Sample Proposal for Professional Risk VPDSS Compliance
Copyright & Confidentiality

This document is copyright IPSec Pty Ltd (IPSec).

This document is provided by IPSec to the Client (as noted in Document Control) on condition that neither it nor any part of it shall be disclosed to any third party without the express written permission of IPSec.

Restrictions on this document do not extend to those details that have previously been published or otherwise provided to the public domain.

Document Control

Document Approval

<table>
<thead>
<tr>
<th>Version #</th>
<th>Date</th>
<th>Presales Approval by:</th>
<th>Comment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

Copyright & Confidentiality ................................................................................................. 2
Document Control .................................................................................................................. 2
Document Approval .............................................................................................................. 2
Table of Contents .................................................................................................................. 3
Executive Summary .............................................................................................................. 4
  Depth of Solution ................................................................................................................ 4
  Proposed Services ............................................................................................................... 4
  Proposed Deliverables ....................................................................................................... 6
Introduction to IPSec & IPSec Consult .................................................................................. 7
What is the Victorian Protective Data Security Standard (VPDSS)? .................................. 8
Understanding Your Victorian Protective Data Security Standards (VPDSS) Obligations .... 9
Proposal Detail - Delivering your VPDSS Compliance ......................................................... 10
  The Commissioner for Privacy and Data Protection’s Five Step Action Plan .................. 10
  Step 1 – Identification of Information Assets ................................................................. 10
  Step 2 – Determine the Value of Information Assets ..................................................... 11
  Step 3 – Identify Risks to Information Assets ................................................................. 13
  Step 4 – Apply Security Measures to Protect the Information Assets ......................... 16
  Step 5 – Manage Risks Across the Information Lifecycle ............................................... 17
Smart Tools, not Spreadsheets .............................................................................................. 19
Executive Summary

Depth of Solution

This proposal addresses all five steps required to comply with the requirements of the Victorian Protective Data Security Framework (VPDSF) action plan. This foundation for this is a purpose built smart tool that adds efficiencies many orders of magnitude greater than spreadsheets and provides a platform for continued leverage for future cycles without having to start all over again each year.

Using a modern Software as a Service (SaaS) platform, the cycle of configuration to useful output is measured in days rather than months and the user interface engages users to positively interact with risk management rather than seeing it as a cumbersome administrative overhead.

Since July 2016 this smart tool has adapting to closely match the requirements of the Five Step Action Plan and we continually refer to the Data Security Resources Material at the OVIC site to ensure we can deliver a single solution meeting all the VPDSF requirements. The solution is currently in use within organisations assisting them to comply with the Victorian Protective Data Security Standard (VPDSS).

FIVE STEP ACTION PLAN

| Identify your Information Assets | Determine the value of this information asset | Identify any risks to this information | Apply security measures to protect the information | Manage risks across the information lifecycle |

Proposed Services

Further to discussions held with Company X, IPSec Consult proposes the following Professional Services will meet company’s VPDSS requirements:

Step 1 – Identify your information assets

A data object has been created that meets the VPDSF requirements and includes additional core and Supplementary requirements. The database is fully maintainable with a security access control overlay.

This task would normally be manually intensive and unstructured using a discovery process of interviewing data owners across the enterprise to uncover information artefacts. The accuracy will be dependent on the consistency of the questioning and the method for recording of the items. A smarter way to do this is to deploy a structured workflow to all information owners to identify the assets and have all of the results automatically recorded in an auditable database.
Step 2 – Determine the Value of this information

Determine the value of this information asset

The workflow follows a similar approach to the BIL App (created by OVIC) to assess the Business Impact Levels of each information asset.

The process has a full audit trail of who / what / when for each BIL assessment. The language of the Impact Guidelines is user editable and there is a workflow to notify selected users of outcomes, and an escalate process to support the Protective Marking and Dissemination Limiting Marker (DLM) process.

As part of the workflow, based on the Impact Levels a Risk Assessment can be automatically launched.

