

2022 Protective Data Security Plan Insights

Victorian Information Security Network (VISN)
May 2023

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.

Commissioner's welcome



Sven Bluemmel

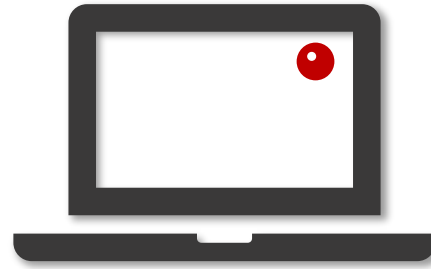
Information Commissioner

- The current and emerging security environment
- What is today all about?
- Transparency and accountability
- Your organisation's Insights Report
- 2023 – an attestation year

Housekeeping



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



Today's session **is being recorded** and will be made available after the session.



slido



Join the conversation using **#PDSPInsights** at **slido.com** or using the chat feature in **MS Teams**.

What we'll explore today

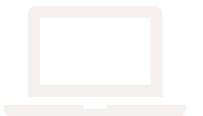
- The Insights Report
- OVIC's observations from PDSP analysis
- A deeper dive into the Standards
- Questions
- Session close

What is a PDSP Insights Report?

We have taken the time to read and analyse all PDSPs from 2022 which has allowed us to develop snapshots of trends and themes for organisations. The PDSP Insights Report is the result of this analysis.

A glimpse inside

- a comparative analysis between your current PDSP submission (2022) and your previous PDSP submission.
- a comparative analysis of Whole of Victorian Government (**WoVG**) and, where applicable, sector submissions
- an overview of subsidiary organisations (only for multi-organisation submissions)
- OVIC's Information Security Unit (**ISU**) observations, in the form of takeouts



How were the PDSPs analysed?

We did a **quantitative** analysis of the **full data set**, as well as a supplementary **qualitative** analysis of **50** sample PDSPs.

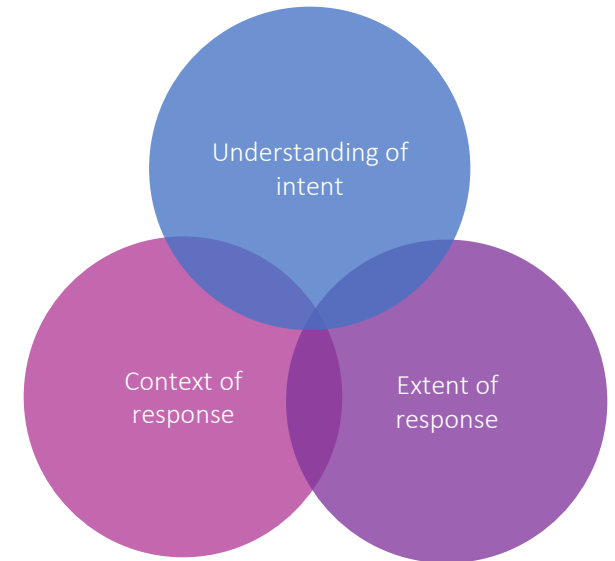
Quantitative review

Statistical review of raw data exported from 2022 PDSP forms. Some of the fields interrogated were:

- Organisational Profile Assessment (**OPA**)
- Element implementation status for each Standard
- Maturity

Qualitative review

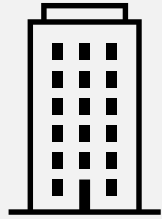
50 PDSPs were sampled, considering organisations of varying portfolios, organisational sizes, and risk profiles.



OVIC's observations

2022 Submission Statistics

Some high-level statistics that helped inform the development of these reports.



3000

organisations have been identified as covered by Part 4 of the Privacy and Data Protection Act, 2014 (PDP Act).



367

VPS PDSPs have been received by OVIC (combination of Multi-Organisation and single Organisation forms).



78%

of VPS bodies submitted a PDSP by the 31 August deadline.

By December 2022, **98%** of VPS organisations had submitted



Consistent with 2020



Increase on 2020

2020 statistics



Increase on 2020

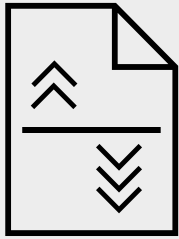
3000* in scope organisations

362 PDSPs received

60% submitted on time

General observations

1 Re-baselined submissions



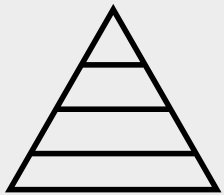
Element statuses and maturity ratings for some organisations were reconsidered and re-baselined.

