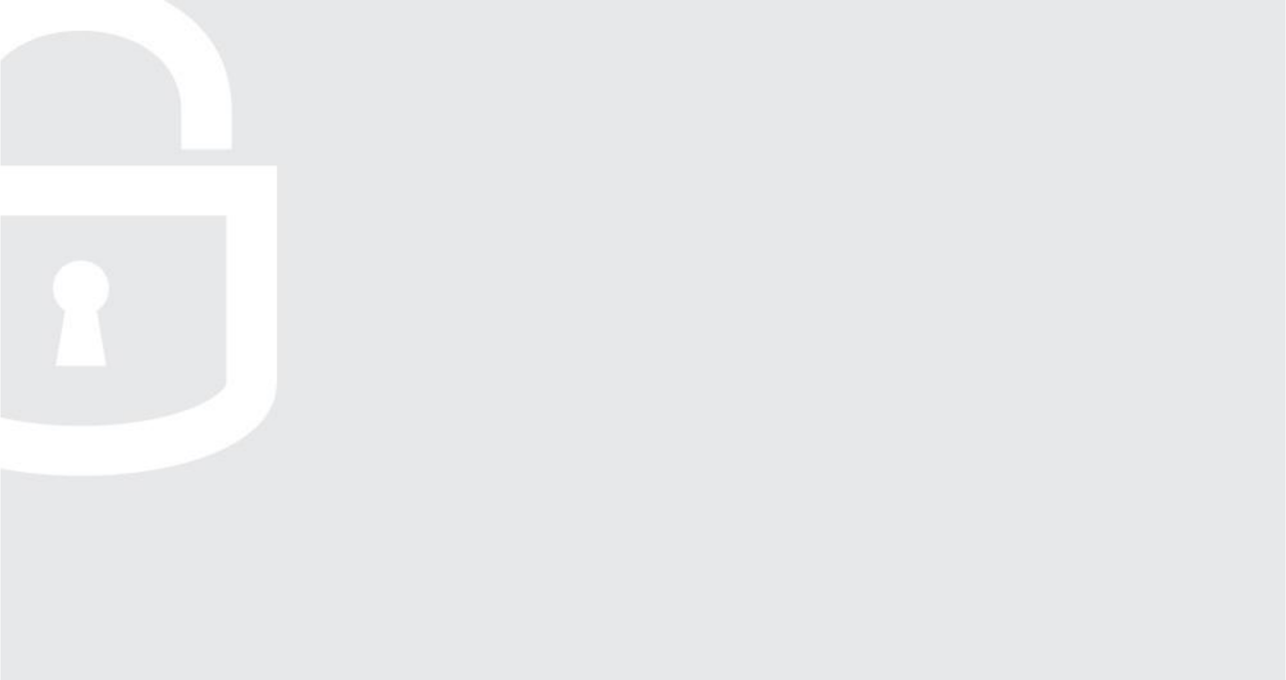
Sample Proposal for Professional Risk VPDSS Compliance



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.

DRAFT

Document Control

Document Approval

Version #	Date	Presales Approval by:	Comment:
1.1			

Table of Contents

DRAFT

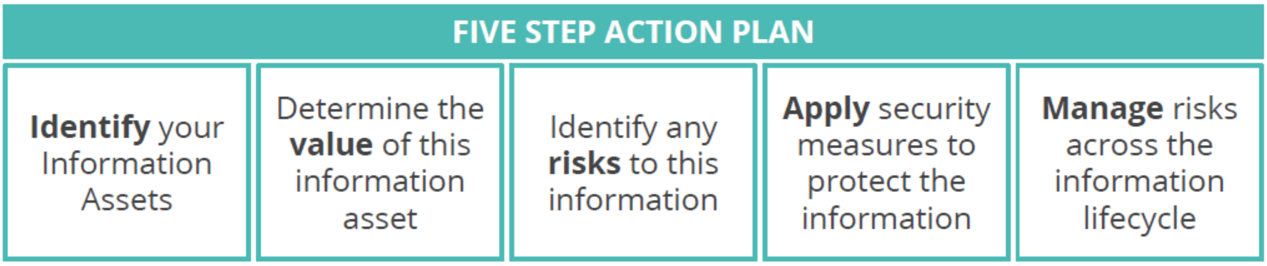
Executive Summary

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 Acton 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)

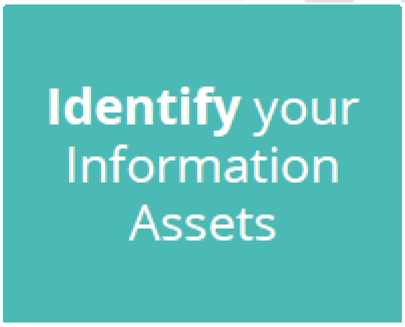


FIVE STEP ACTION PLAN				
Identify your Information Assets	Determine the **value** of this information asset	Identify any **risks** to this information	**Apply** security measures to protect the information	**Manage** risks across the information lifecycle

Proposed Services

Further to discussions held with <Customer Name> IPSec Consult proposes the following Profession Services will meet <Customer Name>'s VPDSS requirements:

Step 1 – Identify your information assets



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

DRAFT

Step 2 – Determine the Value of this information

Determine the **value** of this information asset

The workslow follows a similar apparoach 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.

DRAFT

Step 5 – Manage Risk across the Life Cycle

Manage risks across the information lifecycle

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 <Customer Name> 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 <Chosen Standard> compliance smooth and trouble-free.

DRAFT

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 organisations 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

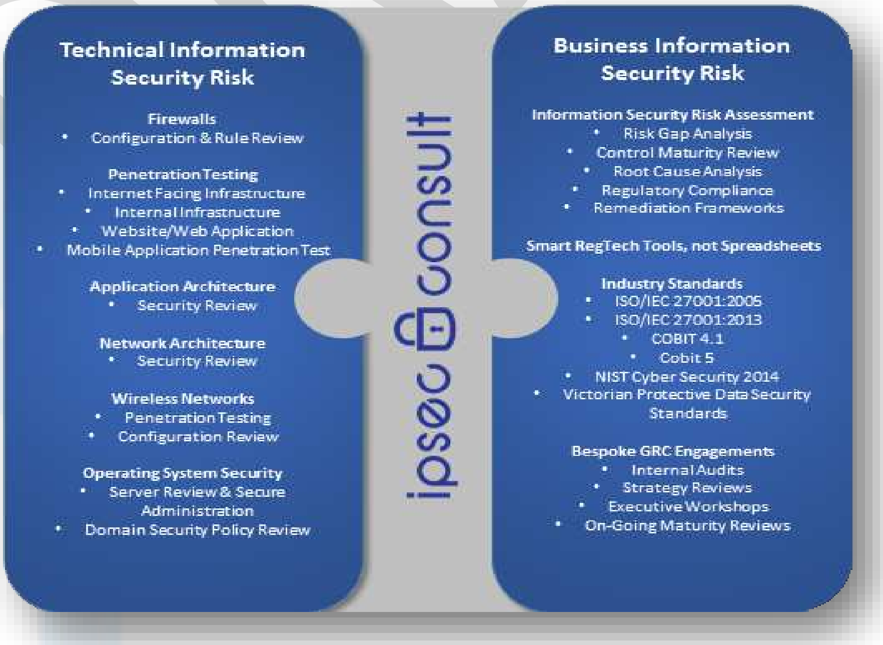
IPSec Consult is a division of IPSec that concentrates on Information and Cyber Security Risk. Our team of expert Risk Management consultants are dedicated to helping our clients mitigate risks to their Information Security environments and general Cyber Security concerns.

