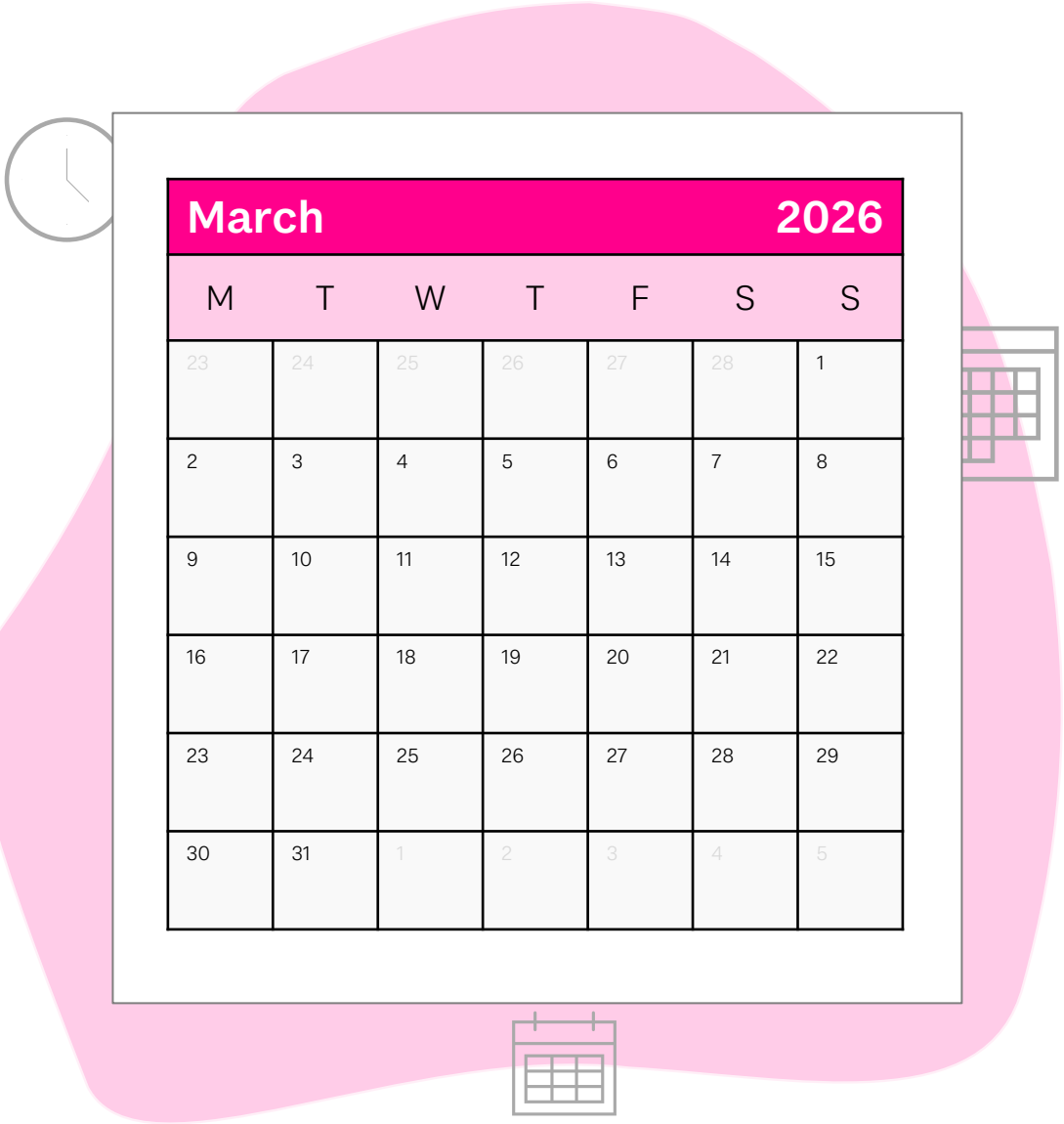
# From now to submission: Suggested approach



