Information Security

Information Security Management Framework

Standard

Agencies must develop an Information Security Management Framework (ISMF) and implement information security in accordance with the ISM and PSPF (as adapted to Victorian Government requirements).

Keywords:	Compliance, alignment, ISM, PSPF, ISMF.	
Identifier: SEC STD 01	**Version no.:** 3.1	**Status:** Final
Issue date: 1 October 2012	**Date of effect:** 1 June 2013	**Next review date:** 1 November 2014
Authority: Victorian Government CIO Council	**Issuer:** Victorian Government Chief Technology Advocate	

Overview

This standard mandates the use of security frameworks specified by the Australian Government, as adapted to Victorian requirements, particularly;

- the Protective Security Policy Framework (PSPF), managed by the Attorney-General's Department (AGD), insofar as it applies to Information and Communication Technology (ICT) information, people, processes and assets; the PSPF Information Security Management protocol, managed by the Attorney-General's Department (AGD);
- the Information Security Manual (ISM), managed by the Defence Signals Directorate (DSD); and
- the National eAuthentication Framework (NeAF), managed by the Australian Government Information Management Office (AGIMO).

The detail of the customisation of the ISM and the PSPF (insofar as it applies to ICT information - people, processes and assets), for use by Victorian Government agencies, is provided in Appendix 1 and Appendix 2, but in summary:

- The centralised whole-of-government ICT function (currently the Digital Government branch of the Department of State Development, Business and Innovation) is responsible for the customisation of the ISM and PSPF for use within the Victorian Government, and in this role generally acts in place of the Defence Signals Directorate (DSD) and Commonwealth Attorney-General's Department (AGD).
- The Security and Emergency Management Branch (SEMB) of the Department of Premier and Cabinet (DPC) is responsible for facilitating Victorian Government security clearances (excluding Victoria Police), and acts in place of the Australian Government Security Vetting Agency (AGSVA).
- The Victorian Auditor General's Office (VAGO) acts in place of the Australian National Audit Office (ANAO).
- The Office of the Victorian Privacy Commissioner acts in place of the Office of the Australian Information Commissioner.
- The Commissioner for Law Enforcement Data Security (CLEDS) is responsible for the enforcement of the Data Security Act 2005 which was passed by the Parliament of Victoria in November 2005 to promote the use by Victoria Police of appropriate and secure law enforcement data management practices.
- Victoria Police acts in place of the Australian Federal Police where appropriate.
- Victorian legislation complements or replaces Commonwealth legislation, as appropriate.
- References to 'Australia' are replaced by references to 'Victoria' where appropriate e.g. 'Victorian Government' replaces 'Australian Government', 'Victorian Public Service' replaces 'Australian Public Service', etc.

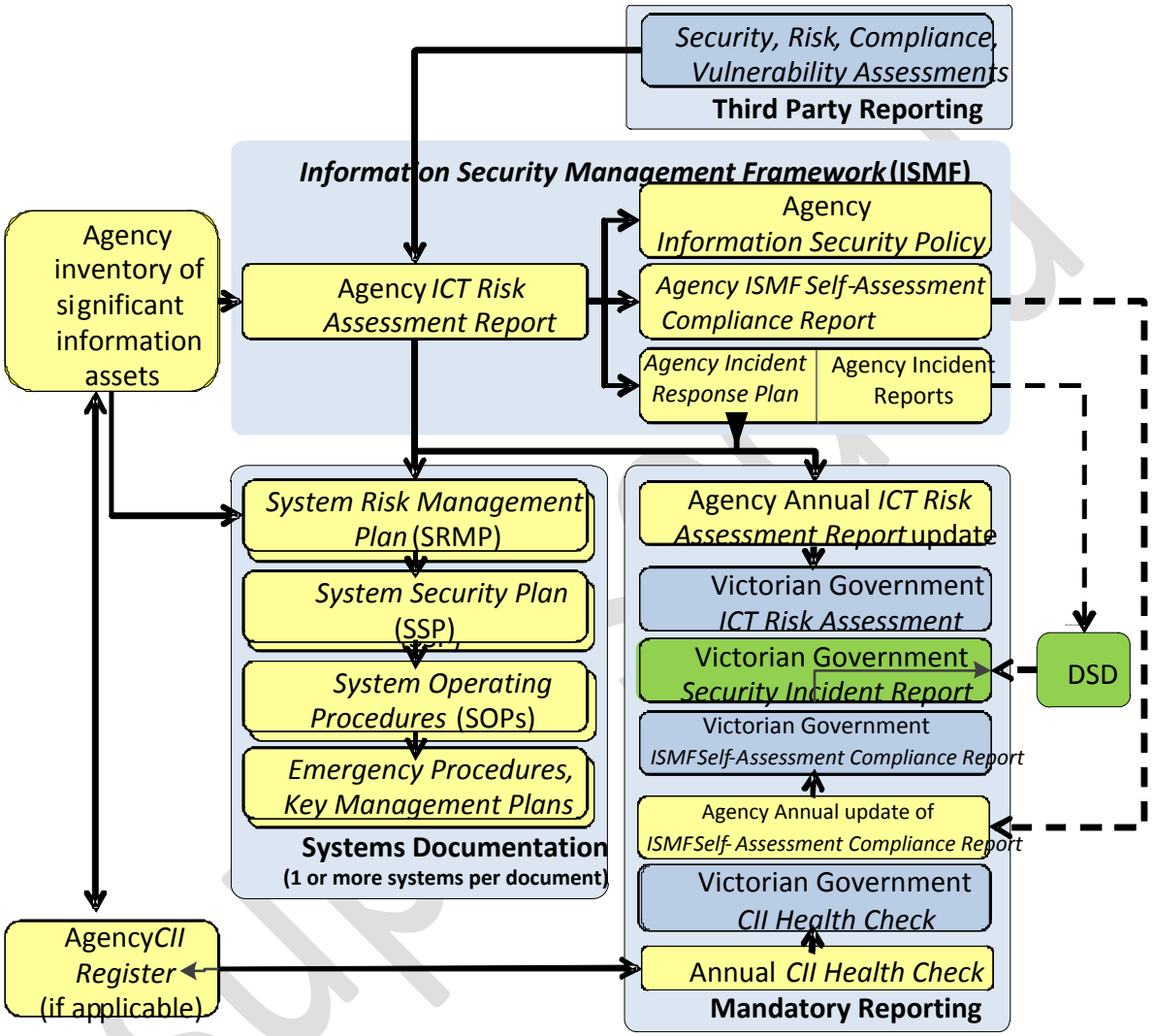
Agencies must develop[1] an *Information Security Management Framework* (ISMF) which will show the progression of the agency over time toward compliance with the Victorian customisation of the ISM and PSPF

[1] Departments and Agencies should / may reuse and update their existing security information / material – alignment to the new policy and standard.

