OVIC Victorian Protective Data Security Framework (VPDSF) obligations require many organisations to complete and submit a formal update to their Protective Data Security Plan (PDSP) to OVIC by August 2024. This requires a review of all organisational information assets and systems, an assessment of the effectiveness of security controls and treatments, an Organisational Profile Assessment (OPA) and a Security Risk Profile Assessment (SRPA) to be completed.

Source: https://ovic.vic.gov.au

The PDSP includes a detailed assessment of the organisation's level of compliance to each of the Victorian Protective Security Standards (VPDSS) and a maturity assessment. The organisation's Secretary or Head of Agency must formally attest to the accuracy and completeness of the PDSP, which usually occurs after Board Risk Committee approval.

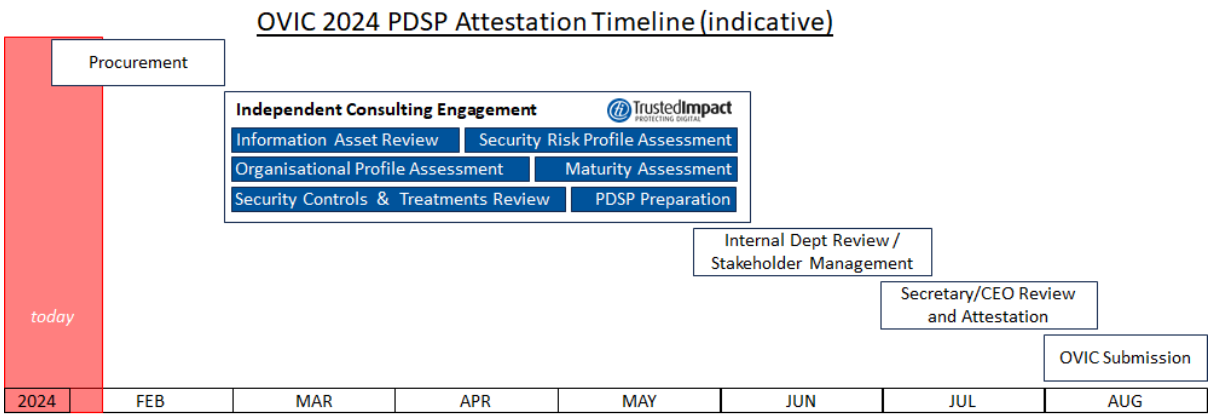
Significant security incidents that occurred in the VPS and across Australia during 2023 will set the scene for increased Board scrutiny. It is important to consider the value of having an independent trusted third-party involved in the preparation or review of your PDSP artefacts to address the potential for unintentional internal bias when reporting your organisational security posture.

Questions to consider:

1. Do you have a plan in place to complete the work required to ensure timely PDSP attestation to OVIC in August 2024?
2. Are you confident in your ability to provide assurance to your Board regarding your security posture (including your use of outsourced third parties)?
3. Do you have the right security controls in place to ensure your ability respond and recover from a security incident to protect your leadership from reputational impact?

If any of these questions raise concerns regarding your current status, please contact Trusted**Impact** for a discussion. We are happy to assist in whole or in part, to help you successfully deliver on your 2024 VPDSF obligations.

Importantly, working backwards from the August submission date and recognising that you may have a multitude of governance reviews to complete, if you need to engage an independent third party to assist in updating your PDSP, **NOW is the time to get started.**



Key deliverables for your 2024 PDSP:

Organisational Profile Assessment (OPA)

- The OPA is Part A of the PDSP, providing OVIC the basis of your risk profile. If your organisation has undergone any changes in organisational structure, such as a MOG, the approach to complying with VPDSF obligations may need to be revisited.
- Outsourcing arrangements or the introduction of significant third-party arrangements may require their engagement to contribute to your SRPA and PDSP.
- The OPA requires a breakdown of information created or held by your organisation, by data classification, the identification of how many third-parties the agency uses (and the value of the information held by those third-parties), and how many information security incidents you have experienced in the last year.

Information Asset Register Review

- Complete a comprehensive review of your current Information Asset Register (IAR) to ensure that it accurately reflects information value as defined by OVIC.
- If you do not have an IAR, this will need to be produced, as this is foundational to OVIC obligations.
- Undertake a discovery exercise to identify and assess new information or system assets that have been introduced to the organisation since the previous formal IAR review.

Security Risk Profile Assessment (SRPA):

- The security risk profile assessment process is a foundational activity that needs to be undertaken prior to developing a PDSP.
- The SRPA, which reflects your current security posture and risk landscape, requires:
    - Risk Identification: Identifying new or updated threats and vulnerabilities.
    - Risk Analysis: Assessing controls, impacts and likelihood of threats to rate risks.
    - Risk Evaluation: Assess risk tolerance and identify treatment options.
    - Risk Treatment: Implementing appropriate controls to mitigate the risks.
    - Assurance: Producing evidence to demonstrate the effectiveness of controls through testing and monitoring.
- These tasks require consultation with information and systems owners, and custodians responsible for operating security controls. These may be internal or external parties.
- Mature organisations that record risks in a central register need to review this register and their SRPA periodically to ensure they reflect the changing threat landscape and organisational profile. Less mature organisations may need to produce such a register to be able to complete the SRPA.
- OVIC advise that “the management of the SRPA […] should be independent of the information owners to ensure all risks to information are given appropriate priority.”