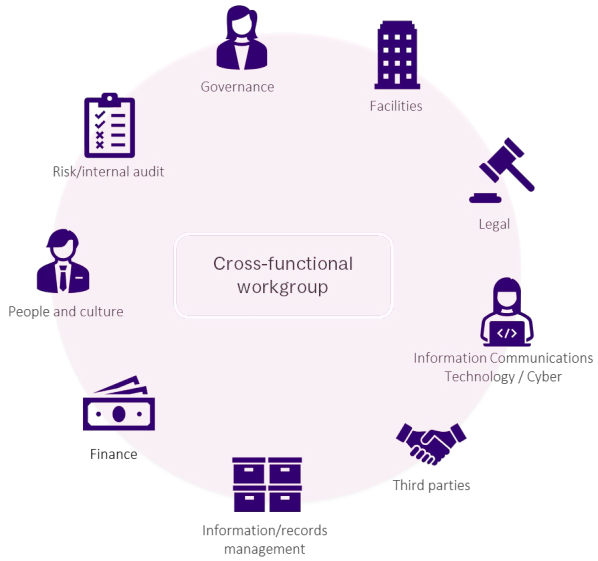

- Confirm your organisation's information security lead and update OVIC of any changes.
- Engage your public sector body Head early, advising them of reporting timeline and any interim activities they need to be aware of or engaged in.
- Download the relevant:
  - *PDSP form(s) for your organisation*
  - *2026 How-to Guide(s)*

**Multi-organisation reporting:**
For organisations that plan to submit using the multi-organisation reporting model, refer to the steps outlined in the Appendix of the *How-To Guide*.

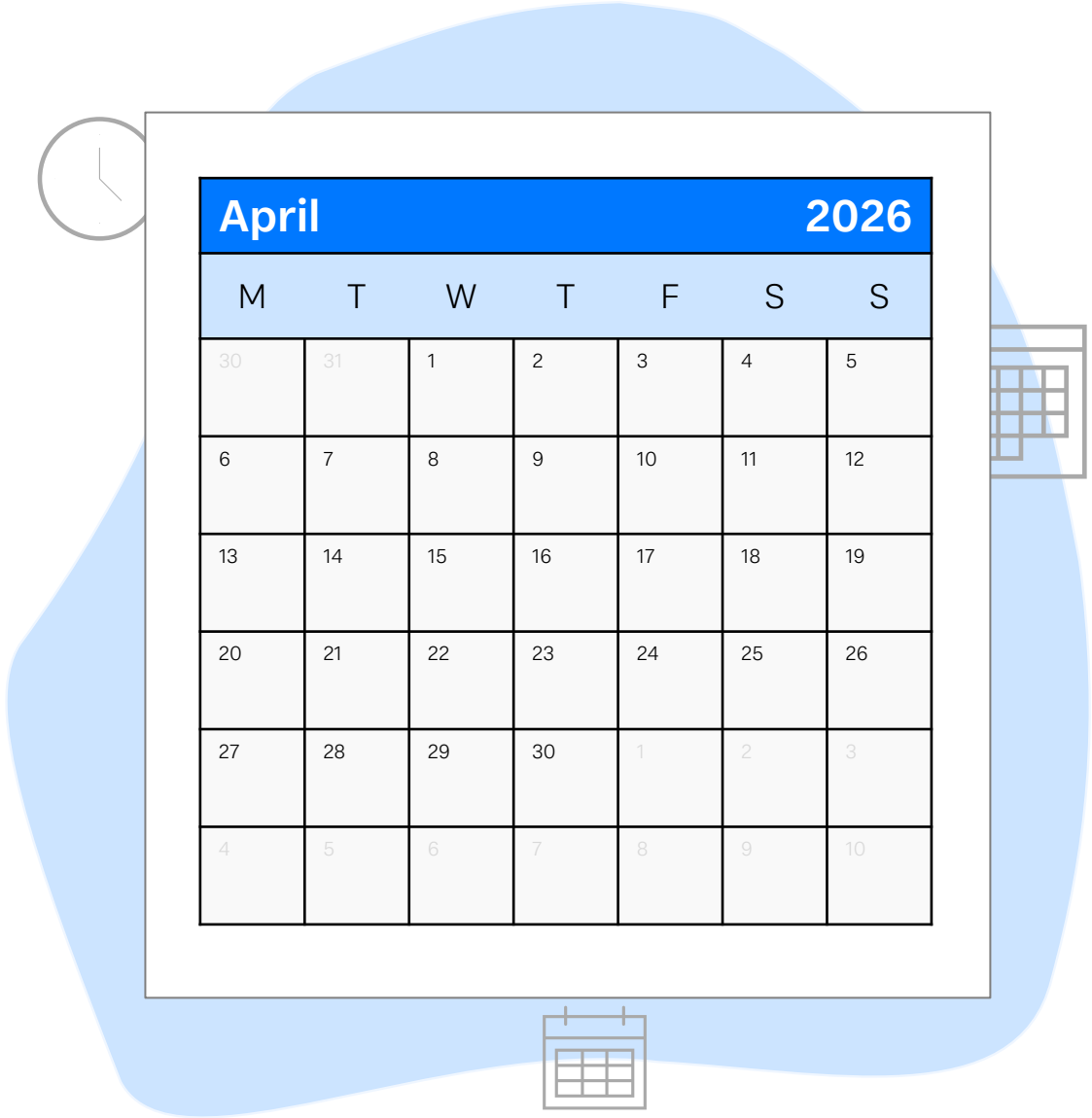
# From now to submission: Suggested approach




- Where possible, engage representatives from across the organisation and relevant contracted service providers who may input into, or support this process.
- Undertake an updated information security risk assessment in support of the SRPA process.
- Remember! The SRPA process must take into account contracted service providers.



