VICTORIAN GOVERNMENT CIO COUNCIL

Information Security

ISMF Implementation

Guideline

Departments, agencies and State-owned enterprises can use this guideline to assist in the implementation of the Information Security Management Framework standard SEC STD 01.

Keywords:	ISMF, PSPF, guideline, implementation, compliance.	
Identifier: SEC GUIDE 01	**Version no.:** 2.0	**Status:** Final
Issue date: 1 October 2012	**Date of effect:** 1 October 2012	**Next review date:** 1 November 2014
Authority: Victorian Government CIO Council	**Issuer:** Victorian Government Chief Technology Advocate	

For Official Use Only

State Government Victoria

Overview

This guideline identifies the activities and supporting information that may assist agencies in implementing SEC STD 01, in particular in developing the key deliverables required by the standard:

- an Information Security Management Framework, comprising an ICT Risk Assessment Report, an Information Security Policy, a Self-assessment Compliance Report and an Incident Response Plan;
- systems documentation such as System Risk Management Plans, System Security Plans, and System Operating Procedures; and
- mandatory reports, including annual updates to the ICT Risk Assessment, Self-Assessment Compliance Report and Critical Information Infrastructure reports where relevant.

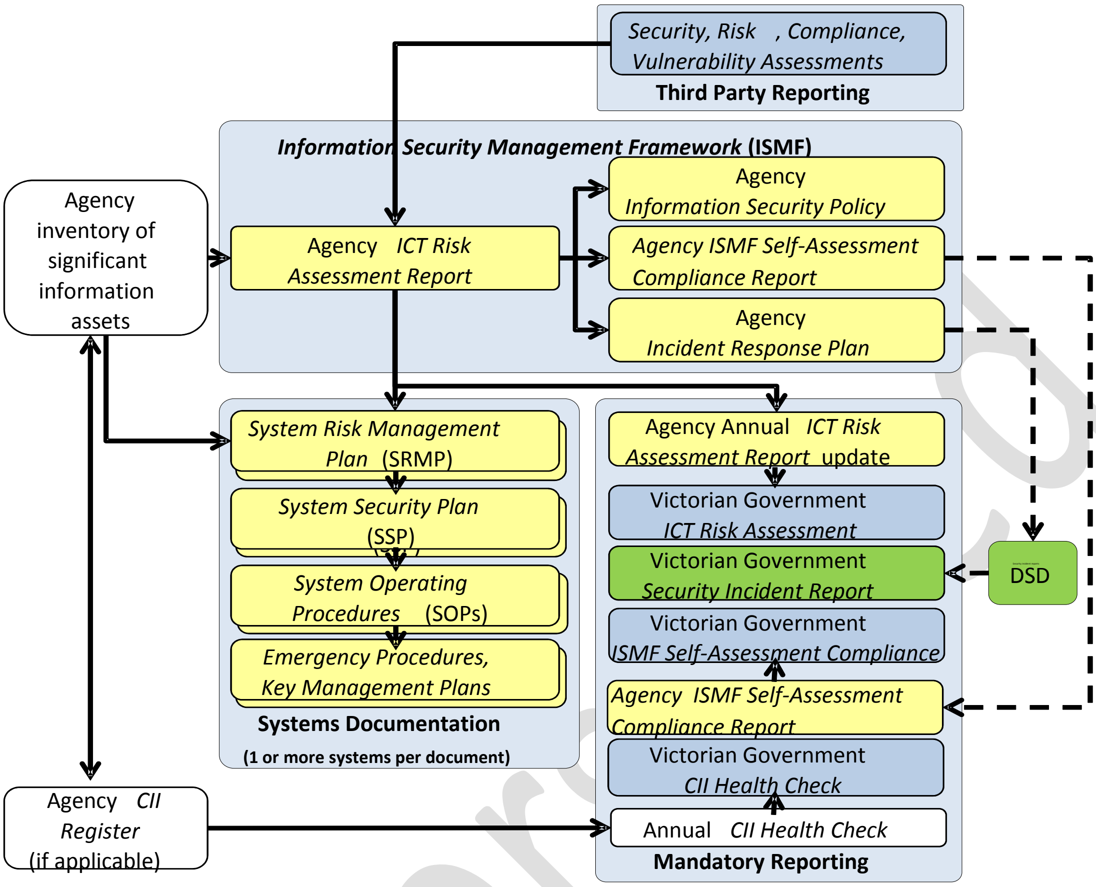
Templates are available for key deliverables, and training will be provided, as well as further support and guidance on request. Where a common approach is required across agencies, a Victorian Government approach will be facilitated.

