



**Office of the Victorian
Information Commissioner**



Victorian Protective Data Security Standards – Version 2.0

Key Changes and Next Steps

November 2019

Acknowledgement

We acknowledge the traditional custodians of the land on which we are meeting today, the Wurundjeri people of the Kulin Nation, 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.

OVIC



Office of the Victorian
Information Commissioner



Agenda

1. Welcome by Anthony Corso, Assistant Commissioner - Information Security
2. Outline of Key Changes in VPDSS 2.0
3. Updated Protective Data Security Plan (PDSP)
4. Introduction of the Incident Notification Scheme
5. Launch of the refreshed online collaboration tool for the VISN – GovTeams
6. Upcoming engagements and events
7. Document Map
8. Questions

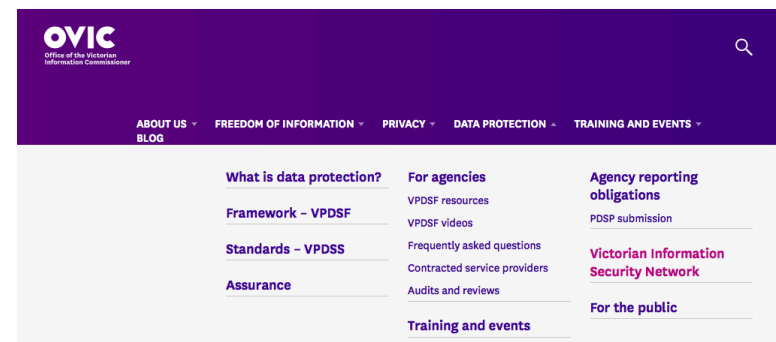
Live Streaming/Recording of Event & Copies of Slides

Live streaming / recording

This event is being live streamed on Periscope. A recording of this be posted on our website after the event.

Slides

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.

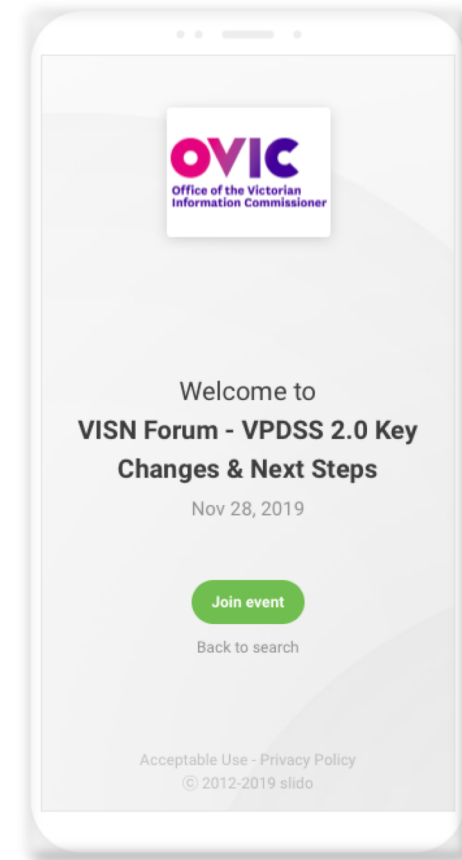


SLiDo

During the event 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 and can also access a link

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



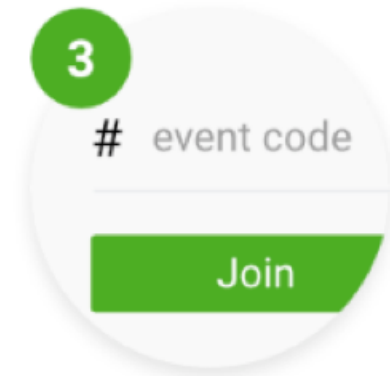
SLiDo



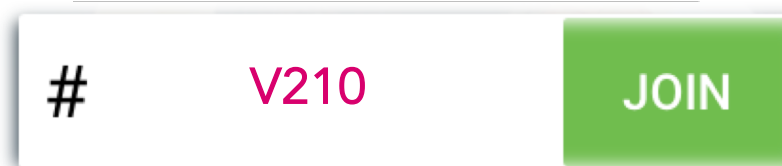
Open browser



Go to slido.com



Join with event code



Key Changes in VPDSS 2.0

OVIC



Lesson learned from VPDSS V1.0

In 2018, OVIC commissioned an independent review of the framework (including the standards) to assess its effectiveness and identify areas for improvement