2 Organisation Profile Assessment (OPA) conflicts



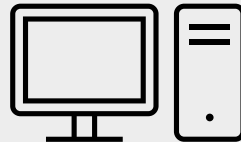
There was some conflict between an organisation's OPA and the reported implementation of related elements.

3 Maturity assessments



The maturity model is not well understood in the context of the VPDSS.

4 Cyber security focus



Some PDSPs had a strong cyber security emphasis.

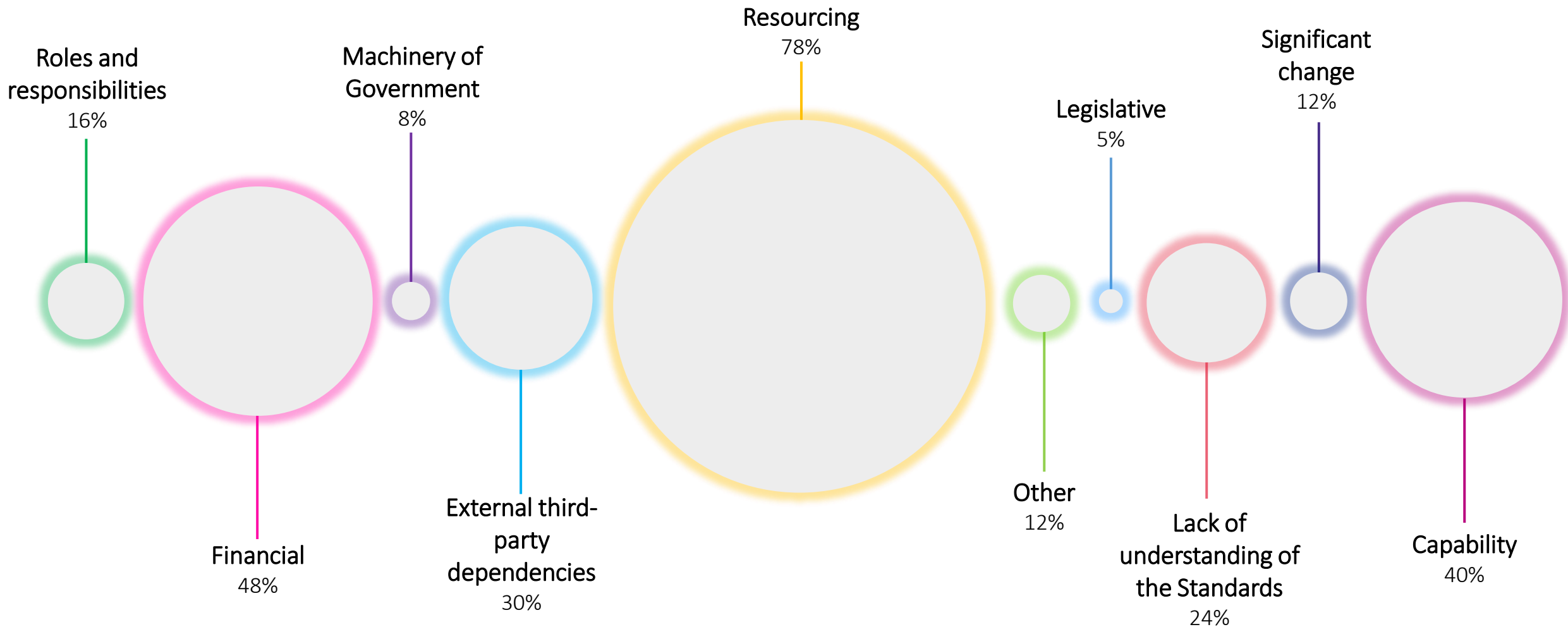
5 Third Party Arrangements (TPA)



Many organisations reported lower than expected TPA numbers in their OPA.

Challenges and Barriers

Below is a represents the challenges and barriers reported across the whole of Victorian Government.

