ISMF

Information Security Management Framework

DPC/F4.1

Government framework on cyber security

Version: 3.3

Date: September 2017

Government of South Australia

GOVERNMENT FRAMEWORK ON CYBER SECURITY

DPC/F4.1 Information Security Management Framework

Coverage:

The South Australian public authorities required to adhere to this framework are defined in DPC/F4.1 Government framework on cyber security – *Information Security Management Framework* [ISMF].

This framework and the policies and standards contained herein are intended for use by South Australian Government agencies and suppliers to Government whose contractual obligations require them to comply with this document. Reliance upon this policy or standard by any other person is entirely at their own risk and the Crown in the right of South Australia disclaims all responsibility or liability to the extent permissible by law for any such reliance.

Document Control

ID	DPC/F4.1
Version	3.3
Classification/DLM	PUBLIC-I2-A1
Compliance	Mandatory
Original authorisation date	4 October 2011 (ISMF version 3.0 by Cabinet)
Last approval date	September 2017
Next review date	September 2018

DOCUMENT TERMINOLOGY AND CONVENTIONS

The terms that are used in this document are to be interpreted as described in Internet Engineering Task Force (IETF) RFC 2119 entitled “Key words for use in RFCs to Indicate Requirement Levels”[1]. The RFC 2119 definitions are summarised in the table below.

Term	Description
MUST	This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase “SHALL NOT”, means that is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective “OPTIONAL”, means that an item is truly optional.

1 www.ietf.org/rfc/rfc2119.txt?number=2119

TABLE OF CONTENTS

1. AUTHORITY

Agencies must comply with the South Australian Government *Information Security Management Framework [ISMF].*

Suppliers with contractual arrangements that require them to do so must comply with the ISMF.

The Information Security Management Framework is a Cabinet-approved document that describes 40 policies and 141 (active) standards in support of contemporary industry practices for the security of information stored, processed, transmitted or otherwise manipulated using Information and Communication Technology [ICT]. It has been revised to align closely with the AS/NZS ISO/IEC 27001:2006 standard for Information Security Management Systems. On the topic of Information Security Management, Agencies must implement whatever control measures are necessary to provide adequate protection for its information and associated assets. The authority of the ISMF is also enabled by section 5.2 of the Department of Premier and Cabinet Circular PC030 *"Protective Security Management Framework"* [PSMF] which first came into effect across Government in April 2008 and has since been revised.

The PSMF states in clause 5.2.3 that "In relation to the security of information and communication technology, Agencies are required to comply with the South Australian Government *Information Security Management Framework*."

Suppliers must comply with the South Australian Government *Information Security Management Framework* to the extent to which their contractual conditions with Agencies require them to do so. Suppliers may also be subject to contractual conditions requiring compliance to the ISMF by way of across government purchasing agreements.

The PSMF describes the role of the Department of the Premier and Cabinet (DPC) in providing advice to South Australian Government Agency personnel on information and communication technology security matters.

The Cyber Security and Risk Assurance Group (DPC) provides:

- advice and other assistance to South Australian Government Agency personnel on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means, and
- Guidance to SA Government Agencies in relation to cryptography, and security requirements for communication and computer technologies.

2. IMPORTANT REVISIONS TO SCOPE AND DOCUMENTATION REQUIREMENTS

This framework has been revised to account for recent amendments to legislation and policy and the revision of certain Australian and International Standards. In particular, this document aligns with the *Government of South Australia Protective Security Management Framework* [PSMF] and *AS/NZS ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements*

Two new terms, namely *"Responsible Party"* and *"Responsible Parties"* are introduced and described herein to clarify the scope of this document which encompasses both Agencies and Suppliers.

Agency Chief Executives retain ultimate accountability for all security matters within their agencies. The application of the ISMF to a Supplier via a contract with the State or Agency shall not absolve the Agency from these obligations and responsibilities.

2.1. New terms

"Responsible Party" is used in two contexts within the ISMF. These are:

- An Agency – the internal to government body that retains ultimate responsibility for all aspects covered by the Information Security Management Framework [ISMF] as it relates to a particular agency and its information assets.
- A Supplier – an external to government entity that is typically responsible for compliance with the ISMF by way of a contractual agreement that contains clauses requiring security of Agency information and the regulation of access to an Agency's information assets. The term "Supplier" shall be read as "Suppliers who are subject to contractual conditions that require them to comply with the ISMF" unless another intention is apparent.

When a Supplier has contracted with the State, the provisions of the ISMF will apply to the Supplier either:

- under the terms of a Purchasing Agreement for whole of Government contracts and associated Customer Agreements; or
- by way of an individual contract with an Agency whereby the Agency has specified the parts of its Information Security Management System [ISMS] for which compliance is sought.

It should be noted that Agency Chief Executives retain ultimate accountability for all security matters within their agencies. The application of the ISMF to a Supplier via a contract with the State or Agency shall not absolve the Agency from these obligations and responsibilities.

"Responsible Parties" includes both Agencies and Suppliers who are subject to contractual conditions that require them to comply with the ISMF. Where any ambiguity arises between these entities in relation to adherence to the ISMF, the Agency Controls implemented in the Customer Agreement shall prevail (i.e. The Agency remains the default party and the Customer

Agreement is used as the vehicle for setting the scope and requirements for the Supplier to comply with either the entirety of the ISMF or part(s) thereof. The Customer Agreement may also introduce additional Agency-specific controls and policies that the Supplier must comply with).

