



Office of the Victorian
Information Commissioner

A background image showing a blurred crowd of people walking on a light-colored tiled floor. The image is split into two color zones: a light grey/white area on the left and a solid purple area on the right.

Information Security Briefing Pack

This briefing pack covers Parts 4 and 5 of the *Privacy and Data Protection Act 2014 (PDP Act)* and the agency and body obligations under these parts of the PDP Act only.

2021

Contents

- The Privacy and Data Protection Act 2014 (**PDP Act**)
 - What is public sector data?
 - Who does Part 4 and 5 of the PDP Act apply to?
- The Victorian Protective Data Security Standards (**VPDSS**)
 - Implementation of the VPDSS
 - Information Security Domains/Areas: A Holistic Approach
- The Victorian Protective Data Security Framework (**VPDSF**)
 - Reporting to OVIC
- Implementation Approach
 - Five Step Action Plan
- Roles and Responsibilities
- Where to start

The *Privacy and Data Protection Act 2014* (PDP Act)

Parts 4 and 5 of the PDP Act detail the information security requirements applicable to:

- Victorian government agencies and bodies (organisations) and
- their contracted service providers

Authorised Version No. 027
Privacy and Data Protection Act 2014
No. 60 of 2014
Authorised Version incorporating amendments as at
26 April 2021

Section	Page
Part 1—Preliminary	1
1 Purposes	1
2 Commencement	1
3 Definitions	2
4 Interpretation	12
5 Objects	13
6 Relationship of this Act to other laws	14
7 Rights and liabilities	14
8 Act binds the Crown	14
Part 1A—Functions, powers of Information Commissioner and appointment of Privacy and Data Protection Deputy Commissioner	15
Division 1—Performance of functions	15
8A Functions of Information Commissioner	15
8B Functions of Privacy and Data Protection Deputy Commissioner	16
8C Information privacy functions	17
8D Protective data security and law enforcement data security functions	19
8E Performance of concurrent functions	20
8F Information Commissioner may confer functions on Privacy and Data Protection Deputy Commissioner	20
8G General powers of Information Commissioner and Privacy and Data Protection Deputy Commissioner	22
Division 2—Privacy and Data Protection Deputy Commissioner	22
8H Appointment of Privacy and Data Protection Deputy Commissioner	22
8I Terms and conditions of appointment of Privacy and Data Protection Deputy Commissioner	23
8J Remuneration	23

Authorised by the Chief Parliamentary Counsel

Part 4

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

Part 4—Protective data security

Division 1—Application of Part

84 Application of Part

(1) Subject to subsection (2), this Part applies to—

(a) a public sector agency; and

(b) a body that is a special body, within the meaning of section 2 of the Public Administration Act 2004, and

(c) a body declared under subsection (2) to be a body to which this Part applies.

(2) This Part does not apply to the following—

(a) a Council;

(b) a university within the meaning of the Education and Training Reform Act 2006;

(c) a body to which, or to the governing body of which, the government or another jurisdiction, or a person appointed or body established under the law of another jurisdiction, has the right to appoint a member, irrespective of how that right arises;

(d) a public hospital within the meaning of the Health Services Act 1988;

(e) a public health service within the meaning of the Health Services Act 1988;

(f) a not-for-profit service within the meaning of the Health Services Act 1988;

(g) an ambulance service, within the meaning of the Ambulance Services Act 1986.

(3) The Governor in Council, may declare a body to be a body to which this Part applies.

Authorised by the Chief Parliamentary Counsel

Part 5

Privacy and Data Protection Act 2014
No. 60 of 2014
Part 5—Law enforcement data security

Part 5—Law enforcement data security

91 Application of Part

This Part applies to—

(a) Victoria Police; and

(b) the Chief Statistician; and

(c) an employee or consultant employed or engaged under section 10 of the Crime Statistics Act 2014.

92 Information Commissioner may issue law enforcement data security standards

(1) The Information Commissioner may issue standards for—

(a) the security and integrity of law enforcement data systems and crime statistics data systems; and

(b) access to, and release of, law enforcement data and crime statistics data, including, but not limited to, the release of law enforcement data and crime statistics data to members of the public.

(2) The Information Commissioner must consult with the Chief Commissioner of Police in developing law enforcement data security standards.