The review involved consultation with selected organisations and analysis of feedback received from OVIC stakeholders.

Findings from the Review included:

- The VPDSF had an **overwhelming overall positive impact** for Victorian government organisations and the Victorian government as a whole
- The **attestation process contributed substantially to executive awareness** of information security, and
- The **VPDSF could be improved by simplifying the VPDSS** and supporting materials.

Issue of VPDSS 2.0



11 October 2019

The Honourable Gavin Jennings MLC, Special Minister of State, agreed to revoke the Victorian Protective Data Security Standards issued in July 2016 and approved the new Standards (V2.0).



28 October 2019

Sven Bluemmel, Victorian Information Commissioner, revoked the Victorian Protective Data Security Standards issued in July 2016 and issued the new Standards (V2.0).



29 October 2019

The new Standards (V2.0) were tabled in Parliament and published in the Gazette, bringing them into full effect.

Key Changes in VPDSS 2.0

- **Simpler** language to support a principles-based approach
- Replacing ‘public sector data’ with ‘**public sector information**’
- **Consolidating** common themes including merging **18 standards to 12**
- **Removing the protocols** from the Standards as the principle of continuous improvement is embedded in the framework
- **Embedding the elements** to assist with implementation of the standards. These can be found in the **VPDSS Implementation Guide**



Key Changes in VPDSS 2.0 continued...


- Replacing the *Compliance* standard with a new *Reporting* standard
- Removing duplicate elements
- Adding new elements where gaps have been identified
- Reordering the standards and elements for logical sequencing, and
- Updating primary source references



Mapping from VPDSS V1.0 to V2.0

To assist organisations align their existing work program to VPDSS 2.0, the Information Security Unit has created a resource that maps the old Standards (V1.0) to the new (V2.0).

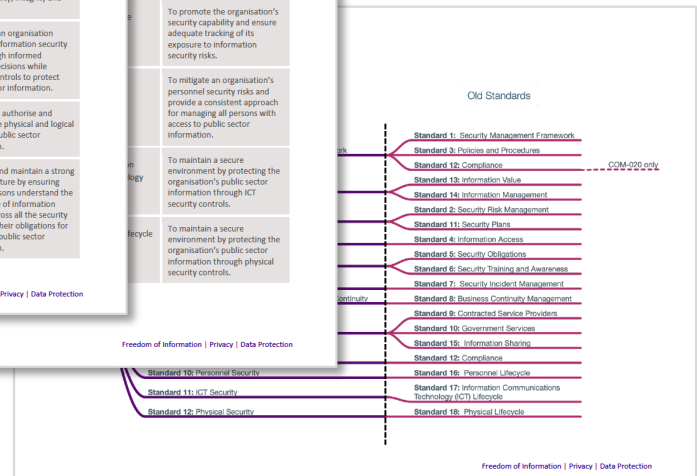
To access a copy, refer to the VPDSF Resources section of the OVIC website.