(insofar as it applies to ICT information, people, processes and assets including software, equipment and computer rooms).

The agency ISMF is to consist of four key documents, as shown in Figure 1:

Figure 1: Structure of ISMF Documents, Systems Documents, and Reporting



Legend: Yellow box - D & A activities ; Blue box - Aggregated Compliance Reporting ; Green box - Commonwealth Government ;

Note: *Agency* in figure 1 above refers to Departments and Agencies - it covers the 15 Inner Budget departments and agencies (D&A), and CenITex (collectively referred to as agencies' hereafter).

1. An ***ICT Risk Assessment Report*** (or equivalent) – A risk assessment performed on the agency's ICT information, people, processes, and assets.
   - For agencies which have a high number of critical information infrastructure (CII - see *SEC STD 02 Critical Information Infrastructure Risk Management*), the scope of the initial draft of this report can be limited to an assessment of CII only, but this must be expanded to all significant information assets in subsequent reports. In this case, a key input to this report will be a list of the CII assets within the

agency.
- For agencies with little or no CII, the scope of the *ICT Risk Assessment Report* should encompass all significant ICT assets within the agency. (Significant information assets are those which are crucial to the achievement of an agency's mission i.e. if these assets are compromised, the agency's ongoing ability to meet its goals and objectives will be affected.)
(**Note**: An ICT *Risk Assessment Report* should already exist as a result of SEC POL 01. Departments and Agencies should consult with their D&A Risk Managers when assessing or re-assessing ICT risks and refer to the Victorian Government Risk Management Framework)

2. An ***Information Security Policy*** (or equivalent) – A high level security document covering the principal information security objectives of the agency (informed by the *ICT Risk Assessment Report*); how they will be achieved; the guidelines and legal framework under which the agency's policy will operate; and how compliance with the agency information security policy will be measured internally.
(**Note**: An *Information Security Policy* should already exist under SEC POL 01).

3. An *ISMF* ***Self-Assessment Compliance Report*** (or equivalent) – In the context of the relevant Mandatory Requirement statements in the PSPF, agencies will complete a self-assessment report (a Statement of Compliance / Compliance Plan[2]). On the basis of this self-assessment (the ISMF Self-Assessment Compliance Report) a Compliance Plan will be developed to address any significant non-compliance issues. Where applicable, this Compliance Plan will also include the actions D&A intend to take to address any gaps identified in the *CII Health Check* report (see *SEC STD 02 Critical Information Infrastructure Risk Management*).

4. An ***Incident Response Plan*** (or equivalent) – What constitutes an information security incident; the minimum level of security incident response and investigation training for users and system administrators; the authority responsible for initiating investigations of information security incidents; the steps necessary to ensure the integrity of evidence supporting an investigation; the steps necessary to ensure that CII remain operational; and how to report information security incidents. DSD's OnSecure online incident reporting application must be used; and, any internal Incident Response register(s). See DSD's ISM Controls – Cyber Security Incidents.

Agencies must develop their ISMF and implement information security in accordance with the ISM and PSPF (as adapted to Victorian Government requirements). In addition, the following system- level documents must be in place:

- A *System Risk Management Plan* (SRMP), a *System Security Plan* (SSP), and *System Operating Procedures* (SOPs). At a minimum, agencies must prepare these documents (or their equivalents) for all significant information assets. For agencies with significant levels of CII, initial SRMPs and SSPs may be limited to CII only, but coverage must be expanded to all significant information assets. . For efficiency, agencies may include multiple similar systems in the one set of system documentation, if this is practical.

- For cryptographic functions, which are important to the security of sensitive information*, Key Management Plans* (or equivalents) must be developed which define how cryptographic keys will be protected from compromise. Similarly, *Emergency Procedures* (or equivalents) will be required to ensure protection of systems in the event that a computer room or other secure area has to be evacuated in an emergency.

- Other documents required under the ISM should already exist, and they should require no (or only minor) change e.g. *Business Continuity Plans*, and *Disaster Recovery Plans* (or equivalents).

[2] Statement of Compliance and Compliance Plan are ISO terms.

Where agencies elect not to comply with the requirements of the PSPF and/or ISM, they must seek approval for the non-compliance from their Agency Head (or his/her delegate).

Rationale

Refer to *SEC POL 01 Information Security Management Policy.*

Derivation

This Standard supports the revised and approved Victorian Government *SEC POL 01 Information Security Management Policy,* which requires agencies to implement a revised set of approved Victorian Government policies, standards and guidelines for information security. In particular, Departments and Agencies must implement this standard, which requires adoption of the PSPF and ISM.

Scope

The scope of this standard is the governance and processes required to establish, implement, operate, monitor, maintain and improve the effectiveness of an agency's Information Security Management System (ISMS).

This standard applies to the management of all aspects of information security. It includes procedures, assessments, tools and documentation. It is to be used by all eleven departments; the inner budget agencies i.e. Victoria Police, VicRoads, State Revenue Office, and the Environment Protection Authority; and any shared services providers (third parties)[3] including CenITex. These organisations are collectively referred to as department and agencies (D&A) in this standard.

Where applicable, legal and or regulatory compliance obligations take precedence over this policy and standards. Departments and agencies may have additional legal and or regulatory information protection compliance requirements. Examples include (but are not limited to) Victoria Police and the Commissioner for Law Enforcement Data Security (CLEDS), credit card processing contract obligations of the Payment Card Industry Data Security Standard (PCI DSS) and the Information Privacy Act 2000.

