IPSec Professional Risk VPDSS Compliance Services
Overview in Brief

Date:
March 2017
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 Title:  VPDSS Overview – March 2017
# Table of Contents

Copyright & Confidentiality ........................................................................................................... 2

Document Control .......................................................................................................................... 2

Table of Contents .......................................................................................................................... 3

Introduction to IPSec & IPSec Consult ......................................................................................... 4

What is the Victorian Protective Data Security Standard (VPDSS)? ............................................ 5

Understanding Your Victorian Protective Data Security Standards (VPDSS) Obligations .......... 5

Proposal Detail - Delivering your VPDSS Compliance ................................................................. 6

  The Commissioner for Privacy and Data Protection’s Five Step Action Plan .................. 6
  Step 1 – Identification of Information Assets ................................................................. 6
  Step 2 – Determine the Value of Information Assets .................................................... 6
  Step 3 – Identify Risks to Information Assets ............................................................... 7
  VPDSS Deliverable 1 - Security Risk Profile Assessment (SRPA) .................................... 7
  Step 4 – Apply Security Measures to Protect the Information Assets ......................... 11
  VPDSS Deliverable 2 - Protective Data Security Plan (PDSP) ........................................ 11
  Step 5 – Manage Risks Across the Information Lifecycle ........................................... 12

Smart Tools, not Spreadsheets ...................................................................................................... 13

Project Management .................................................................................................................. 14

IPSec Consult Staff ...................................................................................................................... 15

IPSec Consult always employ certified consultants ................................................................. 15
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 June 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 updated and every year an attestation from senior management will need to be produced confirming compliance with the VPDSS framework.
Proposal Detail - Delivering your VPDSS Compliance

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 outcome of this step is to produce an Information Asset Register that is pragmatic and straightforward to maintain.

IPSec will ensure that appropriate documentation exists for the identified Information Assets. This is normally performed through a staff interview and documentation review process.

Step 2 – Determine the Value of Information Assets

The outcome of this step is to complete the Information Asset register with classification levels for all identified Information Assets.

Using Victorian Office of the Commissioner for Privacy and Data Protection (CPDP) approved tools, such as the Business Impact Level App, IPSec will identify the appropriate classification for Example Department Information Assets.

The diagram below show a high level visual representation of the Information Asset Assessment Process:
Step 3 – Identify Risks to Information Assets

VPDSS Deliverable 1 - Security Risk Profile Assessment (SRPA)

The foundation for the SRPA is a maturity assessment measured against the 18 Standards of the VPDSS.

This will be completed through the following activities:

1) A Half-Day Workshop

The purpose of this workshop is three-fold:

1) To ensure senior management and project stakeholders understand the purpose and objectives of the VPDSS Standard and the legislative obligations;

2) To establish the required standards alignment levels for the gap analysis; and

3) To identify intended gap analysis assessment participants.

The VPDSS assessment takes the form of an online questionnaire where respondents are required to assess their perceived current level of alignment regarding the required controls. The questionnaire aligns directly to the VPDSS standards requirements and is in English language form that does not require IT expertise to answer. The questions are associated with the way in which information / data is handled within the organisation. Appropriate respondents may be between 3 and 5 key employees (on average) chosen to complete the online surveys based on their job description representing a relevant cross section of Information users. For example, the CIO, HR Manager, IT Manager, key power user, Sys Admin or Records Managers would be a typical survey field.
2) Completion of the self-assessment

Each respondent selected will receive an on-line link to the questionnaire, and can be required to complete the assessment within a specified time. The survey can be completed in multiple sittings and will be deemed complete once submitted. The questionnaire requires the users to select one of five pre-defined responses. A VPDSS survey will take the average person around 2 hours to complete.

The questions and answers are all provided in plain English, avoiding technical jargon. The advantage of this is that the users do not have to have detailed technical knowledge to provide a constructive influence.
3) **Self-assessment results and review**

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

**Examples of Risk Diagram and Associated Gap Analysis**

All identified gaps will be reviewed and displayed within a standards compliant risk matrix, and reported in easy to read graphs as shown below:
4) **Creation of the Security Risk Profile Assessment (SRPA)**

Review of the self-assessment output and acceptance and prioritisation of the risks will form the foundation of the SRPA.

Below is an example of a Risk Assessment Profile of a VPDSS assessment:

![Risk Assessment Profile](image)

The IPSec provided Risk Register will then provide a dynamic link between the risks and remediation activities defined in the security remediation plan for step 4:

![IPSec Consult](image)
Step 4 – Apply Security Measures to Protect the Information Assets

VPDSS Deliverable 2 - 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)

A Post Assessment review will facilitate handover of SRPA responsibilities to Example Department management and the PDSF activities to the persons responsible for ongoing management of the remediation tasks.

IPSec will assist Example Department with forming the PDSF and identifying the required controls for risk mitigation.