# From now to submission: Suggested approach

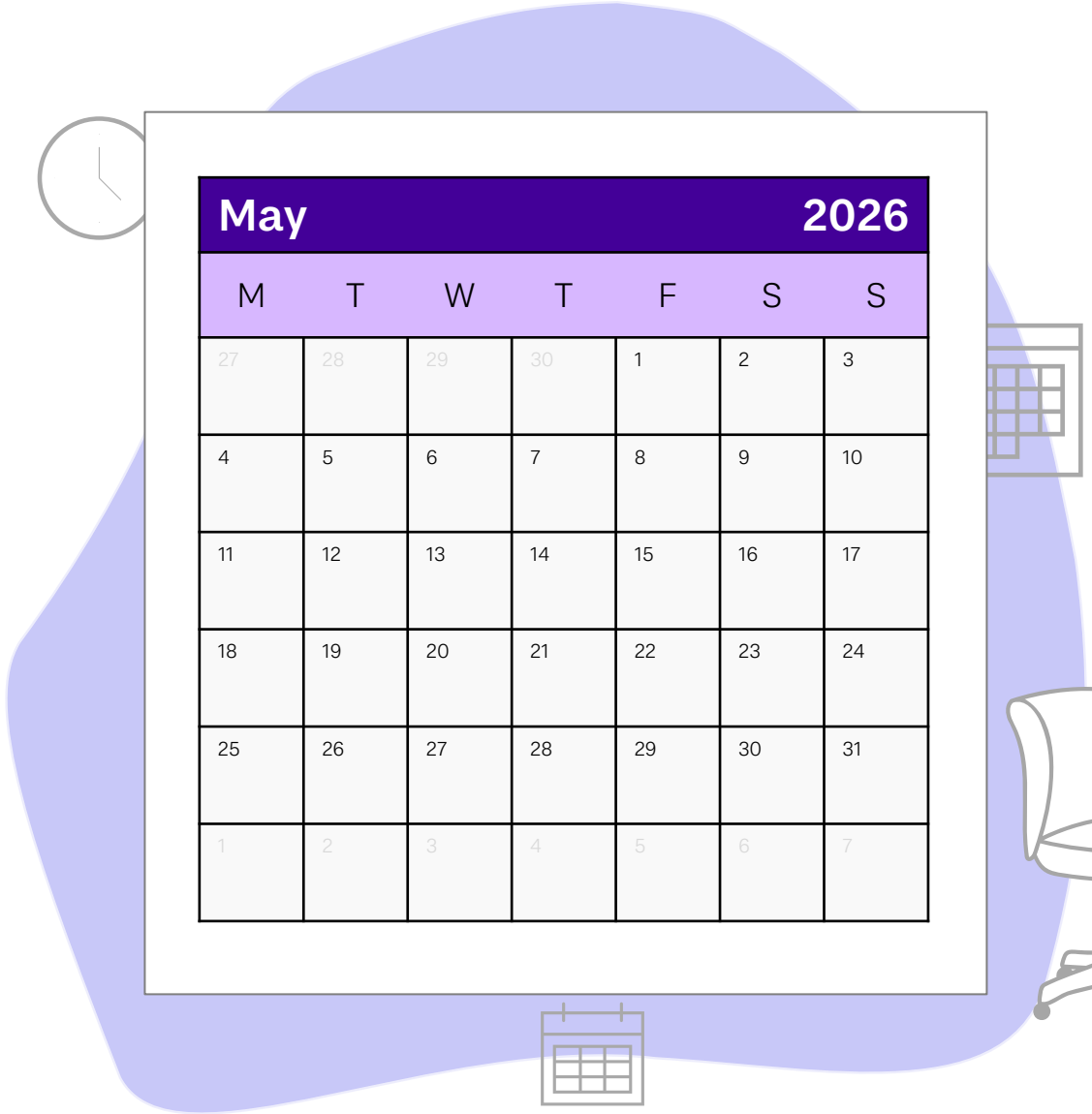



- Once you have completed a refreshed assessment of the organisation's current information security risks, internal risk registers should be updated to reflect any outcomes.