Compliance

Timing

Progressive compliance with this standard is required from the 'Date of Effect' (see front page).

Information security reporting to DSDBI and D&A executives

Annual D&A ISMF self-assessment compliance report

Annual reports are due on 30 May to DSDBI. The report requires the completion of templates (or equivalents).

[3] Some examples of shared service provider within Victorian Government are CenITex, eduPay and Shared Business Systems (SBS). D&A's may have third parties providing similar services.

Where appropriate, D&A reports will be consolidated into a Victorian Government summary for consideration by the Deputy Secretary Leadership Group (DSLG) and the CIO Council.

The annual D&A reporting will:

- support the annual executive risk management assurance requirement of attesting to the adequacy of risk management practices and controls, and
- fulfil commitments made by DTF and DPC in response to the VAGO Performance Audit, (November 2009), *Maintaining the Integrity and Confidentiality of Personal Information.*

ICT risk assessment report

As shown in Figure 1, D&A will be required to complete a mandatory annual update of the *ICT Risk Assessment Report (update the last risk assessment)*, which should reflect an ongoing reduction in residual risk, due to the implementation of the additional risk mitigations planned in the previous ICT Risk Assessment Report and in the *ISMF Self-Assessment Compliance Report.*

This annual update will inform a brief that must be submitted to the D&A Secretary, Risk and/or Audit committee, and the agency Executive. A copy of the brief must be provided.

The content of the Brief is to address the following issues:

- Based on DSD advice, a description of the current threat environment and applicability to agency
- A description of the "AS IS" agency capability to mitigate the current cyber security threat landscape and the level of maturity of agency cyber controls
- A description of the most critical 5 ICT Security Risks and the most at risk data/systems (and CII if in scope)
- A summary of agency compliance with the PSPF, identifying any systemic non-compliance issues and vulnerabilities
- An assessment of additional security measures required within very/ high risk areas
- Annual information security program past 12 months ,(what has been achieved) & next 12 months plan + funded activity

Information security incident reporting

As shown in Figure 1, agencies will make mandatory information security incident reports to DSD (using DSD's web-based OnSecure incident application reporting at http://www.dsd.gov.au/infosec/reportincident.htm).

DSD will provide a six monthly report and analysis of all Victorian Government information security incidents to DSDBI, who will submit it to the CIO Council for consideration.

ICT Risk Mitigation Strategies

Information security risk mitigation priorities are informed by the qualitative *ICT Risk Assessment Report*, regulatory and compliance requirements, and internal and external audit recommendations.

The ISM provides –D&A with a set of detailed controls that can be implemented to mitigate risks to their information and systems. D&A are encouraged to make informed, risk-based decisions specific to their unique environments, circumstances and risk appetite.

As the practice of information security has matured, there is an emerging body of quantitative and evidence based information to support specific risk mitigation recommendations and controls.

DSDBI (on advice from DSD), and working through the Victorian Government governance structures, will release mandatory ICT risk mitigation standards in response to authoritative and evidence based advice from DSD.

The initial mandatory requirement is to support the mitigation of targeted cyber threats. All D&A are to:

- implement DSD's *Top 4 Strategies to Mitigate Targeted Cyber Intrusions* (including any future updates to these Top 4 mitigations), and
- give appropriate consideration to the more extensive list contained in DSD's *Top 35 Mitigation Strategies*.

The impact of these risk mitigations should be recorded in the *ICT Risk Assessment Report*, and compliance reported in the *CII Health Check* (see *SEC STD 02 Critical Information Infrastructure Risk Management*).

Reporting by Third Party and Shared Service Providers

As input to the reporting requirements specified above, D&A must have in place adequate security Service Level Agreements (SLAs) and reporting from third party and shared service providers of ICT services.

The requirement to be applied to third parties is adequately specified in the ISM, Industry Engagement and Outsourcing.

D&A will use these reports to support the development of their annual *ICT Risk Assessment Report (as per department / agency risk guidelines)* and *ISMF Self-Assessment Compliance Report*.

The Victorian Government has established a number of government owned shared service providers. Shared services providers must provide to departments and agencies a standardised set of reports based upon the PSPF and the applicable controls of the ISM. (Individual agencies may negotiate additional specific reporting and auditing as required).

Table 1 – Summary List of Compliance Reports

	Report Name	**Deliver To**	**Due by Date**	**Frequency**
SEC STD 01 Compliance Reports				
	ISMF Self-Assessment Report	DSDBI	30 June	Annual
	• Annual Executive Information Security Brief	D&A Secretary & relevant committees DSDBI	30 June	Annual

	Report Name	Deliver To	Due by Date	Frequency
	Information Security Incidents	DSD	ongoing	At time of Incident Occurring
	DSD provided Information Security Incident Report	DSDBI & D&A	July & Jan / Feb	Half yearly - Aggregate Report
SEC STD 02 CII Security Reports				
	CII Health Check (Statement of Compliance and Compliance Plan	DSDBI & D&A internal governance committee(s)	1 Dec	Annual (December)

Reference and Toolkits

Guidelines and templates will be developed to support this standard. They will include

- templates for the key documents in the ISMF (*Information Security Policy*, and *ISMF Self-Assessment Compliance Report*, and related tools e.g. a self-assessment tool for compliance with the PSPF and ISM; and
- other templates, guidelines and tools as new policies, standards are released, and amended templates, guidelines and tools as existing Victorian Government policies and standards are amended.

Defence Signals Directorate (DSD) Information Security Manual (ISM) March 2012 and Australian Government Information Security Management Protocol: http://www.dsd.gov.au/infosec/ism/index.htm

Information on the development of security risk management plans can be found in the Information Security Risk Management Guidelines available from Standards Australia at: http://www.standards.org.au

Information relating to the Information Security Management Framework is contained in the Australian Government Information Security Management Protocol of the Protective Security Policy Framework.

