Office of the Victorian
Information Commissioner

DATA PROTECTION

Overview of the Framework and 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

1. Introduction

This overview is a short guide to understanding the Victorian Protective Data Security Framework (the Framework) and the five-step action plan. The intended audience is information security leads, practitioners and senior managers.

The Victorian Government has committed to effectively manage protective data security risks within the Victorian public sector. This commitment will benefit the Victorian community by ensuring that government agencies observe a transparent set of security principles and are held accountable for security breaches. The secure management of information is critical to Government service delivery, public trust and confidence.

The Framework has been developed to help Victorian public-sector organisations:

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

1.1. What does the Framework mean for public-sector executives?

The Framework means Victorian public-sector executives are subject to new obligations, and have an accountability for managing information security risks. To meet the reporting requirements of the Framework, concrete actions will be required at the executive level to ensure resourcing is available. But more importantly, the primary objective of the Framework is to increase the maturity of information security management within the Victorian public sector. Employee behavior has a big impact on information security in all organisations. Executives must lead by example and drive positive changes to the culture of protective data security across the Victorian public sector.

1.2. What is protective data security?

Protective data security focuses on maintaining the confidentiality, integrity and availability of public-sector information through the implementation of protective measures from the core security domains (refer to 'What are the Standards?'). This means that any information your organisation holds is protected from unauthorised access, disclosure and use.

- Confidentiality = information is accessed by the right people
- Integrity = information is accurate, complete and up to date
- Availability = people have timely and reliable access to information

1.3. How does protective data security work in practice?

Consider what happens when you login to an online personal bank account. Only authorised users on the account should be able to see the account information (Confidentiality). It needs to be accurate and up-to-date (Integrity), and should be available in the exact moment you want to see it (Availability). Public sector information should be thought of in just the same way – only available to the right people, in the right way and at the right time. Implementation of the Framework will change the way that everyone thinks about and manages public-sector information.

1.4. What is the Framework?

The Framework is the overall scheme for managing protective data security risks in the Victorian public sector. Established under Part Four of the Privacy and Data Protection Act (2014), the Framework consists of the:

- Victorian Protective Data Security Standards (the Standards)
- Assurance Model
- Supplementary security guides and supporting resources

1.5. What are the Standards?

The eighteen standards are consistent with national and international standards and describe the Victorian Government's approach to protecting public sector information. They focus on the outcomes that are required to enable efficient, effective and economic investment in security measures through a risk-managed approach.

The standards cover the following core security domains:

- Governance (e.g. executive sponsorship of and investment in security management, utilising a risk based approach, security policies and procedures, training, business continuity, security incident management, external party engagement and oversight)
- Information security (e.g. protection of information across the information lifecycle from when it is created to when it is disposed or destroyed)
- Personnel security (e.g. engagement and ongoing management to ensure the continued eligibility and suitability of people accessing official information)
- ICT security (e.g. secure communications and technology systems processing or storing information)
- Physical security (e.g. secure physical environment i.e. facilities, equipment and services and the application of physical security measures to protect information)

1.6. What is the Assurance Model?

The Assurance Model sets out the Office of the Victorian Information Commissioner (OVIC)-led activities designed to monitor and measure the protective data security practices of the Victorian public sector, against the Privacy and Data Protection Act (2014) and the Standards. Assurance activities will consider an organisation's application of protective data security measures, commensurate with information value and the organisational security risk profile.

1.7. What is the legislative background?

As required by s85 of the Privacy and Data Protection Act (2014), the Framework and accompanying Standards were issued in July 2016.

1.8. Which Victorian Public-Sector organisations have statutory obligations?

- Departments
- Administrative Offices
- Victorian Public Service Commissioner
- Special bodies listed in Section 6 of the Public Administration Act (2004)
- Victoria Police
- Crime Statistics Agency
- Public entities, as defined in section 5 of the Public Administration Act (2004) (meaning certain bodies created under an Act, by a Minister or by the Governor in Council that exercise a public function on

behalf of the State).

A visual with more detail is available on the OVIC website.

1.9. Is the Framework and its statutory obligations good news or bad news?

It's good news! We hope that you welcome the Framework into your organisation, and note that its implementation provides the potential to reap real and positive changes to the culture of protective data security in your organisation. The Framework can also assist your organisation to achieve its own objectives through improved confidence in information and service delivery.

1.10. What are the compliance requirements of the Framework?

Victorian public-sector organisations are required to meet four compliance outcomes:

- Undertake a Security Risk Profile Assessment
- Develop a Protective Data Security Plan
- Complete a self-assessment
- Review the Protective Data Security Plan at least every two years (or sooner if there is significant organisational change).