Step 3 – Identify Risks

Identify any risks to this information

Using predefined templates, the next stage would be to perform a self-assessment against the VPDSS Elements that have already been mapped into the control library. The risk engine will perform a first pass based on the effectiveness of information security controls and identify potential risk. The Risk Report has 5 components, starting with a definition of the business risk, a heat map allowing the risks to be prioritised based on Likelihood and Consequence, Root Cause diagrams linking risks to controls. The last two sections link the risks to specific VPDSS Elements facilitating the development of Remediation Plans and a Radar Gap Analysis mapped to the 18 VPDSS Standards to enable year on year process improvements.

Included in the Control Library are standards such as Australian Privacy Principles, ISO 27001, NIST C2M2, ASD Protective Security Policy Framework (PSPF), Cobit 5 and many more.

Step 4 – Apply Security Measure to protect the information

Apply security measures to protect the information

An automated direct link ties each control weakness to the specific control objective in the VPDSS Standards providing guidance to the remediation required. This together with an integrated Risk Register allows security measures to be developed.

An activity based remediation plan allows for localisation of the risks based on Likelihood and Consequence, Defining Loss Potential, Allocation to a Risk Group.
Step 5 – Manage Risk across the Life Cycle

A real time Dashboard is the hub of the Risk Management Activities. A single pane shows the current Risk Heat Map, Risk Exposure and Risk Groupings and is dynamically driven by the progress of the security remediation plans.

A task manager ensures tight control of the individual activities of each Security Remediation

Proposed Deliverables

The proposed solution addresses all 5 steps of the VPDSS requirements

Identify and Value Information Assets

Steps 1 and 2 are ongoing activities with Information Asset Database being maintained and BILs being determined and reviewed on a regular basis.

Security Risk Profile Assessment (SRPA)

This is provided by the Self-Assessment process measured against the 18 Standards and VPDSS Elements. created at the end of Step 3

Protective Data Security Plan (PDSP)

This is created at the end of Step 4 and shows the history and current status of the Security Remediation Plans

Ongoing Support & After Sales Care

After the hand-over of the project to Company X for Business-As-Usual activities, IPSec can provide a full suite of offerings to aid with implementing controls for the mitigation of Information Asset Risks.

IPSec’s expert Security Engineers, 24x7x365 Security Operations Centre and Security Consultants are available for your assistance; making your journey to full whatever Standard required by and organisation such as VDPSS with NIST etc compliance smooth and trouble-free.
Introduction to IPSec & IPSec Consult

About IPSec

IPSec are specialists in information asset protection; information security experts who know how to mitigate risk to business by assisting in the protection of their valuable intelligence, data and information. From assessing the risks of vulnerabilities and threats, to designing and implementing customised security strategies, to managing execution and optimising results. IPSec are guardians of business confidence, providing high levels of protection and optimal assurance of an organisation's security posture.

Since 1995, our team have grown with the developments of technology, cementing a practiced, thorough understanding of the potential Cyber Security threats facing organisations.

Introduction to IPSec Consult

IPSec Consult is a division of IPSec that concentrates on Information and Cyber Security Risk. Our team of expert Risk Management consultants are dedicated to helping our clients mitigate risks to their Information Security environments and general Cyber Security concerns.

One of the significant security challenges for any organisation is bridging the divide of understanding and achieving a meaningful engagement between Business Risk and Technology Risk resources.

The unique offering IPSec Consult brings to our clients is that we encompass all areas of Information Security Risk; from highly technical engagements such as Penetration Testing to Business Risk assessments for Governance, Risk and Compliance purposes.

At IPSec Consult, we speak both Technical and Business Risk. We can translate the findings from this technically based engagement to your business stake holders. This enables us to bridge the gap between the IT Managers and the Risk Managers.
What is the Victorian Protective Data Security Standard (VPDSS)?

The VPDSS standard is designed to drive cultural change in the Victorian public sector and its associated entities with the aim of building its information security capability and resilience.

The Commissioner for Privacy and Data Protection under the Department of Premier & Cabinet has mandated a requirement with specific milestone dates of progression towards VPDSS compliance for all Victorian Public Sector Agencies and bodies defined in the Public Administration Act of 2004.

Under the Privacy and Data Protection Act 2014 (PDPA), these bodies must develop and engage in practices that comply with the VPDSS. Other legislative obligations include developing a Security Risk Profile Assessment (SRPA) and submitting a Protective Data Security Plan (PDSP).