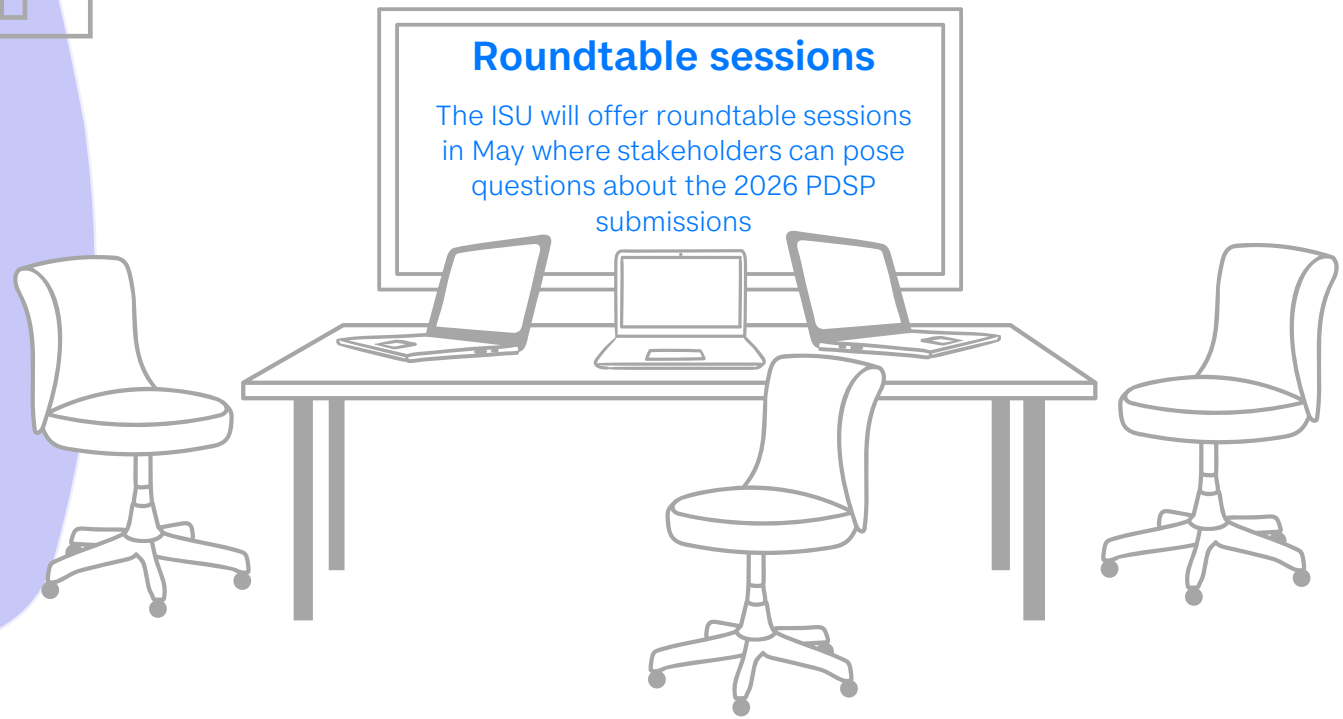
- The next step is to consider:
  - previous PDSP responses
  - current entries in the organisations Information Asset Register (referencing updated security value assessments),
  - current internal risk registers (including any documented information security risks of Contracted Service Providers)
  - incident registers
  - relevant treatment plans, and
  - current internal control library.

**Multi-organisation reporting:**
If you are part of a multi-organisation reporting model, all impacted organisations should be consulted in the development of the PDSP.