"Business Owner" represents the person or group that is ultimately responsible for an information asset. This person or group is distinct from an information custodian, who may take responsibility for the ongoing management of the information (such as a CIO or system administrator). Individual business units should own business critical information, rather than information technology or information security departments (they are custodians, not owners). The manager of the business unit responsible for the creation of any information and / or the business unit directly impacted by the loss of the information is usually the Business Owner. A Business Owner or group of Business Owners must be identified for each information asset. For the purpose of ISO 27001 certification, the 'risk owner' is synonymous with the term Business Owner contained in this framework.

2.2. Scope of the ISMF

The ISMF applies to all Agencies, and to all Suppliers that are subject to contractual conditions that require compliance with this framework.

The ISMF applies to all Official Information, and all information of which the South Australian Government or any of its Agencies has custody, where that information is processed, stored or communicated by ICT equipment.

The ISMF and all security Bulletins, Notifications and standards issued under it shall apply, unless otherwise advised, to all bodies that are:

- South Australian Government public sector agencies (as defined in the *Public Sector Act 2009*), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Public sector agencies are herein referred to as "Agencies"; OR
- Suppliers to the South Australian Government or its Agencies that have contractual conditions which require compliance to the ISMF as described in section 2.1 of this framework

The ISMF and all security Bulletins, Notifications and standards issued under it shall apply to:

- All information processed, stored or communicated by ICT equipment, where that information is either:
  - Official Information of the South Australian Government or its Agencies; or
  - Information of which the South Australian Government or any of its Agencies has custody[2];
  - Information as described above which Suppliers that have contractual conditions that require compliance to the ISMF as described in section 2.1 of this framework hold on behalf of the South Australian Government or any of its Agencies; or

[2] Note the definition of "custody" in Glossary of Terms which differs from State Records' interpretation.

- Anything that acts upon an ICT asset, including creating, controlling, validating, and otherwise managing the ICT asset throughout the lifecycle of the asset.

2.3. Accountability for information security management in agencies

ISMF Standard 137 (Information security management)

Chief executives have ultimate accountability for all security matters within their agencies. Such accountability is derived from Cabinet Circular No. 30, the *Protective Security Management Framework (PSMF)*, as amended from time to time.

Business Controls

The following guidance applies regardless of the classification levels of the information assets:

S137.1. Treasurer's instruction 2, 'Financial Management Policies' establishes certain obligations and expectations on how entities of the South Australian Government manage risk including those pertaining to ICT projects. On the issue of information security management, it is required that the entity implements whatever control measures are necessary to provide adequate protection for its information and that, where applicable, the entity shall comply with the instructions detailed in the Protective Security Management Framework issued as Premier and Cabinet Circular No. 30.

S137.2. The PSMF is subject to ongoing revision.

2.4. Nomenclature

Each policy statement is numbered sequentially. Standards are issued a unique number and support a given policy statement. A table of policy statements and their respective standards is contained in Annex F of this framework.

Controls are prefixed by their associated 'ISMF Standard' number, for example control S2.1 would represent control number 1 applicable to ISMF Standard 2.

Retired controls in any release of the ISMF are prefixed by 'R' in place of 'S' to indicate a retired status. For example, control *R104.2* would indicate that control number 2 in support of ISMF standard 104 has been retired. Note that the entire control will appear *'italicised and in washed out grey colouring'*. The primary objective of listing retired controls is to support Agency environments in transitioning from one version of the ISMF to the next, and to maintain control tracking for legacy systems and ancillary services that may still require the continued use of these controls arising from their respective risk assessment(s).

As from version 3.2.0 of this framework, all independently published ISMF Guidelines use a numbering scheme that correlates to the Policy Statement they have been authored to support.

2.5. Application of Government, Australian and International standards

Responsible Parties are referred to a number of external documents, policies and guidelines, standards and handbooks in accordance with this framework (refer section 2.8 for pre-requisite documents).

The ISMF, as a framework document, is a policy and standards implementation document for cyber security that references relevant government (state and federal), Australian and New Zealand (AS/NZS) and International (ISO/IEC) standards to form a suite of control objectives, controls and guidance to manage information security risks and objectives. It is a matter for Responsible Parties to apply the relevant standards and controls that apply to their environments based on the nature of the activity or work program, and the information classification requirements based on the Confidentiality, Integrity and Availability markings for the services, systems or ICT platforms associated with the information being managed.

The ISMF provides maximum coverage for control and risk management objectives by providing a wide array of risk management controls and is not purely mapped directly to the 'latest' or most recent standards publications. Rather, the ISMF refers to a suite of publications (current or otherwise) in order to provide government agencies with a comprehensive set of risk controls in order to appropriately protect their information and support their business undertakings. In layman's terms: '*consider the ISMF to be the security menu, from which various standards and controls are selected, in any given situation, with the ultimate goal of reducing risk to a level that is acceptable to the business. The sum of these choices used within an organisation becomes the organisational ISMS when all the different information sets and platforms are accounted for*'.