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.

DRAFT



Technical Information Security Risk

Firewalls
- Configuration & Rule Review

Penetration Testing
- Internet Facing Infrastructure
- Internal Infrastructure
- Website/Web Application
- Mobile Application Penetration Test

Application Architecture
- Security Review

Network Architecture
- Security Review

Wireless Networks
- Penetration Testing
- Configuration Review

Operating System Security
- Server Review & Secure Administration
- Domain Security Policy Review

Business Information Security Risk

Information Security Risk Assessment
- Risk Gap Analysis
- Control Maturity Review
- Root Cause Analysis
- Regulatory Compliance
- Remediation Frameworks

Smart RegTech Tools, not Spreadsheets

Industry Standards
- ISO/IEC 27001:2005
- ISO/IEC 27001:2013
- COBIT 4.1
- Cobit 5
- NIST Cyber Security 2014
- Victorian Protective Data Security Standards

Bespoke GRC Engagements
- Internal Audits
- Strategy Reviews
- Executive Workshops
- On-Going Maturity Reviews

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.

DRAFT

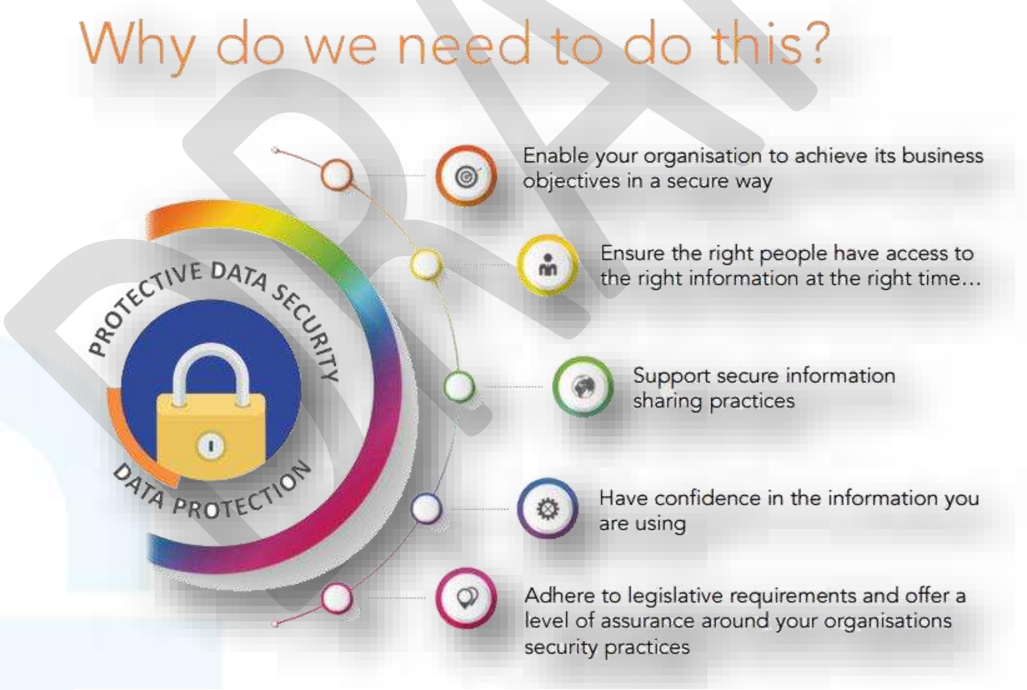

Why do we need to do this?
PROTECTIVE DATA SECURITY
DATA PROTECTION
Enable your organisation to achieve its business objectives in a secure way
Ensure the right people have access to the right information at the right time…
Support secure information sharing practices
Have confidence in the information you are using
Adhere to legislative requirements and offer a level of assurance around your organisations security practices

Figure 1- Image Credit: Commissioner for Privacy and Data Protection.

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.

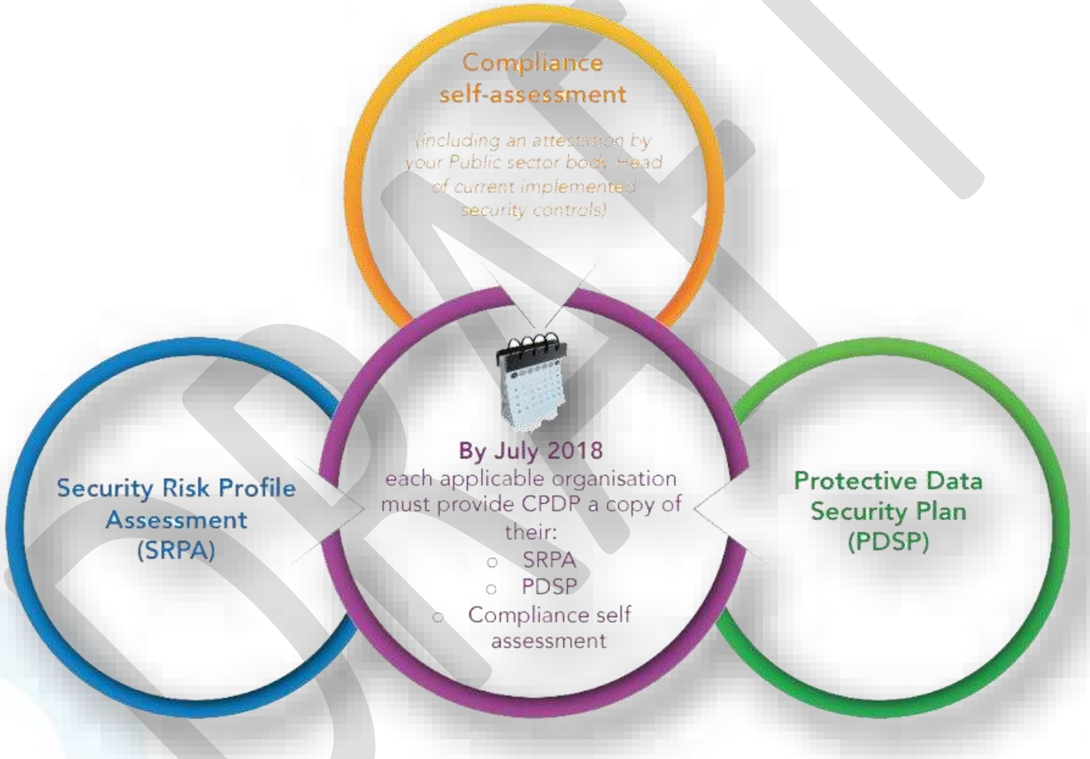

Compliance self-assessment
(including an attestation by your Public sector body Head of current implemented security controls)
Security Risk Profile Assessment (SRPA)
By July 2018
each applicable organisation must provide CPDP a copy of their:
○ SRPA
○ PDSP
○ Compliance self assessment
Protective Data Security Plan (PDSP)