Protective Data Security Plan (PDSP):

- The PDSP includes a robust assessment on the level of implementation of all of the VPDSS elements across their organisation, and a maturity assessment. The 2024 PDSP must be submitted to OVIC along with your Head of Agency attestation to the completeness and accuracy of the document.
- Risks called out in the SRPA are recorded in line with applicable VPDSS elements by providing the risk ID associated with the organisation risk register.
- Each standard element is assessed to indicate the level of implementation of the OVIC requirements, and a target date for completion.
- A maturity assessment is conducted at a whole of Standard level, indicating the maturity level of certain aspects of the organisation's security practices. This provides insight to OVIC on how organisations are prioritising their security investments and whether they need to escalate focus on key gaps, which they do through their 'Insights' reports following annual submissions.

During the course of completing the various deliverables leading up to the final PDSP, many organisations seek to fast-track the completion of some promised artefacts (policies, standards, procedures) or other controls. Time permitting, these can help deliver favourable PDSP results in August. Trusted**Impact** can also help with these activities as required.

Why should you consider Trusted**Impact?**

1. **LOCAL**: We are a boutique cyber-focused consultancy, proudly Victorian Headquartered, with deep experience and appreciation of local compliance requirements – we are not a large generalist or international firm that uses your funding to learn about your requirements and priorities.
2. **PROVEN** IN VICTORIAN GOVERNMENT: For over 18 years we have been working with more than 50 Victorian State and local government organisations, providing a range of specialised cyber insight and advice. We understand and have experience with your OVIC compliance obligations.
3. **SENIOR** PROFESSIONALS: Our business model is to have senior, highly experienced professionals working closely and collaboratively with you to help position you for success, not a junior team all well intentioned, but frankly, learning on the job.

In providing information security services to the Victorian government and commercial sectors for over 18 years, Trusted**Impact** is well equipped to assist government and related organisations address the mandatory requirements and data protection obligations to meet the attestation reporting requirements.

Trusted**Impact** has demonstrable experience conducting successful security assessments for large 'iconic' Australian Brands, Financial institutions, internet-based businesses through to complex Government Agencies and Departments which account to more than:

- **50** Government Departments and Agencies,
- **75** Commercial clients,

- **25** Financial organisations,
- **20** Health organisations, and
- **15** Educational institutions.

Engage Trusted**Impact** to help you align your organisational practices with VPDSS requirements, institute robust security measures, and help foster a culture of compliance, to ensure the confidentiality, integrity, and availability of sensitive data in accordance with the standards set forth by the OVIC.

Trusted**Impact** will help you respond to the VPDSS Requirements with:

- A comprehensive Risk Assessment
- Data Classification and Handling
- Access Controls and Authentication Assessment
- Review Encryption Measures
- Incident Response Planning
- Employee Training and Awareness
- Continuous Monitoring and Auditing
- Collaboration and Reporting
- Documentation and Record-Keeping
- Regular Compliance Reviews

For further information please feel free to call us on 03-9023-9710, or PDSP.2024@trustedimpact.com

Appendix – VPDSF Explained

What is the VPDSF?

The Office of the Victorian Information Commissioner (OVIC) has published the Victorian Protective Data Security Framework (VPDSF) and the accompanying Victorian Protective Data Security Standards (VPDSS) to assist Victorian public sector organisations to meet the requirements set out in the framework in addition to other legal, regulatory and administrative data protection obligations under the Privacy and Data Protection Act 2014 (Vic) (PDP Act).

The VPDSS establishes 12 high level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, Information Communications Technology (ICT) and physical security.

The VPDSF is a mandatory framework that applies to all Victorian public sector organisations, including departments, agencies, local councils, and public hospitals. It sets out the minimum requirements for how these organisations must handle personal information.

What are the benefits of the VPDSF?

The VPDSF helps to protect the privacy of individuals and ensures that personal information is handled securely and responsibly. It also helps to reduce the risk of data breaches and identity theft.

What are the key principles of the VPDSF?

The VPDSF is based on four key principles:

- Privacy: Personal information should be collected, used, stored, and disclosed in a way that respects the privacy of individuals.
- Security: Personal information should be protected from unauthorised access, disclosure, misuse, loss, or modification.
- Data integrity: Personal information should be accurate, complete, and up-to-date.
- Accountability: Organisations are responsible for the personal information they hold and must be able to demonstrate that they are complying with the VPDSF.

What are the requirements of the VPDSF?

The VPDSF sets out a number of requirements for how organisations must handle personal information. These requirements include:

- Having a data security policy
- Classifying personal information
- Implementing appropriate security controls
- Training staff on data security
- Reporting data breaches