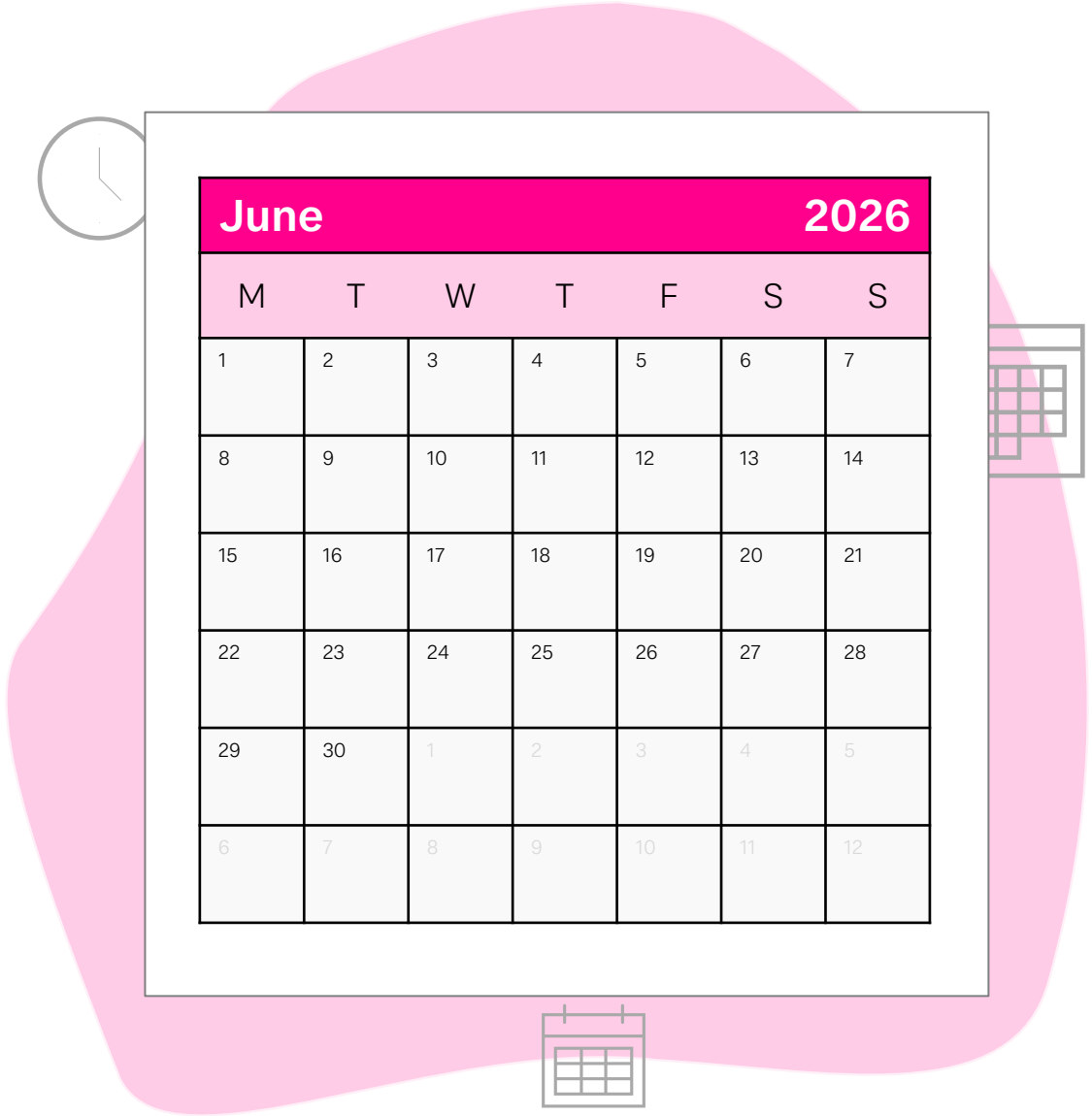
# From now to submission: Suggested approach




- Where possible, leverage off representatives from across the business to validate PDSP responses.
- For organisations that have engaged an external party or provider to help undertake the SRPA process and/or develop the PDSP, use this time to work with them to validate the responses.