Protective Security Policy Framework (PSPF), June 2011 and PSPF Glossary of Terms:
http://www.protectivesecurity.gov.au/Pages/default.aspx
http://www.protectivesecurity.gov.au/pspf/Pages/PSPF-Glossary-of-terms.aspx

Information regarding cloud computing security considerations can be found on the DSD website at:
http://www.dsd.gov.au/infosec/cloudsecurity.htm

National eAuthentication Framework (NeAF): http://agimo.gov.au/files/2012/04/NeAFFramework.pdf

Defence Signals Directorate (DSD) – Incident Reporting using DSD's web-based incident reporting application OnSecure at: http://www.dsd.gov.au/infosec/reportincident.htm

Victorian Government Risk Management Framework (VGRMF):
http://www.dtf.vic.gov.au/Publications/Victoria-Economy-publications/Victorian-risk-management-framework-and-insurance-management-policy

Further information

For further information regarding this standard, please contact digital.government@dsdbi.vic.gov.au.

Glossary

Term	Meaning
Agency	refers to the 15 Inner Budget departments and agencies (D&A), and CenITex
AGSVA	Australian Government Security Vetting Agency
ASA	Agency Security Advisor
CenITex	Centre for Information Technology Excellence
CII (Critical information infrastructure)	ICT infrastructure upon which critical services are delivered to the community. If this ICT infrastructure is compromised, serious damage could be caused to the State of Victoria, the government, commercial entities or members of the public.
Common Criteria	The security evaluation of ICT systems under the international *Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security*.
CORG	Customer Operational Review Group (CenITex)
D&A	Department and Agencies (all inner budget departments plus EPA, SRO, VicRoads, VicPol and CenITex.
DPC	Department of Premier and Cabinet
DSD	Defence Signals Directorate
DSDBI	Department of State Development, Business and Innovation
ICT	Information and Communications Technology
ISMF	Information Security Management Framework
ISMS	Information Security Management System
SAC	Stakeholder Advisory Group (CenITex)
SEMB	Security and Emergency Management Branch
Shared Service Provider	Some examples of shared service provider within Victorian Government are CenITex, eduPay and Shared Business Systems (SBS).

Term	Meaning
Significant information assets	Those information assets which are crucial to the achievement of an agency's mission i.e. if these information assets are compromised, the agency's ongoing ability to meet its goals and objectives will be compromised.
Third Parties	A third party supplier (commercial service provider) which is independent of the primary supplier and customer of information technology services or products.
VG	Victorian Government
VMIA	Victorian Managed Insurance Authority
VGRMF	Victorian Government Risk Management Framework

Version history

Version	Date	TRIM ref	Details
1.0	July 2005	N/A	First promulgated
2.0	9 April 2009	D09/123995	Added reporting requirement, and updated references
2.1	20 May 2010	D09/123995	Specification of reporting dates and templates
2.2	24 March 2011	D09/123995	Aligning reporting to 30 June
2.3	14 May 2012	N/A	Draft of alignment with PSPF and ISM
2.4	17 July 2012	D12/149376	Final revisions prior to submission for Board approval
3.0	31 August 2012	D12/149376	Final text revisions for release to CIO Council
3.1	1 March 2013	D13/45425	Revised as per ISAG feedback

Appendix 1: Customisation details – PSPF

Conceptually the full scope of the PSPF applies to all agency people, processes and assets (including agency business offices). However, the Victorian Government has not accepted such a wide scope. The applicability of the PSPF in this standard is only insofar as it applies to information, people, processes and assets (including software, equipment and computer rooms). Appendix 1 is guidance to be applied to a department or agencies specific situation.

As some computer rooms are located in agency offices, and defence-in-depth is used in physical security, the level of physical security provided in the agency offices which host computer rooms is still relevant to the overall physical security of information, people, processes and assets. For this reason, the full scope of PSPF customisation is provided in the tables below, despite the scope being limited to information, people, processes and assets.

Terminology

Term or Department	Applicable?	Customisation
'Australian Security Intelligence Organisation (ASIO)'	Partially	In the context of audits, reviews and related reporting, DSDBI replaces ASIO. (ASIO still has a role to play in physical security advice, etc.)
'Attorney-General's Department (AGD)'	Partially	Should generally be interpreted as 'Department of State Development, Business and Innovation (DSDBI)' as DSDBI is responsible for the customisation of the PSPF for use within the Victorian Government
'Australian'	Partially	Should be interpreted as 'Victorian' where applicable (e.g. 'Victorian Government' in place of 'Australian Government', 'Victorian Public Service' instead of 'Australian Public Service', etc.)
'Australian National Audit Office (ANAO)'	No	Should be interpreted as 'Victorian Auditor General's Office (VAGO)' where applicable
'Defence Signals Directorate (DSD)'	Partially	Information security incident reports are made directly to DSD who will provide quarterly reports to DSDBI. In the context of audits, reviews and related reporting, DSDBI replaces DSD. (DSD still has a role to play in maintaining the ISM, etc.)
'international'	Partially	Should also be interpreted as 'inter-governmental' (other States/territories), where applicable
'member of Senior Executive Service (SES)' or 'SES officer'	No	Should be interpreted as agency 'Executive Director' or equivalent
'Office of the Australian Information Commissioner'	No	Should be interpreted as 'Office of the Victorian Privacy Commissioner' where applicable
'other countries'	Partially	Should be interpreted as 'other jurisdictions' where applicable
'the Commonwealth'	No	Should be interpreted as 'the State' where applicable

Protective Security Policy Framework

Ref.	PSPF Section or Document	Applicable?	Customisation
	Protective Security Policy Framework		
1	Directive on the security of Government business	Partially	While the content is generally applicable, the authority for the Directive comes from the Victorian Government, coordinated through DSDBI.
2	Overarching Protective Security Policy Statement	Yes	
3	Protective Security Principles	Partially	The Victorian Government is responsible for customising the PSPF to its needs, coordinated through DSDBI. Victorian Government Ministers are responsible for the protective security of the agencies in their portfolio. Agency heads are responsible to their ministers for protective security within their agency.
4	Governance	Yes	
4.1	Mandatory requirements	Yes	
4.2	Overall responsibility for protective security	Partially	DSDBI is responsible for the customisation of the PSPF for use within the Victorian Government
4.3	Australian Government protective security roles and responsibilities	Partially	The roles of the Security Construction and Equipment Committee (SCEC), DSD, and the physical security advisory role of ASIO T4, are applicable to Victorian agencies. Most other roles have less relevance.
4.4	Applicability of the PSPF	Partially	References to Commonwealth Acts only apply where appropriate, and should be complemented by references to relevant Victorian legislation. The PSPF applies to all specified Victorian Government agencies.
4.5	Developing a security culture	Yes	
4.6	Security risk management	Yes	
4.7	Audit, reviews and reporting	Yes	VAGO replaces ANAO, and with the exception of direct reporting of information security incidents to DSD, DSDBI replaces AGD, DSD and ASIO

