Caution

Attribution

Information Security enquiries:

Should you have any questions regarding the interpretation or representation of this material, please contact the Information Security Unit at security@ovic.vic.gov.au prior to replicating or disseminating any of this content.

Media enquiries:

Please direct any questions to media@ovic.vic.gov.au

OVIC
Office of the Victorian
Information Commissioner

Office of the Victorian Information Commissioner

Protective Data Security Plan Insights Forum

Victorian Information Security Network (VISN)

March 2021

Acknowledgement

We acknowledge the traditional custodians of the land on which we are meeting today, and pay our respects to them, their culture and their Elders past, present and emerging. We also acknowledge the Elders from other communities who may be here today.

Office of the Victorian
Information Commissioner

Commissioner Welcome

Standard 2 – Information Security Value

Standard

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

ublic sector
y.

rce

mation
nt Framework

ecurity and Privacy

ifecycle
nt

ioner Guide:
nd Managing
Assets

ioner Guide:
e security value of
information

ioner Guide:
e security value of
information

11

Victorian Protective Data Security Standards

Version 2.0 Implementation Guidance V2.1

SS) is to
actices to
ards are issued

rmation, personnel,

rred to as CIA) of

tcome

y topic area
formational)

hat is required
andatory)

hy it is required
formational)

w to?
sk-based action)

6

OVIC
Office of the Victorian
Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version V2.0

Implementation Guidance V2.1

Freedom of Information | Privacy | Data Protection

Housekeeping

Office of the Victorian Information Commissioner

Agenda

Overview of Victorian Public Sector (VPS) Protective Data Security Plans (PDSPs)

PDSP submission statistics and general insights including:

- general trends and themes observed across VPS;
- a broad breakdown of implementation status of each Standard by WoVG vs. Portfolio; and
- next steps for OVIC and VPS organisations.

Anthony Corso

Assistant Commissioner, Information Security

Laurencia Dimelow

Principal Advisor, Information Security

Q&A

The Information Security Unit

Participate in the Q&A

slido

During the session we will be using an online tool (Sli.do) offering you an opportunity to interact with our presentation, engage in polls and ask questions.

For those using the tool you will have the option of asking questions **anonymously.**

Microsoft Teams

Alternatively, you can submit questions via the Microsoft Teams chat.

Any questions posted in MS Teams **won't be anonymous**.

The team will moderate these tools and will post any relevant comments or material to the audience.

slido

Open browser

Go to slido.com

Join with event code

R352 JOIN

OVIC Summary

Office of the Victorian Information Commissioner

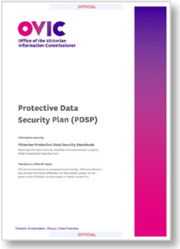
The PDSP Journey

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version 2.0

Freedom of Information | Privacy | Data Protection



OFFICIAL

Protective Data Security Plan (PDSP)

Information Security

Victorian Protective Data Security Standards

Reporting information security capability and implementation progress
Single Organisation Reporting Form

Version 2.1 March 2020

This form is intended to be completed electronically. Different software may preview form fields differently. For best results, please use the latest version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL

OVIC

VPDSS 2.0 Issued — *October 2019*

Updated PDSP Template Released — *November 2019*

Roundtables with VPS organisations

PDSP Submissions — *August 2020*

VPS Organisations

5 Step Action Plan, including:

• IAR • BILs • SRPA • Controls (Elements)

Protective Data Security Plan (**PDSP**) Submission

August 2020

How were the PDSPs analysed by OVIC?

OVIC performed a **quantitative** analysis the **full data set**, as well as a supplementary **qualitative** analysis of **30** sample PDSPs.

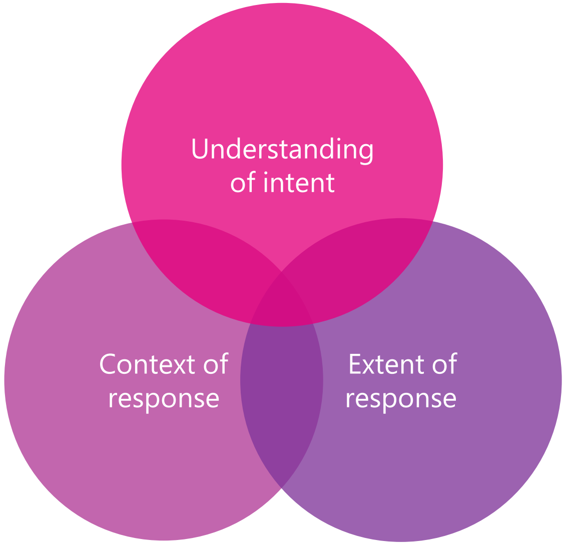
Quantitative review

Statistical review of raw data exported from 2020 PDSP forms. Some of the fields interrogated were:

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

Qualitative review

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



2020 PDSP Submission Statistics

~3000* organisations have been identified as covered by the Part Four of the Privacy and Data Protection Act, 2014 (**PDP Act**).

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

359 Cemetery Trust PDSPs have been received by OVIC, however statistics aren't represented in the following slides.

This indicates a 72% submission rate for Cemetery Trusts.

60% of VPS bodies submitted a PDSP **by the 31 August deadline**

By December 2020, 90% of VPS organisations had submitted.

