Office of the Victorian
Information Commissioner

Victorian Protective Data Security Framework

Version 2.0 February 2020

Published by the Office of the Victorian Information Commissioner
PO Box 24274
Melbourne Victoria 3001
First published June 2016
Amended February 2020
Also published on: https://ovic.vic.gov.au
ISBN 978-0-6486723-6-4

Document Details

Victorian Protective Data Security Framework	
Protective Marking	N/A
Approved for unlimited public release	*Yes – Authorised for release*
Release Date	February 2020
Review Date	February 2021
Document Version	2.0
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit – OVIC

For further information, please contact the Information Security Unit on security@ovic.vic.gov.au

Change log

Version	Publish Date	Amendments in this version
1.0	June 2016	N/A
1.1	March 2018	• Change references of 'Commissioner for Privacy and Data Protection' to 'Office of the Victorian Information Commissioner' • Change references of 'CPDP' to 'OVIC' • Change references of 'PDPA' to 'PDP Act' • Replace 'Foreword' with new Deputy Commissioner's foreword • Insert new section on Victoria Police and the Crime Statistics Agency • Removed reference to annual security attestation in section 12 • Change 'protocol' descriptor • Insert reference to 'elements' • Insert reference to Part 5 – Assurance Model in section 17 for more information • Insert reference to Enterprise Solutions Branch in Section 19 • Remove 'sensitive and significant (valuable)' in section 20 • Updates to some control references • Change Part 5 – Assurance Model – various including revised reporting obligations • Insert new section on single/multiple organisation reporting • Insert new section on the 5-step action plan
2.0	February 2020	Content amended to reflect the monitoring and assurance activities of VPS organisations and OVIC. Relevant content from V1.0 of the Framework is available under the VPDSF Resources section of the OVIC website.

Table of Contents

Part One – Introduction to the Framework

Part Two – Monitoring and Assurance by VPS organisations

Part Three – OVIC Monitoring and Assurance

Commissioner's foreword

The Victorian Protective Data Security Framework (the **Framework**) and accompanying Victorian Protective Data Security Standards (the **Standards**) were released and issued to Victorian Public Sector (**VPS**) agencies and bodies (**VPS organisations**) in 2016. Adherence to the Standards is mandatory for all organisations within the scope of Parts 4 and 5 of the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**).

In 2018, VPS organisations submitted their first Protective Data Security Plans and Attestations to my office. These plans provide important insights into the information security practices of the VPS and describe future work programs to enhance efforts in protecting public sector information.

The VPS operates in an increasingly interconnected and complex world, facing new risks and managing competing priorities. The threat landscape in which the Framework was initially released, and the Standards were first issued, continues to evolve. Given this context, OVIC commissioned an external review of the Framework and Standards in 2017, to assess their effectiveness and identify areas for improvement.

This review found that the Framework and Standards had an overwhelming positive impact for Victorian government, and that the attestation process substantially contributed to executive awareness of information security. These were both welcome findings. It also identified opportunities for improvement by recommending:

- simplification of communications surrounding the Framework and Standards;
- clarification of roles and responsibilities as they relate to information security; and
- enhancement of guidance material to accommodate the varying size and diverse nature of the VPS organisations operating under the scheme.

With these improvements in mind, OVIC's Information Security team sought input from a wide variety of stakeholders before and during the drafting of the revised Standards, resulting in a streamlined and easier-to-understand set of requirements. The revised Standards were agreed to by the Special Minister of State, The Honourable Gavin Jennings MLC in October 2019 and have been issued in accordance with my powers under the PDP Act. The latest version of the Standards contains references to supporting material to help VPS organisations map their existing security efforts to the updated requirements, as well as providing the basis for these information security obligations.

In addition, the Framework has been updated to address the recommendations from the Review.

I encourage VPS organisations to continue to build resilient business practices, supported by a strong information security culture. By doing so, we help build public trust and ensure a solid future for all Victorians. OVIC will continue to develop support for VPS organisations by developing resources to assist in implementing the Standards. My office looks forward to working with the VPS to deliver efficient, effective and secure outcomes for all.

Sven Bluemmel
Information Commissioner
February 2020

Part One

Introduction to the Framework

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.

1. Commencement of the PDP Act

In 2014, the 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[1] the Victorian Information Commissioner to:

- develop the Framework for monitoring and assuring public sector data security; and
- issue the Standards[2].

2. What is protective data security?

Protective data security is a risk management process designed to safeguard information assets and systems in a way that is proportionate to threats and supportive of business outcomes.

A combination of procedural, information, personnel, information communications technology and physical security measures are used to protect information assets against a range of security threats.

The Framework and the Standards rely on protective data security principles, to maintain the confidentiality, integrity and availability of public sector information.