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

DRAFT

Proposal Detail - Delivering your VPDSS Compliance

The Commissioner for Privacy and Data Protection’s Five Step Action Plan

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

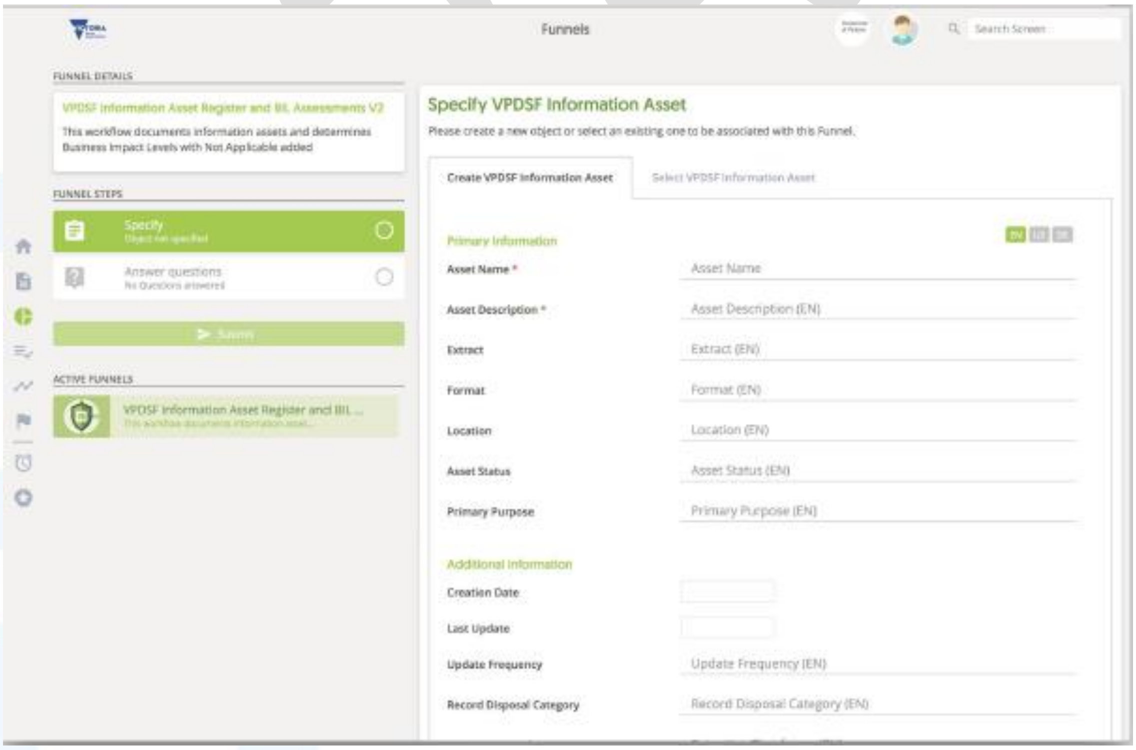
DRAFT

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.



VPDSF Information Asset Register and BIL Assessments V2

This workflow documents information assets and determines Business Impact Levels with Not Applicable added

Specify
Object not specified

Answer questions
No Questions answered

VPDSF Information Asset Register and BIL ...
This workflow documents information asset...

Specify VPDSF Information Asset

Please create a new object or select an existing one to be associated with this Funnel.

Create VPDSF Information Asset | Select VPDSF Information Asset

Primary Information

Asset Name * — Asset Name

Asset Description * — Asset Description (EN)

Extract — Extract (EN)

Format — Format (EN)

Location — Location (EN)

Asset Status — Asset Status (EN)

Primary Purpose — Primary Purpose (EN)

Additional Information

Creation Date

Last Update

Update Frequency — Update Frequency (EN)

Record Disposal Category — Record Disposal Category (EN)

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

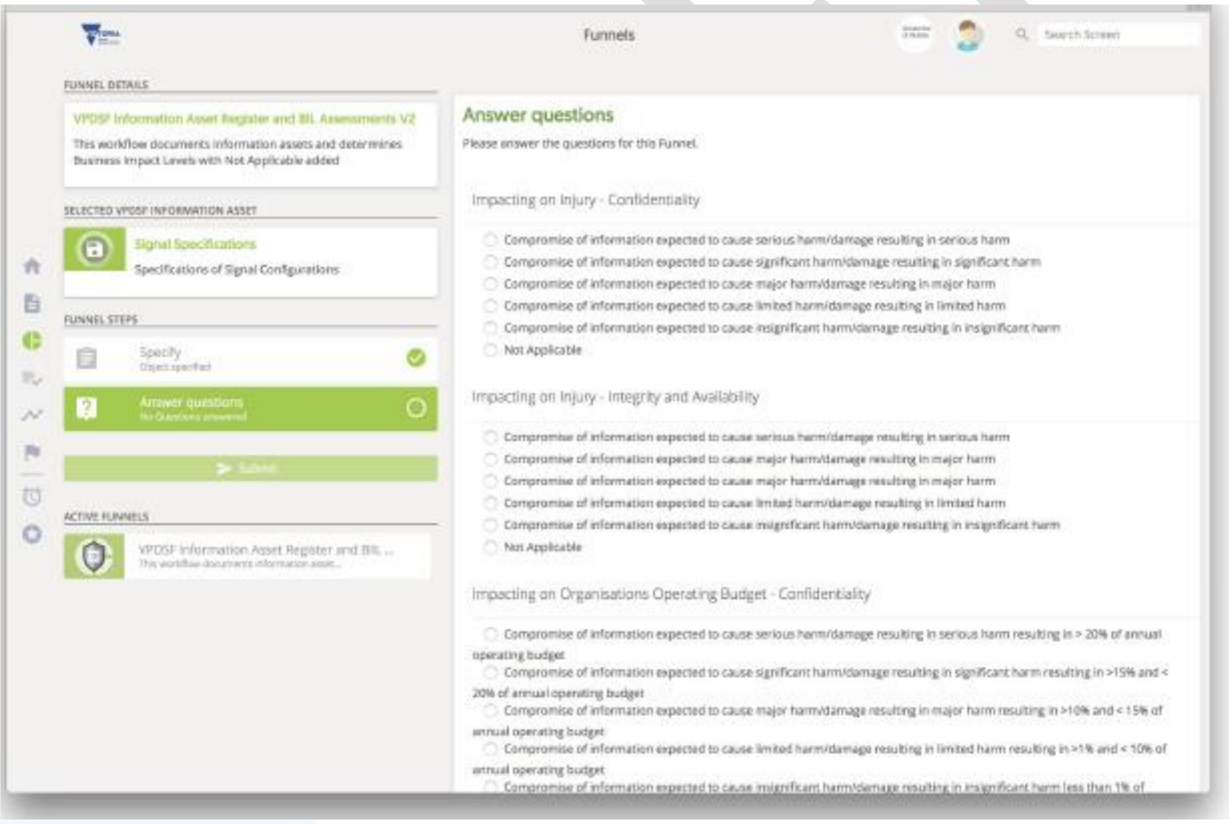
The objective of this exercise is to:

- 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



VPDSF Information Asset Register and BIL Assessments V2

This workflow documents information assets and determines Business Impact Levels with Not Applicable added

Signal Specifications

Specifications of Signal Configurations

VPDSF Information Asset Register and BIL ...