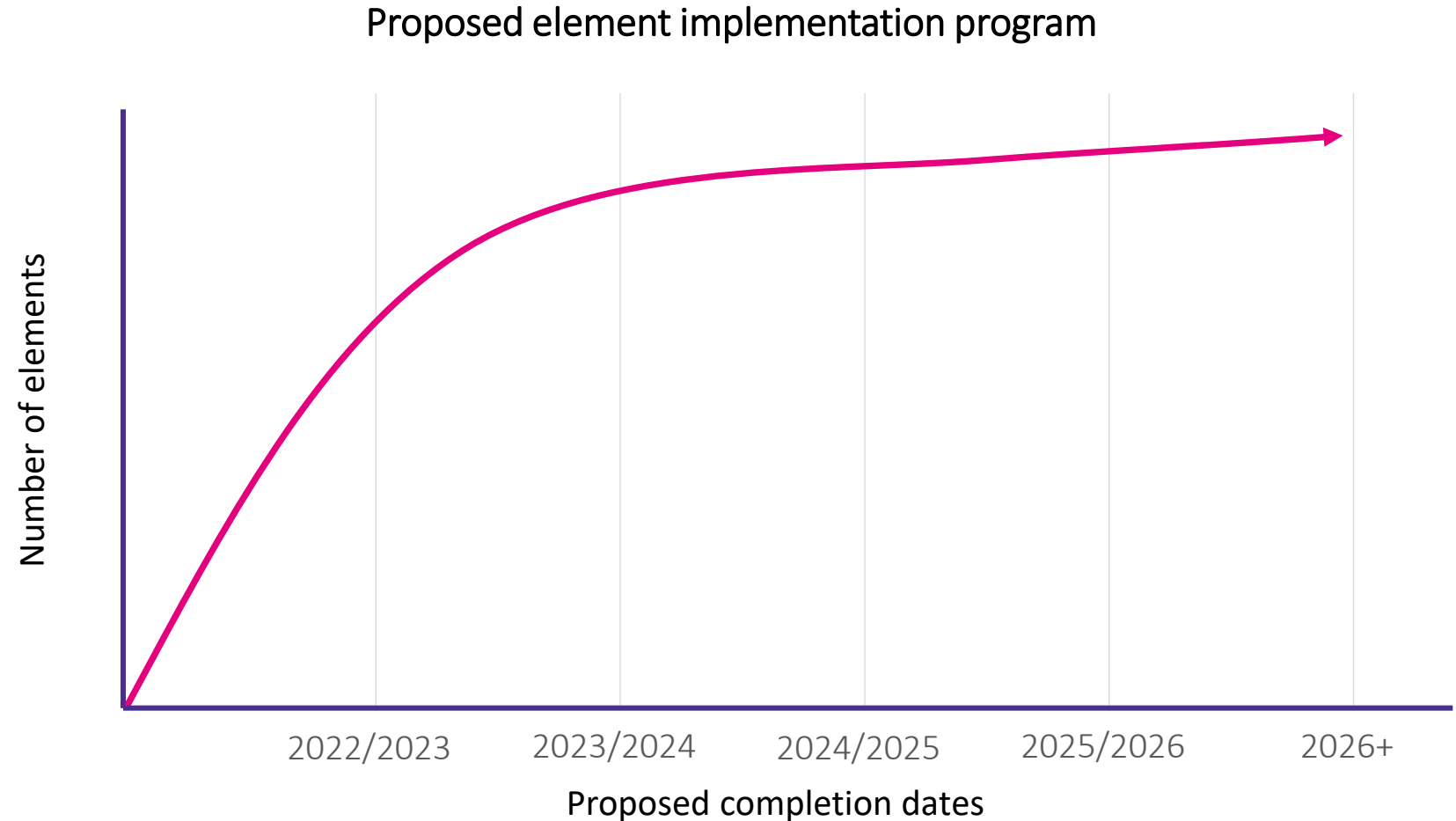


A word on Implementation of the Elements

Some organisations have ambitious implementation programs that may not match their capacity or capability.

Consider what is realistic in the timeline for implementation across elements and standards

Review any elements you may have listed as “Not applicable”, in many cases these elements might need reconsideration



Key Implementation Takeouts

1

Implemented elements now form part of your regular review cycle. They are not set and forget!

2

A general increase in implementation status (of the elements) across the Standards at a WoVG level. This is a positive development that reflects a growing awareness of information security.

3

Implementing security Standards does not guarantee complete security. Effective implementation requires ongoing risk management activities including monitoring, evaluating, and updating risks to adapt to changing information security threats and vulnerabilities.

A deeper dive into the Standards

Standard 2 – Information Security Value

Standard 2 is an integral part of the **Five-Step Action Plan** and is considered foundational to implementing many elements within the PDSP.