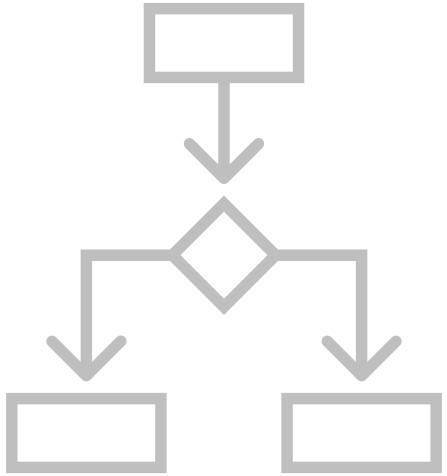


# From now to submission: Suggested approach

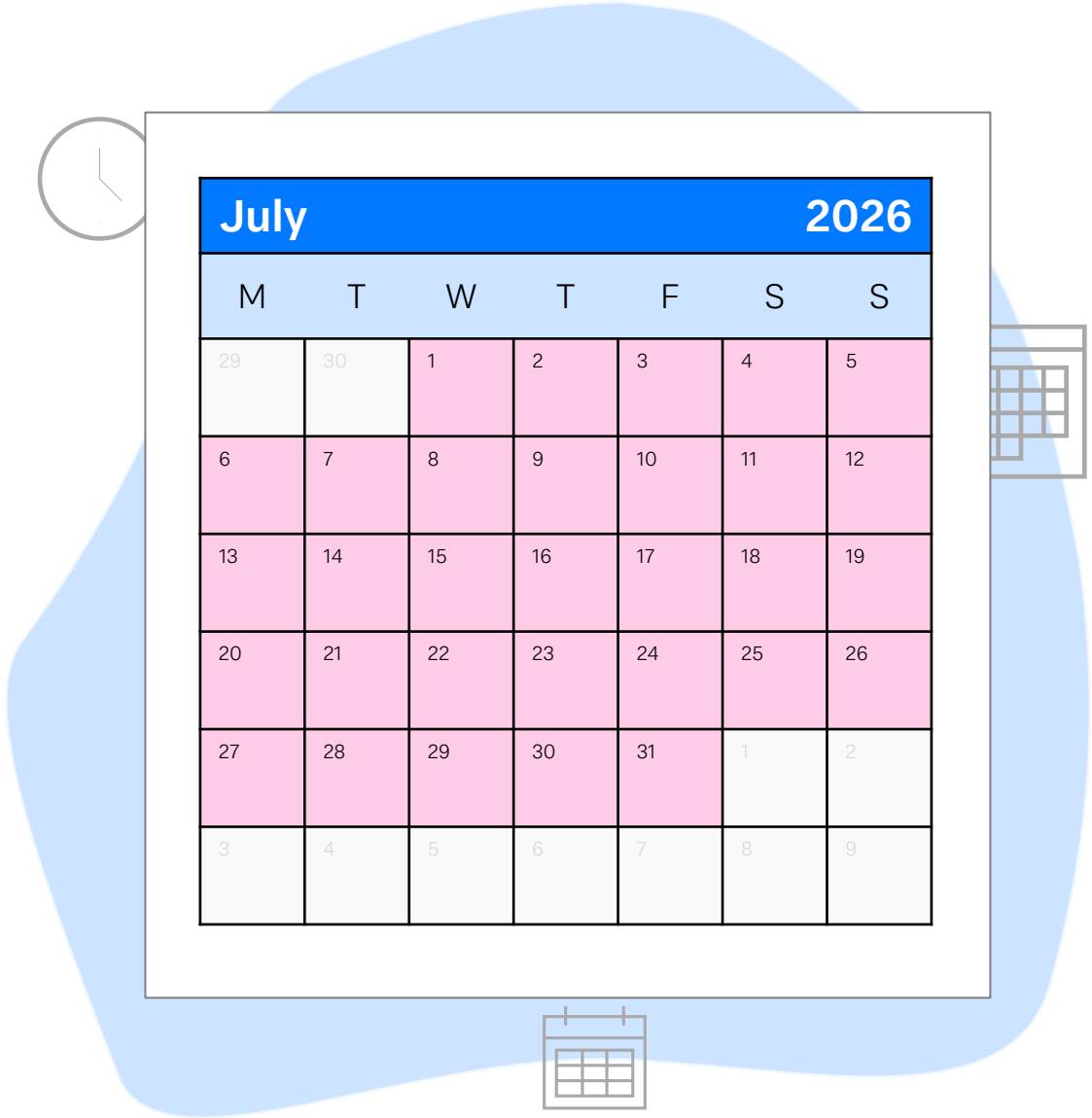



Allow enough time:

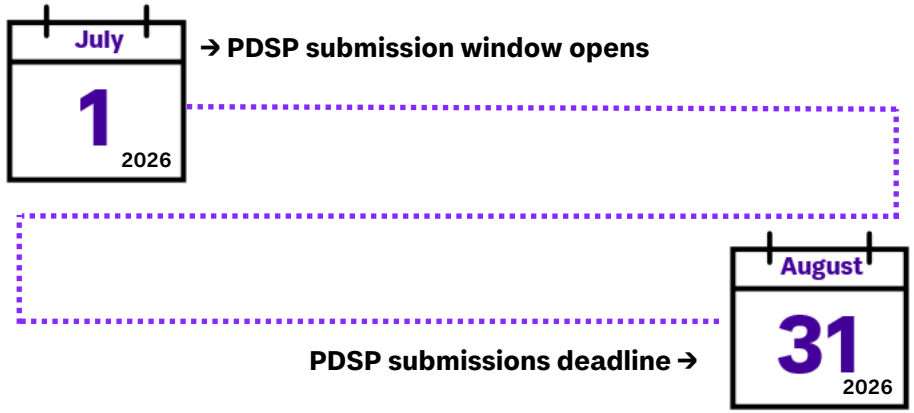
- to brief your public sector body Head on the draft PDSP responses
- adjust any responses following feedback
- to follow internal governance processes to get final sign off of the PDSP by the public sector body Head