Agencies are required to bear the cost of compliance to the standard, including:

- costs associated with developing required documents;
- costs of any new or upgraded ICT products required to meet security standards;
- operational costs associated with meeting security standards, such as email security marking; and
- any other costs associated with ensuring compliance with ISM and PSPF.

The initial requirement is for each agency to develop a plan which outlines the agency’s approach to progressive compliance with this standard over time. Some ISM requirements may mean that agencies have to upgrade or replace some existing systems or networks (e.g. older wireless networks) which have weaker security. Immediate replacement of these systems or networks is not required if a risk assessment indicates the residual risk is acceptable. In these cases they should be replaced with ISM-compliant technology (with stronger security) during normal agency technology refresh cycles.

Figure 1: Structure of ISMF documents, system documents and reporting.


Security, Risk , Compliance, Vulnerability Assessments
Third Party Reporting
Information Security Management Framework (ISMF)
Agency inventory of significant information assets
Agency ICT Risk Assessment Report
Agency Information Security Policy
Agency ISMF Self-Assessment Compliance Report
Agency Incident Response Plan
System Risk Management Plan (SRMP)
System Security Plan (SSP)
System Operating Procedures (SOPs)
Emergency Procedures, Key Management Plans
Systems Documentation
(1 or more systems per document)
Agency Annual ICT Risk Assessment Report update
Victorian Government ICT Risk Assessment
Victorian Government Security Incident Report
DSD
Victorian Government ISMF Self-Assessment Compliance
Agency ISMF Self-Assessment Compliance Report
Victorian Government CII Health Check
Annual CII Health Check
Mandatory Reporting
Agency CII Register (if applicable)

Implementing the standard

Information security governance

The governing body for information security within the agency will need to approve the ISMF deliverables and approve (or request approval for) the funding of projects to implement the controls needed to reduce the risks to significant information assets (see definition in the *Glossary* of this guide).

If the agency does not yet have an effective structure for information security governance, it should review the structure and authority for information security governance within the agency and resolve any issues that arise.

At a minimum, agencies should implement four roles (which may be added to the roles of existing agency Executives or managers):

ISM roles:

- A Chief Information Security Officer (CISO), who is responsible for the strategic direction of information security.

- An Information Technology Security Advisor (ITSA), who coordinates information security across the agency, and who may also be an IT security manager (ITSM) or security officer (ITSO).

PSPF roles:

- A security Executive, responsible for the agency protective security policy and oversight of protective security practices.
- An Agency Security Adviser (ASA), who is responsible for the day-to-day performance of protective security functions.

In smaller agencies, some roles may be combined if the competencies match. (See the PSPF document *Agency security adviser and IT security adviser functions and competencies*, and the ISM *Controls* section on *Roles and Responsibilities.*)

The information security governing body should report through an appropriate Executive of the agency (e.g. the Executive nominated to perform the role of the CISO) and should be responsible for:

- protecting the agency's information and information assets;
- managing vulnerabilities within the agency's ICT infrastructure;
- reviewing threats and incidents which adversely impact on the agency's information assets;
- assuring (through policy) the appropriate use of the agency's information assets; and
- educating staff about their information security and privacy protection responsibilities.

Inventory of significant information assets

Significant information assets are those which are crucial to the achievement of the agency's mission. The identification of significant information assets is an essential prerequisite to the completion of the *ICT Risk Assessment*. Agencies which have significant levels of Critical Information Infrastructure (CII – *see SEC STD 02 Critical Information Infrastructure*) may choose to use their *CII Register* as the initial list of significant information assets. However, in subsequent reports, they will need to extend the scope of the report to all significant information assets.