The Senior Management Attestation

The selected PDSP elements will be prioritised, budgeted and project managed. IPSec will assist with this activity 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 IPSec methodology and associated smart tools empower Example Department to easily manage their Information Asset Risks across their entire lifecycle.

The philosophy of the IPSec Methodology 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 Example Department risk profile.

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

**Ongoing Support & After Sales Care**

After the hand-over of the project to Example Department 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.
Project Management

IPSec Consult’s consultants are very conscious of the importance of proper project management to ensure the quality outcomes required by Example Department.

As such we maintain strict project initiation, delivery and completion regimes to achieve the best possible outcome for Example Department and to ensure the least possible interference to both the project delivery and the impacted information environment.

Upon being engaged by Example Department to deliver professional risk services, IPSec Consult will request that a primary point of contact be assigned by Example Department to act as the ultimate owner of the project within Example Department’s organisation.

IPSec Consult projects all require an initiation, delivery and completion stage. Whilst the specific components that make up these stages may vary based on the deliverables of the project, IPSec Consult maintains these consistent aspects to ensure a quality outcome. These include:

Project Kick-Off (Initiation)

- Liaise with client to establish primary contact and other key contact points.
- Liaise with client to establish high-level schedule of activities and resources.
- Liaise with client regarding additional details that may be required for the project.

Project Delivery

- If the project delivery time is longer than a week, hold weekly meetings (telephone or in person) to:
  - Update client on delivery progress.
  - Review schedule of activities and resources.
  - Liaise with client regarding additional technical details that may be required.
  - Liaise with client regarding other issues affecting delivery of project outcomes.

Project Completion

- Provide the client with a project completion report outlining activities undertaken, findings of the project (where appropriate), recommendations from the project, and references useful to the client as a result of the project.
  - Where appropriate IPSec Consult may recommend for a draft report to be provided and/or a report presentation be given prior to the final report to allow the client to review the findings and outcomes of the project and to seek clarification on points of the project outcomes.
  - Upon acceptance of the final report, IPSec Consult will remove all drafts and supporting information from its servers and workstations. Only the final report will be stored on a secure file server.
IPSec Consult Staff

IPSec Consult is committed to delivering quality outcomes to Example Department and as such is committed to providing highly experienced information security professionals capable of meeting the expectations of Example Department.

Upon being engaged by Example Department IPSec Consult will assign a principal staff member responsible for the delivery of the project. Where additional resources are required for the project, IPSec Consult will assign a small, controlled number of risk professionals to focus on the project and to ensure that all IPSec staff interacting with the project are fully aware of the specific circumstances and sensitivities under which it is being delivered.

All IPSec Consult staff are under strict confidentiality agreements and as such all information gathered by them as a result of a project or proposal will be treated with the strictest confidence and handled with the utmost sensitivity to the client’s intellectual property.

In addition, all security testing staff maintain current Police Check Certificates (copies can be provided at request).

IPSec Consult always employ certified consultants

ISO Certified Consultants

IPSec employ consultants who have broad industry experience combined with deep understanding of best practice in the world of compliance.

Certifications include:
- ISO 270091:2013 Lead Auditor
- ISO 9001:2015 Lead Auditor
- ISO 22301:2012 Business Continuity Implementer

Crest Certified Penetration Testers

In an unregulated and often confusing information security supplier market, businesses increasingly require reliable, professional, high quality information security testing services.

CREST Certified staff, with proven technical capabilities and a commitment to integrity and high quality service, are the natural choice in information security testing providers.
 Credentials- Jeff Sussman (Senior Risk Consultant assigned to Example Department)

Professional Background

Jeff Sussman is IPSec’s Lead Senior Risk Consultant. Over the past twenty-five years, he has worked at the forefront of enabling technology to drive business success. He has worked across a broad spectrum of organisations advising on technical infrastructure and more recently has focussed on assisting organisations to best manage their information and cyber security.

He comes from a strong technology background at a senior executive level combined with hands on experience implementing Quality (ISO 9001) and Information Security (ISO 27001) and Business Continuity (ISO 22301) programs. His current focus is specialising in Security Assessments, Gap Analysis and Risk Assessments based on smart assessment tools and international standards.

Jeff has also spent many years in the academic world sharing his knowledge and experience at a post Graduate level at a leading Business School. This experience has been invaluable in further developing his analytical, report writing and presentation skills.

Education & Certification

Jeff has embarked on a wide range of education opportunities starting off in Engineering and then moving into mainstream commercial world after completing an MBA. He has also completed a BCom (Hons) in Information Systems and a Graduate Certificate in Change Management.

His current certifications include Lead Auditor in both IOS 9001:2015 and ISO 27001:2013.

Core Skills:

- Disaster Recovery Strategy
- Business Continuity Planning
- Information Security Risk Assessments
- Cyber Risk Assessments
- Information Security Gap Analysis
- Remediation Strategies
- Standards Control Mapping

Major Clients he has worked with:

- Australian Taxation Office
- Centrelink
- Optus
- Telstra
- NAB
- Amex