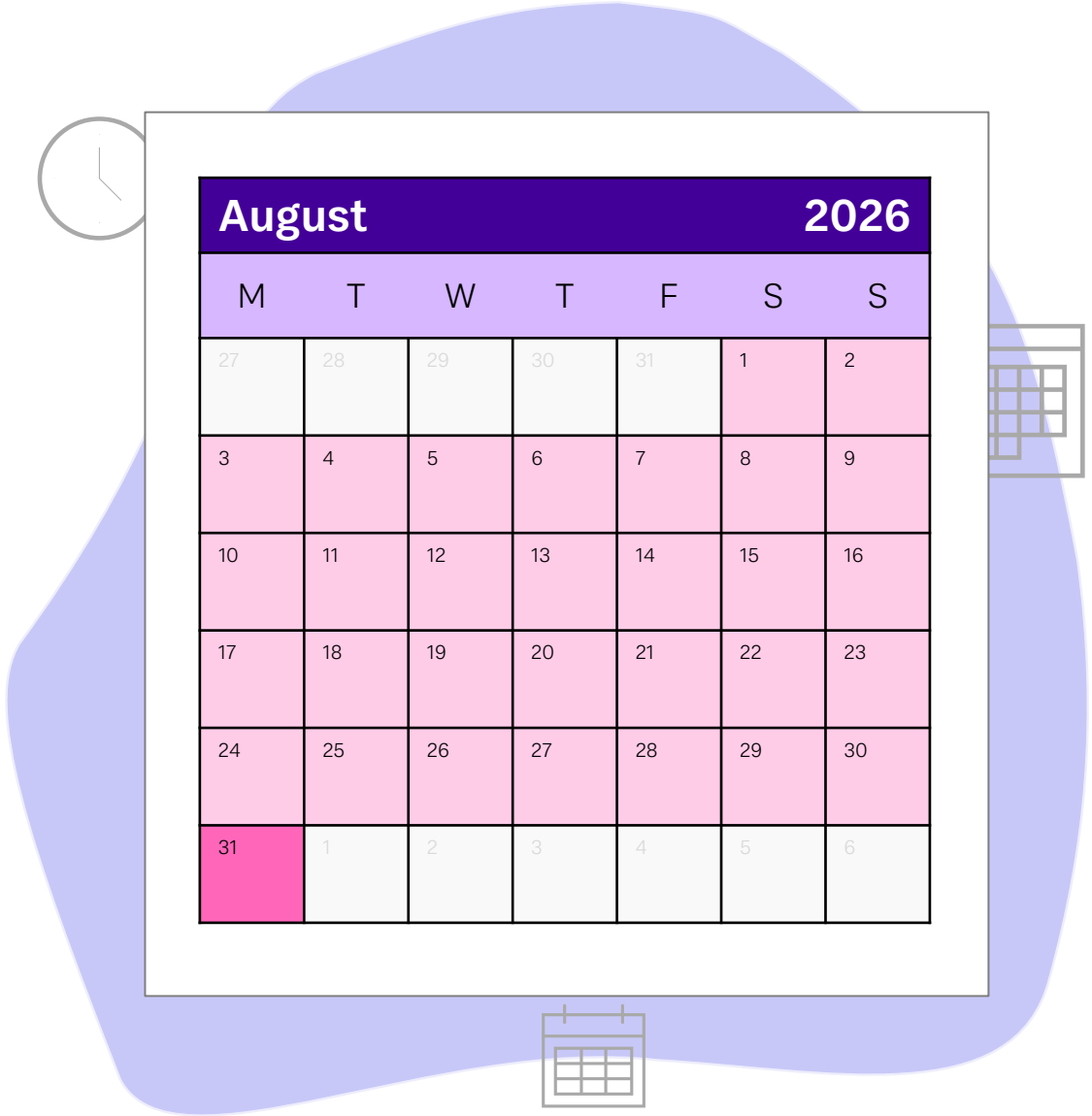
# From now to submission: Suggested approach




- VPS organisations should organise for the public sector body Head to sign the PDSP Attestation after 1 July 2026.
- Class B CT and CoMs must ensure the PDSP is signed off by the relevant Chairperson or their authorised representative (as specified in Part A of their PDSP form).
- The PDSP submission window opens 1 July 2026 and closes 31 August 2026.



# From now to submission: Suggested approach




The PDSP submission window closes 31 August 2026.

**Note:**
Submissions received after 31 August 2026 will be considered late.

For more information on how OVIC intends to manage late submissions, visit OVIC's Regulatory Action Policy.

# Implications of non-compliance

# A word on late submissions and non-compliance

By conducting a **SRPA** and submitting a **PDSP**, organisations are fulfilling some of their obligations outlined in Part 4 of the PDP Act.