Victorian Protective Data Security Standards
Version 2.0 (2019) to Version 1.0 (2016) Mapping

Standard #	Previous Standard # (VPDSS 1.0)	Statement of Objective
1 Information Security Management Framework	Standard 1 – Security Management Framework Standard 3 – Policies and Procedures Standard 12 - Compliance (COM-020 only)	To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information.
2 Information Security Value	Standard 13 – Information Value Standard 14 – Information Management	To ensure an organisation uses consistent identification and assessment criteria for public sector information across its lifecycle to maintain its confidentiality, integrity and availability.
3 Information Security Risk Management	Standard 2 – Security Risk Management Standard 11 – Security Plans	To ensure an organisation manages information security risks through informed business decisions while applying controls to protect public sector information.
4 Information Access	Standard 4 – Information Access	To formally authorise and manage the physical and logical access to public sector information.
5 Information Security Obligations	Standard 5 – Security Obligations Standard 6 – Security Training and Awareness	To create and maintain a strong security culture by ensuring that all persons understand the importance of information security across all the security areas and their obligations for protecting public sector information.

Freedom of Information | Privacy | Data Protection



Freedom of Information | Privacy | Data Protection

VPDSS Implementation Guide

The **VPDSS Implementation Guide** provides detailed explanation of the relationship between the VPDSS Elements to the primary source.

These primary sources can assist organisations in implementing the element.

To access a copy, refer to the VPDSF Resources section of the OVIC website.



Standard 1 – Information Security Management Framework

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

Statement of Objective
To clearly establish, articulate, support and promote the security governance arrangements across the organisation and manage security risks to public sector information.

Elements

V2.0 #	V1.1 #	Element	Primary Source
E1.010	SMF-010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.	AS ISO/IEC 27001:2015 Information security management systems - Requirements § 4 § 5.2 § 6.2
E1.020	SMF-020	The organisation's information security management framework contains and references all legislative and regulatory drivers.	AS ISO/IEC 27001:2015 § 4.2
E1.030	SMF-050	The organisation's information security management framework aligns with its risk management framework.	AS ISO/IEC 27001:2015 § 6.1 AS ISO/IEC 27005:2012 Information security risk management § 5
E1.040	SMF-040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.	AS ISO/IEC 27001:2015 § 5.3
E1.050	–	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.	Victorian Protective Data Security Framework (VPDSF) V2.0 § Nomination of an information security lead

Freedom of Information | Privacy | Data Protection 7

Updated Protective Data Security Plan (PDSP)

OVIC



Office of the Victorian
Information Commissioner



Protective Data Security Plans (PDSPs)

In a bid to simplify the reporting obligations of organisations, OVIC reviewed the requirements for the development of a:

- High-level PDSP
- Detailed PDSP
- Self Assessment, and

Attestation by the public sector body Head.

In the spirit of simplification, we have created a new PDSP form.

This PDSP form combines each of the former requirements into a single document that can be submitted to OVIC at the conclusion of the reporting cycle.

This form should deliver administrative efficiencies, whilst enabling more detailed insight into the information security programs within organisations. It will also enable OVIC to provide customised reports back to organisations.



The New PDSP Form

The new form is set out across four parts:

Part A – Security Program Executive Summary, including an Organisational Profile Assessment (OPA)

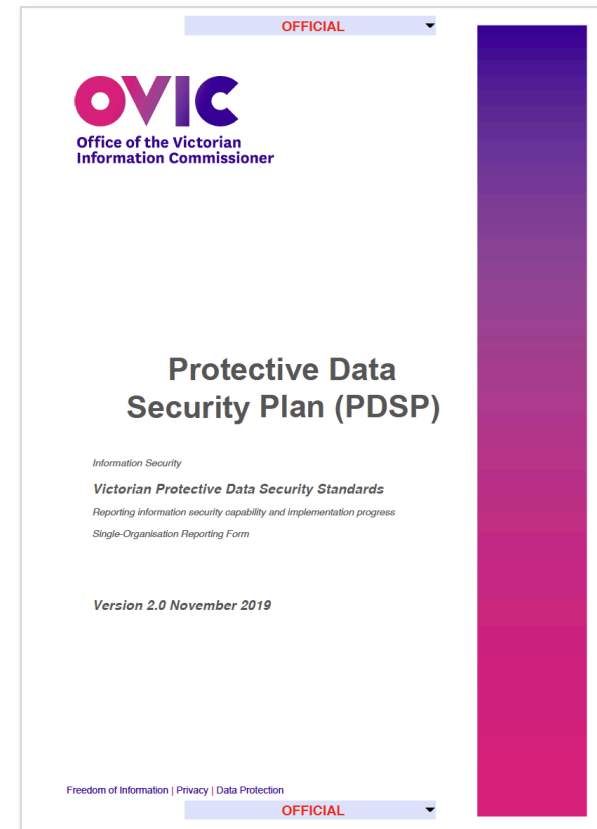
Part B – Information security self-assessment and implementation plan