Ref.	PSPF Section or Document	Applicable?	Customisation
4.8	Security Investigations	Yes	Victoria Police replaces the Australian Federal Police, PROTECTED replaces CONFIDENTIAL, and with the exception of direct reporting of information security incidents to DSD, DSDBI replaces ASIO and DSD
4.9	Legislation	Yes	Victorian legislation complements, or replaces, Commonwealth legislation, where appropriate e.g. *Crimes Act* 1958, *Freedom of Information Act* 1982, *Information Privacy Act* 2000, *Health Records Act* 2001, *Public Records Act* 1973; Commissioner for Law Enforcement Data Security Act 2005 ('Act').
4.10	International security agreements	Yes	'other jurisdictions' replaces 'other countries' i.e. the 'international' context is largely replaced by an 'inter-government' context
4.11	Business continuity management	Yes	
4.12	Contracting	Yes	
4.13	Fraud control	Partially	Reference to Commonwealth legislation is deleted, and the *Financial Management Compliance Framework* (FMCF), Supplementary Material, *Theft and Losses*, replaces the *Commonwealth Fraud Control Guidelines*
5	Core Policies	Yes	
5.1	Personnel Security Core Policy	Yes	Security clearances must be sponsored through the Department of Premier and Cabinet (DPC Appropriate levels of vetting are required for accessing National Security Information.
5.2	Information Security Core Policy	Yes	
5.3	Physical Security Core Policy	Yes	Compliance with the *Occupational Health and Safety Act* 2004 is also required
6	Understanding the PSP and FAQs	Partially	DSDBI is responsible for the customisation of the PSPF for use in Victoria and effectively acts in place of the Attorney-General's Department (AGD)

Personnel Security

PSPF Section or Document	Applicable?	Customisation
Personnel Security Protocol		
Introduction	Partially	Relevant Victorian legislation (e.g. the *Public Administration Act* 2004) may replace the *Public Service Act* 1999
Components of personnel security	Yes	Relevant Victorian legislation (e.g. the *Public Administration Act* 2004) may replace the *Public Service Act* 1999
Personnel security risk review	Yes	
Agency-specific character (fit and proper person) employment checks	Yes	
Security clearances	Partially	Appropriate levels of vetting are required for any position accessing National Security Information. Contact DPC SEMB for advice on authorisation to waive the requirement for Australian citizenship,
Special access arrangements	Partially	The section on persons employed under the *Members of Parliament (Staff) Act* 1984 (MoPS Act) is not applicable
Overview of personnel security clearance responsibilities	Yes	In the second step the agency must advise the DPC SEMB of the clearance requirement. (The outcome of vetting will be notified via DPC, not by AGSVA).
Temporary access to classified information arrangements	Yes	The Agency Head
Identifying Designated Security Assessment Positions (DSAPs)	Yes	DSAPs are very uncommon within Victorian Government and only apply to positions handling National Security Information
Agency responsibilities in personnel security	Yes	
Transfer of security clearance	Yes	

PSPF Section or Document	Applicable?	Customisation
AGSVA and exempt agencies' management of outsourced vetting providers	Yes	The DPC SEMB acts in place of the AGSVA.
Vetting decisions – assessment of whole person	Yes	The DPC SEMB acts in place of the AGSVA.
Ongoing personnel security management ('Aftercare')	Yes	The DPC SEMB acts in place of the AGSVA. Security clearance holders are to report changes in personal circumstances to the DPC ASA.
Attachment A	Yes	
Attachment B	No	The section on persons employed under the *Members of Parliament (Staff) Act* 1984 (MoPS Act) is not applicable
Attachment C	Yes	
Attachment D	Yes	The DPC SEMB acts in place of the AGSVA.
Agency personnel security guidelines		
Personnel security risk review	Yes	
Determining the need for a security clearance	Yes	The DPC SEMB acts in place of the AGSVA.
Temporary access	Yes	The DPC SEMB acts in place of the AGSVA.
Additional agency specific character (fit and proper person) checks	Yes	The provisions of the *Information Privacy Act* 2000 also apply. Relevant Victorian legislation (e.g. the *Public Administration Act* 2004) replaces the *Public Service Act* 1999.
Agency actions when advised of the clearance outcome by AGSVA	Yes	The DPC SEMB acts in place of the AGSVA. Termination of employment is covered by the *Fair Work (Commonwealth Powers) Act* 2009
Security awareness training	Yes	
Ongoing personnel security management ('Aftercare')	Yes	Security clearance holders are to report changes in personal circumstances to the DPC SEMB , not AGVSA.
Action when a clearance subject leaves an agency	Yes	The DPC SEMB acts in place of the AGSVA.

PSPF Section or Document	Applicable?	Customisation
Attachment A	Yes	
Attachment B	Yes	
Attachment C	Yes	
Attachment D	Yes	The DPC SEMB acts in place of the AGSVA. In the second step the agency must advise the DPC SEMB of the concern. (DPC will notify the outcome of the review, not AGSVA).

