Office of the Victorian Information Commissioner

Information Security

The Five Step Action Plan

Victorian Protective Data Security Framework

Version Information

Version	Publish Date	Amendments in this version
1.0	18 December 2017	NA
1.1	19 February 2018	New formatting and design for OVIC branding
1.2	31 October 2018	Website links fixed
2.0	July 2020	Amended content throughout, referencing major changes to the Framework V2.0 and the Standards V2.0

1. Background

The secure management of information is critical to Government service delivery, public trust, and confidence. In 2014, the *Privacy and Data Protection Act* (**PDP Act**) was passed by the Parliament, ushering in Australia's first broad-based legislated information security requirements.

The PDP Act significantly changed the information security regulatory landscape, empowering the Victorian Information Commissioner to:

- develop the Victorian Protective Data Security Framework (the **Framework**) for monitoring and assuring public sector data security; and
- issue the Victorian Protective Data Security Standards (the **Standards**).

The Framework and Standards have been developed to help Victorian public-sector organisations:

- identify information assets,
- assess the value of information,
- identify and manage information security risks,
- apply security measures,
- create a positive security culture, and
- mature their information security capability.

To assist organisations in meeting the requirements of the Framework and Standards, OVIC has developed a five-step action plan that sets out practical activities designed to assist in managing information security risks.

2. Purpose

This document provides an overview of the Five-Step Action Plan and explains its relationship to the Framework and Standards.

3. Audience

This document is intended for VPS organisations (including employees, contractors, and external parties) that are subject to the protective data security provisions under Part 4 of Victoria's PDP Act. This document is primarily written to inform executives and designed to support information security practitioners.

4. What is the Five-Step Action Plan?

The Five-Step Action Plan presents a risk-based approach to securing information assets in a logical and staged manner, whilst meeting the requirements of the Framework and Standards.
Some organisations will have existing business practices or programs of work that complement the activities set out in the Five-Step Action Plan.

Five Step Action Plan				
01	02	03	04	05
Identify your information assets	Determine the **'value'** of this information	Identify any **risks** to this information	**Apply** security measures to protect the information	**Manage** risks across the information lifecycle

Step 1:

Identify the organisation's information assets

An essential first step in establishing an information security program, is identifying the organisation's information assets. Simply put: you cannot protect what you do not know.

Step one helps prompts an organisation to:

- conduct an information review, where they survey of their information holdings to discover all their information assets; and
- establish an Information Asset Register (**IAR**) where information assets can be centrally recorded and managed.

Organisations who complete this step will have a central record of the organisation's information assets that not only promotes good but also acts as an essential input in any future risk assessments.

Deliverables from Step One	Resources and templates available from OVIC website
Conduct an information review	Practitioner Guide: Identifying and Managing Information Assets (V2.0)
Establish an IAR	A sample IAR Template (available in excel format)

Step 2:

Determine the security value of information assets

Business Impact Levels (**BIL**) are a common assessment tool used by VPS organisations to determine the security value of public sector information. BILs also inform the protective marking needed for certain types of public sector information.

Assessing information in a standardised manner means VPS organisations can collaboratively articulate and manage information security risks.

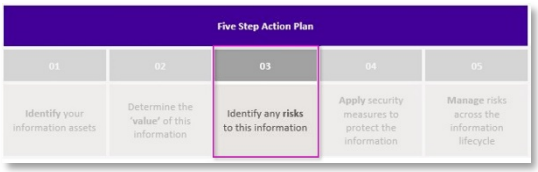
The standardised BIL assessment process also promotes secure information sharing, using commonly understood security terms and offering a basis for informed discussions about the most appropriate security measures needed to protect public sector information.

Step Two prompts an organisation to:

- use the BILs to assess potential compromise of the:
    - Confidentiality,
    - Integrity; and
    - Availability

  of public sector information; and
- record the outcomes of the BILs assessment in an IAR.