It is an implicit requirement of the VPDSS standard to gain executive sponsorship which means that the mandated security strategy and risk management activities are endorsed & signed off at a senior level when reporting compliance to the Commissioner for Privacy. The Security Risk Profile Assessment (SRPA) should measure the organisations maturity against the 12 governance standards and 4 security domains of the VPDSS. The resulting gap analysis should then lead to the development of a Protective Data Security Plan (PDSP) with remediation activities prioritised on a Risk Basis and managed to ensure objectives are achieved.
Understanding Your Victorian Protective Data Security Standards (VPDSS) Obligations

The first deliverable is due by August 2018 and requires the organisation to submit their Protective Data Security Plan (PDSP) to the Commissioner for Privacy and Data Protection (CPDP) with supporting evidence of the remediation plan and progress. Thereafter every two years a Security Risk Profile Assessment (SRPA) and the Protective Data Security Plan (PDSP) will need to be completed (but not submitted) and every year an attestation from senior management will need to be produced confirming compliance with the VPDSS framework.

Figure 2- Image Credit: Commissioner for Privacy and Data Protection.

Amended from OVIC 10 November 2017 update:

- A high-level Protective Data Security Plan and an attestation (capturing compliance status) is due for submission to OVIC in August 2018.
- removal of the requirement (from the Framework) for organisations to provide OVIC with a copy of their Security Risk Profile Assessment (SRPA);
The Commissioner for Privacy and Data Protection’s Five Step Action Plan

**Step 1 – Identification of Information Assets**

The first step to being able to provide appropriate protection to your information assets is to know what Information Assets you have.

The process for this is to deploy a template from the “funnel” library that already has all the functionality built in to efficiently perform this task.

Using the predefined object – Data Record (see below) – a communication can be sent out to an audience in order to create an Information Asset Register.

This register will then serve as a centralised Information Asset Register that is fully auditable.
Step 2 – Determine the Value of Information Assets

The outcome of this step is to determine the “value” of the Information Assets and classify them based on potential impact resulting from a compromise to Confidentiality, Integrity and Availability.

The objective of this exercise is to:

- Provide a consistent method for assessing the value of Information Assets
- Determine the applicable protective markings
- Understand the effectiveness of the controls required to protect these assets
- Prioritise risk treatment resources based on the risk profiles

How this is achieved

The process deployed in Step 1 will already have captured the Information Assets as part of a predefined workflow.

This stage will determine the Business Impact Level based on a predefined set of questions.

In this workflow the Protective Marking will be determined and a workflow can then escalate the process of determining the applicable DLM – see sample screen below.
A valuable addition to this workflow is the ability to automate the launching of a “comprehensive” Risk Assessments for based on the required Protective Marking by customising an assessment configured to match the VPDSS Elements.

<table>
<thead>
<tr>
<th>Specify Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please define the specific outcomes that are possible based on answering defined questions. Keep it short. Two outcomes are required at a minimum (e.g., positive case an outcome.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1</th>
<th>Secret</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Protected</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Unclassified with DLM</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Unclassified no DLM</td>
<td></td>
</tr>
</tbody>
</table>
Step 3 – Identify Risks to Information Assets

VPDSS Deliverable – Security Risk Profile Assessment (SRPA)

The foundation for the SRPA is a maturity assessment measured against the 18 Standards of the VPDSS. This assessment duplicates the controls released in July 2017 Self-Assessment Spreadsheet.

The purpose of activity is as follows:

1) Determine the level of maturity required of each of the 18 Standards to compliance VPDSS Standard and the legislative obligations;

2) Perform a Self-Assessment to determine the gaps between Expected and Assessed Outcomes

At the completion of the assessment, the following output is generated:

- Management Summary of High Business Risks
- Risk Diagram grouping by Likelihood and Consequence
- Root cause Graphs showing links from business risks back to control weaknesses
- Gap Analysis showing deviation between Expected and Assessed Maturity
- Compliance Summary mapping deviations to specific clauses in the VPDSS Standards
3) Prioritise the risks and understand the underlying root cause analysis
4) Review the Gap between Expected and Assessed Outcomes