In either case, there will also be a need for a good knowledge of the agency's overall inventory of information assets, including tools and utilities used for systems and network operations and management, which may potentially be used to compromise significant information assets.

If the agency does not have such an inventory of information assets, or the inventory is out of date or otherwise inadequate, it will need to ensure that any inventory deficiencies are identified and rectified before the process described in this implementation guide is started.

Third party reporting

Where applicable, reporting by third parties including service providers is also an important input to the *ICT Risk Assessment*. If the required reporting has not been received, or has not been contracted for, you will need to make arrangements to obtain it. Where this is not possible in the timeframe required to meet the requirements of the initial *ICT Risk Assessment*, you will need to take appropriate action to ensure that this reporting is available for the subsequent *ICT Risk Assessment*. Refer to SEC STD 01 for reporting requirements.

Developing the ICT Risk Assessment Report

The ICT Risk Assessment Report is a high level self-assessment performed against the list of significant information assets within the agency. It reviews the high level risks to the portfolio of significant information assets, and develops high level risk mitigations to reduce the risks to an acceptable level. (Detailed risk analysis of an individual significant information asset is handled in a *System Risk Management Plan*). The *ICT Risk Assessment Report* should not attempt to 're-invent the wheel'. Existing material which may be re-used to reduce the effort required includes;

- previously developed agency ICT risk assessments (e.g. within a Risk Management unit); and/ or
- an existing *Risk Assessment Report* (as a result of SEC POL 01); and/ or
- previous assessments of agency information classifications; and/ or
- reports from third parties, including ICT shared services providers; and/ or
- other similar documents.

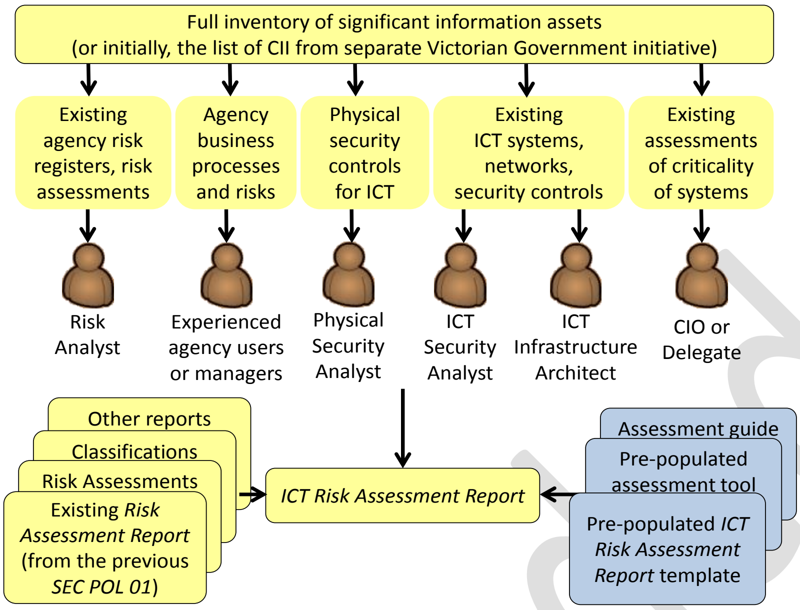
The *ICT Risk Assessment Report* template and assessment tool have been heavily pre-populated with example content to minimise the effort required by agencies.

Establishing the team

Completing an *ICT Risk Assessment* requires multiple skills. As shown in Figure 2 it may require:

- experienced agency users or management who are familiar with agency services and processes and the related ICT risks the agency faces;
- information and physical security staff, who are familiar with the agency's security controls;
- ICT infrastructure or systems administration staff, who are familiar with the way the agency's ICT assets interconnect, the risks to systems and networks, and the existing information security controls; and
- agency or ICT risk management staff, who may have performed ICT risk assessments in the past.