Organisational reporting obligations for August 2018 will include:

- An attestation capturing compliance status at a high-level
- A high-level Protective Data Security Plan

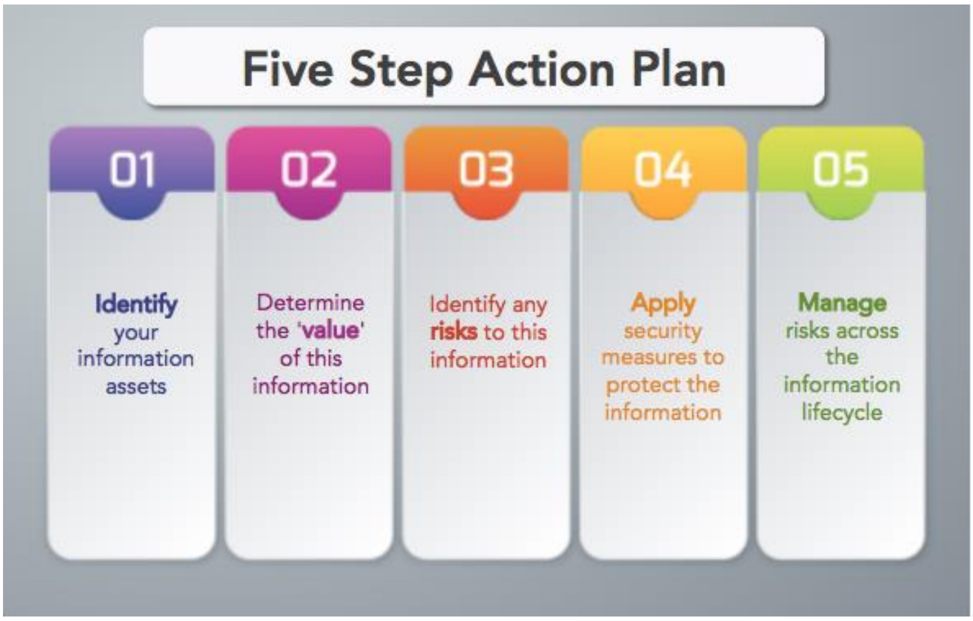
1.11. How will OVIC help you to get started?

OVIC has provided a range of guides, templates and supporting resources on its website to help you on your way. You can also join the Victorian Information Security Network (VISN) to receive information and forum updates.

1.12. How does your organisation get started?

OVIC has created a suggested Five Step Action Plan to assist you to effectively manage your protective data security risks. By completing the five steps, you should have all the information you need to develop your Protective Data Security Plan, ready for submission in August 2018.

2. The Five Step Action Plan


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

The above diagram shows the recommended five steps to inform the development of your Protective Data Security Plan and secure your organisation's information assets. For some organisations, many of the activities will dovetail with existing security and information management practices that are already in place.

2.1. Step One: Identify your information assets

The starting point for this step is for management to make a decision about the definition of information assets within your organisation and the granularity of the information you want to record in an Information Asset Register (IAR).

Your decisions here may be influenced by the size of your organisation, and by the amount of information assets being held. You should define your information assets at a level of granularity that allows any individual components to be managed usefully as a single unit. Too broad and your organisation will not have enough detail to properly manage the material; too fine and the number of assets may be cumbersome to manage. There is no right or wrong way to group information assets, however you should ensure that any groupings are consistent and relevant to your organisation's operating requirements.

An information asset can be a specific report, a collection of reports, information contained in a database, or information about a specific function, subject or process (either paper-based or electronic) that is held or created by your organisation.

Once the decision has been made by management about the definition and granularity of information assets, the next step is to survey your organisation to identify what exists, and then record the information assets in your Information Asset Register (IAR).

Deliverables from Step 1 • Define information assets (including granularity) • Survey your organisations' information assets • Record information assets in your Information Asset Register (IAR)	**Resources available from OVIC website** • Chapter 1 of the Victorian Protective Data Security Framework Information Security Management Collection
	Templates available from OVIC website • Sample Information Asset Register (IAR) Template

2.2. Step Two: Determine the value of your information assets

To ensure that all Victorian public sector organisations are valuing information in a consistent manner, organisations are required to use valuation criteria called Business Impact Levels (BILs) to determine the value of information assets. This will ensure that a protective marking (e.g. For Official Use Only) has been assessed using common criteria and therefore means the same thing across diverse Victorian public-sector organisations. Consistency is essential, especially given the need for information sharing across the Victorian public sector.

BILs provide a description of scaled consequences and impacts arising from a compromise to your public-sector information using the categories of: finance, legal & regulatory, personal, public services, public order & public safety & law enforcement.

It is important to contextualise the BILs, so they are meaningful to your employees. For example, if the BIL describing financial loss says '10% of budget', and your annual budget is $1M, you can modify the descriptor to be $100,000.

The outcome of this step is that your organisation's Information Asset Register (IAR) should now have a value attached to each asset. The value will be represented with two outputs:

A protective marking (e.g. PROTECTED)	→	to address confidentiality requirements
Identification of the need for additional security measures to protect the integrity and availability of the information asset (if required)	→	to address integrity and availability requirements

Deliverables from Step 2

- Contextualise the BILs to your organisation
- Conduct a value assessment of your information assets
- Record the value assessments in your Information Asset Register (IAR)

Resources available from OVIC website

- Chapter 2 of the Victorian Protective Data Security Framework Information Security Management Collection
- Chapter 3 of the Victorian Protective Data Security Framework Information Security Management Collection

Templates available from OVIC website

- Sample Information Asset Register (IAR) Template

2.3. Step Three: Assess any risks to the information

This step calls on management to review the organisation’s risk management framework and risk register to ensure protective data security risks have been captured. If they haven’t, these need to be considered and the risk register updated to reflect these.