Takeout 1

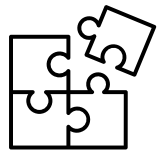
Organisations are maturing in their understanding of information security value in addition to progressing their implementation status.

Takeout 2

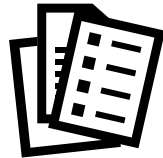
The over-valuation of assets may lead to unnecessary increased costs to protect this level of information.

Takeout 3

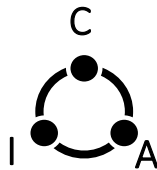
Understanding the security value of information underscores a risk-based approach to information security.



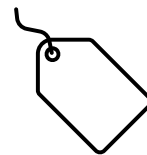
IM Framework



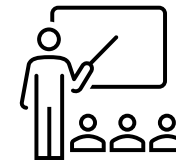
IAR



BILs



Protective Markings



Originator's Instructions



Destruction & Archiving

Standard 6 – Information Security Incident Management

Managing information security incidents enables organisations to respond quickly and prevent the incident from escalating. Remember this includes incidents that compromise the **confidentiality, integrity, or availability** of public sector information in all forms.

Takeout 1

There were inconsistencies between incidents reported in the OPA and what incidents were reported to OVIC under the incident notification scheme.

Takeout 2

Some organisation did not identify ANY information security incidents and have reported this Standard as implemented. It is very unusual for organisations to have no information security incidents.

Takeout 3

Test, test, test. An important element of this Standard is testing your incident response plan.

For deeper insight, check out our most recent report - [Incident Insights Report: 1 July 2022 – 31 December 2022](#)

Standard 8 – Third Party Arrangements

It's the organisation's responsibility to confirm that third parties are protecting the public sector information it collects, holds, manages, uses, discloses, and/or transfers on your behalf.

Takeout 1

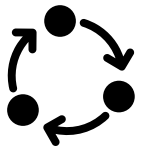
Some third parties have direct access to sensitive or security classified information. Consider what appropriate security measures are implemented, and where these are not, record the associated risk in the appropriate risk register(s).

Takeout 2

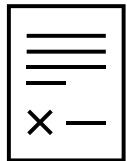
When reviewing third-party arrangements, include a review of the clauses to ensure they reflect your current operating environment and commensurate security controls.

Takeout 3

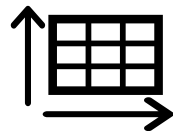
TPAs recorded within OPAs was lower than expected. Consider any third party with direct access to information.



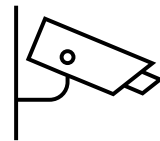
Policies & procedures



Contracts / MOUs



TPA Register



Monitor



Info release



Onsite repairs



End of agreement

Standard 10 – Personnel Security

Gaining assurance of the eligibility of the people who have access to your organisation's information is a critical step in protecting it.

Takeout 1

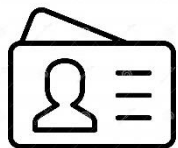
Organisations that do not handle security classified information may not be required to undertake personnel security clearances. However, due diligence is still required when engaging and managing personnel.

Takeout 2

Organisations that handle security classified information are expected to undertake the relevant personnel security measures to protect that information. This is an expectation from other organisations that might share sensitive or security classified information with you.

Takeout 3

Organisations are considering security clearances for high assurance roles and not just for personnel working with security classified information.