Figure 2: Developing the ICT Risk Assessment Report

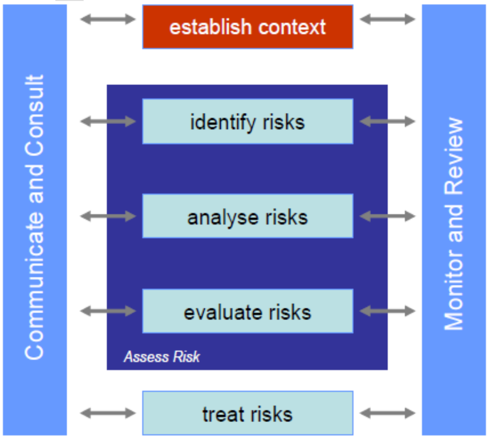

Full inventory of significant information assets
(or initially, the list of CII from separate Victorian Government initiative)
Existing agency risk registers, risk assessments
Agency business processes and risks
Physical security controls for ICT
Existing ICT systems, networks, security controls
Existing assessments of criticality of systems
Risk Analyst
Experienced agency users or managers
Physical Security Analyst
ICT Security Analyst
ICT Infrastructure Architect
CIO or Delegate
Other reports
Classifications
Risk Assessments
Existing Risk Assessment Report (from the previous SEC POL 01)
ICT Risk Assessment Report
Assessment guide
Pre-populated assessment tool
Pre-populated ICT Risk Assessment Report template

Ideally, there should be no more than 5-6 people on the team. If there are more, the process will tend to 'bog down'. You should ensure that the skills required to complete the report are made available in a timely fashion, and where necessary organise workshops to complete the assessment.

Process overview

The steps for completing the *ICT Risk Assessment* are summarised in Figure, which is taken from the *Victorian Risk Management Framework*, and is based on *AS/NZS/ISO 31000: 2009 Risk Management.*

Figure 3: System Security Risk Management Process



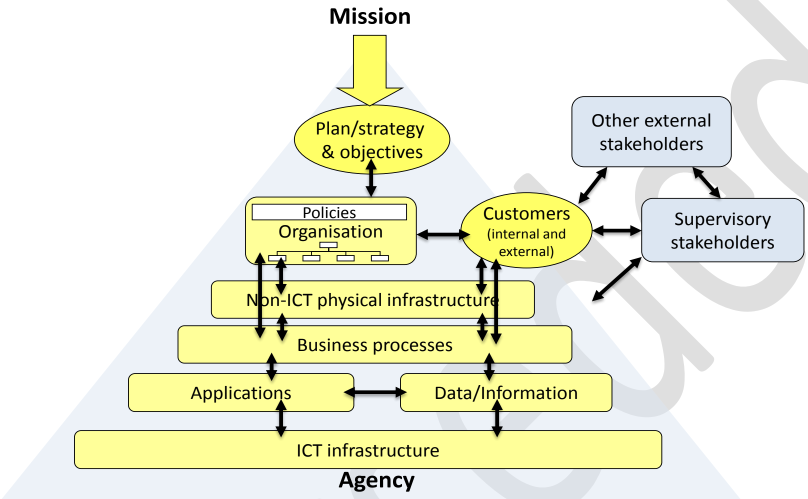
Source: VMIA, *Developing and Implementing a Risk Management Framework,* March 2010

Each of the major steps shown in this diagram is described in the sections which follow.

Establish the context

The risks to information assets cannot be fully understood unless the business context is known (e.g. the criticality of the business processes that are supported by ICT assets). A high level operational model of the agency will provide this context. It may already exist, for example in agency strategic planning documents, or induction information used for new staff. If no high level operational model exists, it may help if you develop one. Figure 4 may assist in thinking this through.

Figure 4: Example Framework for Business Model



Assess risks

Identify significant information assets

If it hasn't already done so, the agency should develop a list of significant information assets. The agency operational model should allow the identification of these assets, which can then be used for the identification of risks.

Where applicable, agencies with significant levels of CII may choose to restrict the scope of their initial *ICT Risk Assessment Report* to these CII assets only (see *SEC STD 02 Critical Information Infrastructure*.) In this case, the identification of significant assets will have already been completed.