Annex A in this framework describes the baseline requirements for ISMF compliance. Simply stated, organisations are required to adhere to all 40 Policy Statements and then implement subordinate ISMF Standards under these policies arising from a risk assessment. Responsible Parties must record their decisions as to which ISMF Standards have been implemented and which ones have been waived or considered as not being applicable to a particular environment within the organisation.

Where, more than one version of standard exists, the year of the publication referenced by the ISMF is cited. New controls from recent publications may be introduced where there is a tangible improvement or benefit to agencies. In such instances, the relevant document is cited.

Agencies and Suppliers that elect to obtain independent certification to the ISO 27001 standard should consult Annex F of this document to identify control objectives that have been retired from the international standard, yet have been retained, as valid risk mitigation techniques for government information and associated information assets.

Standards and controls in the ISMF are only retired if the techniques have been determined as no longer effective, obsolete, duplicated or irrelevant in the context of contemporary information security management in government.

2.6. Application of the ISMF – order of preference

The following list describes the order of preference for ISMF implementation by Responsible Parties. The first three items are mandatory:

1. The baseline of the ISMF described in Annex A applies to all Agencies. An ISMS must be established in alignment to this across the organisation (refer ISMF Guideline 1a for further details).
2. Responsible Parties that own or manage State Government Critical Information Infrastructure (SGCII) must have an ISMS in place that encompasses this infrastructure (refer ISMF Ruling 1 for further details).
3. Agencies must clearly communicate which ISMF Policies and ISMF Standards apply to their Suppliers. The selection of relevant ISMF Standards and controls that apply to Suppliers should be based on the outcome of a risk assessment (refer ISMF Ruling 2 for guidance on information to be managed outside of Australia).
4. Responsible Parties may elect to obtain ISO 27001 certification for parts of their environment. The decision to certify should be based on the relevant significance and importance of the information and/or infrastructure being managed. Typically the decision to certify is driven by a requirement to attain independent assurance that State Government or Agency critical information is being suitably managed.

This order of preference clarifies the position of SA Government in that ISMF adherence is an absolute requirement, that an ISMS encompassing the baseline in the ISMF and for SGCII is established and that the decision to certify an ISMS is at the discretion of the Responsible Party.

2.7. Critical Infrastructure requirements

There are two aspects to Critical Infrastructure that must be accounted for in adherence to the ISMF:

1. All organisations will have some type of ICT systems, services and information assets that are essential to the ongoing operation and survivability of the organisation. These essential functions or activities must be catered for within the organisation's ISMS. Agency Critical Infrastructure is defined below:

Agency Critical Infrastructure [ACI]	Systems, Services, Functions, Platforms, Solutions and associated people, processes and technology which are fundamental to the ongoing functioning and survivability of an organisation. Certain ACI may also be critical to the State (refer SGCII).

2. State Government Critical Information Infrastructure extends beyond a single agency, with adverse impacts or compromise to such services significantly impacting on the social or economic well-being of the State. State Government Critical Information Infrastructure is defined below:

State Government Critical Information Infrastructure [SGCII]	State Government Critical ICT Infrastructure upon which '*Critical Services'* are delivered to the community. If the confidentiality, integrity or availability of this ICT infrastructure is compromised then it could significantly impact on the social or economic well-being of the State, the government, commercial entities or members of the public. (*refer* ISMF Guideline 37a)

Responsible Parties must account for the presence of ACI and/or SGCII when scoping their ISMS implementations.

2.8. Pre-requisite documents

Responsible Parties are referred to a number of external documents, policies and guidelines, standards and handbooks in accordance with this framework.

Electronic versions of the documents referred to within this framework are provided using embedded links where permissible. Certain standards used by the Framework are controlled by strict copyright controls and may be accessed by Agencies that have access to the "autologin" feature provided by SAI Global[3] and those accessing the Internet via the StateNet proxy server. In order to use the "autologin" functions, agency personnel will need to login to their SAI Global account with their subscription credentials. Other Responsible Parties with an active SAI Global subscription can access standards at http://www.saiglobal.com/online or should consult their own hardcopy versions of the standards listed herein.

It is a requirement that, as a minimum, the reference documents described herein are available for referral to the extent permitted by law and applicable government policies and standards:

Required document	Description
Department of the Premier and Cabinet Circular PC030 *"Protective Security Management Framework"* (PSMF)	The Protective Security Management Framework supports the South Australian Government's risk management policy through the requirement for a risk-based approach for the protection of assets and resources to minimise disruption to service delivery and Government operations. This circular outlines the strategic approach approved by Cabinet for a whole of government protective security policy based on the Australian Government's Protective Security Policy Framework (see below). The PSMF addresses the security requirements for Government assets through the application of minimum standards in each of the areas comprising the protective security regime, in order to appropriately treat identified risks.
Australian Government Protective Security Policy Framework (PSPF)	The PSPF is a reflection of the requirements of contemporary Government and private-sector partnership, agile procedural change and the dynamic landscape of information security, particularly in light of constantly evolving ICT technologies and services delivery capabilities. The PSPF is designed to progressively replace the PSM over a period of time.
Australian Government Information Security Manual, Controls (ISM)	The ISM (formerly known as ACSI 33) is a standard that forms part of a suite produced by the Australian Government Australian Signals Directorate [ASD] relating to information security. Its role is to promote a consistent approach to information security across all Australian Government, State and Territory agencies and bodies. It provides a controls and guidance for information that is processed, stored or communicated by government systems with corresponding risk treatments to reduce the level of security risk to an acceptable level. As of 2012 the ISM is issued in three distinct publications: *Executive Companion*, *Principles* and *Controls*. The Government of South Australia ISMF utilises the *Controls* publication extensively as

[3] SAI Global is the retail arm of Standards Australia and provides subscription based and one-off access to Australian and International standards publications.