In this document, protective data security and information security are used interchangeably.

3. 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[3] of VPS organisations; and
- OVIC's responsibilities, powers and functions[4].

[1] Commissioners functions set out under Part 6 – Division 2, s 103(2) of the PDP Act

[2] For a current copy of the Standards, or VPDSS Implementation Guide, refer to the VPDSF resources section of the OVIC website.

[3] Part 4S, Section 88 and Section 89, of the PDP Act

[4] Commissioners functions set out under Part 6 – Division 2, s 103(2) of the PDP Act

The Framework provides a model to monitor and measure the extent to which VPS organisations implement the Standards and comply with the requirements under the PDP Act. It employs a risk-based approach, seeking to enhance information security capability and maturity of VPS organisations, through the use of existing risk management principles and guidelines.

The Framework is based on an outcome focused regulatory model that concentrates on high-level assurance principles, supported by risk-informed monitoring activities. It is intended to reflect the sector's unique operating requirements and delivers scalable, efficient, effective and economic security outcomes.

The monitoring and assurance activities set out in the Framework are formulated from statutory obligations of VPS organisations[5] and OVIC's statutory responsibilities, powers and functions[6] in the PDP Act. They are designed to assist VPS organisations mitigate information security risks and provides OVIC with insight into information security practices across the VPS.

The Framework draws on intelligence feeds and insights from information security incidents, research projects, enquiries and referrals. OVIC uses these insights to report back to Government.

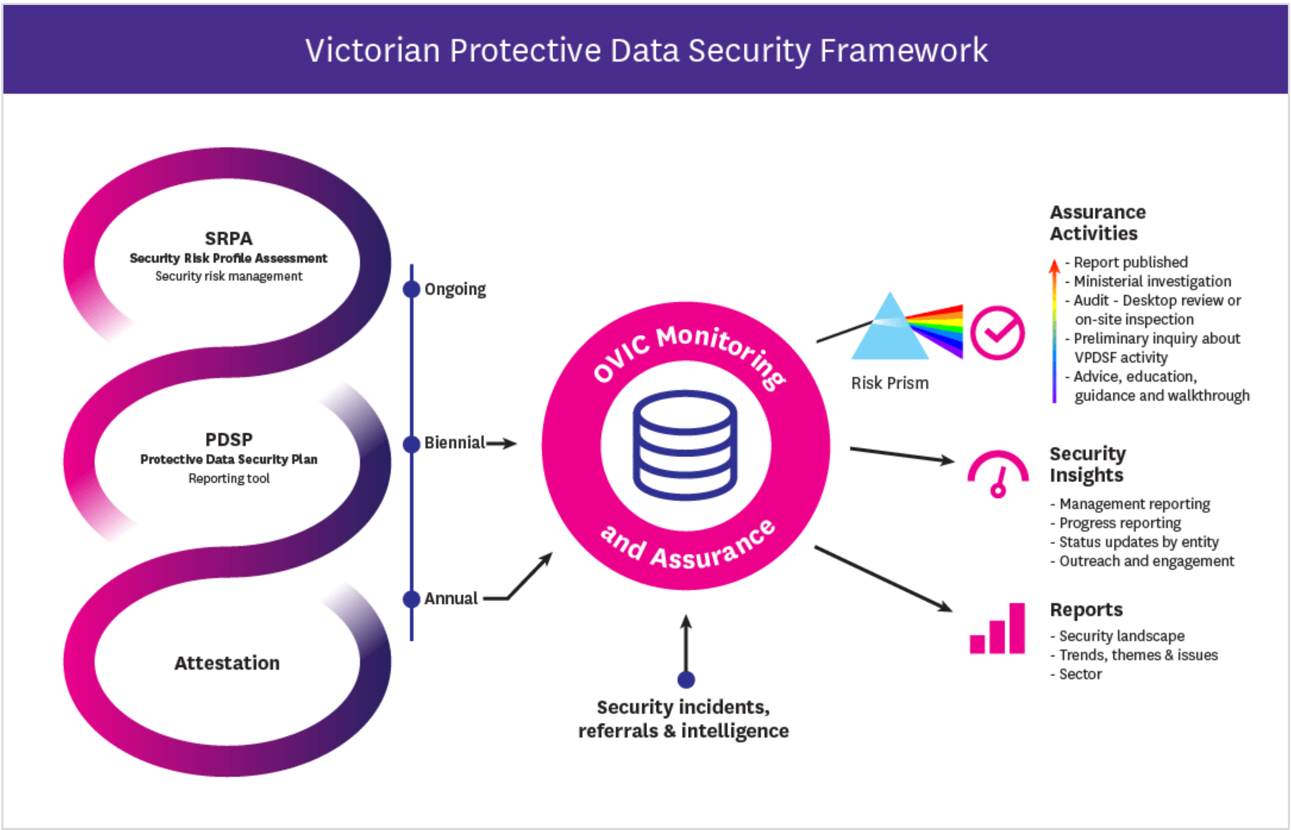
Victorian Protective Data Security Framework
SRPA
Security Risk Profile Assessment
Security risk management
PDSP
Protective Data Security Plan
Reporting tool
Attestation
Ongoing
Biennial
Annual
OVIC Monitoring and Assurance
Security incidents, referrals & intelligence
Risk Prism
Assurance Activities
- Report published
- Ministerial investigation
- Audit - Desktop review or on-site inspection
- Preliminary inquiry about VPDSF activity
- Advice, education, guidance and walkthrough
Security Insights
- Management reporting
- Progress reporting
- Status updates by entity
- Outreach and engagement
Reports
- Security landscape
- Trends, themes & issues
- Sector