This workflow documents information asset...

Answer questions

Please answer the questions for this Funnel.

Impacting on Injury - Confidentiality

○ Compromise of information expected to cause serious harm/damage resulting in serious harm
○ Compromise of information expected to cause significant harm/damage resulting in significant harm
○ Compromise of information expected to cause major harm/damage resulting in major harm
○ Compromise of information expected to cause limited harm/damage resulting in limited harm
○ Compromise of information expected to cause insignificant harm/damage resulting in insignificant harm
○ Not Applicable

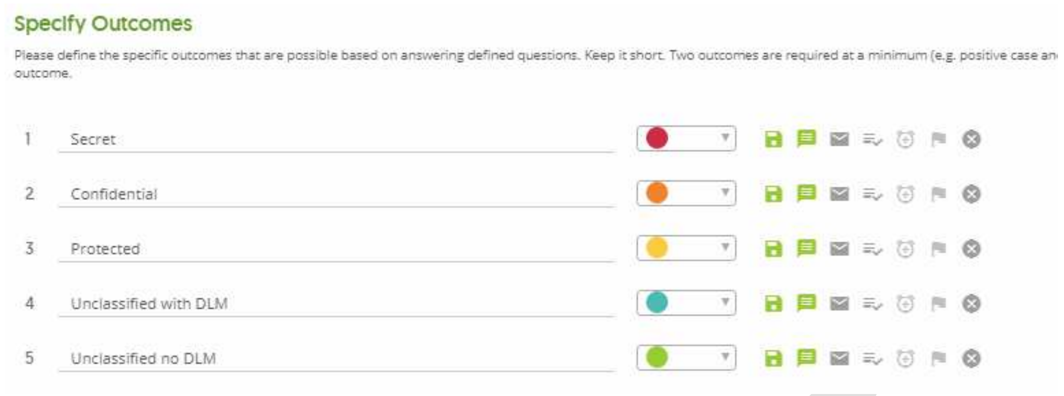
Impacting on Injury - Integrity and Availability

○ Compromise of information expected to cause serious harm/damage resulting in serious harm
○ Compromise of information expected to cause major harm/damage resulting in major harm
○ Compromise of information expected to cause major harm/damage resulting in major harm
○ Compromise of information expected to cause limited harm/damage resulting in limited harm
○ Compromise of information expected to cause insignificant harm/damage resulting in insignificant harm
○ Not Applicable

Impacting on Organisations Operating Budget - Confidentiality

○ Compromise of information expected to cause serious harm/damage resulting in serious harm resulting in > 20% of annual operating budget
○ Compromise of information expected to cause significant harm/damage resulting in significant harm resulting in >15% and < 20% of annual operating budget
○ Compromise of information expected to cause major harm/damage resulting in major harm resulting in >10% and < 15% of annual operating budget
○ Compromise of information expected to cause limited harm/damage resulting in limited harm resulting in >1% and < 10% of annual operating budget
○ Compromise of information expected to cause insignificant harm/damage resulting in insignificant harm less than 1% of

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



Specify Outcomes

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.

1 Secret ●

2 Confidential ●

3 Protected ●

4 Unclassified with DLM ●

5 Unclassified no DLM ●

A valuable addition to this workflow is the ability 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

DRAFT

Step 3 – Identify Risks to Information Assets

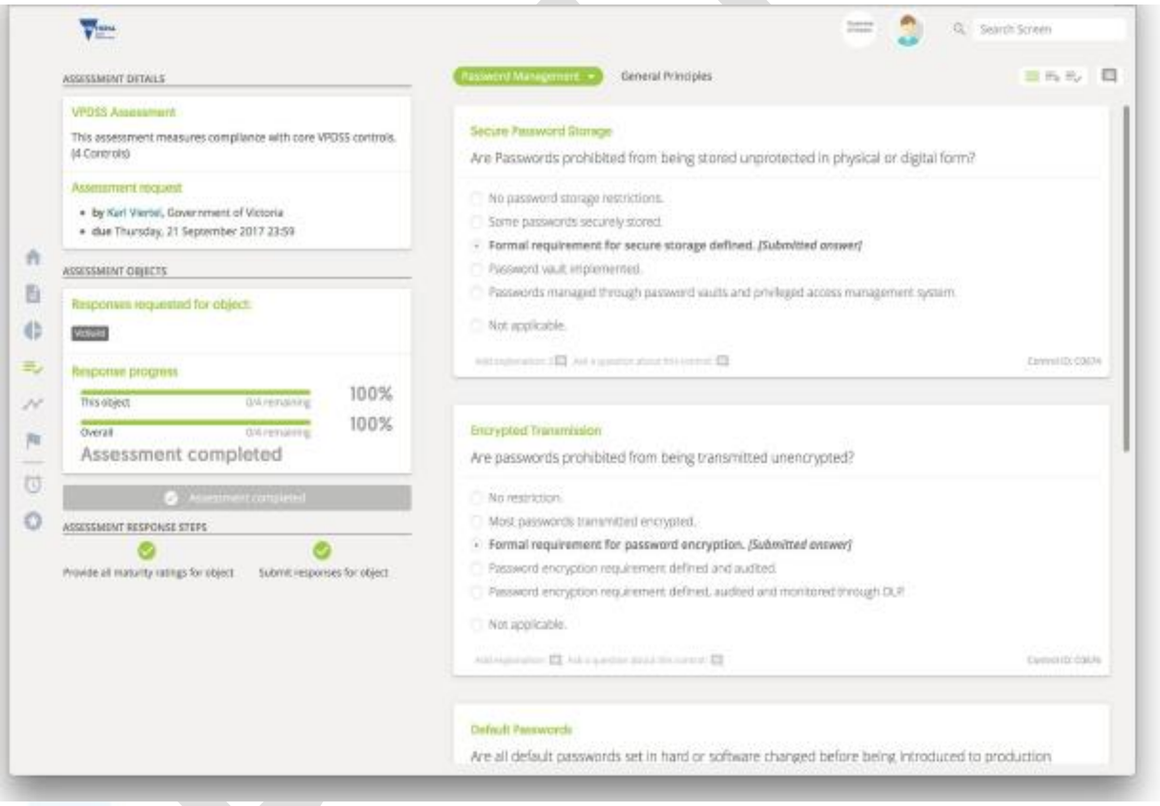
VPDSS Deliverable – Security Risk Profile Assessment (SRPA)

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



ASSESSMENT DETAILS

VPDSS Assessment

This assessment measures compliance with core VPDSS controls. (4 Controls)

Assessment request

- by Karl Viertel, Government of Victoria
- due Thursday, 21 September 2017 23:59

ASSESSMENT OBJECTS

Responses requested for object:

Response progress

This object 0/4 remaining 100%

Overall 0/4 remaining 100%

Assessment completed

ASSESSMENT RESPONSE STEPS

Provide all maturity ratings for object

Submit responses for object

Secure Password Storage

Are Passwords prohibited from being stored unprotected in physical or digital form?

○ No password storage restrictions.
○ Some passwords securely stored.
● **Formal requirement for secure storage defined. *[Submitted answer]***
○ Password vault implemented.
○ Passwords managed through password vaults and privileged access management system.
○ Not applicable.