Part C – Feedback to OVIC

Part D – Attestation by the public sector body Head.

N.B. The new PDSP form will be available on the OVIC website in the coming days.

Refer to the VPDSF Resources section of the OVIC website for more information.



Part B - Information security self-assessment and implementation plan

Pictured is a preview *Standard 1* from the new PDSP form.

For each Standard, organisations are required to perform an assessment of their maturity:

- Current
- Target (2020)
- Aspirational (2024)

Organisations are also expected to perform an element assessment:

- selecting the **implementation status** of each element
- noting the entity's **risk reference**
- selecting the **supporting control library** underpinning the implementation of the element
- nominating a proposed **completion date** for implementation of the element

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.

Maturity assessment

Current	2022 Target	2024 Aspiration
Informal	Informal	Informal

Element assessment

Elements	Status	Entity Risk Ref(s)	Supporting Control Library	Proposed Completion
E1.010 The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.	Not Commenced		VPDSSE	30/19/2020
E1.020 The organisation's information security management framework contains and references all legislative and regulatory drivers.	Not Applicable Not Commenced Planned		A3 27001:2015 ISM PSPF NIST VPDSSE Other	2019/2020 2020/2021 2021/2022+ Completed
E1.030 The organisation's information security management framework aligns with its risk management framework.	Not Commenced		Other	2019/2020
E1.040 Executive management defines information security functions, roles, responsibilities, competencies and authorities.	Not Commenced		VPDSSE	2019/2020
E1.050 Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.	Not Commenced		VPDSSE	2019/2020
E1.060 Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.	Not Commenced		VPDSSE	2019/2020
E1.070 The organisation identifies information security performance indicators and monitors information security obligations against these.	Not Commenced		VPDSSE	2019/2020
E1.080 Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).	Not Commenced		VPDSSE	2019/2020
E1.090 The organisation sufficiently communicates its information security management framework and ensures it is accessible.	Not Commenced		VPDSSE	2019/2020

Freedom of Information | Privacy | Data Protection
12

OFFICIAL

PDSP Submissions

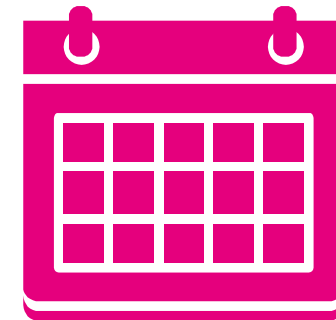
PDSP Submission Window

Submissions open 1 July 2020 and close 31 August 2020.

August 2020 Reporting

All organisations must submit a copy of their PDSP, including attestation to OVIC.

Reporting is due by **31 August 2020**, or upon significant organisational change*.



PDSP Submission Options

Submission options vary, depending on the protective marking assigned to the PDSP.

Refer to the OVIC website for more information on submission options.

PDSP's capturing multiple organisation

Should your organisation be interested in submitting a multiple organisation PDSP, please contact the Information Security Unit to discuss.