Information Security

Ref.	PSPF Section or Document	Applicable?	Customisation
	Information security management protocol		
1	Status and applicability	Yes	Authority comes from the Victorian Government (coordinated through DSDBI), not the Australian Government. The protocol applies to all specified Victorian agencies
2	Terms and definitions	Yes	Some terms are substituted or added as part of the customisation of the PSPF for use by the Victorian Government. (See *Terminology* table at the beginning of this Appendix 1).
3	How this protocol fits into the PSPF structure	Yes	
4	Compliance	Yes	
4.1	Compliance with legal requirements	Yes	With the exception of direct reporting of information security incidents to DSD, reporting to DSDBI replaces requirements to report to AGD, DSD and ASIO. Reporting to VAGO replaces reporting to ANAO.
4.2	Compliance with information security core policy, mandatory requirements, protocols, standards and technical advice	Yes	
4.3	Information systems audit considerations	Yes	
5	Risk assessment and treatment	Yes	

Ref.	PSPF Section or Document	Applicable?	Customisation
5.1	Information security risk assessments	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
6	Agency information security policy and planning	Yes	
7	Information security framework and external party access	Yes	
7.1	Internal framework	Yes	
7.2	External parties	Yes	
8	Asset management	Yes	
8.1	Responsibility for assets	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
8.2	Information classification	Yes	
8.3	Business impact levels	Partially	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
8.4	Aggregation	Yes	
8.5	Foreign government information (FGI)	Yes	
8.6	Information declassification	Yes	
9	Operational security management	Yes	
9.1	Operational procedures and responsibilities	Yes	
9.2	External party service delivery management	Yes	Compliance with ACSI 53 is not required
9.3	System planning and acceptance	Yes	

Ref.	PSPF Section or Document	Applicable?	Customisation
9.4	Protection against malicious and mobile code	Yes	
9.5	Back-up	Yes	
9.6	Network security management	Yes	
9.7	Media handling	Yes	
9.8	Exchange of information	Yes	
9.9	Electronic commerce services	Yes	
9.10	Monitoring	Yes	The Public Records Office and/or the agency, replaces the National Archives of Australia where applicable.
10	Information access controls	Yes	
10.1	Business requirements for access control	Yes	
10.2	User access management	Yes	
10.3	User responsibilities	Yes	
10.4	Network access control	Yes	
10.5	Operating system access control	Yes	
10.6	Application and information access control	Yes	
10.7	Mobile computing and tele-working	Yes	Compliance with ACSI 128, 129 and 140 is not required
11	Information systems development and maintenance	Yes	
11.1	Security requirements of information systems	Yes	
11.2	Correct processing of applications	Yes	
11.3	Cryptographic controls	Yes	

Ref.	PSPF Section or Document	Applicable?	Customisation
11.4	Security of system files	Yes	
11.5	Security in development and support activities	Yes	
11.6	Technical vulnerability management	Yes	
	Australian Government security classification system		
1	Introduction	Yes	
2	Background	Yes	
3	Sensitive and security classified information		
3.1	Two types of official information	Yes	The *Information Privacy Act 2000* applies in place of the *Privacy Act* 1998
3.2	Who is responsible for the decision to apply protective markings?	Yes	
3.3	When to apply protective markings	Yes	
3.4	Confirmation of protective making	Yes	
3.5	Who can alter a protective marking?	Yes	The Public Records Office replaces the National Archives of Australia. Where applicable.
3.6	What to protectively mark	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
3.7	Over-classification	Yes	
3.8	Limiting the duration of the security classification	Yes	The *Public Records Act* 1973 replaces the *Archives Act* 1983, where applicable.
3.9	Review of security classification	Yes	

Ref.	PSPF Section or Document	Applicable?	Customisation
3.10	Agency security classification policy	Yes	
3.11	How to identify national security information	Yes	
3.12	How to identify other information to be security classified	Yes	The *Information Privacy Act 2000* replaces the *Privacy Act* 1998, and the *Public Records Act* 1973 replaces the *Archives Act* 1983. The *Health Records Act* 2001 also applies; Commissioner for Law Enforcement Data Security Act 2005 ('Act').
4	Protective markings	Yes	
4.1	How to security classify information	Yes	The Victorian Government Business Impact Levels also assist with classification (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
4.2	How to use dissemination limiting markers	Yes	The Victorian Government Business Impact Levels also assist with dissemination limiting markers (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.) The *Information Privacy Act* 2000 complements the *Privacy Act* 1998, and the *Health Records Act* 2001 also applies to information privacy; Commissioner for Law Enforcement Data Security Act 2005 ('Act').
4.3	How to use caveats	Yes	
5	Cabinet documents	Yes	
5.1	Security classifying and marking Cabinet documents	Yes	
6	Foreign government information	Yes	
Annex A	Classification and marking ready reckoner	Yes	The *Information Privacy Act* 2000 replaces the *Privacy Act* 1998, and the *Health Records Act* 2001 also applies to information privacy.

Physical Security

Ref.	PSPF Section or Document	Applicable?	Customisation
	Physical security management protocol		
1	Scope	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms). The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
2	Terms and definitions	Yes	Some terms are substituted or added as part of the customisation of the PSPF for use by the Victorian Government (see the *Terminology* table at the beginning of this Appendix 1.)
3	How this protocol fits into the PSPF structure	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
4	Agency physical security policies and procedures	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
5	Agency physical security risk management and planning	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
5.1	Risk management	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.) Compliance with the *Occupational Health and Safety Act* 2004 is required
5.2	Assurance levels	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
5.3	Security-in-depth	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
5.4	Elements of physical security planning	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
6	Physical security treatments	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
7	Protection of people	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)

Ref.	PSPF Section or Document	Applicable?	Customisation
7.1	Occupational health and safety considerations in physical security	Yes	Compliance with the *Occupational Health and Safety Act* 2004 is required
7.2	Emergency procedures	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
8	Physical security of information and ICT equipment	Yes	
8.1	Single items or limited amounts of information	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
8.2	Aggregations of information	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
8.3	ICT systems	Yes	
9	Physical security in emergency and increased threat situations	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
Annex A	References standards, handbooks and codes	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
Annex B	Physical terms for inclusion in the Australian Government lexicon of security terms	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
Annex C	Physical security in an agency's risk management and planning	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
	Physical security of ICT equipment, systems and facilities		
1	Introduction	Yes	
2	Background	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
3	Physical security of ICT equipment	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)

Ref.	PSPF Section or Document	Applicable?	Customisation
4	Physical security of ICT system equipment	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
5	Physical security of ICT facilities	Yes	The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
6	Protection of information and ICT equipment against environmental or man-made threats	Yes	
	Security zones and risk mitigation control measures		
1	Introduction	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
2	Background	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
3	Risk mitigation and assurance measures	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms). The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
3.1	The risk management process	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
3.2	Assurance required for information and physical asset sharing	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms). The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
3.3	Site security plans	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
4	Security Zones	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms). The PSPF Business Impact Levels are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)