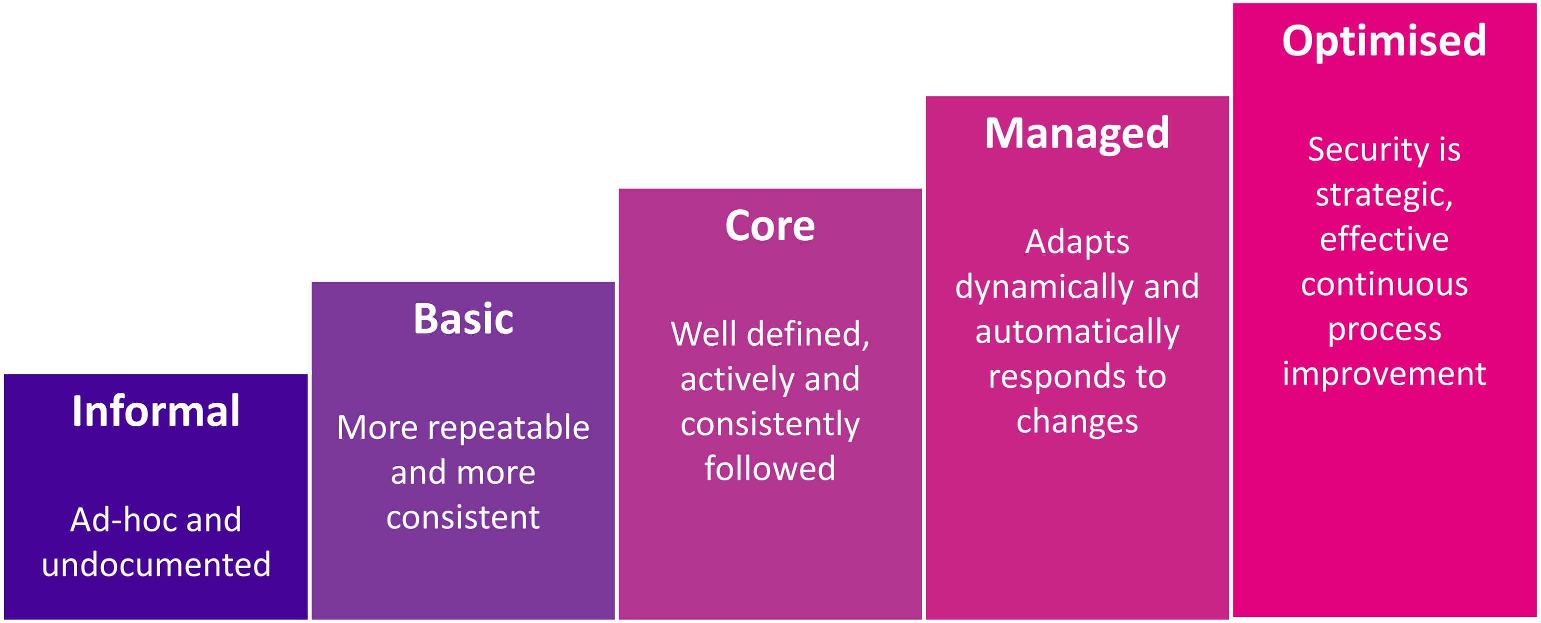
27 PDSPs from the 2020 reporting period are yet to be submitted to OVIC.

***Note**: Figures are as of the **1st of Feb 2021** and subject to change due to MoG's etc.*

A word on maturity

OVIC observed that organisations tended to report maturity ratings, one level higher than evidence supports.

Some organisations suggested an aspirational maturity rating of **Optimised**, whereas others provided a more calibrated response of **Basic** or **Core**.



Informal

Ad-hoc and undocumented

Basic

More repeatable and more consistent

Core

Well defined, actively and consistently followed

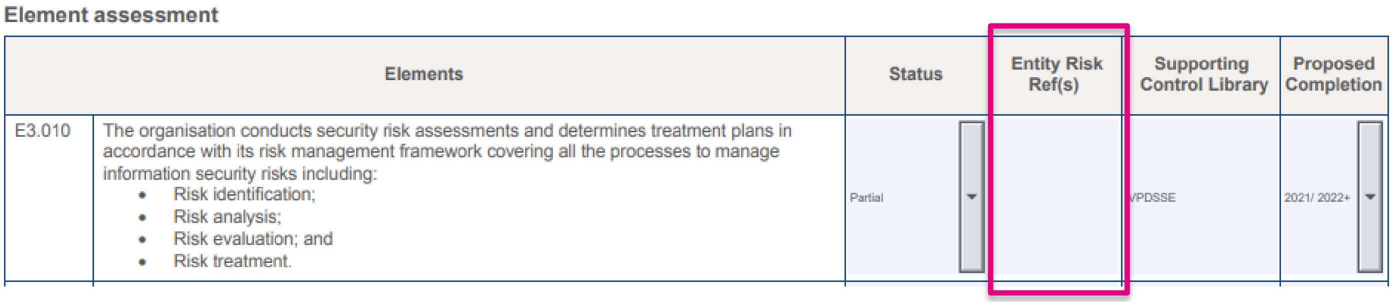
Managed

Adapts dynamically and automatically responds to changes

Optimised

Security is strategic, effective continuous process improvement

Engaging with risk



Element assessment

Elements		Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E3.010	The organisation conducts security risk assessments and determines treatment plans in accordance with its risk management framework covering all the processes to manage information security risks including: • Risk identification; • Risk analysis; • Risk evaluation; and • Risk treatment.	Partial		VPDSSE	2021/ 2022+

Approximately **40%** of 'Entity risk reference' fields were **not completed** on PDSPs.

This could indicate that organisations:

- are yet to undertake the Security Risk Profile Assessment (**SRPA**) process,
- have existing controls in place that may not have been formally tied back to an organisation risk, and/or
- were unsure how to interact with or complete this field in their PDSP.

OVIC would expect that an organisation records at least one information security risk in their risk register, and subsequently on their PDSP. To find out more download OVIC's *Practitioner Guide Information Security Risk Management* available on the OVIC website – VPDSF Resources page.