Introduction of the Incident Notification Scheme

OVIC



Office of the Victorian
Information Commissioner



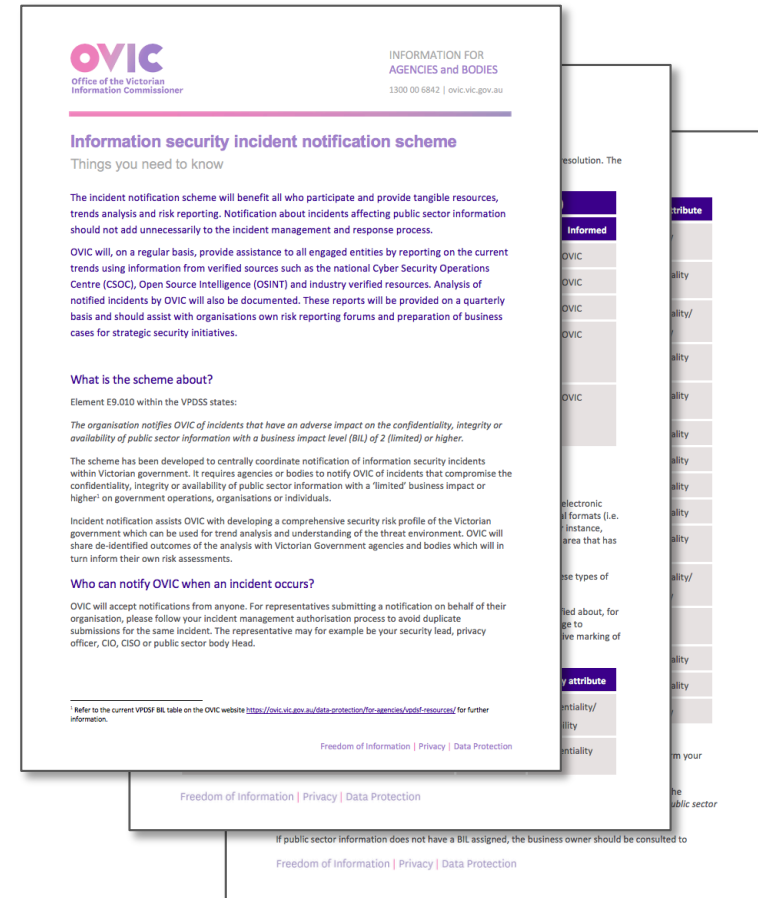
Benefits of the Incident Notification Scheme

How will the new scheme benefit organisations?

OVIC will, on a regular basis, provide assistance to all engaged organisations by **reporting on the current trends** using information from verified sources (i.e. industry reports, PDSPs and incident notifications).

These reports will be provided on a quarterly basis and should **assist with organisations own risk reporting** forums and preparation of **business cases** for strategic security initiatives.

More information about the Incident Notification Scheme will be published to the OVIC website in the coming days and it will be discussed in more detail at the February VISA forum.



Introduction of the Incident Notification Scheme

Element 9.010

- VPDSS 2.0 introduced a new requirement under **Element 9.010** for information security incident notifications

Notification threshold

- Organisation's must notify OVIC of information security incidents that have an impact on the confidentiality, integrity or availability of public sector information with a business impact level (BIL) of **2 (limited) or higher**

How to notify OVIC of an information security incidents

- An **incident notification form** will be soon be published to the OVIC website.
- In the **interim**, refer to the **Incident Notification** page on the OVIC website which lists what to include in an email to OVIC. [Send to >](#)



Standard 9 – Information Security Reporting to OVIC			
Standard			
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).			
Statement of Objective			
To promote the organisation's security capability and ensure adequate tracking of its exposure to information security risks.			
Elements			
V2.0 #	V1.1 #	Element	Primary Source
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. ⁴	Victorian Protective Data Security Framework (VPDSF) V2.0 § Part 6



incidents@ovic.vic.gov.au

Refreshed online collaboration tool for the VISN – GovTEAMS!