Figure 1 - Depiction of the monitoring and assurance activities of the Framework

[5] Part 4, Section 88 and Section 89, of the PDP Act.
[6] Commissioners functions set out under Part 6 – Division 2, s 103(2) of the PDP Act.

4. Applicability of the Framework

4.1. Information covered by the Framework

The Framework captures ‘public sector data’ which is broadly defined by section 3 of the PDP Act as:

> *any information (including personal information) obtained, received or held by an agency or body which Part 4 applies, whether or not the agency or body obtained, received or holds that information in connection with the functions of that agency or body*[7]*.*

The definition of public sector data is broad, as it includes:

- any information received by or on behalf of the VPS organisation, not just information connected to their functions;
- information collected or held by contracted service providers of the VPS organisation such as contractors and consultants; and
- health information.

In this document, public sector data is also referred to as public sector information or information.

4.2. VPS Organisations covered by the Framework (Part 4 of the PDP Act)

Section 84 of the PDP Act defines the VPS organisations that are covered by the Framework and the Standards as well as those that are exempt.

The Framework regulates Victorian public sector agencies and bodies defined in section 84 of the PDP Act. This includes including departments, public entities[8] and Victoria Police and the Crime Statistics Agency.[9] The Framework generally excludes[10] councils, universities, ambulance services, public hospitals, public health services and multipurpose services under the *Health Services Act 1988* (Vic).

Extract of Part 4, Section 84, PDP Act	
(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 6 of the *Public Administration Act 2004*; and (c) a body declared under subsection (3) to be a body to which this Part applies.
(2)	This Part does not apply to the following – (a) a Council;

[7] Part 1, Section 3 of the PDP Act

[8] Defined In section 5 of the Public Administration Act 2004 (Vic).

[9] Part 5 of the PDP Act specifically regulates information security of Victoria Police and the Crime Statistics Agency. Nevertheless, in 2017, the Victorian Information Commissioner transitioned Victoria Police and the Crime Statistics Agency to the Framework and Standards under Part 4 of the PDP Act.

[10] While Section 84 (2) provides exemptions from Part 4 of the PDP Act, for particular VPS organisations, these exemptions need to be applied with care. If exempt entities are performing a public function on behalf of a regulated VPS organisation, they may have obligations under the PDP Act. For further clarification refer to VPDSF resources section of the OVIC website, and resource ‘*Does the VPDSF apply to your organisation*?’

Extract of Part 4, Section 84, PDP Act	
	(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 of 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 multi-purpose 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, by Order published in the Government Gazette, may declare a body to be a body to which this Part applies.

For more information on whether the Framework and Standards apply to your VPS organisation, refer to the VPDSF resources section of the OVIC website.

4.3. Victoria Police and Crime Statistics Agency (Part 5 of the PDP Act)

Part 5 of the PDP Act describes the information security responsibilities of Victoria Police and the Crime Statistics Agency.

From 2017, Victoria Police and the Crime Statistics Agency are covered by the Framework and Standards, in line with other VPS organisations to which Part 4 of the PDP Act applies.

4.4. Contracted Service Providers / Third Parties

Part 4 of the PDP Act applies to all staff, contractors and consultants of VPS organisations identified in Section 84(1) of the PDP Act.

Section 88 (2) of the PDP Act extends the information security obligations of VPS organisations to contracted service providers (**CSPs**), which states:

> *A public sector body Head for an agency or a body to which this Part applies must ensure that a contracted service provider of the agency or bod does not do an act or engage in a practice that contravenes a protective data security standard, in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider for the agency or body.*

VPS organisations must include assessments of CSPs in their Security Risk Profile Assessment (**SRPA**) process[11].