Required document	Description
	a pre-requisite document. The *Executive Companion* and *Principles* documents may also be accessed directly at the ASD website: http://www.asd.gov.au/infosec/ism/index.htm
ISO/IEC 27001:2013 (International Standard)	Information technology – Security techniques – Information security management systems – Requirements The International Standard for an ISMS, by which, independent certification may be applied.
AS/NZS ISO/IEC 27001:2006 (Australian Standard)	Information technology – Security techniques – Information security management systems - Requirements
ISO/IEC 27002:2013 (International Standard)	Information technology – Security techniques – Code of practice for information security controls
AS/NZS ISO/IEC 27002:2006 (Australian Standard)	Information technology – Security techniques – Code of practice for Information security management
ISO/IEC 27005:2008	Information technology – Security techniques – Information security risk management
AS/NZS ISO 31000:2009	Risk Management – Principles and Guidelines
Code of Ethics for the South Australian Public Sector	Encompasses topics such as: *Handling Official Information*, *Public Comment*, *Use of Government Resources* and *Conflicts of Interest*

2.9. Other relevant materials and services

2.8.1. Supporting publications and literature

Responsible Parties should have regard to publications including, but not limited to, those listed below:

Reference	Description
AS 4811-2006	Australian Standard for Employment Screening (for baseline vetting processes and procedures)
AS ISO/IEC 20000.1:2007 standard	Information technology – Service Management – Part 1: Specification
AS ISO/IEC 20000.2:2007 standard	Information technology – Service Management – Part 2: Code of Practice
AS 13335:2003 standards	Information technology – Guidelines for the Management of Information Technology Security (5 volume standards series)
Australian Government Protective Security Manual, 2005 Edition with revised pages October 2007 [PSM]	The PSM, which has been replaced by the *Australian Government Protective Security Policy Framework* [PSPF], has an aggregate classification of SECURITY-IN-CONFIDENCE which is applied to whole parts, or more of the PSM. Individual sections remain UNCLASSIFIED (For Official Use Only). Access to the PSM is limited to government officers with an established *need-to-know*. The classification systems described in the PSM have been replaced nevertheless it remains a useful reference document for older systems, services and information security deployments that are still used within government.
ISO/IEC 27031:2011	Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity
ISO 22301:2012	Societal security - Business continuity management systems – Requirements
Department of Premier and Cabinet Circular PC012 *"Information Privacy Principles (IPPS) Instruction"* [IPPs]	Government of South Australia Cabinet Administrative Instruction 1/89 also known as the Information Privacy Principles (IPPS) Instruction.
Department of Premier and Cabinet Intellectual Property Policy	This policy provides an enabling and overarching framework to create a supportive environment to: ○ achieve best practice in IP management in Government;

Reference	Description
	○ where appropriate, to facilitate effectiveness of knowledge transfer by Government agencies to the public and private sectors; and ○ achieve effective and timely protection of Government IP and, where appropriate, its commercialisation.
HB 167:2006	Standards Australia handbook *Security Risk Management*
HB 171:2003	Standards Australia handbook *Guidelines for the Management of Information Technology Evidence*
HB 221:2004	Standards Australia handbook *Business Continuity Management*
HB 231:2004	Standards Australia handbook *Information Security Risk Management Guidelines*
HB 254-2005	Standards Australia handbook *Governance, Risk Management and Control Assurance*
HB 292-2006	Standards Australia handbook *A Practitioners Guide to Business Continuity Management*
ISO/IEC 24762:2008 standard	Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
PCI-DSS v1.2.1 (July 2009)	Payment Card Industry (PCI) Data Security Standard. Later versions may be applied. Version 1.2.1 is the minimum version for reference purposes.
Public Sector Act 2009	The Public Sector Act 2009, together with the Public Sector (Honesty and Accountability) Act 1995, replaced the Public Sector Management Act 1995, following proclamation, on 1 February 2010. The Act provides a modern and streamlined employment framework in support of a high performance public sector. Under the Act, agencies and employees across the whole of the public sector will be governed by a comprehensive set of principles, with greater emphasis on 'one government'.
Social Media – Guidance for Agencies and Staff	Social Media Guideline - creates awareness of the opportunities that social media presents, as well as making agencies and staff aware of how to manage the risks associated with the use of this kind of technology
StateNet Conditions of Connection	An implementation of ISMF access control requirements stipulating mandatory requirements to the enterprise network that is centrally operated and managed on behalf of South Australian Government

Reference	Description
	Agencies. (internal to SA Government: available to ITSAs via GovDex).
State Records Act 1997	South Australian Records Act
Treasurer's Instruction 2	Financial management policies, stipulates obligations and expectations on how South Australian Government entities manage risk management requirements (such as major ICT projects and initiatives).