Beyond this, there are other information assets which may be used to compromise the security of significant information assets. These must also be identified. A good question to ask is: 'Could this asset be used to bypass normal security and compromise sensitive information, and would the impact be High or Very High, using the Victorian Government Business Impact Levels?' If the answer is 'Yes', then this information asset must also be included in the *ICT Risk Assessment*.

Examples of significant information assets could include:

- data centres which host agency systems;
- applications used for the delivery of agency services online, or through agency offices, or through downstream customer service organisations, etc;

- applications containing information classified as PROTECTED; or
- networks that allow:
  - agency customers to communicate with the agency online, or by telephone, etc; or
  - agency offices or downstream customer service organisations to access significant agency applications.

Examples of other information assets which may be used to compromise the security of significant information assets are:

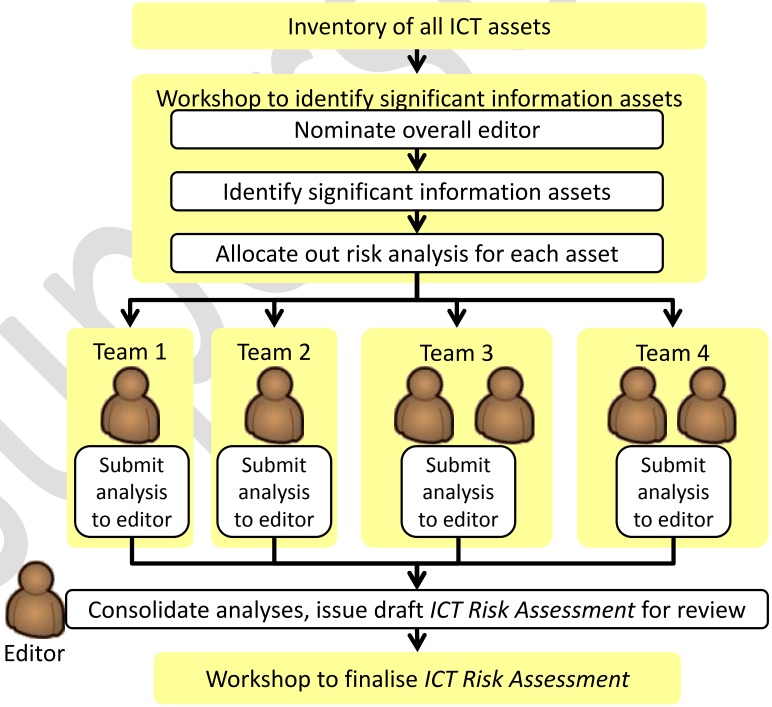
- Systems/ network management tools which can be used by systems administrators to look at server information, network traffic, application databases, etc.

Identify and analyse the risks to the significant information assets

The threats to each of the significant information assets then inform the identification, analysis, and evaluation of risks.

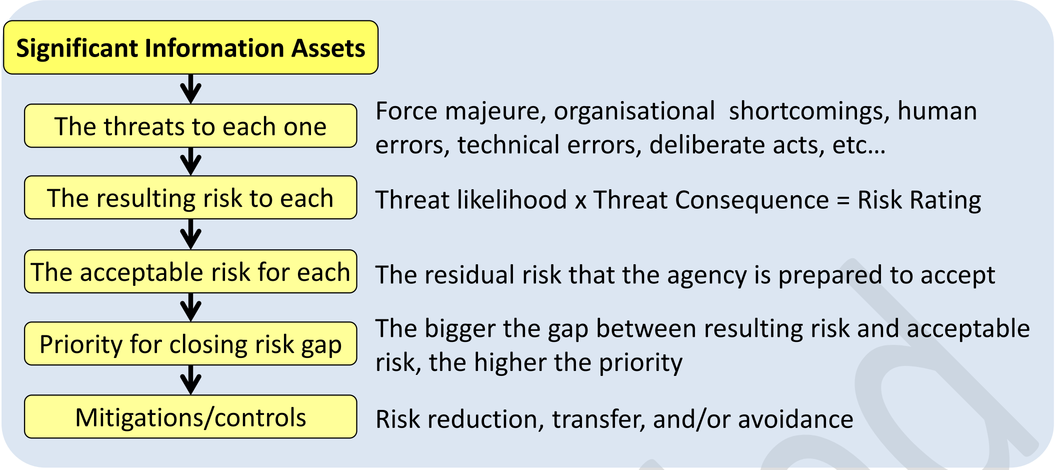
If appropriate, agencies may choose to allocate the analysis of risks across the team, as shown in Figure 5.