[11] See section 9.1 of this document for more information and refer to Practitioner Guides: Information Security Risk Management available under the VPDSF resources section of the OVIC website

5. The Framework in context

The Framework has been developed to monitor and assure the security of public sector information12.

To do this, OVIC's monitors and measures VPS organisations':

- implementation of the Standards; and
- compliance with the PDP Act.

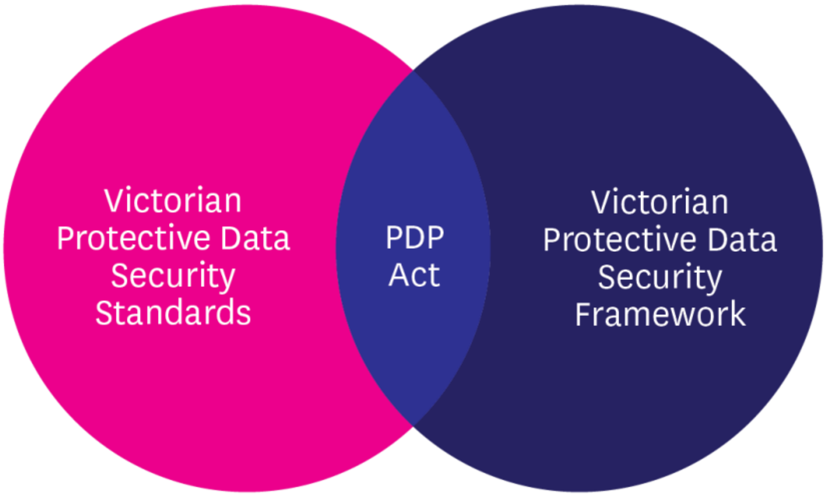
Victorian Protective Data Security Standards
PDP Act
Victorian Protective Data Security Framework

Figure 2 – Visual representation of the interlinked nature of the PDP Act, Standards and Framework

The monitoring and assurance activities outlined in this Framework are complemented by the regulatory actions outlined in OVIC's *Regulatory Action Policy*, available on the OVIC website.

5.1. How the Framework interacts with other legal obligations

VPS organisations have a variety of legal, regulatory and administrative obligations governing the access, use, security and preservation of their information. As such, VPS organisations should read the Framework and accompanying Standards in conjunction with existing requirements and consider how these may intersect with obligations under Part 4 of the PDP Act.

Where relevant legislation mandates lower requirements than those of the Framework or Standards, VPS organisations are encouraged to meet the highest applicable standard.

Where VPS organisations handle information of "national interest", the Commonwealth Protective Security Policy Framework (**PSPF**) requirements remain mandatory.

To access a current copy of the Standards and guidance material, refer to the VPDSF resources section of the OVIC website.

6. Roles, responsibilities and relationships

The Victorian Public Sector is made up of a diverse range of VPS organisations, each delivering specific services or functions. Due to the distinct nature of these services and functions, different VPS organisations face different threats to their information assets and information systems. The Framework recognises that these threats cannot be entirely eliminated and that VPS organisations have operational responsibilities

[12] Part 4 s85 (1) of the PDP Act

and finite resources to draw on. The Framework assists VPS organisations mitigate information security risks as much as possible by using risk management principles and guidelines.

Given this complex operational landscape, coupled with the varied nature of the threats facing VPS organisations, it is essential that all parties work together to foster a strong information security culture based on robust information security work practices. By building these relationships, we can establish governance arrangements that support the protection of public sector information.

In support of these efforts and to illustrate these connections, the following section describes the roles and responsibilities of:

- OVIC;
- VPS organisations[13]; and
- partnering entities.

6.1. Office of the Victorian Information Commissioner

Part 6 of the PDP Act details the functions and powers of OVIC as they relate to the monitoring and assurance activities for the security of public sector information. These functions and powers include:

- developing a protective data security framework for monitoring and assuring the security of public sector information;
- promoting responsible information security practices in the public sector;
- conducting monitoring and assurance activities, including audits, to ascertain compliance with information security standards;
- formal reporting and recommendations regarding information security;
- referring findings of monitoring and assurance activities, including audits, to an appropriate person or body for further action;
- undertaking research relevant to information security in the VPS; and
- retaining copies of protective data security plans.

These functions and powers enable OVIC to provide reasonable assurance to Government that VPS organisations' information security risks are being managed effectively, whilst still providing them the autonomy to determine how to achieve their business objectives in an efficient, effective and economic manner.

6.2. VPS organisations

When implementing the Standards and performing assurance activities in accordance with the Framework, VPS organisations should remain mindful of the broader context in which they operate, and how these requirements intersect with their obligations under Part 4 of the PDP Act.

All VPS organisations identified in section 84 of the PDP Act must monitor their information security practices and provide assurance around the measures they take to protect public sector information.