(3) The Information Commissioner must consult with the Chief Statistician in developing law enforcement data security standards in relation to crime statistics data and crime statistics data systems.

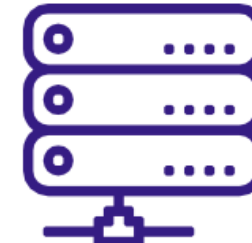
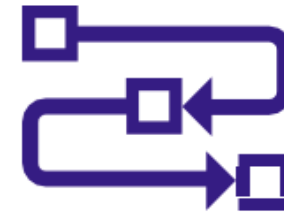
Authorised by the Chief Parliamentary Counsel

What is public sector data?

Public sector data is also referred to as **public sector information**.

This includes any information (including personal information) **obtained, generated, received** or **held** by or for a Victorian public sector organisation for an **official purpose** or supporting **official activities**.

It encompasses both **soft and hard** copy information, regardless of media or format, as well as **verbal** information.



Who does Part 4 and 5 of the PDP Act apply to?

Organisations covered by Part 4 and 5 of the PDP Act include:



A public sector
agency



A special body



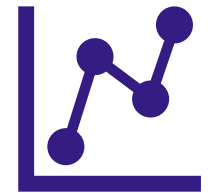
A body as
declared by the
Governor in
Council



Contracted
service providers
with direct and
indirect access to
public sector
information



Victoria Police



Chief Statistician
and personnel
engaged under
the *Crime
Statistics Act 2014*

The Victorian Protective Data Security Standards (VPDSS)

What are they and what do they do?

- **12 high-level mandatory requirements** to protect public sector information across all security domains/areas
- Consistent with national and international standards and describe the **Victorian Government's approach to protecting public sector information**
- Focus on the outcomes that are required to **enable efficient, effective and economic investment** in security measures through a risk-managed approach



Implementation of the VPDSS

To assist organisations’ adoption and implementation of the Standards, OVIC released **VPDSS Implementation Guidance** which sets out each of the **12 Standards** with a corresponding list of **Elements** (security measures).

Each **Element** is accompanied by **primary source** reference material that contains further detailed guidance on how to implement these measures.

Elements can assist organisations in protecting information assets based on the assessed security value and associated information security risks.



Standard 1 – Information Security Management Framework			Standard
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		Element	Primary Source
V2.0 #	Element		Primary Source
E1.010	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

Link to the VPDSS Implementation:
<https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-implementation-guidance/>

Information Security Domains/Areas: A Holistic Approach

The Standards cover all aspects of the business.