OVIC

OVIC

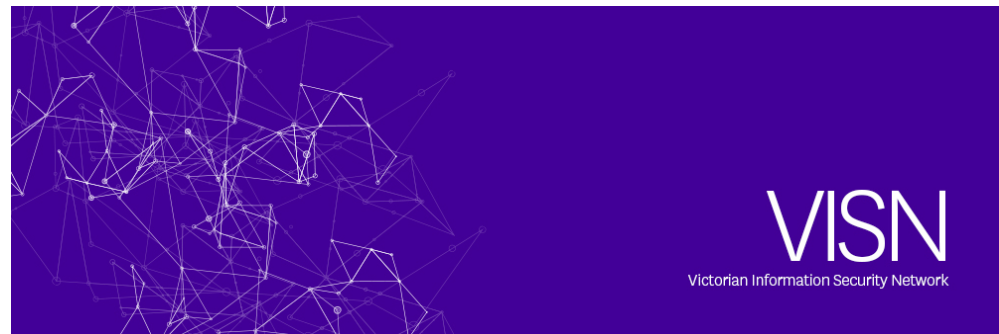
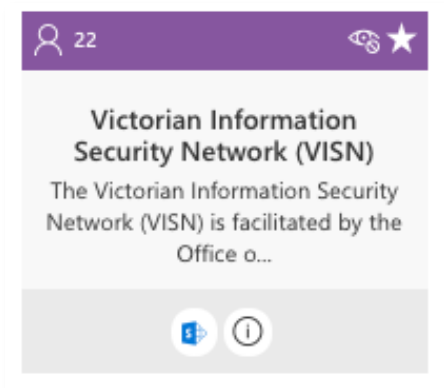
Office of the Victorian
Information Commissioner



What is GovTEAMS?

GovTEAMS is a digital platform that provides a space to collaborate and network.

OVIC uses GovTEAMS to host an online community supporting the Victorian Information Security Network (VISN).



GovTEAMS Membership

FORMER

Former *active* GovDEX members will automatically receive an email from the GovTEAMS, inviting them to join the new online VISN community.

Simply follow the instructions outlined in the email to create your account and join the community.