2.8.2. Advice and assistance on aspects of cyber security management and policy

Agency personnel are reminded to contact their IT Security Adviser [ITSA] for initial guidance on cyber security matters and/or their Agency Security Adviser [ASA] for advice and assistance on protective security matters. These contacts are provided for additional assistance and escalation purposes only:

Topic	Organisational contact
Protective security (SAPOL)	Police Security Services Branch Telephone: (08) 8207 - 4008
Cyber security policy (DPC)	Cyber Security and Risk Assurance Group Telephone: (08) 8226 - 3383 CISO@sa.gov.au
Cyber-crime (SAPOL)	Electronic Crimes Section Telephone: (08) 8127 - 5030
Identity crime (SAPOL)	Your local police station https://www.police.sa.gov.au/contact-us/find-your-local-police-station
Freedom of Information and privacy hotline (State Records SA)	State Records of South Australia Telephone: (08) 8204 - 8786 privacy@sa.gov.au foi@sa.gov.au
State Records of South Australia (State Records SA)	General Enquiries Telephone: (08) 8204 - 8791 srsaGeneralEnquiries@sa.gov.au

3. EXECUTIVE OVERVIEW

This framework references a set of policies, standards, guidelines and control mechanisms for South Australian Government Agencies to use in developing their information security capabilities. It is a companion framework to the South Australian Government's Protective Security Management Framework [PSMF] and has been designed as a practical, useable framework, which can be implemented readily by South Australian Government Agencies and Suppliers to the Government of South Australia. The framework, when used in conjunction with the PSMF, addresses all aspects of security that are relevant to an Agency's use of Information and Communication Technology [ICT] to support and advance its business objectives.

The ISMF deals with cyber security management.

Responsible Parties must comply with the ISMF for all of their cyber security undertakings including in circumstances where information has a National Security classification.

Responsible Parties that use ICT equipment to store, process or communicate classified information should also comply with the Australian Government Information Security Manual [ISM] as far as practicable. Agencies contemplating the use and/or handling of National Security classified information should refer to the State's Chief Information Security Officer [CISO] for further advice or guidance.

The PSMF sets out the strategic approach approved by the SA Government for a whole of government approach to protective security based on the Australian Government's protective security policies. This document sets out the requirements for the protective security of information stored on or processed by Information and Communication Technology [ICT] equipment (cyber security). The *Background* and *Information Security* sections contained in the PSMF serve as the introduction to the ISMF. The Australian Government PSPF, (*Information Security Management Protocol*) must also be read and understood and it should be noted that this section pertains to security of both ICT and non-ICT information (e.g. paper documents).

The PSMF makes it clear[4] that:

- The Chief Executive of an Agency is accountable for the development and management of an Agency Security Plan. Section 4.2 and 4.3 of the PSMF describe in detail the roles and responsibilities of the Chief Executive.
- A risk-based approach is to be taken to Protective Security, supporting the Agency's goals and resources.
- Information security is one component of security, and must be addressed in an Agency's Security Plan (using a risk management approach, typically an Information Security Management System or ISMS).

[4] See Section 5.1 of the PSMF

- ICT Security is one component of information security, and must also be addressed in an Agency's Security Plan.

- Agencies must comply with this Framework for all their cyber security (including in circumstances where information has a National Security classification).

- Agencies that use ICT equipment to store, process or communicate classified information must comply with this Framework, and should also apply relevant controls from the Australian Government Information Security Manual [ISM]. Agencies contemplating the use and/or handling of National Security classified information should refer to the State's Chief Information Security Officer [CISO] for further advice or guidance.

Suppliers, who store, process or communicate Official Information, or otherwise interact with the South Australian Government ICT environment have the potential to disrupt the assured ICT environment that is the objective of this framework. Suppliers will have contractual arrangements as described in section 2.1 of this framework that require them to comply with this framework and, by association, specified parts of the Australian Government Information Security Manual.

The most significant changes from previous versions of the ISMF are that this version:

- Takes a standards-based approach and requires parties to establish and maintain an Information Security Management System [ISMS].

- Is a framework to direct Responsible Parties in the development of their internal policies and procedures to secure information on behalf of the South Australian Government, rather than a security manual.

- Leverages the PSMF, relevant ISO and AS/NZS standards and refers the reader to Australian Government documents such as the Australian Government Protective Security Policy Framework [PSPF], Protective Security Manual [PSM] and Information Security Manual controls [ISM] as appropriate.

The revised ISMF defines requirements principally by referencing Australian, International and other recognised standards. The most significant of the standards referenced are:

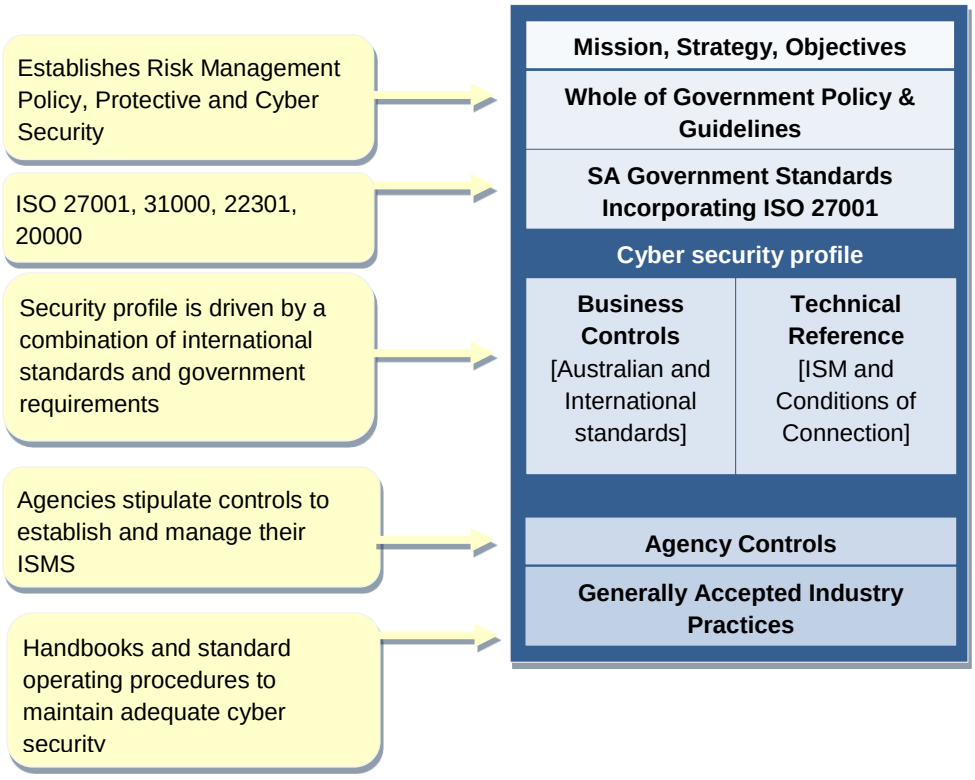
- AS/NZS ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements;

- AS/NZS ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls

Agencies are encouraged to consider certification of all or part of their Information Security Management Systems to Australian Standard 27001.

Responsible Parties, with contractual conditions that require it, are required to obtain certification of relevant parts of their Information Security Management Systems to Australian Standard 27001 (or conversely the ISO/IEC equivalent publication in the case of offshore and foreign entities).

Figure 1. Structure of the SA Government ISMF



The ISMF:

- Deals with cyber security management.
- Is a framework, designed to align with existing policies and standards to the greatest extent possible.
- Aims to provide compatibility with successor versions of the standards referenced in this document as they are released, with minimal requirement for revision of the framework.
- Provides the basis to obtain objective independent assessment of the Responsible Party's level of compliance with the requirements of the ISMF.
- Requires:
    - Agencies to incorporate a cyber security management plan as a component of their Agency Security Plan as introduced in the PSMF.
    - Agencies to consider certification of all or part of their Information Security Management Systems to Australian Standard 27001.
    - Suppliers, with contractual conditions that require it as described in section 2.1 of this framework, to obtain certification of relevant parts of their Information Security Management Systems to Australian Standard 27001.
- Describes requirements for cyber security management in the conduct of business between an Agency and its Suppliers and also between a Supplier and its suppliers.

3.1. ISMF objectives

The ISMF provides a framework for an assured information security environment, utilising risk management and other processes and principles stipulated in the PSMF.

The objectives of the ISMF are to:

- support the attainment and realisation of three information security objectives across Government: Confidentiality (including information the Government keeps about members of the public), Integrity and Availability of information.
- provide a framework to enable government to achieve an assured cyber security environment.
- achieve the assured cyber security environment by using risk management and other processes and principles required by the PSMF; and by:
    - Conforming to the PSMF
    - Facilitating, not hindering Agencies' business
    - Conforming with State Records management requirements as set out in the *State Records Act 1997* and any other Standards and Guidelines issued under the State Records Act
    - Maintaining consistency with:
        - The Organisation for Economic Co-operation and Development's [OECD] nine principles for the security of information systems and networks[5]
- describe the data classification mechanisms required by the PSMF;
- prescribe a risk assessment process to identify ICT information assets and the level of risk associated with these assets in a manner that is appropriate to the business of the Agency and that can be consistently applied by Responsible Parties;
- assist the Responsible Party in developing an Information Security Management System [ISMS] suitable for use with South Australian Government information assets that applies appropriate security controls to permit the efficient and secure access to information assets in a manner that is consistent across all SA Government Agencies;
- refer Responsible Parties to best practise control processes and measures that are regularly updated to account for new technologies, threats and risks as they may arise;
- identify management processes to enable Agencies to obtain assurance on an ongoing basis as to the effectiveness of their information security measures;

[5] Available at http://www.oecd.org/

- establish a communication process to ensure that there is a high level of awareness and commitment to information, particularly ICT based information, security requirements across government;

- protect the privacy, confidentiality and integrity of all electronic government information including that of SA Government clients and any information the Government keeps about members of the public.

3.2. Agency program and policy creation

When South Australian Government Agencies create their own information security programs and specific policies, it is a requirement that they align with South Australian Government cyber security policies and the standards detailed in this framework[6], and be guided and informed by the remainder of this framework.

3.3. Risk assessment and classification

Responsible Parties must address the risk assessment and classification requirements outlined in this framework with regard to their information assets, to ensure appropriate, business focused standards and controls are implemented.