5) Link back to VPDSS Standards to drive remediation plans

<table>
<thead>
<tr>
<th>Control Statement Title</th>
<th>Target</th>
<th>Assessed</th>
<th>Primary Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linkage to Control Statements</td>
<td>3</td>
<td>1</td>
<td>2.2</td>
</tr>
<tr>
<td>Strategy Definition</td>
<td>3</td>
<td>1</td>
<td>8.2, 8.3</td>
</tr>
<tr>
<td>Recovery Profiles</td>
<td>3</td>
<td>1</td>
<td>8.2, 8.3</td>
</tr>
<tr>
<td>Strategy Review</td>
<td>3</td>
<td>1</td>
<td>8.2, 8.3, 8.4</td>
</tr>
<tr>
<td>Data Austerity</td>
<td>3</td>
<td>1</td>
<td>14.2, 14.3</td>
</tr>
<tr>
<td>Integrity of Public Information</td>
<td>3</td>
<td>1</td>
<td>13.2, 13.3, 13.4</td>
</tr>
<tr>
<td>Right to Audit</td>
<td>3</td>
<td>1</td>
<td>9.2, 9.3, 9.4</td>
</tr>
<tr>
<td>Linkage to Control Statements</td>
<td>3</td>
<td>1</td>
<td>2.2</td>
</tr>
<tr>
<td>Training Needs Analysis</td>
<td>3</td>
<td>1</td>
<td>8.2, 8.3, 8.4</td>
</tr>
<tr>
<td>Incident Response</td>
<td>3</td>
<td>1</td>
<td>7.1, 7.2, 7.3</td>
</tr>
</tbody>
</table>
Step 4 – Apply Security Measures to Protect the Information Assets

VPDSS Deliverable – Protective Data Security Plan (PDSP)

At the completion of the SRPA, this step will focus on planning the remediation activities required to address the Information Security Risks leading to the formulation of a PDSP.

The Protective Data Security Plan (PDSP)

Using the real time Risk Dashboard, the remediation plans will be categorised under the headings of Risk Tags. This allows for aggregation of Risk Treatment Plans for both reporting, management and prioritisation.

The selected PDSP elements will be prioritised, budgeted and project managed and will provide evidence to support the required senior management attestation for the Privacy Commissioner that the PDSP addresses the VPDSS standards.
Step 5 – Manage Risks Across the Information Lifecycle

The philosophy of the Risk Dashboard is that managing risk should be a daily activity, in a similar manner to checking email or social media feeds. This way, risk management is performed in small, bite sized pieces that are manageable and non-intrusive.

Risk Register Dashboard & Task Manager

The on-line dashboard allows the risks to be grouped (on an inclusive or exclusive basis) showing the Risk appetite vs Residual risk based on the Protective Data Security Plan (PDSP). As risks are mitigated through control improvements, the dashboard shows in real time the reduction in the Company X risk profile.

The components of the Risk Dashboard are as follows:

Heat Map

![Heat Map Image]

Risk Rating Summary

![Risk Rating Summary Image]
Risk Exposure

This is dynamically driven by the Mitigation Projects showing the buy down potential of each step of the project plans.

The inbuilt task manager makes assigning and managing individual tasks straightforward.

Ongoing Support & After Sales Care

After the hand-over of the project to Company X for Business-As-Usual activities, IPSec can provide a full suite of offerings to aid with implementing controls for the mitigation of Information Asset Risks.

IPSec’s expert Security Engineers, 24x7x365 Security Operations Centre and Security Consultants are available for your assistance; making your journey to full VPDSS compliance smooth and trouble-free.
Smart Tools, not Spreadsheets

Using smart, sophisticated next generation tools (not spreadsheets), IPSec provides Information Security Standards based services in a dramatically reduced timeframe, customised to your organisation’s requirements.

IPSec delivers the critical interaction with your originations appropriate business users via a specialist SAAS tool that delivers crucial support for regulatory and compliance based activities in a flexible and very time efficient manner.

Using smart technology, all the hard, manual work of standards based assessment alignment and gap analysis is dramatically reduced; providing Industry Standards content contained in a user-friendly interface. It centralises reporting and analysis, with mature methodologies for performing compliance analysis in a cost effective and efficient manner.