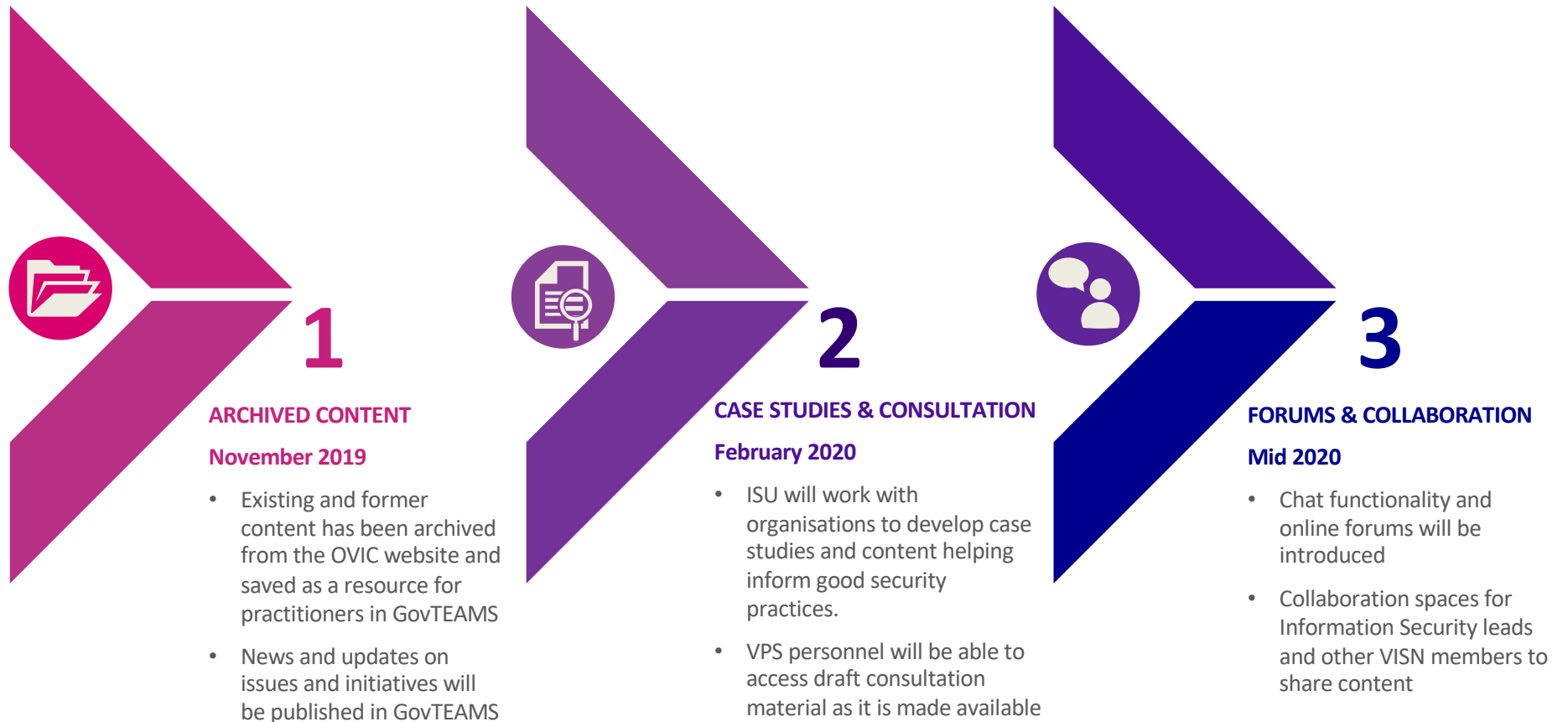
NEW

For those who:

- did not previously have an *active* GovDEX account, or
- those who are **new and looking to join the GovTEAMS community**, please email security@ovic.vic.gov.au with the following details:
 - Name
 - Job title
 - Organisation
 - Email address
 - Why they want to be a part of the online VISN community

The team will answer all requests with instructions on how to create an account and join the community. GovTEAMS members will also be added to the VISN mailing list.

GovTEAMS Release Schedule



Upcoming Engagements & Events

OVIC



Upcoming Engagements & Events

- **Communities of Practice (CoPs)**

Communities of Practice will commence in February 2020, with expressions of interest and invites to follow. The Information Security Unit's Business Engagement Officers (BEOs) are leading this piece of work.

Two initial CoP's will target:

- *Information Security Leads*
- *Private Industry Partners*

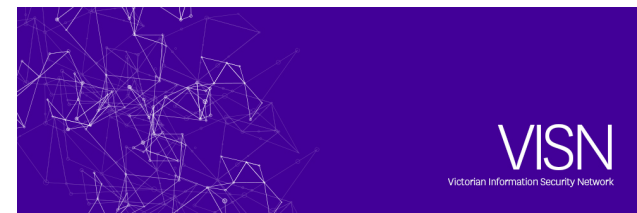


- **Next VISN Forum – 27 February, 2020**

This event will cover in more detail -

- Framework
- Assurance
- Reporting obligations
- Incident Notifications

This event will be held in Melbourne, with regional events to follow.