Figure 5: Allocation of risk analysis across the team


Inventory of all ICT assets
Workshop to identify significant information assets
Nominate overall editor
Identify significant information assets
Allocate out risk analysis for each asset
Team 1
Submit analysis to editor
Team 2
Submit analysis to editor
Team 3
Submit analysis to editor
Team 4
Submit analysis to editor
Consolidate analyses, issue draft ICT Risk Assessment for review
Editor
Workshop to finalise ICT Risk Assessment

The overall risk analysis process is summarised in Figure 6. A set of criteria to be used for Threat Likelihood, Threat Impact and Risk Ratings, and which will also allow the security classification of the significant information assets is provided in *SEC GUIDE 02 Business Impact Levels and Other Criteria*.

Figure 6: Applying the Process to the Significant Information Assets



Significant Information Assets

The threats to each one — Force majeure, organisational shortcomings, human errors, technical errors, deliberate acts, etc…

The resulting risk to each — Threat likelihood x Threat Consequence = Risk Rating

The acceptable risk for each — The residual risk that the agency is prepared to accept

Priority for closing risk gap — The bigger the gap between resulting risk and acceptable risk, the higher the priority

Mitigations/controls — Risk reduction, transfer, and/or avoidance

Evaluate risks

As shown in Figure 6, risk evaluation involves comparing the resulting Risk Rating against the acceptable Risk Rating (assumed to be Low). The greater the gap between the resulting Risk Rating and the acceptable Risk Rating, the higher the priority for closing the gap (i.e. for reducing, transferring or avoiding the level of risk to the significant information asset).

Treat risks

A high level strategy for mitigating the high priority risks must be provided as part of the *ICT Risk Assessment Report*. Risk treatment involves:

- identifying the range of options available to treat the risk (the security classification of the significant information asset may determine which risk mitigations must be implemented under either the ISM or the PSPF),
- assessing the effectiveness of the treatment alternatives, and the residual risk that remains,
- including the selected treatments in the risk mitigation section of the *ICT Risk Assessment Report*, and
- implementing the risk treatment.

The agency head and the agency CISO must sign off on the residual risk profile i.e. attest that it is acceptable to the agency.

Monitoring and review

Risk management is a process, and risks are not static:

- The business context which information assets operate within is subject to continual change.
- Threats to systems are continually evolving.

- The effectiveness of risk mitigations/controls often alter over time.

As a consequence, ICT risk assessments must be reviewed and updated at least annually.

Communication and consultation

Both internal and external stakeholders must be effectively consulted with, and communicated with, throughout the development (and subsequent maintenance) of the *ICT Risk Assessment Report*.

Updating the Information Security Management Policy

An *Information Security Management Policy* should already exist within the agency as a result of the SEC POL 01. In this case, all that is required is to review the policy in the light of the issues identified in the *ICT Risk Assessment Report*, and update it as required. (New policies, standards or processes may be needed to reduce risks to significant information assets to acceptable levels).

Once the policy has been updated, the changes will need to be implemented i.e. funded, communicated, included in induction and security awareness training, etc.

Completing the Self-Assessment Compliance Report

The template for the ISMF Self-Assessment Compliance Report (which is in ISO terms a *Statement of Compliance and Compliance Plan)* will be provided.

You need to indicate whether you have already complied with PSPF requirements for all relevant significant information assets, or if not, what your agency's plan is to achieve compliance.

Where applicable, you also need to include your plan to close any gaps identified in *CII Health Check* reports.

You will then need to implement the plan.

Preparing the Incident Response Plan

Your agency should already have a plan or policy for dealing with major information security incidents if not; DSD's OnSecure Incident Reporting application should be used.