Under the PDP Act, VPS organisations are specifically required to:

- adhere to the Standards;
- undertake a SRPA;
- develop, implement and maintain a Protective Data Security Plan (**PDSP**);

[13] Agencies and bodies identified in Part 4 (s84) of the PDP Act

- provide OVIC free and full access to public sector information or information systems, when requested, including participating in any monitoring and assurance activities conducted by OVIC[14]; and
- ensure that a CSP of a VPS organisation, does not do an act or engage in a practice that contravenes the Standards, regarding public sector information collected, held, used, managed, disclosed or transferred by the provider for the VPS organisation.
- Further, the Standards require VPS organisations to:
- provide an annual attestation to OVIC; and
- notify OVIC of information security incidents[15].

6.3. Partnering entities that also have a role to play in information security

OVIC's information security efforts are supported by a range of partnering entities. A brief outline of these entities is depicted below.

For more information on the relationship between these entities and the Framework and Standards, refer to the Info Sheet *Partnering Entities*[16] refer to the VPDSF resources section of the OVIC website.

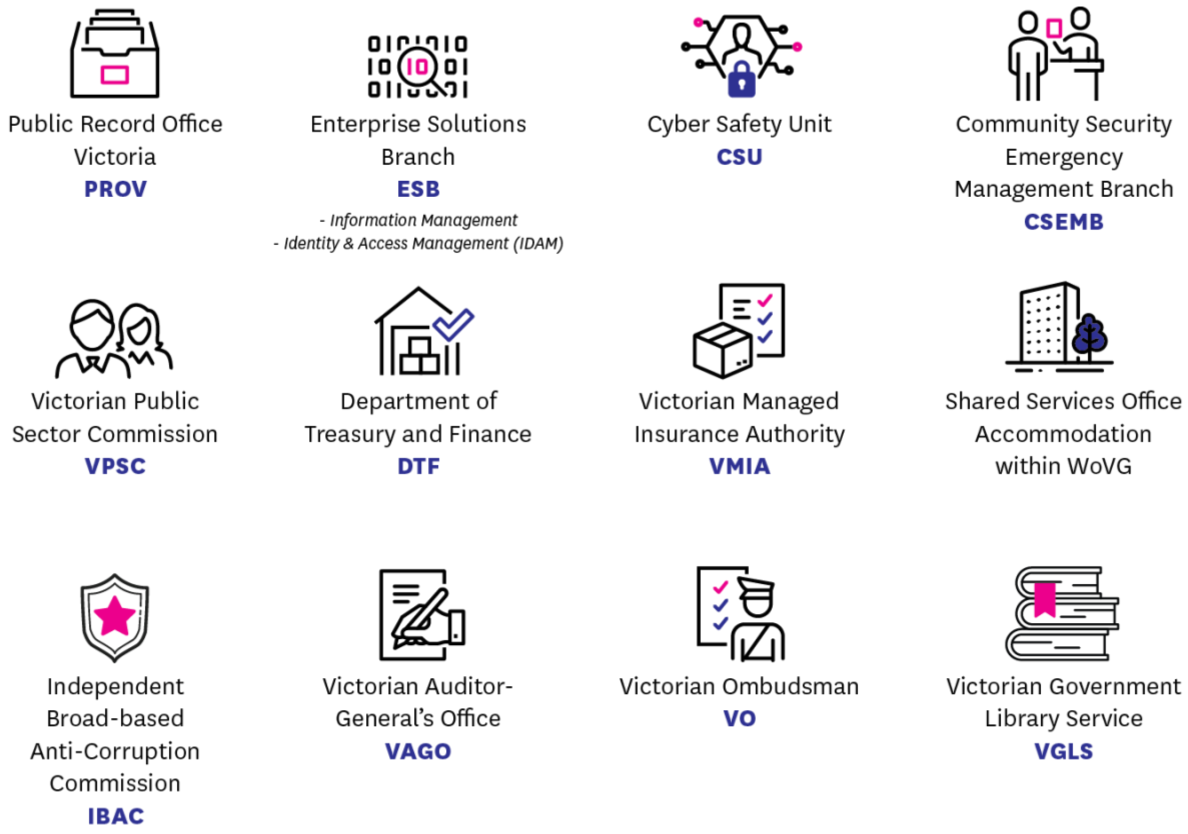
Public Record Office Victoria
PROV
Enterprise Solutions Branch
ESB
- Information Management
- Identity & Access Management (IDAM)
Cyber Safety Unit
CSU
Community Security Emergency Management Branch
CSEMB
Victorian Public Sector Commission
VPSC
Department of Treasury and Finance
DTF
Victorian Managed Insurance Authority
VMIA
Shared Services Office Accommodation within WoVG
Independent Broad-based Anti-Corruption Commission
IBAC
Victorian Auditor-General's Office
VAGO
Victorian Ombudsman
VO
Victorian Government Library Service
VGLS