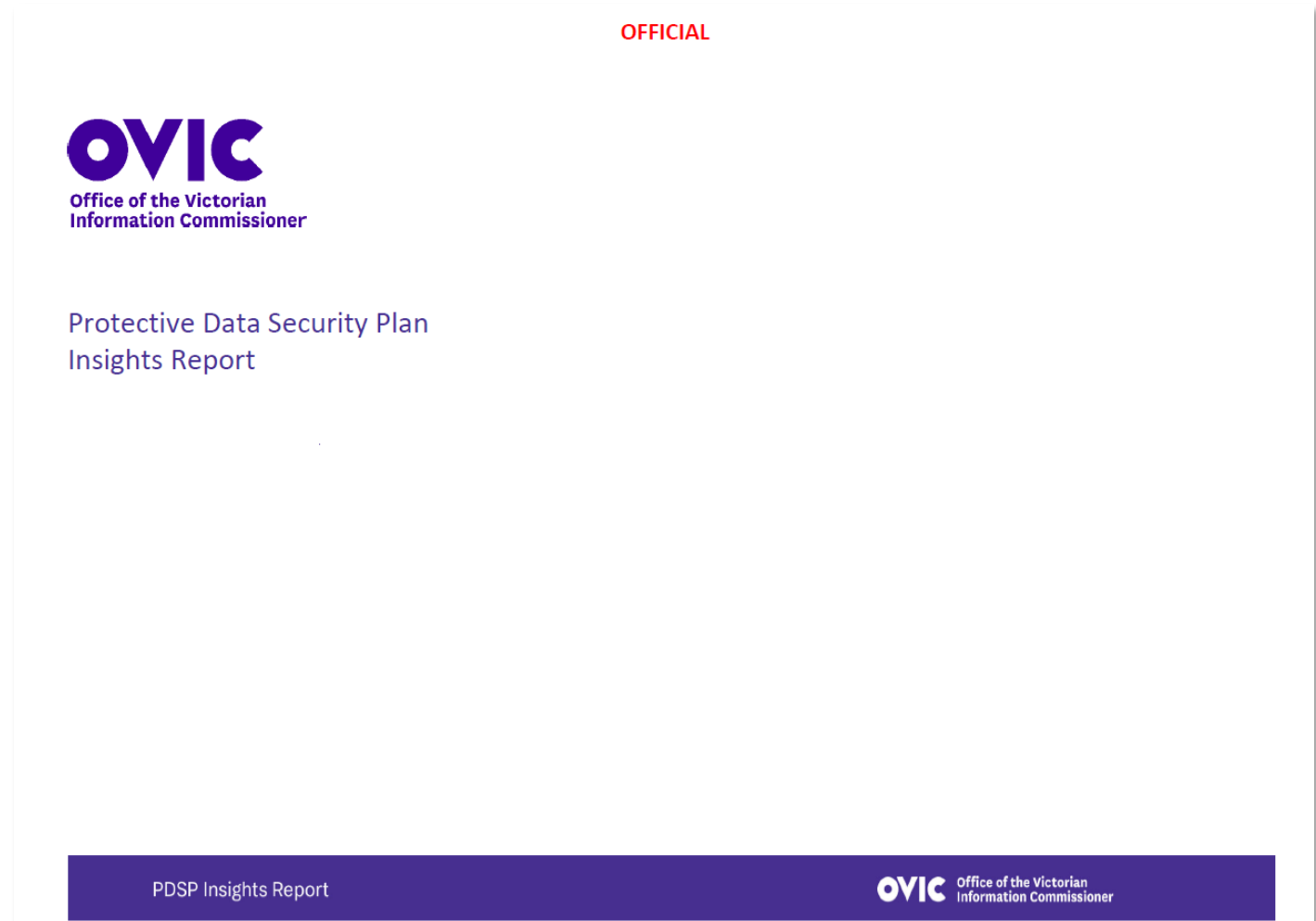
Questions?

Contact the Information Security Unit
security@ovic.vic.gov.au

What's next?

In the coming weeks, OVIC will send out a customised Protective Data Security Plan (PDSP) Insights Report to your Agency Head and Information Security Lead.

If any questions arise from this, reach out to the Information Security Unit (ISU) by emailing security@ovic.vic.gov.au