High-level Observations

Office of the Victorian Information Commissioner

Six key takeout's

1. Failure to complete **foundational activities**, resulting in some **critical gaps** in information security programs
2. **Higher rates of implementation** in more **'traditional' areas** of information security (e.g., information access, ICT security and physical security)
3. A lack of **oversight** and **assurance** around **third parties**
4. **Discrepancies** between **implementation status** and self-assessed **maturity ratings**
5. Opportunities to enhance **information security incident management** and response
6. Increased engagement and understanding of the **risk-based nature of the Standards**

Roles and responsibilities

25%

of PDSPs indicated that their **IT team** is responsible for managing their information security program

OVIC understands that different organisations approached the 2020 PDSP submission process in various ways with some:

- **encouraging different teams to come together** and work on the responses collaboratively, providing their unique insight or subject matter expertise;
- **relying upon a central individual (often the Information Security Lead**) to document their understanding of implementation efforts across the business, sometimes in consultation with key personnel; **or**,
- **engaging outside personnel** (such as a security consultant or contractor) to assist.

A mature information security program should involve extensive consultation and collaboration.

- Strong support and endorsement of key personnel involved in the project is also essential, providing them a mandate to reach out to the business and get their critical insights.

20%

of organisations reported a *"lack of clarity around roles and responsibilities within organisation"*

Trends and Themes

Office of the Victorian
Information Commissioner

WoVG trends by Standard

VPS organisations generally reported:

Stronger implementation statuses for

- **Std 3 (Risk)**
- **Std 4 (Access)**
- **Std 11 (ICT)**
- **Std 12 (Physical)**

Weaker implementation statuses for

- **Std 2 (Security Value)**
- **Std 6 (Incidents)**
- **Std 8 (Third Parties)**
- **Std 10 (Personnel)**

Mid-range implementation statuses were provided for

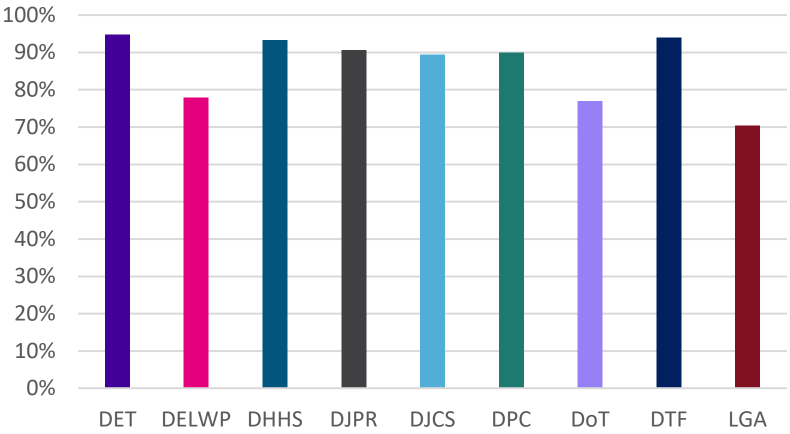
- **Std 1 (ISMF)**
- **Std 5 (Security Obligations)**
- **Std 7 (BCP/DR)**
- **Std 9 (Reporting to OVIC)**

Implementation status represents a combination of both **Partial and **Implemented** statuses*

Stronger implementation statuses

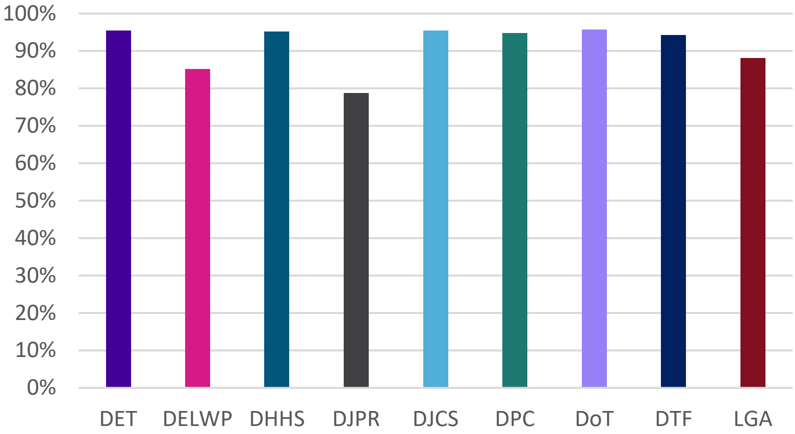
Std 3 Information Security Risk Management

- It wasn't always clear whether an organisation had undertaken the SRPA process
- **60%** of PDSPs included an entity risk reference
- Organisations are generally familiar risk management, however responses indicated information security risk management was less understood



Std 4 Information Access

- Establishing strong governance around identity and access management is critical given **80%** of organisations reported that third parties had direct access to their information
- **43%** of organisations reported ***Partial*** when noting their progress towards establishing an identity and access management policy