Submissions received after 31 August 2026 are considered late, and failure to submit a current PDSP may be subject to further regulatory action by OVIC.

For more information regarding OVIC's regulatory action, please visit our website:
*Schedule 3 – Information security regulatory activities*.

**The PDP Act requires OVIC to research, promote, monitor and assure information security under the PDP Act.**

**OVIC may choose to conduct regulatory action which can include:**

- education and guidance
- preliminary inquiries
- examinations and audits
- investigation
- prosecutions of offences

# An update on OVIC's review of the Victorian Protective Data Security Standards

# VPDSS 3.0

In 2025, OVIC informed stakeholders that the current Victorian Protective Data Security Standards (**VPDSS or *Standards***) were being reviewed, with the intent to issue an updated set of Standards.

While OVIC anticipated the review of the Standards may have been completed in time for 2026 reporting, we have determined that more work needs to be undertaken to meet the needs of stakeholders and provide sufficient time for organisations to adopt revised Standards.

OVIC seeks to ensure any revisions to the Standards account for the varied risks, maturity levels, resourcing and operating requirements of regulated organisations.

In the interim, regulated organisations are expected to continue to use the current Standards and supporting material and remain in effect for organisations reporting in 2026.

# Questions?

Have your say on this VISN event –
https://forms.office.com/r/Ai5mcF7rsH

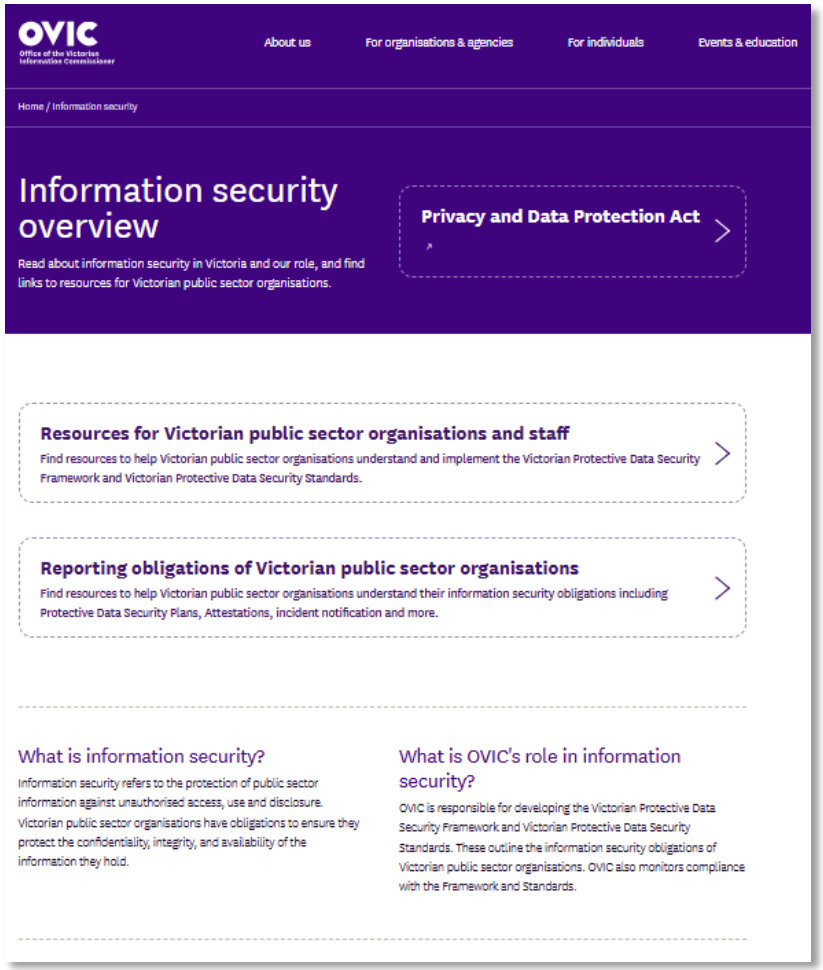
# Final thoughts

Anthony Corso

*Privacy and Data Protection, Acting Deputy Commissioner*

Have your say on this VISN event –
https://forms.office.com/r/Ai5mcF7rsH

# Find out more




Visit the OVIC website to:

- download the relevant *2026 Protective Data Security Plan*
- download the relevant *2026 - How to: A Guide to completing a PDSP*

  or

- view additional guidance material

ovic.vic.gov.au

If after reviewing these resources, and you require further help, reach out to security@ovic.vic.gov.au

Have your say on this VISN event – https://forms.office.com/r/Ai5mcF7rsH

OVIC

www.ovic.vic.gov.au