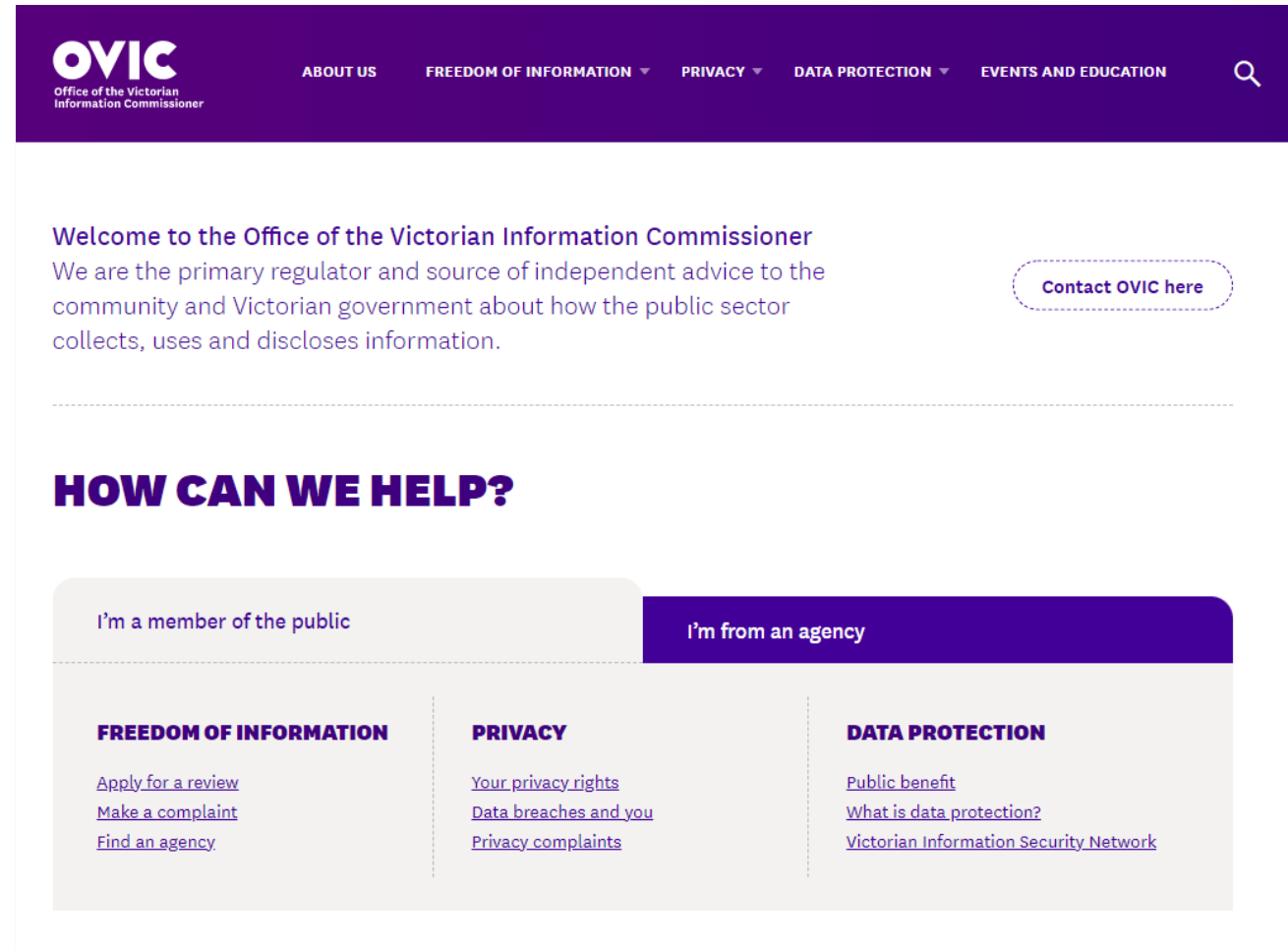
Find out more

Visit the OVIC website to download our guidance material and find out more!

ovic.vic.gov.au

Contact the Information Security Unit

security@ovic.vic.gov.au



The screenshot shows the OVIC website homepage. At the top is a dark purple navigation bar with the OVIC logo on the left and menu items: ABOUT US, FREEDOM OF INFORMATION, PRIVACY, DATA PROTECTION, and EVENTS AND EDUCATION. A search icon is on the right. Below the navigation bar, the main content area has a white background. It starts with a welcome message: "Welcome to the Office of the Victorian Information Commissioner" followed by a paragraph: "We are the primary regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses and discloses information." To the right of this text is a button labeled "Contact OVIC here". Below this is a section titled "HOW CAN WE HELP?" in large purple letters. Underneath are two tabs: "I'm a member of the public" (light grey) and "I'm from an agency" (dark purple). The "I'm from an agency" tab is selected. Below the tabs are three columns of links under the headings "FREEDOM OF INFORMATION", "PRIVACY", and "DATA PROTECTION".

OVIC
Office of the Victorian Information Commissioner

ABOUT US FREEDOM OF INFORMATION PRIVACY DATA PROTECTION EVENTS AND EDUCATION

Welcome to the Office of the Victorian Information Commissioner
We are the primary regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses and discloses information.

Contact OVIC here

HOW CAN WE HELP?

I'm a member of the public I'm from an agency

FREEDOM OF INFORMATION
[Apply for a review](#)
[Make a complaint](#)
[Find an agency](#)

PRIVACY
[Your privacy rights](#)
[Data breaches and you](#)
[Privacy complaints](#)

DATA PROTECTION
[Public benefit](#)
[What is data protection?](#)
[Victorian Information Security Network](#)