** LGA refers to Local Government Authorities*

** The acronyms provided are representative of the portfolios, rather than the departments themselves*

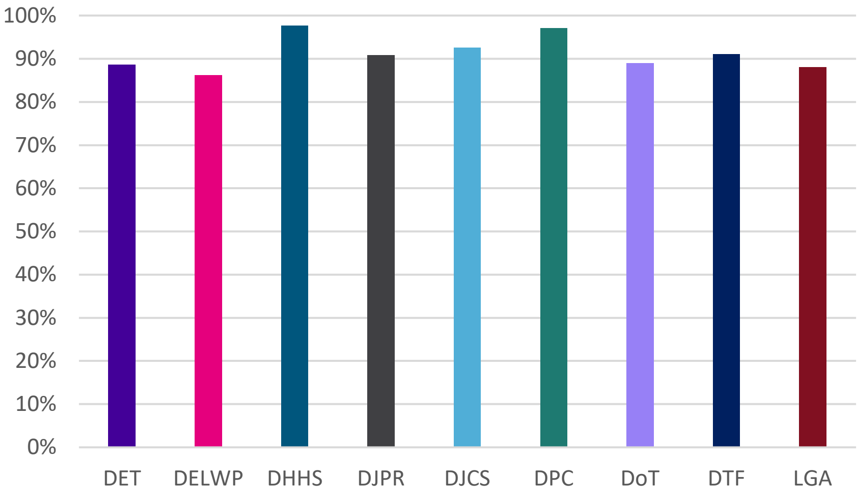
Stronger implementation statuses

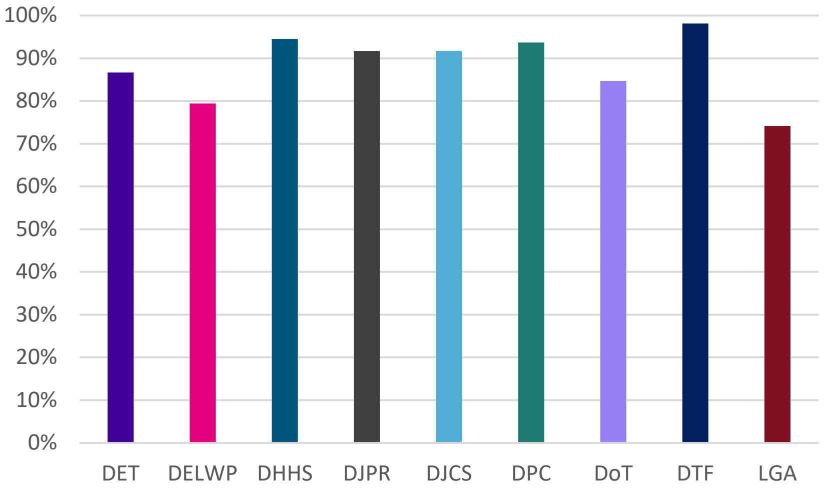
Std 11 ICT Security

- OVIC saw a strong trend in the uptake of ICT/cyber-focused information security activities
- Some organisations who use third parties to perform functions or services on their behalf, incorrectly marked certain VPDSS Elements as ***Not Applicable*** or ***Implemented***. Accountability cannot be outsourced under Part 4 of the PDP Act

Std 12 Physical Security

- This Standard has broad coverage and considers the physical security arrangements regarding facilities, equipment and services.
- Implementation rates for this Standard were relatively high, however comparatively few organisations sought to go beyond a maturity level of ***Core***