Encrypted Transmission

Are passwords prohibited from being transmitted unencrypted?

○ No restriction.
○ Most passwords transmitted encrypted.
● **Formal requirement for password encryption. *[Submitted answer]***
○ Password encryption requirement defined and audited.
○ Password encryption requirement defined, audited and monitored through DLP.
○ Not applicable.

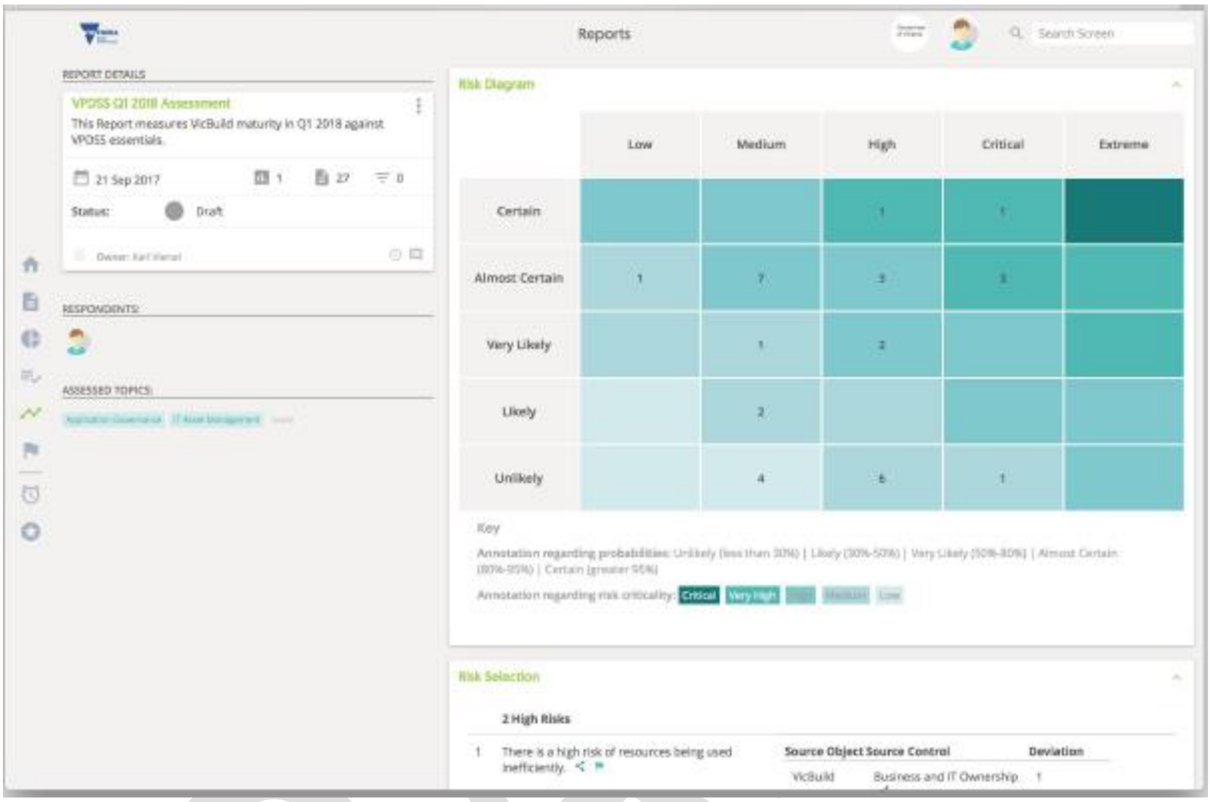
Default Passwords

Are all default passwords set in hard or software changed before being introduced to production

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



REPORT DETAILS

VPOSS Q1 2018 Assessment

This Report measures VicBuild maturity in Q1 2018 against VPOSS essentials.

21 Sep 2017 | 1 | 27 | 0

Status: ● Draft

Owner: [illegible]

RESPONDENTS:

ASSESSED TOPICS:

Risk Diagram

	Low	Medium	High	Critical	Extreme
Certain			1	1	
Almost Certain	1	7	3	3	
Very Likely		1	2		
Likely		2			
Unlikely		4	6	1	

Key

Annotation regarding probabilities: Unlikely (less than 30%) | Likely (30%-50%) | Very Likely (50%-80%) | Almost Certain (80%-95%) | Certain (greater 95%)

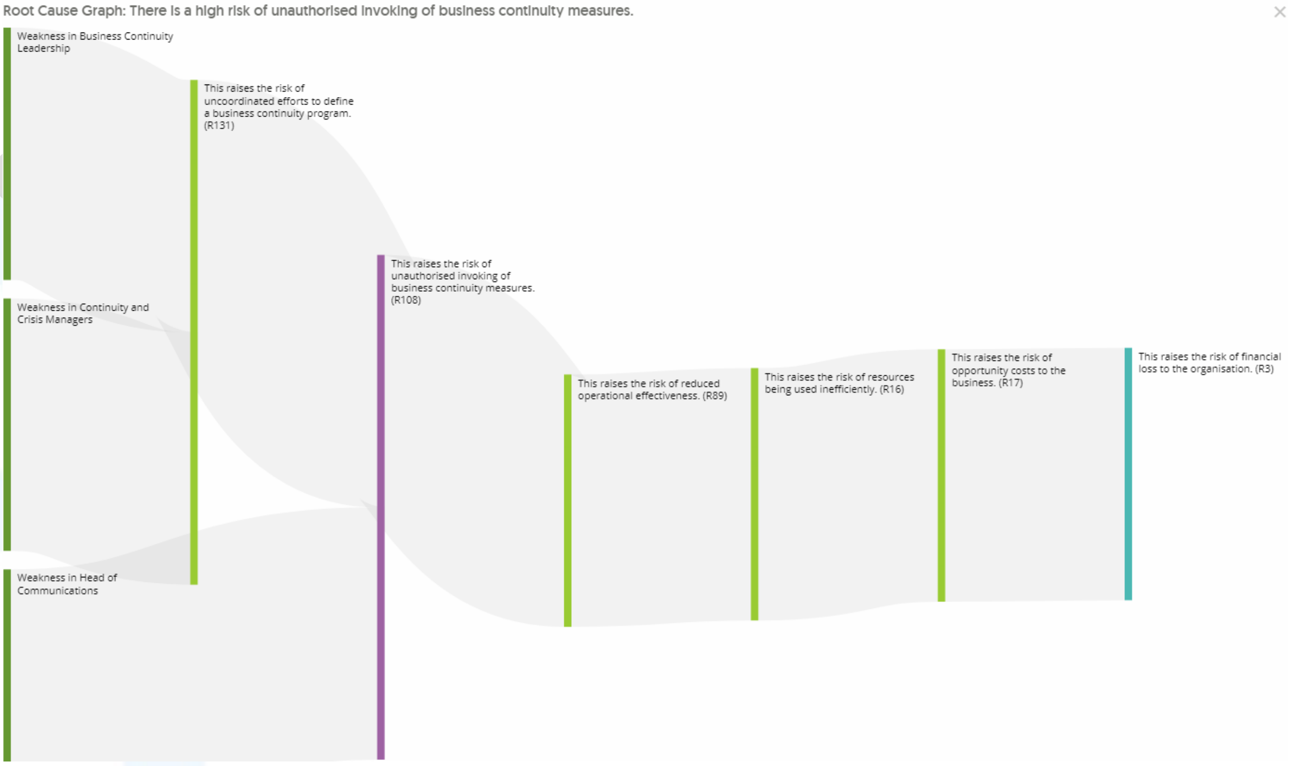
Annotation regarding risk criticality: Critical | Very High | High | Medium | Low

Risk Selection

2 High Risks

1 There is a high risk of resources being used inefficiently.

Source Object	Source Control	Deviation
VicBuild	Business and IT Ownership	1



Root Cause Graph: There is a high risk of unauthorised invoking of business continuity measures.