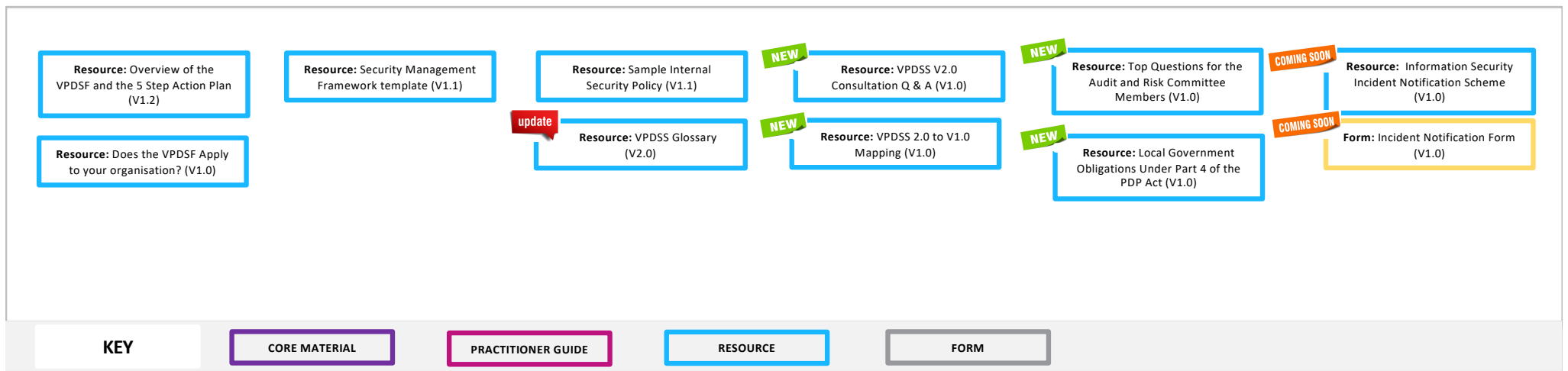
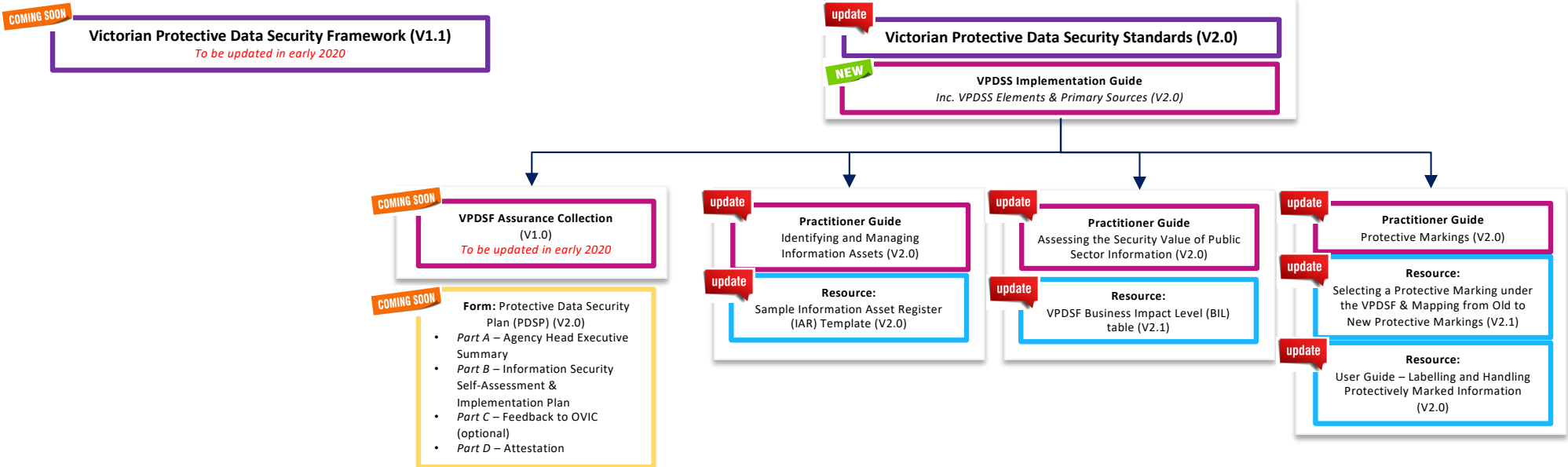


Document Map

OVIC

OVIC
Office of the Victorian
Information Commissioner





KEY

CORE MATERIAL

PRACTITIONER GUIDE

RESOURCE

FORM

Questions

*For those with questions regarding the launch of the VPDSS Version 2.0,
please email security@ovic.vic.gov.au*

OVIC



Office of the Victorian
Information Commissioner