At a minimum, the plan should include:

- what constitutes an information security incident (e.g. definitions and examples of major and minor security incidents to guide the level of response to the 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 (e.g. the CISO or ITSA);
- the steps necessary to ensure the integrity of evidence supporting an investigation;

- the steps necessary to ensure that significant systems remain operational during the investigation of an incident; and

- how to report an information security incident.

Reporting of information security incidents to the Defence Signals Directorate (DSD) will be a requirement under the new framework. Refer to ISM Controls – Cyber Security Incidents and D&A internal Incident Response procedures or reporting incidents.

Preparing System Level Documentation

The *ICT Risk Assessment* is at a high level, and looks at the portfolio of significant information assets as a whole. System level documentation looks in detail at individual significant information assets.

System Risk Management Plans (SRMPs) use the same process as the *ICT Risk Assessment Report*, but focus on the individual components of one or more individual significant information assets, and a more detailed, low level analysis of threats and risks to these individual components. It also supports the security classification of agency data. The related *System Security Plan* (SSP) provides the detailed implementation plan for the security controls and risk mitigations that will be used to reduce the risks to the individual components of the significant information asset to acceptable levels. The related *System Operating Procedures* (SOPs) include detailed processes for security operations for the system.

For cryptographic functions, which are crucial for the security of sensitive information*, Key Management Plans* must be developed which define how cryptographic keys will be protected from compromise. The plan must include, at a minimum, the contents specified in the ISM.

Similarly, *Emergency Procedures* will be required to ensure that information and systems are secured during the warning phase of a building emergency i.e. before the evacuation phase.

As the documents listed above are completed, new significant information assets, or new risks which require additional risk mitigations, may be identified. This may mean that there is a need to update the *ICT Risk Assessment*, or the ISMF Self-Assessment Compliance Report, or the *Information Security Management Policy* (i.e. the overall process may prove to be iterative).

Annual reporting

Annual reporting under the revised framework comprises:

- An annual update of the *ICT Risk Assessment Report*, which should include a review of:
  - any changes to the business context (including any new systems that may have been implemented, or old systems that have been retired), and an update to the significant information assets list;
  - new or emerging threats to significant information assets; and
  - the effectiveness of existing risk mitigations/controls, and the need for new risk mitigations/controls.

- An annual update of the *ISMF Self-Assessment Compliance Report*. This will record progress against the agency compliance plan including the status of any remaining non-compliance, and identify any new requirements for compliance arising from the updated *ICT Risk Assessment Report*, and any gaps identified in *CII Health Check* reports.

Note that Appendix 1 has an ISMF Implementation Checklist which may assist in helping agencies to complete the identified tasks.

Rationale

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

Derivation

- SEC STD 01 Information Security Management Framework

References and toolkits

Australian Government Information Security Manual: 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.

Australian Government PSPF Glossary of Terms:
http://www.protectivesecurity.gov.au/pspf/Pages/PSPF-Glossary-of-terms.aspx

Australian Government PSPF Policy: http://www.protectivesecurity.gov.au/Pages/default.aspx

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

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

Further information

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

Glossary

Term	Meaning
Access management	The capability and processes that permit or deny access to systems, thus controlling the ability to read, modify or remove information.

Term	Meaning
CISO	Chief Information Security Officer (a role defined in the ISM)
Critical information asset	ICT systems, applications or infrastructure (including computer rooms) which • are used to deliver essential or important agency services to agency clients (e.g. the Victorian public), and/or • if compromised, could cause serious damage to government, the public, commercial entities, or the physical, social or economic wellbeing of the State.
ICT	Information and Communications Technology
ISM	The Australian Government *Information Security Manual*
ISMF	Information Security Management Framework
ITSA	Information Technology Security Advisor (a role defined in the ISM)
PSPF	Protective Security Policy Framework
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.
VMIA	Victorian Managed Insurance Authority
VG	Victorian Government

Version history

Version	Date	TRIM ref	Details
1.0	9 October 2009		Implementation guide for previous SEC STD 01
1.1	21 May 2012	N/A	Draft of implementation for new SEC STD 01
1.2	17 July 2012	D12/156744	Final revisions for board approval
2.0	31 August 2012	D12/156744	Final text updates for release to CIO Council