Protective data security risk management should ideally be incorporated into your existing risk management process, rather than creating two parallel processes. OVIC has provided a security risk profile assessment template for those organisations who do not already have a risk management process. Please note that there is no need to create a separate document at this stage unless risk management is new to your organisation.

The outcome of this step is that your organisation’s risk management register has been reviewed to ensure it includes protective data security risks, and those risks are being actively managed. Once this outcome has been achieved, your organisation has met the compliance obligation as stated in the Privacy and Data Protection Act (2014) to ‘develop a security risk profile assessment’.[1]

Deliverables from Step 3	Resources available from OVIC website
- Review your organisation’s risk register to ensure it captures protective data security risks. - At regular intervals into the future, organisations should review their risk register and update as required.	- Chapter 1 of the Victorian Protective Data Security Framework Assurance Collection
	Templates available from OVIC website
	- Example Security Risk Profile Assessment Template (within Assurance Collection)

2.4. Step Four: Apply security measures to protect the information and self-assessment

By this step, you will have an Information Asset Register (IAR), you will understand the value of each asset, and you will understand the risks associated with the compromise to their security. It is now time to consider what security measures should be applied to manage your information risks and meet any regulatory, legal or administrative requirements of your organisation.

It is important to note that the Framework does not prescribe what security measures public sector organisations are to apply, but offers guidance in the form of central references under each standard. The adoption of a risk-based approach to the application of security measures is a fundamental principle of the Framework. This provides organisations with flexibility and autonomy to interpret your business needs and articulate your risk tolerance within your operating environment.

OVIC has produced a guide called the Victorian Protective Data Security Standards Elements – this is a holistic list of security outcomes for your organisation to consider (addressing each standard), and will be useful for planning how to manage your information risks moving forward.

OVIC has also developed a Self-Assessment Template for your organisation to use in measuring the effectiveness of your organisation’s implementation of the Standards and applicable security measures. Once your organisation has completed its self-assessment, any identified gaps and opportunities for improvement should also be transferred into your risk management register where applicable.

The outcome of step four is that your organisation’s protective data security plan can now be developed,

[1] Privacy and Data Protection Act (2014) s89 (1a)

ready for submission in August 2018.

The protective data security plan is your organisation's roadmap for how it addresses security risks and supports the implementation of the Standards. This plan is directly informed by the treatment of risks assessed and gaps in the implementation of the standards identified in your self-assessment.

The submission of protective data security plans by all public sector organisations will assist the Victorian Government to achieve a consolidated (whole of Victorian Government) view of protective data security issues and security profiles.

Deliverables from Step 4 • Complete a self-assessment against the Victorian Protective Data Security Standards • Develop a Protective Data Security Plan	**Resources available from OVIC website** • Chapter 2 of the Victorian Protective Data Security Framework Assurance Collection • Chapter 3 of the Victorian Protective Data Security Framework Assurance Collection • Victorian Protective Data Security Standards Elements
	Templates available from OVIC website • Victorian Protective Data Security Standards self-assessment template • Protective Data Security Plan Template

2.5. Step Five: Manage risks across the information lifecycle

The key message for this step is not to set and forget.

A key concept used throughout the Framework (and the underlying theme of many international standards) is the continuous improvement lifecycle model. This means that organisations need to systematically and formally, at set intervals of time, identify opportunities to mature their protective data security practices.

This quality-driven philosophy is designed to integrate protective data security into an organisation's existing business practices (like risk management, information management, personnel management, ICT management and physical management).

The Framework requires organisations to:

- PLAN – Contextualise your business objectives: understand the business and its core functions, and plan accordingly.
- DO – Integrate security measures proportionate to business risks: enhance business operations.
- CHECK – Consistently monitor business operations: undertake monitoring and assurance activities to ensure that implemented security measures support the business objectives while minimising business risks.
- ACT – Review, validate and update business objectives, risks and operations based on lessons learnt: ensure security measures are updated to support an agile business response to a dynamic environment.

By adopting this model, your organisation will systematically identify opportunities to mature your protective data security practices and secure information through all stages of its lifecycle.

Deliverables from Step 5

- Systematically and formally, at set periods of time, schedule the evaluation and review of the Protective Data Security Plan including policies and procedures and all mitigating actions and controls within the risk register.

3. Further resources on Protective Data Security

- The Victorian Protective Data Security Framework
- The Victorian Protective Data Security Standards
- Data Protection and You Video: By way of introduction to our office, and in particular to Part Four of the Privacy and Data Protection Act (2014), we created a video to assist the Victorian public sector in understanding their protective data security obligations within Victorian Government.
- VPDSF Applicability Visual
- Rosetta Stone – Core and Supplementary: A mapping of the VPDSS against existing security standards adopted by Victorian public sector organisations
- VPDSF Glossary: Glossary of Terms used in the Victorian Protective Data Security Framework

4. 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