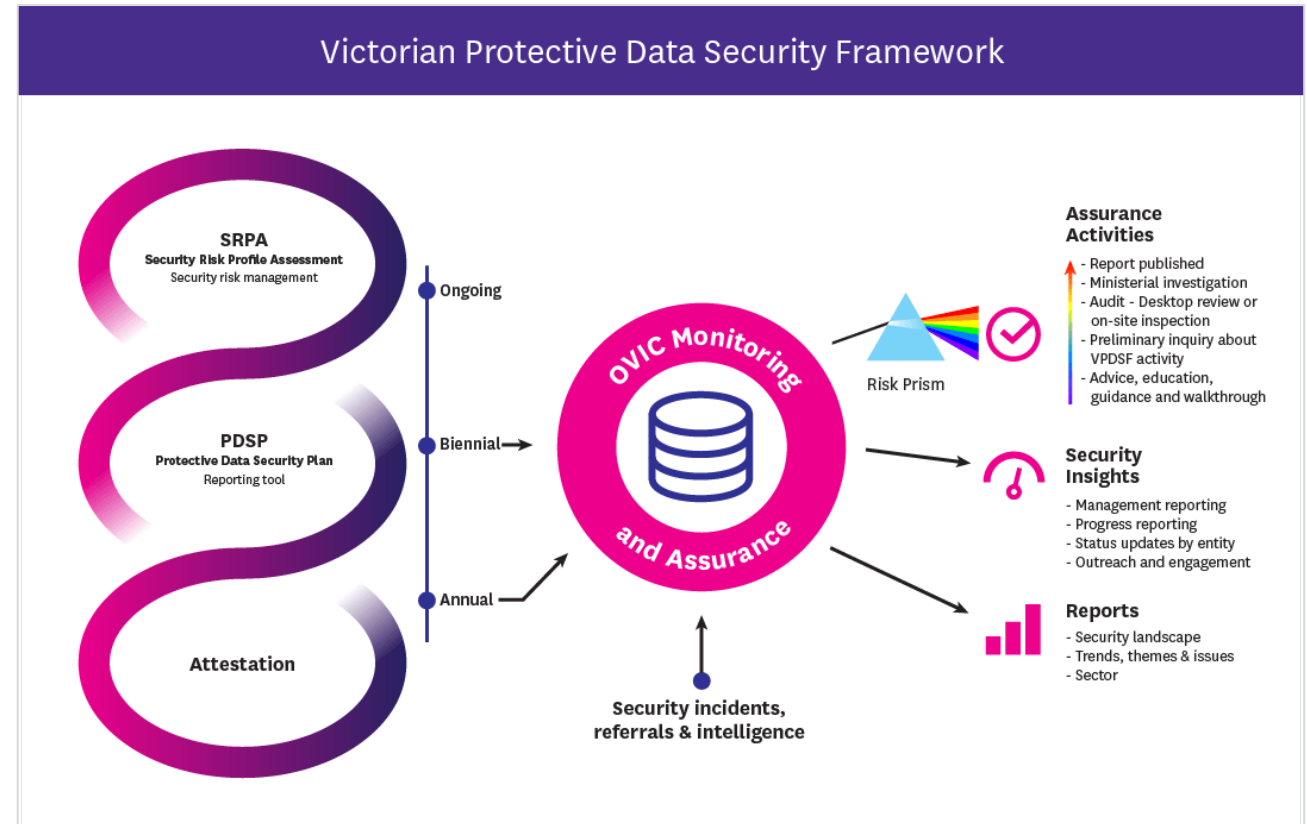
The Victorian Protective Data Security Framework (VPDSF)

What is the Framework?

Established under Part 4 of the PDP Act, the Framework has been developed to monitor and assure the security of public sector information and information systems across the VPS.

The monitoring and assurance activities outlined in the Framework are based on:

- the compliance requirements of VPS organisations; and
- OVIC's responsibilities, powers and functions.



Link to the VPDSF:

<https://ovic.vic.gov.au/data-protection/framework-vpdsf/>

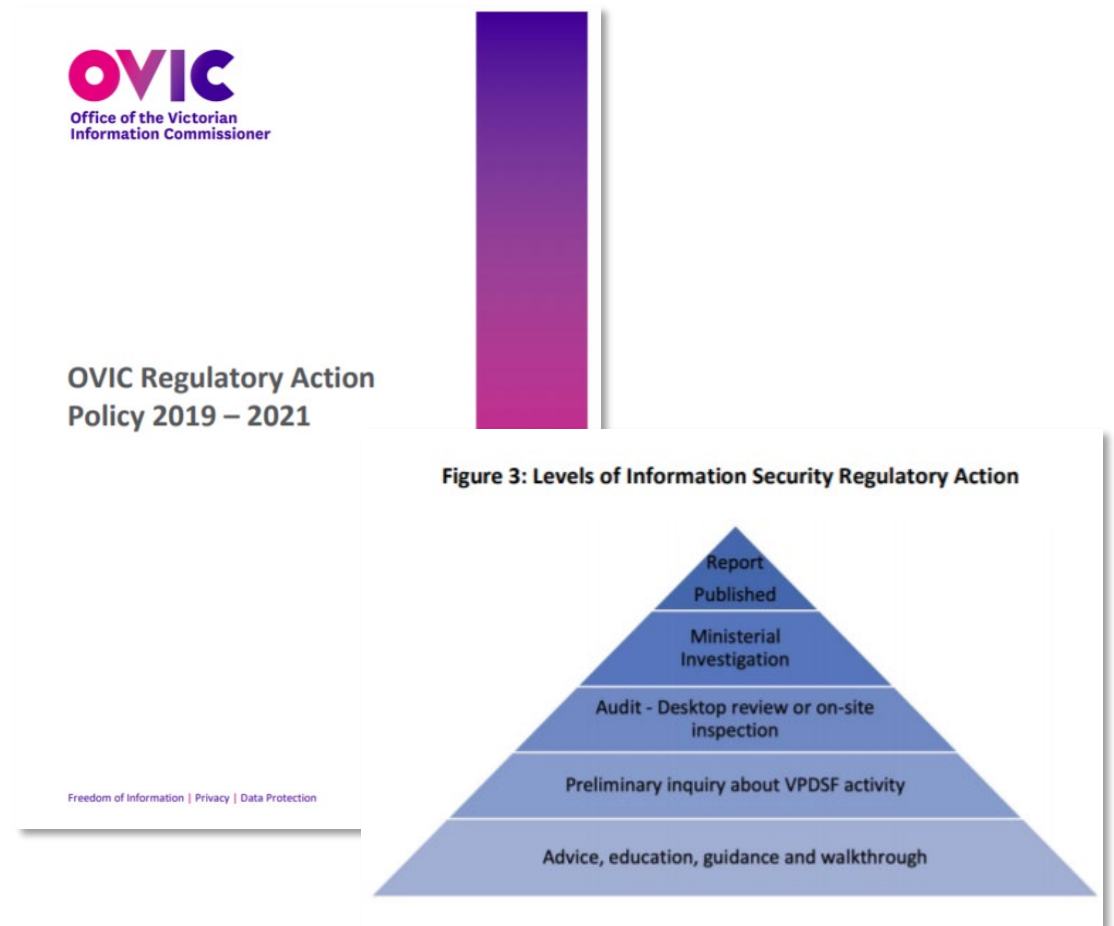
OVIC Regulatory Action Policy