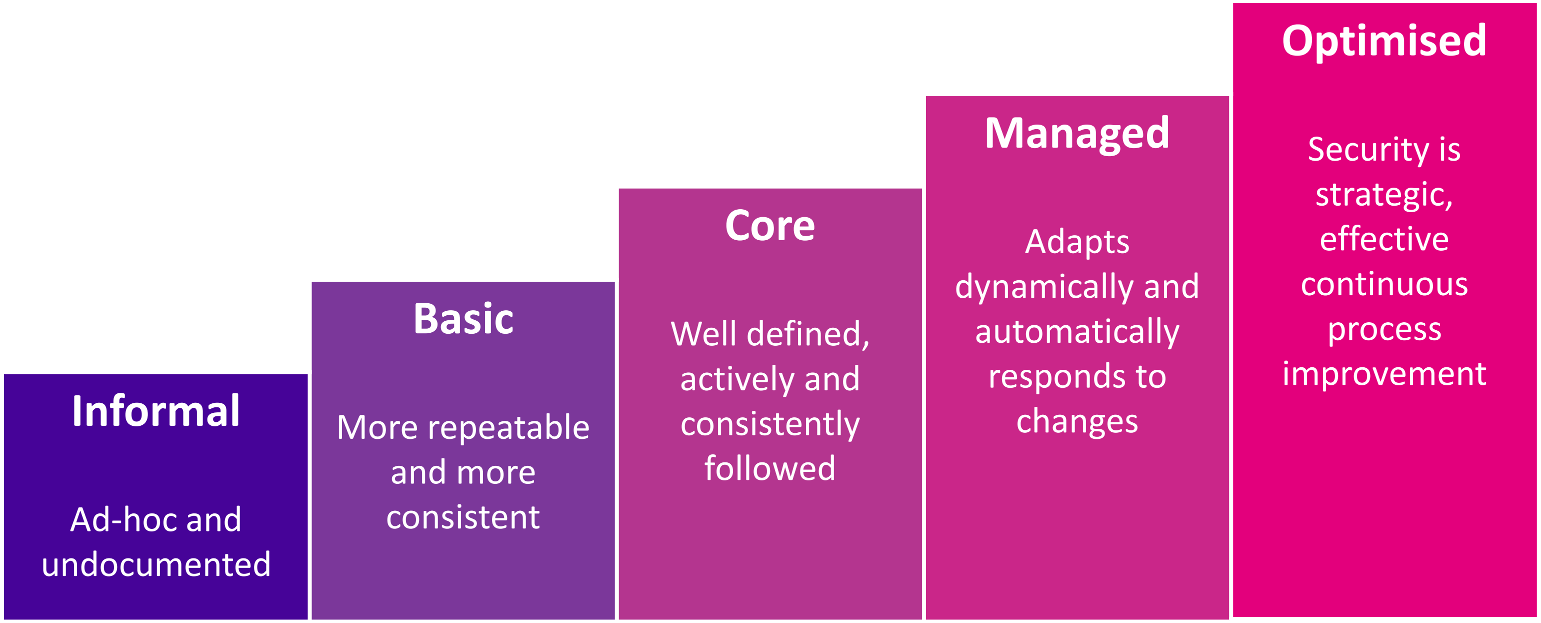




** LGA refers to Local Government Authorities*

** The acronyms provided are representative of the portfolios, rather than the departments themselves*

Maturity levels



Informal

Ad-hoc and undocumented

Basic

More repeatable and more consistent

Core

Well defined, actively and consistently followed

Managed

Adapts dynamically and automatically responds to changes

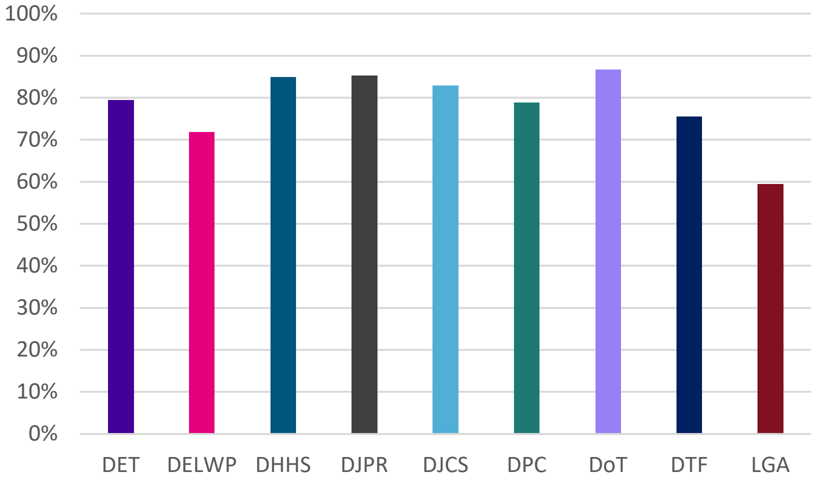
Optimised

Security is strategic, effective continuous process improvement

Mid-range implementation statuses

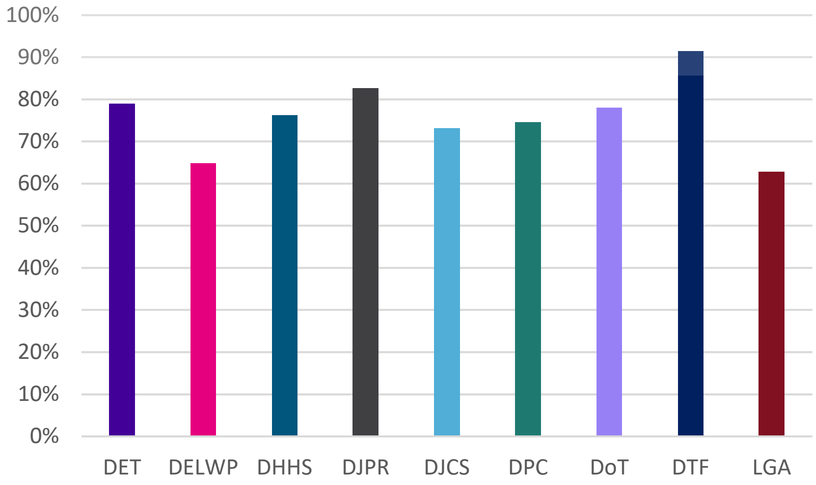
Std 1 Information Security Management Framework

- Implementation status of this Standard has a significant impact on the organisations ability to properly implement, manage and review security controls across the subsequent standards
- Under Standard 1 (E1.050), organisations must nominate an **'Information Security Lead**' and notify OVIC of any changes to this point of contact. Keep this in mind if any personnel or governance structures change, especially with upcoming **Attestations due by 31 August 2021.**



Std 5 Information Security Obligations

- Standard 5 had a moderate implementation rate in comparison to other responses. Of note:
  - **lower** implementation **rates** for **targeted training** for staff in high-risk functions, or with specific information security obligations,
  - **higher rates** for **generalised** information security **training**.
- It is encouraging that many VPS organisations indicated that activities supporting this standard were ***Planned***.



** LGA refers to Local Government Authorities*

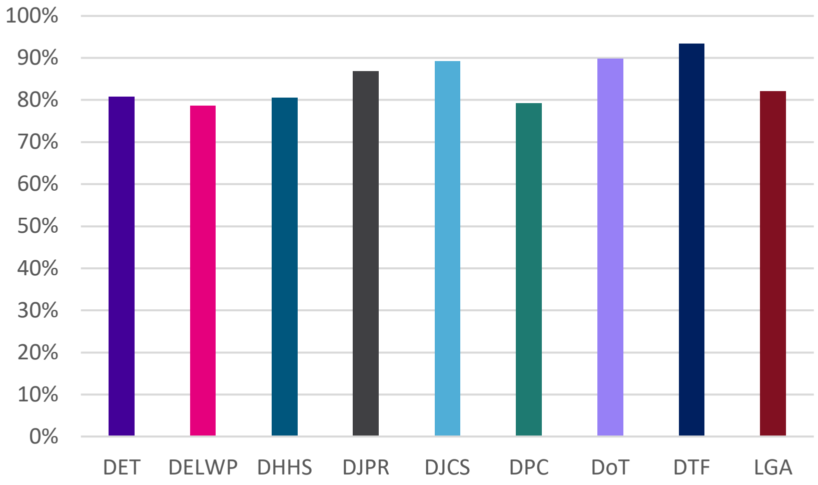
** The acronyms provided are representative of the portfolios, rather than the departments themselves*

Mid-range implementation statuses

Std 7 Business Continuity and Disaster Recovery

- 2018 reports noted higher implementation rates for business continuity and disaster recovery across WoVG than 2020.