Ref.	PSPF Section or Document	Applicable?	Customisation
5	Individual control elements	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms). References to Commonwealth legislation are replaced/complemented by the Victorian equivalent where appropriate.
6	Physical security elements in administrative security	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
Annex A	Physical security measures checklist	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms)
Annex B	Physical security terms for inclusion in the Australian Government lexicon of security terms	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms). Some terms are substituted or added as part of the customisation of the PSPF for use by the Victorian Government (see *Terminology* table at the beginning of this Appendix 1).
Annex C	Summary of equipment tested by the SCEC and guidelines to assist agencies in selecting commercial equipment	Yes	
Annex D	Summary of jurisdictional guard licencing legislation	Yes	
Annex E	Legislation covering CCTV installation and usage	Yes	
Annex F	Safe and vault types	Yes	

Governance Guidelines

Ref.	PSPF Section or Document	Applicable?	Customisation
	Security awareness training guidelines		
-	Introduction	Yes	

Ref.	PSPF Section or Document	Applicable?	Customisation
-	Who gets security awareness training	Yes	
-	Security awareness training content	Yes	The *Occupational Health and Safety Act* 2004 is also relevant
	Business impact levels		
1	Introduction	Yes	
2	Background	Partially	The PSPF Business Impact Levels (Annex A) are replaced by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
3	Using business impact levels	Yes	Information classifications and dissemination limiting markers are driven by the Victorian Government Business Impact Levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*)
Annex A	Australian Government business impact levels	No	Replaced with Victorian Government business impact levels (see *SEC GUIDE 02 Business Impact Levels and Other Criteria*.)
	Reporting incidents and conducting security investigations		
1	Introduction	Yes	
2	Background	Yes	
3	Security incidents	Partially	In the context of reporting, DSDBI replaces ASIO. (DSDBI will report to ASIO if necessary).
3.2	Roles and responsibilities	Partially	With the exception of direct reporting of information security incidents to DSD, DSDBI replaces ASIO and DSD for reporting purposes. (DSDBI will report to ASIO and/or DSD if necessary).
3.3	Procedures for ensuring staff report security incidents which are recorded	Yes	
3.4	Recording incidents	Yes	
3.5	Dealing with minor security incidents	Partially	In the context of reporting under 3.5.1, the DPC SEMB replaces AGSVA.

Ref.	PSPF Section or Document	Applicable?	Customisation
3.6	Dealing with major security incidents	Partially	In the context of reporting, DSDBI replaces ASIO. (DSDBI will report to ASIO if necessary). Reporting of information security incidents should be to DSD directly, who will provide quarterly reports to DSDBI. Victoria Police will generally replace, or work with, the AFP. The *Occupational Health and Safety Act* 2004 is also relevant.
4	Investigations		
4.1	Principles of procedural fairness	Yes	
4.2	Types of investigations	Yes	Victoria Police will advise whether there is a possible offence against Victorian law. The Victorian *Crimes Act* 1958 applies.
4.3	Agency procedures for investigating security incidents	Yes	In the context of reporting, DSDBI replaces ASIO. (DSDBI will report to ASIO if necessary). Reporting of information security incidents should be to DSD directly. DSD will provide quarterly reports. Reporting to Victoria Police replaces reporting to the AFP.
4.4	Appointing investigators	Yes	
4.5	Understand the role of investigator	Yes	
4.6	Determine the nature of the investigations	Yes	
4.7	Terms of reference for investigations	Yes	
4.8	Conducting investigations	Yes	
Annex A	Categories of security incidents	Yes	
	Agency security advisor and IT security adviser functions and competencies		
1	Introduction	Yes	
2	Background	Yes	
3	ASA and ITSA roles	Yes	The *Financial Management Compliance Framework* (FMCF), Supplementary Material, *Theft and Losses*, complements the *Commonwealth Fraud Control Guidelines*
4	ASA functions and competencies	Yes	

Ref.	PSPF Section or Document	Applicable?	Customisation
5	ITSA functions and competencies	Yes	
6	Use of specialist service providers	Yes	With the exception of reporting information security incidents to DSD directly, all contact with ASIO or DSD should be referred to DSDBI in the first instance. The DPC SEMB replaces AGVSA.
	Security of outsourced services and functions		
1	Introduction	Yes	
2	Background	Yes	
3	Including protective security terms and conditions in contracts	Yes	Compliance with Victorian Government Purchasing Board (VGPB) requirements is required in place of *Commonwealth Procurement Guidelines*. Compliance with the Privacy Principles contained in the *Information Privacy Act* 2000, and *Health Records Act* 2001 is required in place of the Commonwealth *Privacy Act* 1988.
4	Security clearances for service providers' staff	Yes	All contact with AGVSA should be referred to DPC SEMB in the first instance.
5	Information security	Yes	Compliance with the *Public Records Act* 1973 is also required
6	Physical security	Yes	Applies only to information, people, processes and assets (including software, equipment and computer rooms)
7	Contract management	Yes	Guidelines and requirements are specified by the Victorian Government Purchasing Board (VGPB) in place of the Department of Finance and Regulation
Annex A	Example Non-Disclosure Agreement	Yes	Most agencies have their own Non-Disclosure Agreements

Appendix 2: Customisation details – ISM

Terminology

Refer to the Terminology table at the beginning of Appendix 1. (Note: Some of the terms used in the PSPF are not used in the ISM).

ISM Executive Companion

ISM Document Section	Applicable ?	Customisation
Forward	Yes	While the content is generally applicable, the authority for use of the ISM comes from the Victorian Government, coordinated through DSDBI
The Threat Environment	Yes	The threat environment defined by DSD is equally applicable to State Government, which is included within DSD's mandate.
Countering the Cyber Threat	Yes	
Case Study	Yes	
The Australian Government Information Security Manual	Yes	The authority for adoption of the ISM comes from the Victorian Government, coordinated through DSDBI
DSD's Role	Yes	In the context of reporting information security incidents, agencies should report them to DSD directly. DSD will provide a quarterly report to DSDBI.