Weakness in Business Continuity Leadership

Weakness in Continuity and Crisis Managers

Weakness in Head of Communications

This raises the risk of uncoordinated efforts to define a business continuity program. (R131)

This raises the risk of unauthorised invoking of business continuity measures. (R108)

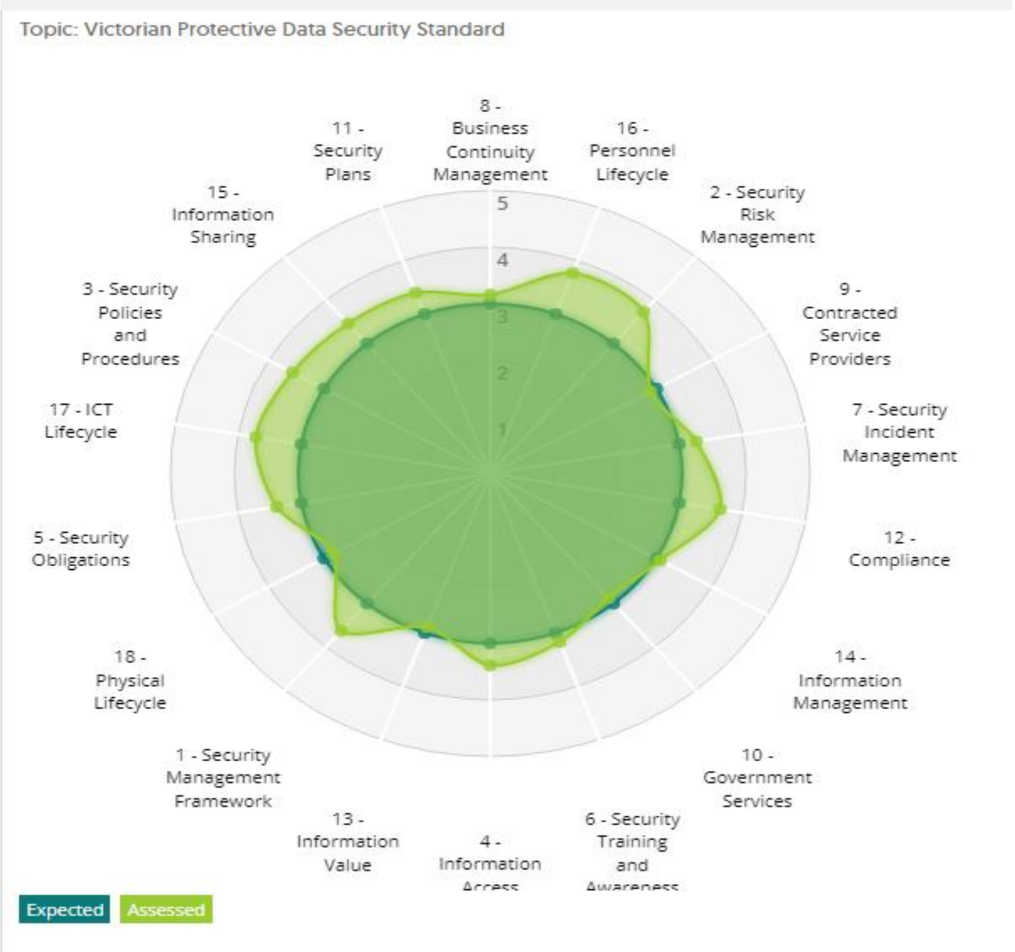
This raises the risk of reduced operational effectiveness. (R89)

This raises the risk of resources being used inefficiently. (R16)

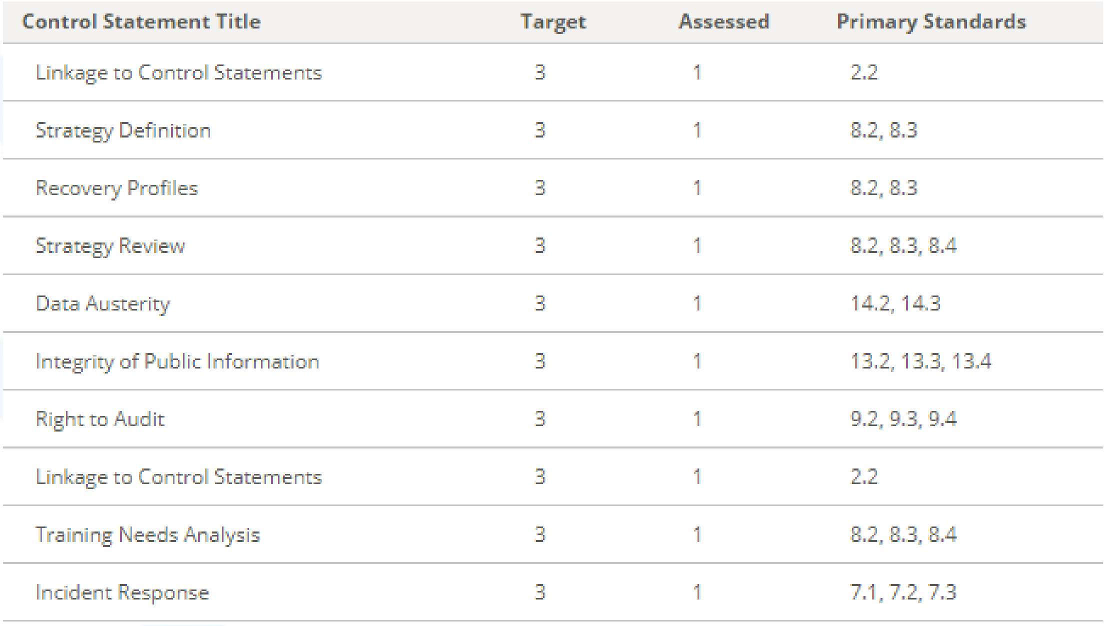
This raises the risk of opportunity costs to the business. (R17)

This raises the risk of financial loss to the organisation. (R3)

4) Review the Gap between Expected and Assessed Outcomes



5) Link back to VPDSS Standards to drive remediation plans



Control Statement Title	Target	Assessed	Primary Standards
Linkage to Control Statements	3	1	2.2
Strategy Definition	3	1	8.2, 8.3
Recovery Profiles	3	1	8.2, 8.3
Strategy Review	3	1	8.2, 8.3, 8.4
Data Austerity	3	1	14.2, 14.3
Integrity of Public Information	3	1	13.2, 13.3, 13.4
Right to Audit	3	1	9.2, 9.3, 9.4
Linkage to Control Statements	3	1	2.2
Training Needs Analysis	3	1	8.2, 8.3, 8.4
Incident Response	3	1	7.1, 7.2, 7.3