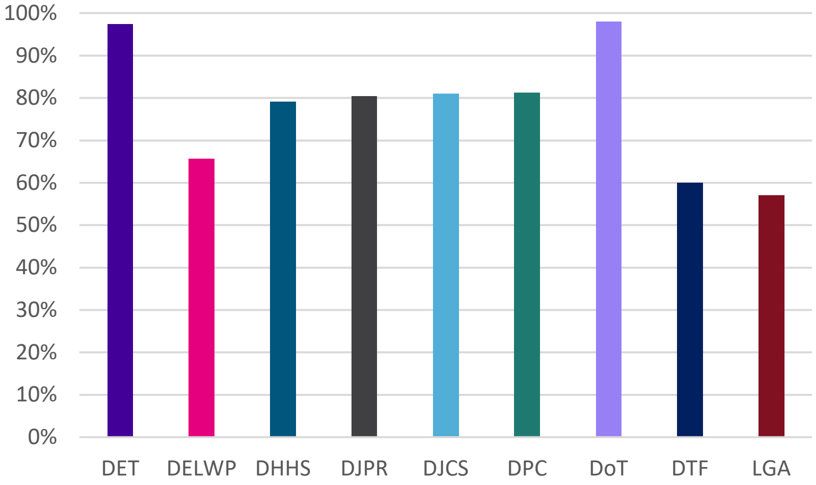
- **2020** reporting may have presented an opportunity for VPS organisations to **recalibrate** their understanding and appreciation of what is required by this Standard, after critically reflecting on business disruptions ushered in by COVID-19.



Std 9 Information Security Reporting to OVIC

- **Responses** for this Standard **varied** greatly. This may be based on interpretation of the wording, or the way the PDSP form was structured. The ISU will address this in product revisions.

- Standard 9 (E9.010) requires organisations notify OVIC of information security incidents. Responses to this requirement varied great, perhaps based on:
  - the ability of an organisation to **identify** information security **incidents** as they occur; and/or
  - their understanding when the notification **threshold of BIL 2** or higher has been reached.



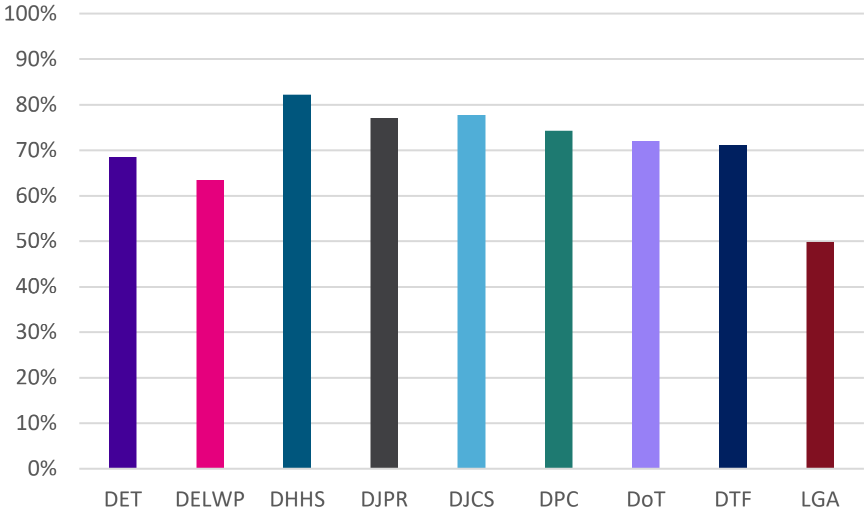
** LGA refers to Local Government Authorities*

** The acronyms provided are representative of the portfolios, rather than the departments themselves*

Weaker implementation statuses

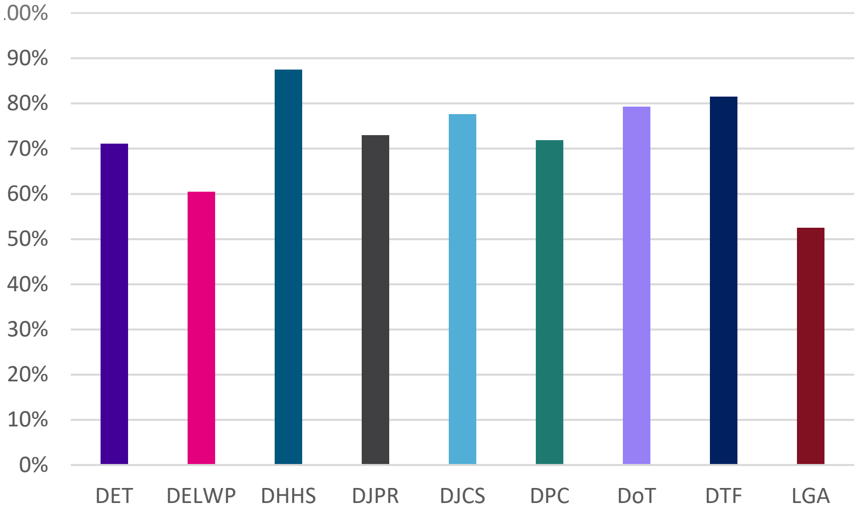
Std 2 Information Security Value

- Standard 2 had the lowest implementation rate
- Some organisations provided conflicting responses noting:
  - they had information at **PROTECTED or above**, but
  - they did not have information at **BIL 3 or above**, and/or
  - selected ***Not Applicable*** for certain elements that are typically tied to the protection of higher value material. Justifications included - "*The organisation does not have security classified information*".