Information security is founded on risk management. Responsible Parties must manage risks to reduce their likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes. Absolute security is unaffordable, often unachievable, and may impede business objectives and/or efficiencies.

Appropriate risk management and information classification, controls and handling ensure that cyber security is implemented proportionately to and in alignment with business requirements.

3.4. Cyber security considerations

Every organisation (Responsible Parties in the context of this framework) uses information; most depend upon it. A vast amount of Official Information[7] is stored on, processed by, or communicated using ICT equipment. Responsible Parties are reliant on information systems and networks that are faced with a wide range of threats that have the potential to damage the confidentiality, integrity or availability of their ICT information. Such threats continue to increase as society's broader dependence on electronically stored, processed and transmitted information increases.

Sources of threats include computer-assisted fraud and cyber-crime, identity theft, espionage, sabotage, vandalism, natural hazards such as fire and flood, computer virus infections and

[6] Section 17 of this framework describes legal and regulatory obligations

[7] *Official Information* is a defined term, consult the glossary for full definition

malware, computer hacking, denial-of-service attacks and social engineering attacks such as phishing. Incidents and attacks have become more common, more ambitious and increasingly sophisticated. Monetary gain rather than notoriety and/or nuisance now motivate a significant proportion of attacks. Further, the interconnecting of public and private networks, and sharing of information resources increases the difficulty of achieving an assured environment. Inappropriately or poorly managed technology and/or neglect of human factors may increase vulnerability and hence risk.

Protecting the information is of vital importance. The consequences of damage to the confidentiality, integrity or availability of an Agency's or its Suppliers' information includes:

- Inability to maintain important community services such as healthcare, transportation, policing and emergency/crisis response,
- Inability to maintain vital Government operations such as revenue collection,
- Failure to maintain legal compliance
- Financial loss
- Loss of public confidence in government ICT systems and consequential loss of public confidence in Government

Information security is founded on risk management. Responsible Parties must manage risks to reduce their likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes. Appropriate risk management and information classification, controls and handling ensure that cyber security is implemented proportionately to and in alignment with business requirements.

3.5. Effecting behavioural change with cyber security governance

Responsible Parties must establish Governance of cyber security that demonstrates commitment from the highest levels of the organisation to a culture of security and appropriate information handling based upon information classification and handling relative to that classification.

The Governance group must establish, maintain, review and refine strategy, policy and objectives for ICT security.

Cyber security is driven by business requirements and objectives, and is therefore no different from any other form of security, in that it is a matter for governance and for management. Security should contribute to, rather than hinder such goals and objectives. Successful security requires an organisation culture that emphasises the importance of security at all levels and across all business units. Only the executive management (or the board, if there is one) has the necessary authority, accountability, knowledge and experience to:

- Establish strategy, policy and objectives for cyber security in accordance with the organisation's business needs, as part of its overall Protective Security strategy and its overall risk management strategy.

- Assess the value of the ICT assets, identifying those that are most critical (i.e. Essential or Important), and deciding the safeguard level for such assets.
- Assign priorities to the investment in information security.
- Establish an organisation wide security management system.
- Ensure organisational compliance with information related legislation.
- Establish a culture of security-awareness throughout the organisation, so that security is regarded as a part of doing business.

3.6. Waivers (Exemptions) to certain provisions or standards

ISMF version 3 introduces the requirement for Agencies to establish an Information Security Management System [ISMS] that conforms to the principles of the AS/NZS ISO/IEC 27001 standard. Therefore it is expected that the 'Statement of Applicability' for the ISMS will identify relevant standards and controls that reflect the information security requirements for each business.

In exceptional circumstances, it may be necessary for an Agency to seek an exemption to select standards or provisions issued under the ISMF. In such instances the waiver must be approved by the Agency Chief Executive and the decision recorded in supporting ISMS documentation.

In all circumstances, the waiver must be in accordance with the conditions described in section 5.8 of the PSMF.

3.7. Acknowledgements

The development and on-going maintenance of this framework has been co-ordinated by the Office of the Chief Information Officer on behalf of the South Australian Government.

The significant assistance and contributions provided by the members of the South Australian Government Information Security Reference Group and by the members of the ICT Security Special Interest Group and the members of the Chief Technology Officer Reference Group in the development of preceding versions of the ISMF prior to version 3 is acknowledged.

The project team for version 3.0 of the framework acknowledges members of the Department of Premier and Cabinet [DPC], Information Technology Security Advisers [ITSAs], the CTO Reference Group (now defunct), the Internal Audit Forum, the Crown Solicitor's Office and the Security and Risk Steering Committee (now defunct) for their assistance during development of this edition of the ISMF.