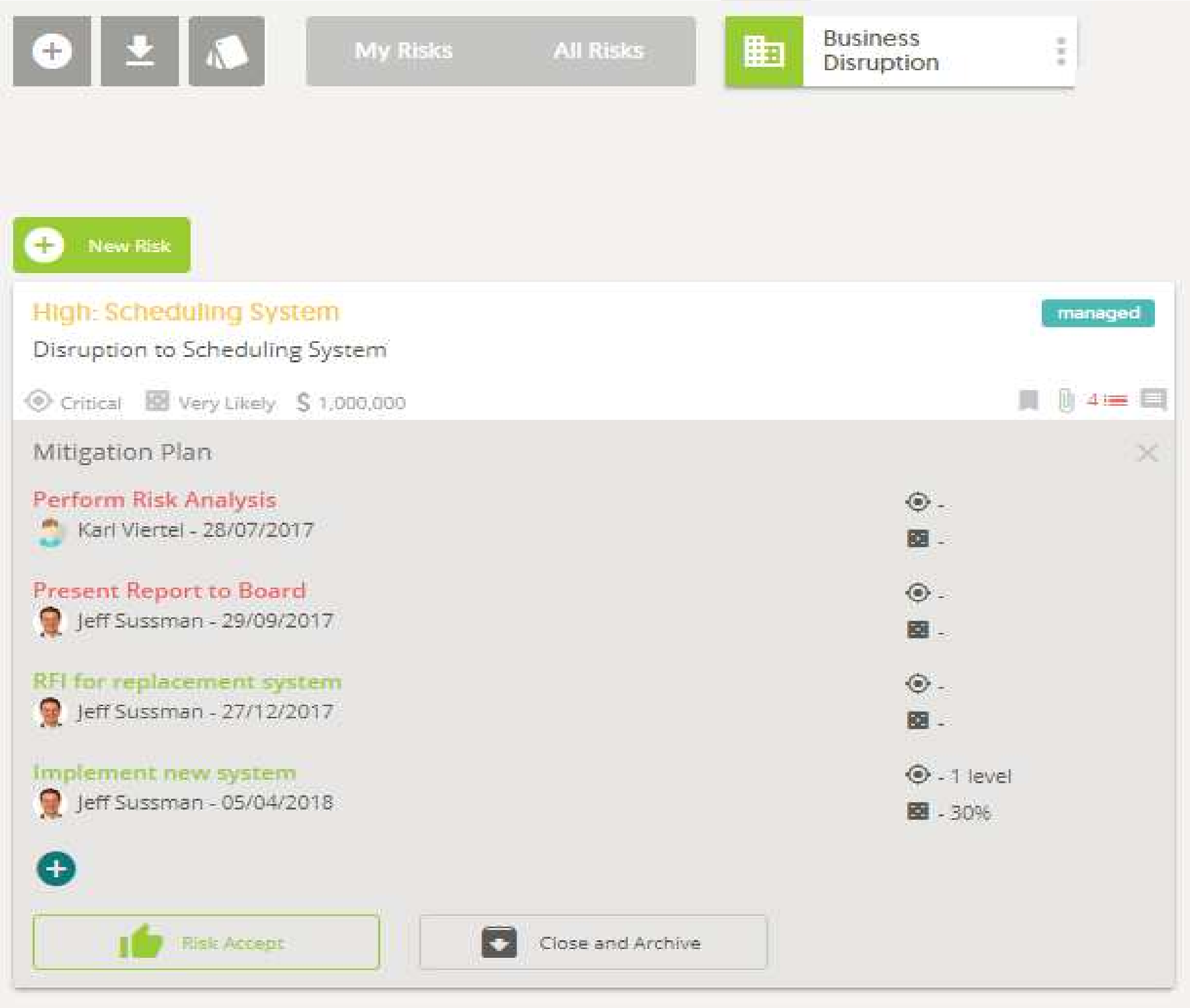
Step 4 – Apply Security Measures to Protect the Information Assets

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



High: Scheduling System

managed

Disruption to Scheduling System

Critical Very Likely $ 1,000,000 4

Mitigation Plan

Perform Risk Analysis
Karl Viertel - 28/07/2017 -
-

Present Report to Board
Jeff Sussman - 29/09/2017 -
-

RFI for replacement system
Jeff Sussman - 27/12/2017 -
-

Implement new system
Jeff Sussman - 05/04/2018 - 1 level
- 30%

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

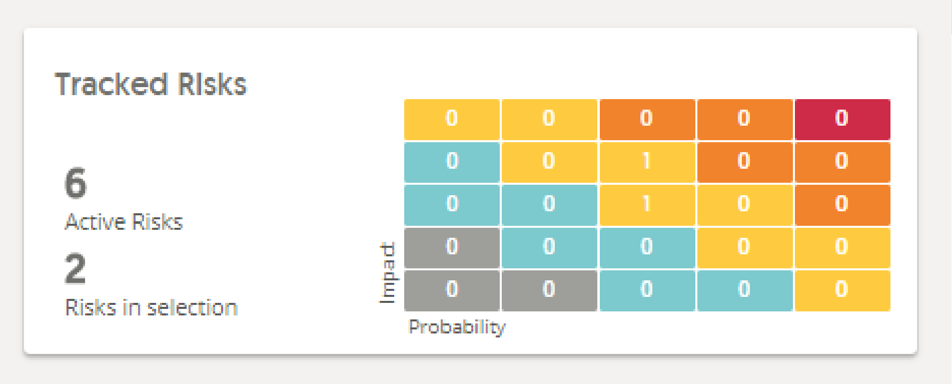
The philosophy of the Risk Dashboard is that managing risk should be a daily activity, in a similar manner to checking email or social media feeds. This way, risk management is performed in small, bite sized pieces that are manageable and non-intrusive.

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 <Customer Name> risk profile.

The components of the Risk Dashboard are as follows:

Heat Map



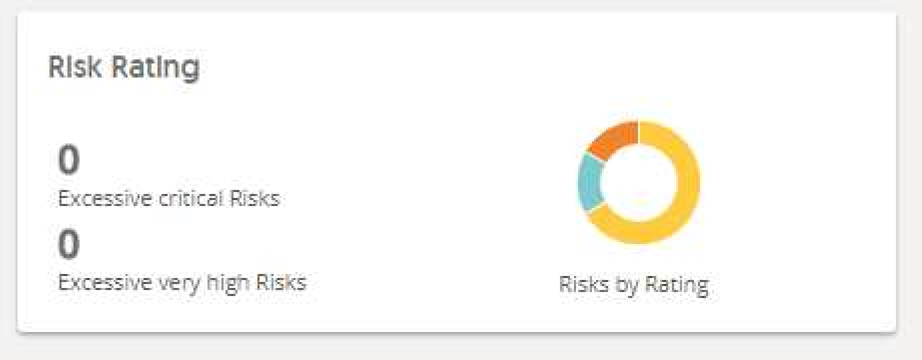
Tracked Risks

6
Active Risks

2
Risks in selection

0	0	0	0	0
0	0	1	0	0
0	0	1	0	0
0	0	0	0	0
0	0	0	0	0

Risk Rating Summary

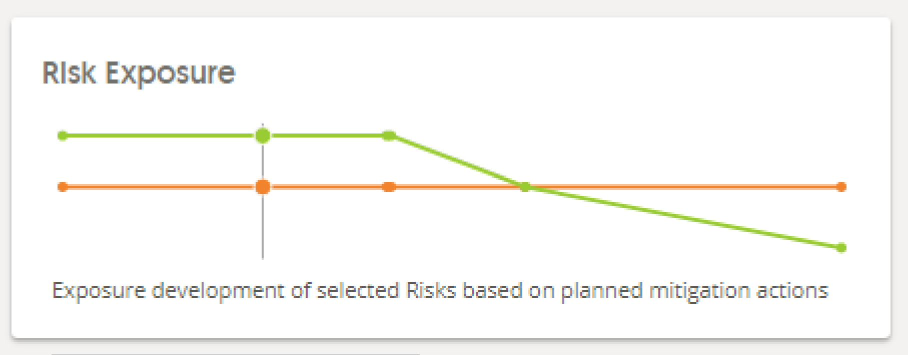


Risk Rating

0
Excessive critical Risks

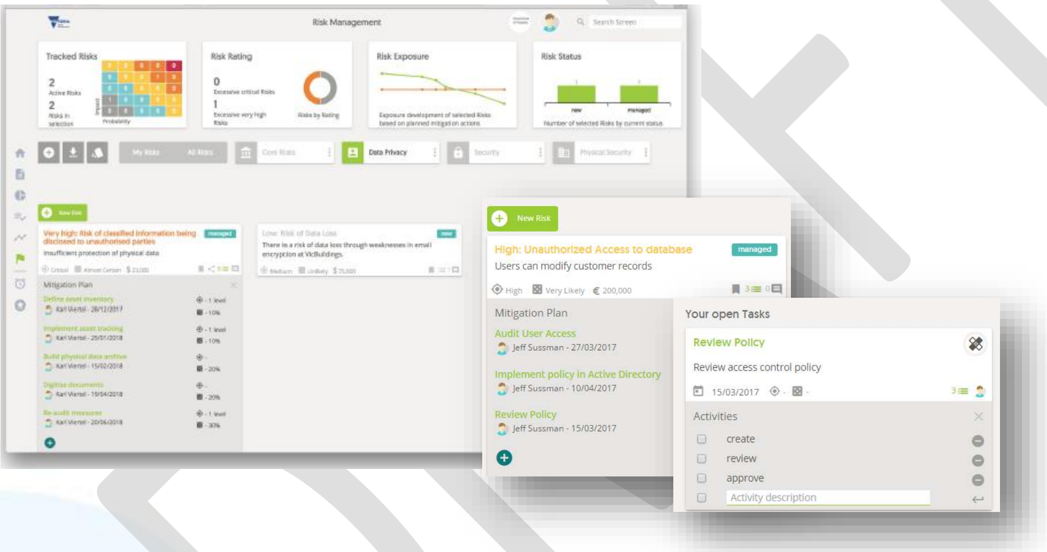
0
Excessive very high Risks

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.


Risk Management

Tracked Risks: 2 Active Risks; 2 Risks in selection

Risk Rating: 0 Excessive critical Risks; 1 Excessive very high Risks

Risk Exposure: Exposure development of selected Risks based on planned mitigation actions

Risk Status: Number of selected Risks by current status

Very high: Risk of classified information being disclosed to unauthorised parties — managed
Insufficient protection of physical data

Mitigation Plan
Define asset inventory — Karl Wiertel - 28/12/2017
Implement asset tracking — Karl Wiertel - 25/01/2018
Build physical data archive — Karl Wiertel - 15/02/2018
Digitise documents — Karl Wiertel - 10/04/2018
Re-audit measures — Karl Wiertel - 20/06/2018

Low: Risk of Data Loss — new
There is a risk of data loss through weaknesses in email encryption at VicBuildings.

High: Unauthorized Access to database — managed
Users can modify customer records
High · Very Likely · € 200,000

Mitigation Plan
Audit User Access — Jeff Sussman - 27/03/2017
Implement policy in Active Directory — Jeff Sussman - 10/04/2017
Review Policy — Jeff Sussman - 15/03/2017

Your open Tasks
Review Policy
Review access control policy
15/03/2017

Activities
□ create
□ review
□ approve
□ Activity description

Ongoing Support & After Sales Care

After the hand-over of the project to <Customer Name> 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.

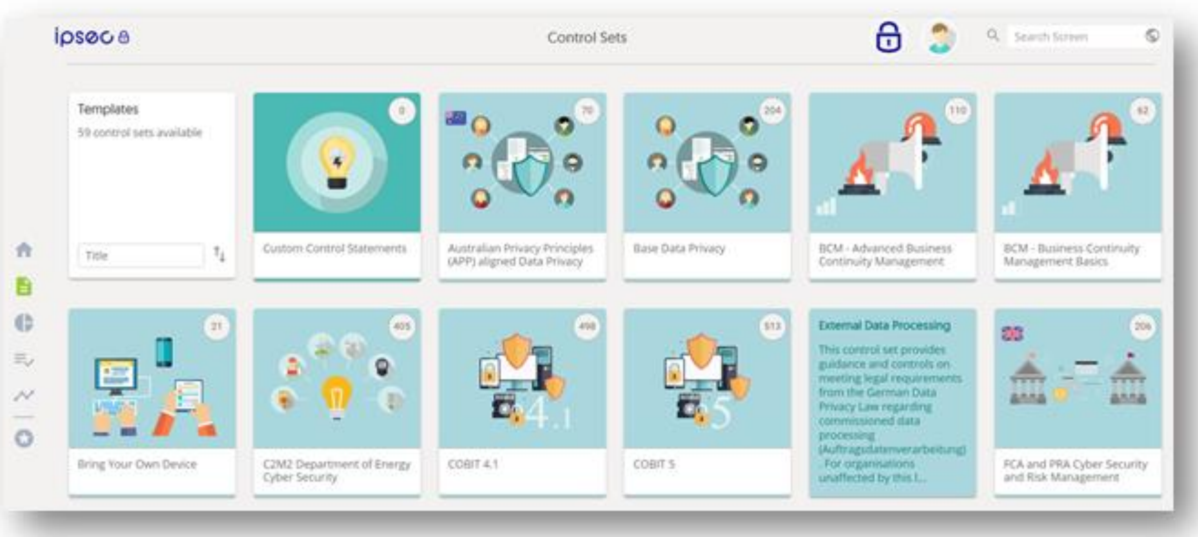
DRAFT

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.



Control Sets

Templates
59 control sets available

Custom Control Statements

Australian Privacy Principles (APP) aligned Data Privacy

Base Data Privacy

BCM - Advanced Business Continuity Management

BCM - Business Continuity Management Basics

Bring Your Own Device

C2M2 Department of Energy Cyber Security

COBIT 4.1

COBIT 5

External Data Processing

This control set provides guidance and controls on meeting legal requirements from the German Data Privacy Law regarding commissioned data processing (Auftragsdatenverarbeitung) . For organisations unaffected by this l...

FCA and PRA Cyber Security and Risk Management

DRAFT