Figure 3- Partnering entities

[14] Part 6, Division 1, section 106 of the PDP Act

[15] Refer to the VPDSF resources section on the OVIC website for more information on the Information Security Incident Notification Scheme

[16] Refer to the VPDSF resources section on the OVIC website to access this document

Part Two

Monitoring and Assurance by VPS organisations

7. VPS organisations' obligations

VPS organisations are required to conduct their own monitoring and assurance activities in accordance with:

- the PDP Act[17];
- the Standards[18]; and
- the Framework.

These monitoring and assurance activities track a VPS organisation's exposure to information security risks and articulate how they plan to identify, mitigate or manage these risks.

The monitoring and assurance activities outlined in this Framework are based upon a capability maturity model (**CMM**). Using CMM, OVIC expects VPS organisations to monitor their progress, and assess their adherence to the Standards, nominating both a current and target maturity rating.

This model helps VPS organisations assess their existing information security capabilities, as well as identify opportunities to improve through the nomination of target maturity ratings.

8. Accountability of the public sector body Head

Public sector body Heads are ultimately accountable for the 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 CSP/ third party with access to[19] the VPS organisation's public sector information.

When developing a monitoring and assurance program, the public sector body Head (or delegate) should seek input from internal subject matter experts and relevant external stakeholders. These stakeholders could include:

- originators of information assets, information owners, stewards, custodians, users or administrators;
- local work unit managers;
- procurement teams / managers;
- risk managers; internal / external auditors;
- information security practitioners; information security leads;
- contracted service providers; and
- partnering organisations.

[17] As outlined under Section 88(1) and (2) of the PDP Act

[18] As outlined in Standard Nine – Information Security Reporting

[19] This includes where a third party collects, holds, uses, manages, discloses or transfers public sector information on behalf of the VPS organisation, as outlined in Section 88 and 89 of the PDP Act.

9. Compliance obligations of VPS organisations

Sections 88 and Section 89 of the PDP Act outline the compliance obligations of VPS organisations with respect to the Standards, and require VPS organisations to:

- undertake a SRPA; and
- develop a PDSP and submit a copy to OVIC.

OVIC also requires VPS organisations to constructively assist OVIC in performing any monitoring and assurance activities. This includes assisting OVIC by providing free and full access, at all reasonable times, to public sector information or systems[20].

9.1. What is a Security Risk Profile Assessment (SRPA)?

A SRPA is a four-stage process that enables VPS organisations to identify, analyse, evaluate and treat information security risks.

A VPS organisation should undertake a SRPA regularly (at least annually). The SRPA process must include assessments of third parties that deal with public sector information for the VPS organisation, for example, contracted service providers[21].

The outcomes of a SRPA should be documented in a VPS organisation's risk register.

The SPRA process facilitates efficient, effective and economic investment decisions to meet both business objectives and in the selection and implementation of controls.

For more information about how to undertake the SRPA process, refer to *Practitioner Guide: Information Security Risk Management* available under the VPDSF resources section of the OVIC website.

9.2. What is a Protective Data Security Plan (PDSP)?

A PDSP is a reporting tool, used by VPS organisations to:

- advise OVIC of their maturity level, and implementation status of the Standards, referencing information security risks as identified as part of the SRPA process;
- articulate the VPS organisation's security profile[22]; and
- attest to the implementation activities as required by the Standards.

This formally endorsed document is OVIC's primary information source, to assess the state of information security across the VPS. Consequently, it is essential for VPS organisations to accurately self-report in their PDSPs.

To download a current copy of the PDSP template, please refer to the Agency reporting obligations page on the OVIC website.

[20] s106, 109, 110 of the PDP Act

[21] As outlined under s89 (2) of the PDP Act

[22] Part A of the PDSP template contains a section for an 'Organisation Profile Assessment'. For a current copy of the PDSP template, refer to the VPDSF resources section of the OVIC website.

9.3. Timeframes and deliverables in practice

VPS organisations operate under a reporting cycle that provides VPS organisations time to complete the necessary deliverables in accordance with the PDP Act and the Standards. The following table sets out the reporting cycle with associated timeframes and deliverables.