Std 6 Information Security Incident Management

- Roughly **50%** of organisations **recorded <u>no</u>** information security incidents over the **past 2 years**. Given this, organisations should consider opportunities to enhance information security incidents management practices.
- Reporting indicated a **disconnect** between the number of **incidents recorded** by an organisation, and **implementation statuses** for this Standard. This perhaps signaled some operational challenges for organisations in recording incidents.



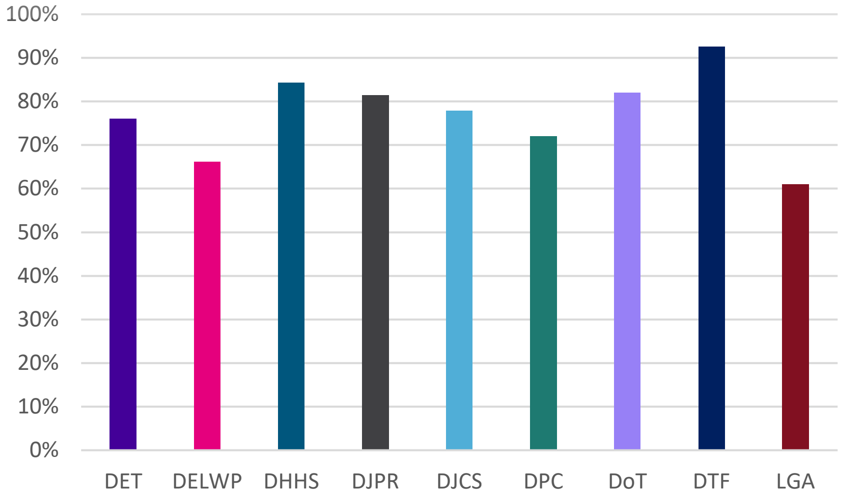
** LGA refers to Local Government Authorities*

** The acronyms provided are representative of the portfolios, rather than the departments themselves*

Weaker implementation statuses

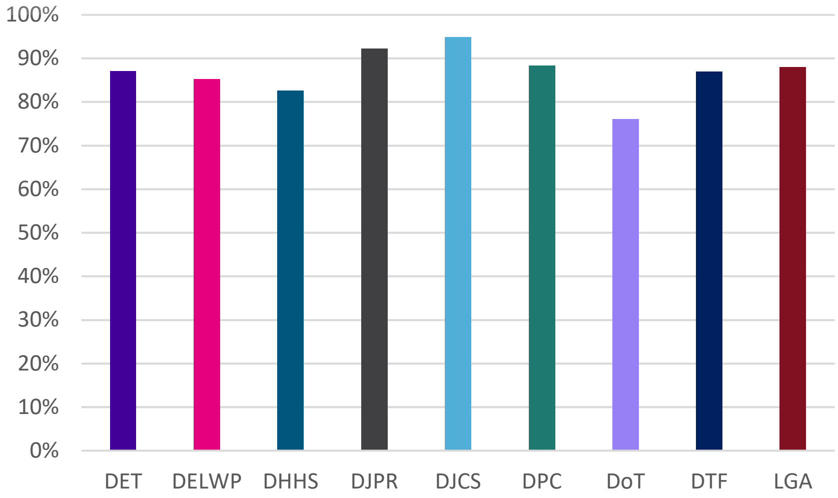
Std 8 Third Party Arrangements

- Roughly **20%** of organisations indicated they **did not have third party arrangements** with **direct access** to information. This figure stood out as unusually high to the Information Security Unit.
- Lower implementation rates for this Standard were often coupled with lower maturity levels. This presents an opportunity to improve guidance around third party assurance.



Std 10 Personnel Security

- Elements E10.060 – E10.080 (i.e., requirements regarding security clearances) had the highest reported rate of ***Not Applicable.***
  - In support of this, some organisations stated in their rationale that they did not '*collect, hold, use, manage, disclose or transfer security classified information*'.
  - However, **20%** of these organisations reported that they had **security classified information** (Part A of their PDSP).



** LGA refers to Local Government Authorities*

** The acronyms provided are representative of the portfolios, rather than the departments themselves*

Next steps for Organisations

OVIC

Office of the Victorian Information Commissioner

Check list of next steps for organisations

Consider:

Brief your Executive on the upcoming **Attestation**.
These must be submitted to **OVIC by August 31st**

If your organisation has undergone **significant change**, contact the Information Security Unit (ISU) by emailing security@ovic.vic.gov.au.
A new PDSP submission is required in accordance with Part 4 of the PDP Act.

Review, validate and update:

☑ Information Asset Register (IAR)

☑ Information Security Risks via the Security Risk Profile Assessment (**SPRA**) process

☑ Any '**In Progress**' or '**Planned**' activities outlined in your organisation's PDSP's

Next Steps for OVIC

OVIC

Office of the Victorian
Information Commissioner

OVIC in 2021

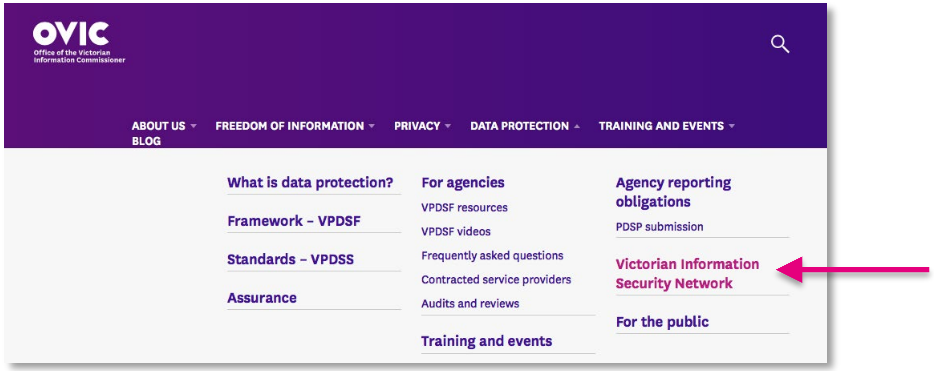
OVIC will:

- send out a customised report to all VPS organisations that submitted a PDSP in the 2020 reporting cycle
- provide targeted one-on-one sessions to some VPS organisations, running through OVICs observations on their PDSPs. Invites and details to these sessions coming soon!
- kick off Special Interest Group (SIG) meetings for Information Security Leads – due to commence in May 2021.
- continue to host VISN events and forums, with a moderated panel discussing Insights into the Information Security Incident Notification Scheme to be held on the **30th of March** – invites and event details to follow on the OVIC website (VPS only)
- conduct monitoring and assurance activities based on PDSP submissions (or lack thereof)
- continue to develop and update guidance material to support the uptake of the Standards

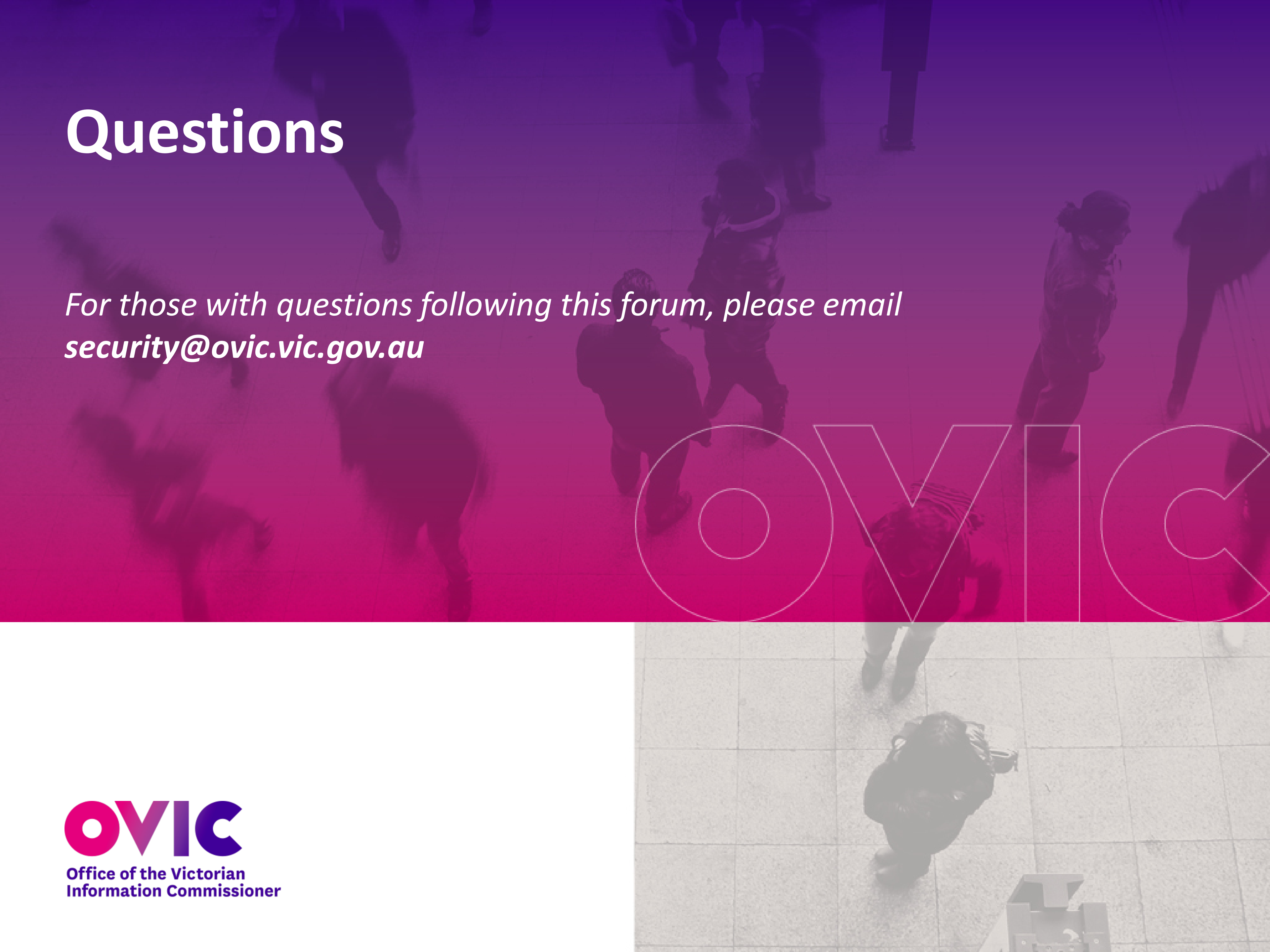
Copies of Slides and Q&A

Slides and Q&A

For those who want to access a copy of this slide deck please refer to the **Victorian Information Security Network** page on the OVIC website.



OVIC
Office of the Victorian Information Commissioner
Protective Data Security Plan Insights Forum
Victorian Information Security Network (VISN)
March 2021
P



Questions

For those with questions following this forum, please email ***security@ovic.vic.gov.au***

OVIC
Office of the Victorian
Information Commissioner