What is the Regulatory Action Policy?

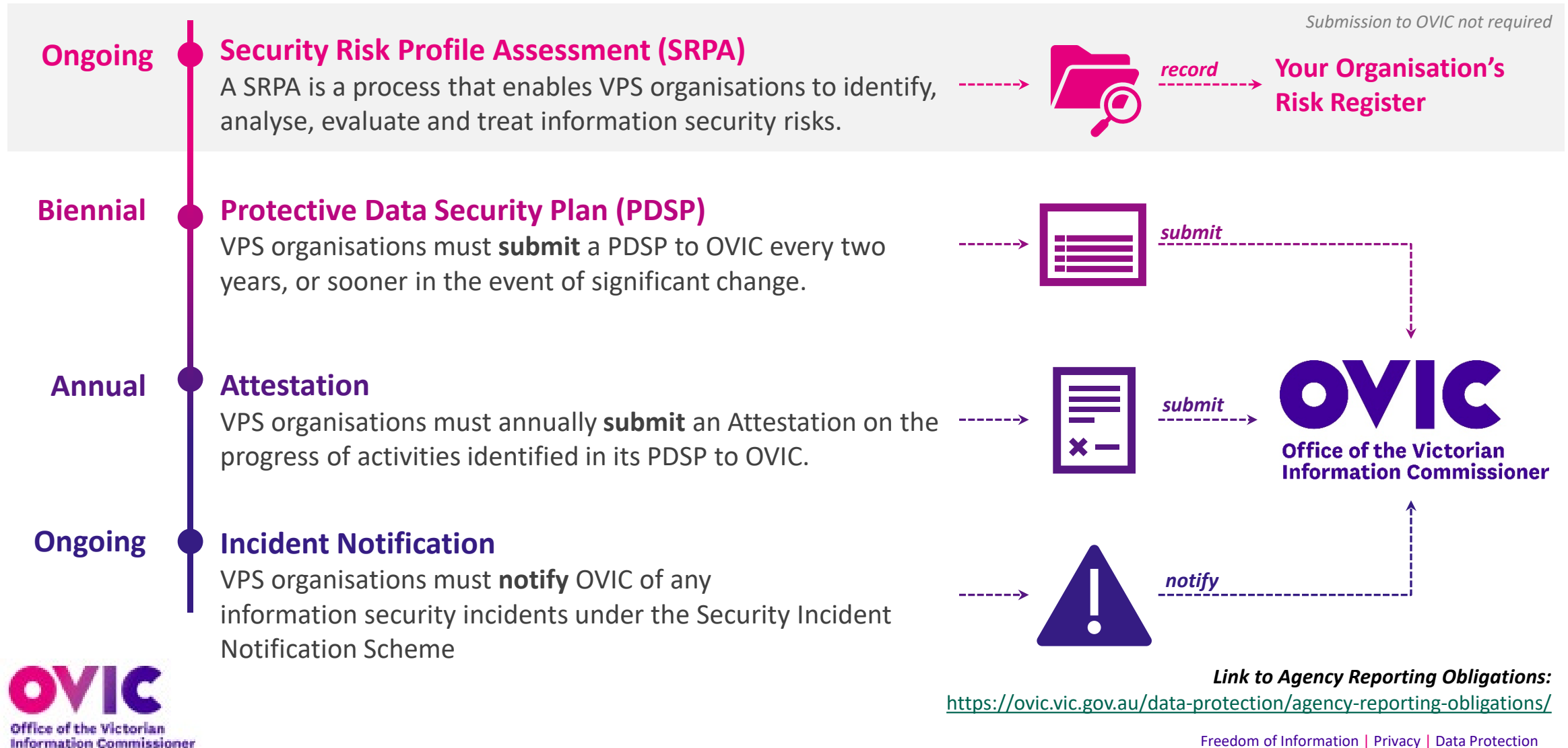
The Regulatory Action Policy explains how OVIC will use its powers.