Deliverable	Timeframe
Undertake (and/or) update a SRPA for the organisation.	**Annual** *(at least)*
Provide OVIC with an Attestation by the public sector body Head.	**Annual**
Submit a PDSP (including an Attestation) by the public sector body Head.	**Biennial** *(every 2 years)*
Submit an updated PDSP to OVIC within an agreed timeframe, if there is significant change to the: • operating environment of the VPS organisation; or • security risks relevant to the VPS organisation.	***In consultation with OVIC***
Notify OVIC of any information security incidents that compromise the confidentiality, integrity or availability of public sector information, with a 'limited' business impact or higher, on government operations, organisations or individuals[23].	***As required***

10. Developing an organisational monitoring and assurance program

Information security monitoring and assurance programs will differ depending on the VPS organisation. There are a variety of factors that can influence the scope and subsequent delivery of these activities, including the size, nature and complexity of the VPS organisation.

[23] For more information on the *Information Security Incident Notification Scheme*, refer to the Incident Notification section of the OVIC website.

10.1. Scoping an organisational monitoring and assurance program

In order for a VPS organisation to develop a robust plan to mitigate or manage these, they must first establish a detailed appreciation of:

- the security value[24] of their information assets;
- the risks posed to these information assets; and
- the effectiveness of the security controls that are currently in place.
- VPS organisations should remain mindful of the ongoing need to continually monitor:
- their information security programs;
- their adherence to the Standards;
- CSPs' adherence to the Standards;
- obligations under the Framework; and
- compliance with the PDP Act.

In support of these requirements, OVIC recommends VPS organisations reference 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

For more information on the Five Step Action Plan, refer to the VPDSF resources section of the OVIC website.

10.2. Contracted service provider / third party assurance

VPS organisations should seek advice and input from partnering entities and relevant stakeholders (including CSPs and other government organisations) who have direct, or in-direct access to the VPS organisation's information assets. These parties can introduce new risks when handling public sector information which need to be identified and captured as part of the VPS organisation's SRPA, and subsequently managed via the VPS organisation's PDSP.

VPS organisations may consider taking a risk-prioritised approach when scoping third-party assurance activities. Prior to entering into any third-party arrangement, it is expected that the VPS organisation undertakes an information security risk assessment of the third party's service offering and addresses any residual risks prior to finalising the arrangement.

[24] For more information on this activity, refer to Practitioner Guide: Assessing the Security Value of Public Sector Information available under the VPDSF resources section of the OVIC website

When undertaking this assessment, VPS organisations should take into account:

- the type, nature and priority of the third-party arrangement;
- the security value of the information accessed or used under that arrangement; and
- the level of access and ongoing oversight of the CSP or third-party throughout the engagement.
- Once an engagement is in place, VPS organisations may seek ongoing assurance via scalable activities such as:
- obtaining a 'letter of comfort'/annual confirmation letter/self-assessment;
- conducting a desktop audit of processes and practices;
- conducting an onsite audit; and/or
- undertaking an investigation.

11. Undertaking organisational monitoring and assurance activities

VPS organisations are expected to perform the following monitoring and assurance activities to help demonstrate their adherence to the Standards and Framework, as well as their compliance with the requirements in the PDP Act. These activities include:

- assessing the security value of their information assets[25];
- undertaking a SRPA (at least annually);
- reviewing, validating and updating internal control libraries[26] (including validating the appropriateness of security controls);
- developing a PDSP that:
    - assesses the information security capability of the VPS organisation;
    - summarises their progress towards implementation of the Standards; and
    - provides a level of assurance to OVIC that the they are making progress towards improving information security;
- reviewing their PDSP at least every two years (or sooner if there is significant organisational change);
- monitoring for information security incidents and notifying OVIC if required under the Information Security Incident Notification Scheme[27]; and
- providing assurance through Attestation to OVIC (annually).

[25] For more information on this activity, refer to Practitioner Guide: Assessing the Security Value of Public Sector Information available under the VPDSF resources section of the OVIC website.

[26] An internal control library is a collection of documented specific security measures as selected by the VPS organisation. This internal control library is based on the VPDSS Elements and the organisation's unique operating requirements.

[27] VPS organisations must notify OVIC of incidents that compromise the confidentiality, integrity or availability of public sector information with a 'limited' business impact (BIL of 2) or higher on government operations, organisations or individuals, as soon as practical and no later than 30 days after an incident has been identified. To download a current copy of the incident notification form and corresponding instructions, refer to the Incident Notification section of the OVIC website.

Part Three
OVIC monitoring and assurance

12. OVIC's regulatory approach

OVIC employs an outcome-focused regulatory model. It concentrates on high-level assurance principles, supported by risk-informed monitoring activities. This model is aimed at delivering efficient, effective and economic security outcomes, is scalable in its implementation, and is backed by firm enforcement action where required.

In support of this regulatory approach, OVIC educates and supports VPS organisations, promoting understanding of the PDP Act and adherence to the Standards. Given this, the monitoring and assurance activities outlined in the Framework are typically based on a coordinated approach between OVIC and VPS organisations.