Deliverables from Step Two	Resources and templates available from OVIC website
Contextualise the VPDSF BILs to reflect your organisation Conduct a security value assessment of your information assets, using the BILs	Practitioner Guide: Assessing the security value of public sector information (V2.0) VPDSF Business Impact Level (BIL) table (V2.1) Protective Marking Flowchart (ready reckoner)
Record the outcome of these security value assessments in your organisation's IAR	A sample IAR Template (available in excel format) *The security value assessment will help determine which the BILs for the information and the appropriate protective marking for the information. You will need this information for your IAR.* For more information on protective markings, refer to Practitioner Guide: Protective Markings (V2.0)



Step 3:

Assess any risks to the information assets

Organisations need to actively manage security risks to their information assets. To do so, regular information security risk assessments need to be performed, assessing:

- information security,
- physical security,
- personnel security; and
- information technology risks

as it relates to information assets. This process is referred to as a Security Risk Profile Assessment[1] (**SRPA**).

Step three prompts organisations to:

- identify, analyse, and evaluate security risks related to their information assets, utilising the organisations risk management framework; and
- regularly review and update organisational risk registers, reflecting any new or changed information security risks.

Organisations who complete this step satisfy the requirement to undertake a SRPA under Part 4 of the PDP Act, and complete the foundational work needed to develop a Protective Data Security Plan (**PDSP**).

Deliverables from Step Three	Resources and templates available from OVIC website
Review your organisation's risk register to ensure it captures current information security risks	Practitioner Guide: Information Security Risk Management (V2.0)
Ensure the organisation's risk register is reviewed at regular intervals (at least annually) and updated as required	A generic risk register template is available on the VMIA website for organisations that do not have their own

[1] A SRPA is defined as a process that organisations undertake to assess and manage information security risks. Undertaking a SRPA is also a legislative requirement under s89(1a) of the PDP Act.

Step 4:

Apply security measures to protect the information assets

The risk-based nature of the Framework and Standards provides organisations with flexibility and autonomy to interpret their business needs and based on their risk appetite.

OVIC does not prescribe what specific security measures organisations are to apply but do es provide a holistic list of security outcomes (VPDSS Elements[2]) for organisations to consider. The VPDSS Elements unpack the operational intent of each standard and should be referenced by organisations when defining their own internal control library and planning information security programs.

Step Four prompts organisations to:

- document their own internal control library (based on the VPDSS elements, and the organisations unique operating requirements); and
- develop a PDSP.

The PDSP acts as a roadmap for how the organisation addresses information security risks and supports the implementation of the Standards. The PDSP is directly informed by the treatment of risks assessed, and gaps in the implementation of the Standards.

Deliverables from Step Four	Resources and templates available from OVIC website
The organisation documents its internal control library that addresses its information security risks	Practitioner Guide: Information Security Risk Management The VPDSS Elements can be found in the Victorian Protective Data Security Standards V2.0 – Implementation Guide
The organisation develops a current PDSP	A copy of the PDSP template (single organisation)

[2] An element is security measure that modifies risk. Elements often depend on a supportive control environment to be effective. To access a current copy of the VPDSS Elements, refer to the "Victorian Protective Data Security Standards V2.0 – Implementation Guide".

Step 5:

Manage information security risks across the information lifecycle

Continuous improvement is a core principle of the Framework and Standards. This quality-driven philosophy is designed to integrate information security into an organisation's existing business practices (like risk management, information management, personnel management, ICT management, and facilities, services, and equipment management).

Step Five prompts organisations to:

- continually assess the security value of their information assets, helping identify and manage any changes,
- consider updates to the organisation's IAR as attributes (BILs, roles and responsibilities, etc.) relating to information assets change,
- notify OVIC of information security incidents[3],
- update risk registers to reflect any changed or new risks,
- systematically and formally identify opportunities to mature information security practices, and
- update information security programs ensuring any changes are reflected in their PDSP.

Deliverables from Step Five	Resources and templates available from OVIC website
Continually consider the security value of information assets	Practitioner Guide: Assessing the security value of public sector information (V2.0)
Update the organisation's IAR	Practitioner Guide: Identifying and Managing Information Assets (V2.0)
Notify OVIC of any Information Security Incidents	Information Security Incident Notification Scheme
Update risk registers	Practitioner Guide: Information Security Risk Management
Updates the PDSP as required	PDSP template (single organisation)

[3] For more information on the Information Security Incident Notification Scheme, refer to the Incident Notification page on the OVIC website: https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/

5. Further resources

To find out more about the Framework and Standards, refer to the VPDSF Resources page on the OVIC website.

6. Contact Details

Office of the Victorian Information Commissioner

Freedom of Information | Privacy | Data Protection

Email: security@ovic.vic.gov.au

Website: ovic.vic.gov.au

PO Box 24274 Melbourne VIC 3001