Our goal is to continue to instill in the Victorian public sector a culture that promotes fair public access to information while ensuring its proper use and protection. By doing so, we aim to build community trust in government handling of information.

The regulatory action that OVIC can take includes informal preliminary enquiries and engagement, audits and examinations, investigations, compliance notices and associated penalties as well as public reports.



Key Activities and Reporting



Implementation Approach

Organisations need to consider what implementation approach will work best for their business.

1

Nominate an Executive Sponsor

An important first step includes the nomination of an **Executive Sponsor** who will champion the importance of information security throughout the business.

2

Establish an internal working group or body to coordinate efforts

To help focus efforts within the organisation, the Executive Sponsor may consider establishing an **internal working group** to help coordinate efforts in implementing the VPDSS. This group should **include representatives** from **all areas of the business**. This includes:

- Governance areas;
- Legal;
- People and Culture;
- Facilities;
- Information/Records Management;
- ICT;
- Finance;
- Risk/Internal Audit.

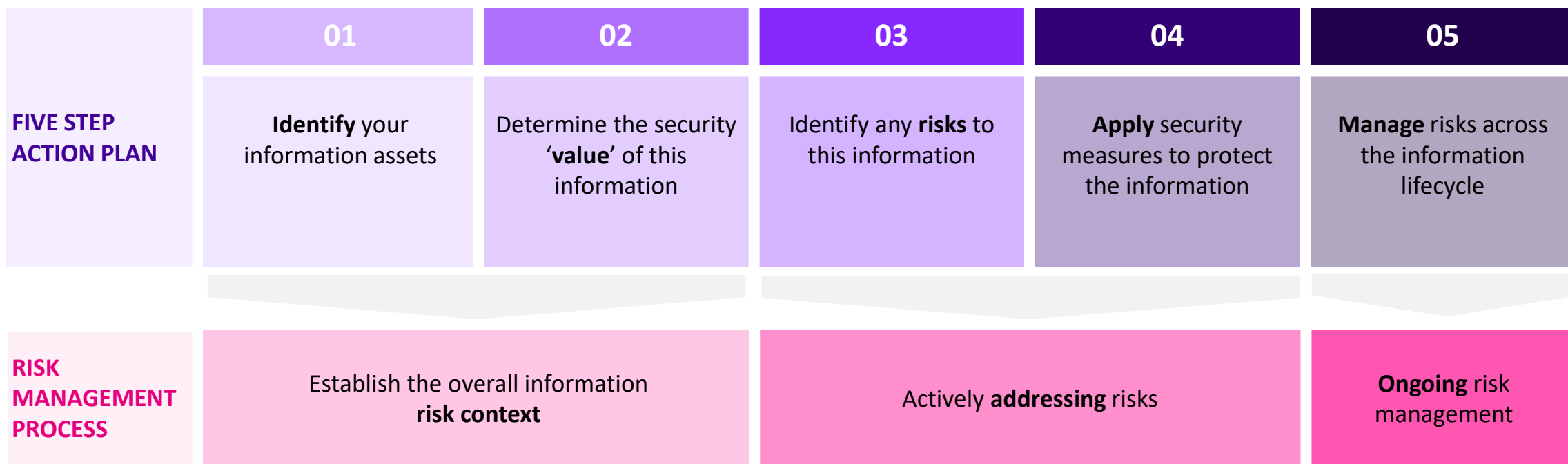
3

Confirm your organisation's Information Security Lead

While accountability for adhering to the VPDSS rests with the public sector body Head, they need to be supported by personnel who are appropriately skilled, resourced and empowered.

Your **information security lead** acts as a central point of contact for OVIC, helping deliver important information security messages and updates relating to the Framework and Standards.

Five Step Action Plan and Risk Management



Roles and Responsibilities



Public Sector Body Head

Under Part 4 of the PDP Act, public sector body Heads are ultimately accountable for the adherence to the VPDSS, and monitoring and assurance activities of their VPS organisation.

The public sector body Head is also required to seek their own form of assurance from any Contracted Service Provider/third party with access to the VPS organisation's public sector information and information systems.



Information Security Lead (ISL)

Each public sector body Head must nominate an information security lead for their organisation.

An organisation must notify OVIC of any changes to the lead, providing an alternative point of contact if they move roles or cease working for the organisation.

An ISL will:

- Act as a central point of contact for OVIC;
- Deliver important information security messages and updates relating to the Framework and Standards;
- Help coordinate or guide the implementation of the Standards on behalf of the organisation.

Where to start:



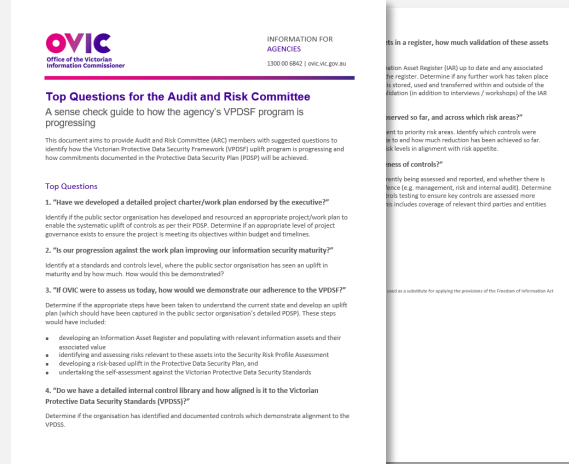
The Five Step Action Plan



The Five Step Action Plan outlines practical activities designed to assist organisations in managing information security risks.



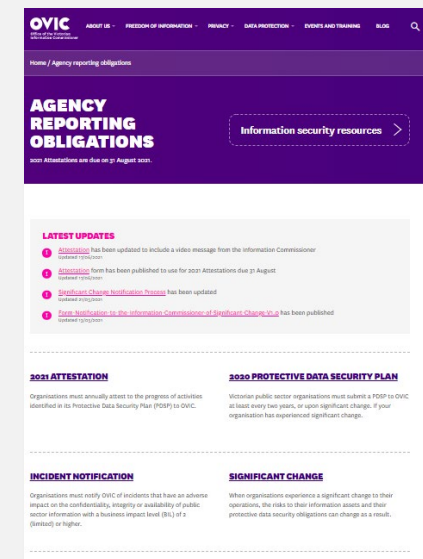
Top Questions for the Audit and Risk Committee



This info sheet provides suggested questions to pose to an Audit and Risk Committee to identify how an organisation's information security program is progressing.




Agency Reporting Obligations




Find out your agency's reporting obligations by visiting OVIC's Agency Reporting Obligations page.

OVIC Information Security Video Series


Watch and share these videos to educate staff on information security matters and the importance of protecting public sector information.



Watch this video to find out more about how information security safeguards public sector information.



Watch this video to find out more about the VPDSS.



Watch this video to find out which organisations Parts 4 and 5 apply to.



Information security is everyone's responsibility. Watch this video to find out how you can play your part in protecting public sector information.



**Contact the Information Security Unit
for additional support and guidance.**

security@ovic.vic.gov.au