ISM Principles

ISM Document Section	Applicable ?	Customisation
Forward	Yes	While the content is applicable, the authority for use of the ISM comes from the Victorian Government, coordinated through DSDBI.
Information Security: Countering the Threat		
The Threat Environment	Yes	The threat environment defined by DSD is equally applicable to State Government, which is included within DSD's mandate.
Countering the Cyber Threat	Yes	
The Australian Government Information Security Manual	Yes	The authority for adoption of the ISM comes from the Victorian Government, coordinated through DSDBI.
DSD's Role	Yes	In the context of reporting information security incidents, agencies should report them directly to DSD. DSD will provide quarterly reports to DSDBI.
Principles		
Roles and Responsibilities	Yes	
Industry Engagement and Outsourcing	Yes	
Information Security Documentation	Yes	The titles of documents may be varied by agencies, but the security scope of the documentation suite must be maintained. In addition there is an over-arching Victorian Government *ICT Risk Assessment Report* which is required.
System accreditation	Yes	The Accreditation Authority is the Agency Head (or his/her Delegate), who accepts the residual risk of the system(s), and the Certification Authority is the agency ITSA
Information Security Monitoring	Yes	
Cyber Security Incidents	Yes	In the context of reporting information security incidents, agencies should report them to DSD directly. DSD will provide quarterly security incident reporting and analyses to DSDBI. The *Public Records Act* 1973 and the Public Records Office determines archival retention periods.
Physical Security	Yes	Applies only to ICT information, people, processes and assets (including software, equipment and computer rooms).

ISM Document Section	Applicable ?	Customisation
Personnel Security	Yes	Agency *Acceptable Use Policies* should be aligned to these requirements
Communications Infrastructure	Yes	
Communications Systems and Devices	Yes	
Product Security	Yes	
Media security	Yes	
Software security	Yes	Victorian Government standards mandating implementation of appropriate *Strategies to Mitigate Targeted Cyber Intrusions* will be released over time.
Access Control	Yes	The *Public Records Act* 1973 and the Public Records Office determines archival retention periods.
Cryptography	Yes	
Network Security	Yes	
Gateway Security	Yes	
Working Off-Site	Yes	Agency *Acceptable Use Policies* should be aligned to these requirements

ISM controls

While the ISM covers all types of information, from public domain to TOP SECRET, many of the provisions contained in the ISM relate to special protections for National Security Information (CONFIDENTIAL, SECRET, and TOP SECRET, which are denoted by 'C', 'S' and 'TS' respectively in the ISM to indicate whether a control is applicable). There is very little information in Victorian Government agencies that fit into these classifications. In general for most Victorian agencies,

- the highest classification of information is PROTECTED, which is denoted as 'P' in the ISM to indicate whether a control is applicable, and
- the vast majority of information is UNCLASSIFIED, although it may carry a Dissemination Limiting Marker (DLM) which is denoted as 'G' (Government) in the ISM to indicate whether a control is applicable.

As a consequence, where controls are indicated as applicable by a 'Yes' in the 'Applicable?' column in the tables below, it is only applicable to the extent that it applies to the classification or sensitivity of the information held by the agency.

ISM Document Section	Applicable ?	Customisation
Forward	Yes	While the content is generally applicable, the authority for use of the ISM comes from the Victorian Government, coordinated through DSDBI.
About Information security		
Using This Manual	Yes	The Accreditation Authority for approving non-compliance with 'should' or 'should not' ISM requirements is the Agency Head (or his/her Delegate e.g. the agency CISO). DSDBI replaces DSD in relation to approving non-compliance with 'must' and 'must not' ISM requirements. (DSDBI will refer to DSD if necessary). References to Commonwealth legislation should be supplemented by references to the comparable Victorian legislation, where appropriate.
Applicability, Authority and Compliance	Yes	The ISM applies to all Victorian agencies. The authority for adoption of the ISM is the Victorian Government, coordinated through DSDBI, who will also set timeframes for compliance. The VAGO will act in place of the ANAO.
Information Security Governance		
Information Security Engagement	Yes	With the exception of direct reporting of information security incidents to DSD, all contacts with DSD should be referred to DSDBI in the first instance. The Victorian equivalents of the agencies listed act in place of Commonwealth agencies. (VAGO for ANAO, Victorian Police for AFP, Public Records Office for National Archives of Australia, etc.)

ISM Document Section	Applicable ?	Customisation
Industry Engagement and Outsourcing	Yes	
Roles and Responsibilities	Yes	
Information Security Documentation	Yes	The titles of documents may be varied by agencies, but the security scope of the documentation suite must be maintained. In addition there is an over-arching *ICT Risk Assessment Report* required.
System Accreditation	Yes	The Accreditation Authority is the Agency Head (or his/her Delegate e.g. the CISO), who accepts the residual risk of the system(s), and the Certification Authority is the agency ITSA. DSDBI replaces DSD in relation to approvals. (DSDBI will refer to DSD if necessary).
Information Security Monitoring	Yes	In the context of reporting information security incidents, agencies should report them to DSD directly. DSD will provide quarterly reporting to DSDBI.
Physical Security		
Facilities and Network Infrastructure	Yes	
Servers and Network Devices	Yes	
ICT Equipment and Media	Yes	
Personnel Security		
Information Security Awareness and Training	Yes	
Authorisations, Security Clearances and Briefings	Yes	
Using the Internet	Yes	Agency *Acceptable Use Policies* should be aligned to these requirements
Communications Security		
Communications Infrastructure	Yes	
Communications Systems and Devices	Yes	
Information Technology Security		
Product Security	Yes	All contacts with DSD should be referred to DSDBI in the first instance.
Media Security	Yes	

ISM Document Section	Applicable ?	Customisation
Software Security	Yes	Agency *Acceptable Use Policies* should be aligned to these requirements e.g. for web and email usage, etc.
Access Control	Yes	
Cryptography	Yes	
Network Security	Yes	
Gateway Security	Yes	
Working Off-Site	Yes	