Nevertheless, OVIC has a legislative function to monitor organisational compliance with the PDP Act and adherence to the Standards. OVIC is also required to provide the Victorian Government with a level of assurance around the state of information security across the VPS.

The monitoring and assurance activities outlined in the Framework are based on a scalable approach including consultation, engagements, site walk-throughs and reviews, and more formal audits or investigations if warranted. These activities aim to drive improvements in information security practices, using a continuous improvement model28.

OVIC's Regulatory Action Policy articulates the conditions under which OVIC led monitoring and assurance activities may be triggered. For a full outline of OVIC's regulatory assurance functions, powers and associated triggers, refer to the *Regulatory Action Policy* available on the OVIC website.

13. Overview of OVIC's monitoring and assurance activities

As an information security regulator, OVIC has a duty to oversee and support VPS organisations' adherence to the Standards and Framework, as well as compliance with the PDP Act.

To fulfil its regulatory functions OVIC performs a variety of monitoring and assurance activities, designed to:

- foster confidence in the information security practices of Victorian Government;
- uplift VPS organisations' information security capability and maturity;
- promote accountability, integrity and continuous improvement within the VPS regarding information security;
- empower risk-based decisions within the VPS regarding information security practices;
- measure effectiveness, efficiency and economic implementation of information security practices within the VPS;
- support VPS organisations' compliance with requirements of Part 4 of the PDP Act and adherence to the Standards;
- verify and validate VPS organisations' information security practices;
- investigate breaches of the Standards or PDP Act; and
- regulate the information security environment across the Victorian public sector.

[28] Refer to *Info Sheet: Guiding Principles of the Framework and Standards* available under the VPDSF resources section of the OVIC website

By conducting these monitoring and assurance activities, OVIC can identify trends and themes in information security, issue advice or recommendations to VPS organisations, and report to government on the state of information security across the VPS.

14. Outline of OVIC's monitoring activities

OVIC's monitoring and assurance activities include:

- clarifying requirements of the PDP Act;
- assisting with enquiries regarding the intent of the Framework and Standards;
- overseeing VPS organisations' application of the Standards, adherence to the requirements of the Framework and compliance with Part 4 PDP Act obligations;
- maintaining oversight of information security incident notifications;
- hosting awareness sessions in support of the Framework and Standards;
- facilitating an outreach program through its business engagement officers;
- conducting site walk-throughs, preliminary enquiries or reviews of a VPS organisation's information security practices;
- staying abreast of information security trends and themes;
- identifying emerging issues and proactively consulting with VPS organisations on these matters; and
- ensuring the Standards are as consistent as possible with standards relating to information security (including international standards[29]).

In addition to this, OVIC regularly reviews its own information security product suite (Framework, Standards and supporting material) to validate the content and its currency. These reviews occur:

- on an annual basis;
- as the threat environment changes;
- if there are legislative or administrative changes to intersecting products that highlight the need for a review of the Framework or Standards; and/or
- as required.

15. Risk-prioritised monitoring and assurance activities

OVIC takes a risk-prioritised approach in scoping its assurance activities, considering:

- the security value of the VPS organisation's information;
- their security risk profile;
- the VPS organisation's control environment;
- notifications of any information security incidents of the VPS organisation; and
- the harm or damage that the PDP Act aims to reduce.

[29] Division 2, Section 85 (2) of the PDP Act

OVIC subsequently applies assurance resources to areas where:

- the risk is deemed the greatest; or
- the harm or damage would have the greatest impact.

Each of these factors help OVIC make informed decisions regarding the type, nature, scale, priority and timing of relevant monitoring and assurance activities. These monitoring and assurance activities include:

- consultations with VPS organisations;
- outreach activities via business engagement officers;
- research projects and initiatives;
- monitoring developments in national and international standards;
- monitoring the current threat environment;
- information security incident notifications;
- review of VPS organisational PDSP reporting;
- failures by VPS organisations to report; and
- referrals from other regulators or administrative bodies.

Outcomes of these monitoring activities inform subsequent assurance activities, such as:

- site walkthroughs;
- conducting an audit;
- undertaking an investigation;
- referring a matter, or findings, to a partnering regulatory or administrative body;
- reporting to government on VPS organisational compliance with the PDP Act, or adherence to the Standards and/or Framework;
- reporting to a Minister on an information security matter; or
- publishing a public report on an information security matter.

VPS organisations are expected to cooperate during any monitoring and assurance activity led by OVIC.

15.1. Referral of findings or matters

Information obtained by OVIC can be referred to responsible parties (i.e. Victoria Police, Independent Broad-based Anti-Corruption Commission, Cyber Safety Unit) for urgent investigation or attention.

End of document