4. INTRODUCTION

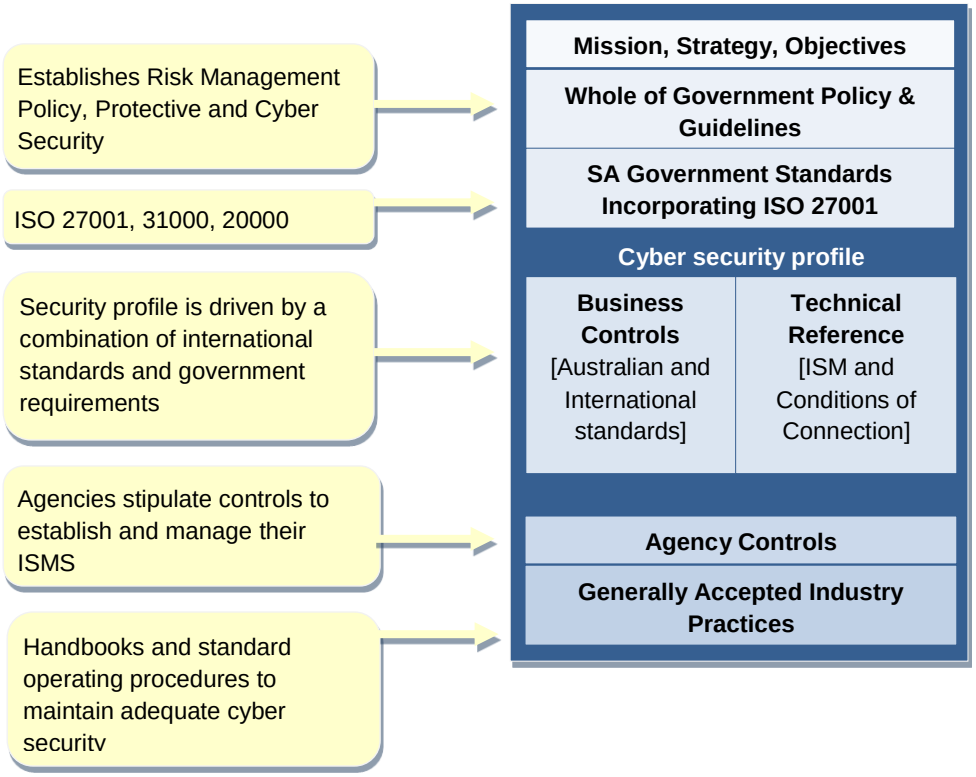
This framework for the management of ICT information security ('cyber security') has been established as an initiative of the South Australian Government.

The framework presents a consistent approach to information security management and development, regardless of the size, complexity or nature of the Information and Communication Technology [ICT] environment.

This section describes the key components required to establish a security profile based upon AS/NZS ISO/IEC 27000 series standards, guidelines and practices.

The figure below depicts a conceptual model of the South Australian Government ISMF. It is designed in a way that allows an interoperable and consultative process for the agreement, implementation and ongoing management/refinement of a whole of government approach to information security management.

Figure 2. Structure of the SA Government ISMF



This framework comprises the following key elements:

- **South Australian Government Information Security Policies**

  Each major section of this document (sections 4 to 17) contains Policy Statements that apply to Responsible Parties. They are high-level statements of the South Australian Government's position with respect to information security. The policy statements contained herein should be considered a baseline of policy statement applicable to all Responsible Parties that may incorporate additional policy statements applicable to the specific activities and nature of their respective business undertakings.

- **South Australian Government Information Security Standards**

  Each sub-section from section 5 onwards contains a number of South Australian Government ISMF Standards in support of that section's policy statements. They describe specific obligations under each of the South Australian Government information security policies. The application of these standards in supporting Policy Statements is the outcome of a risk assessment and the specific nature of the activity being conducted by the Responsible Party.

- **Recommended South Australian Government Agency Information Security Standards and Control Measures**

  Additional guidance is provided to assist Responsible Parties in developing their own specific information security standards in order to implement the required South Australian Government standards, based on their risk assessment outcomes. Some of this guidance is general in nature. Each section contains, where appropriate, additional controls for Responsible Parties to consider and/or implement that are based upon the respective classification levels of ICT information assets.

- **Generally-Accepted Industry Practices**

  Included in the framework are a set of practices that have been developed to provide additional guidance to Responsible Parties where appropriate. These guidelines constitute the most dynamic part of the framework as additional cyber security issues are addressed or updated. External publications entitled 'ISMF Guidelines' are also available for consultation and implementation to fulfil the stated objectives of South Australian Government cyber security policy and corresponding standards.

4.1. Establishing an Information Security Management System

Policy Statement 1

Responsible Parties must develop or have in place an Information Security Management System [ISMS] that conforms to the principles of AS/NZS ISO/IEC 27001.

When the Responsible Party is a Supplier, they must obtain and maintain certification that their information security management system conforms to AS/NZS ISO/IEC 27001 if their contractual obligations require this as described in section 2.1 of the Information Security Management Framework.

Agencies should obtain independent Certification from a recognised authority, such as an Accredited certifying body, that they comply with the AS/NZS ISO/IEC 27001 standard.

The scope of the ISMS (processes, systems, and geographic locations) must be documented and a Statement of Applicability must be developed. It should be noted that Agencies wishing to certify all or part of their ISMS against the AS/NZS ISO/IEC 27001 standard will need to align their controls with the Annex contained in that standard.

Executive management and Boards of those Agencies that do not pursue full certification must satisfy themselves that information security measures are adequate.

Management decisions concerning Certification of all, part or none of the ISMS must be recorded as part of the ISMS documentation.

For the purposes of practical implementation guidance, the controls described in this framework have been aligned with the AS/NZS ISO/IEC 27002:2006 standard which is a guideline document and cannot be used for certification. The controls in AS/NZS ISO/IEC 27002 are prefixed by an “A” for certification purposes and are described in Annex A of the AS/NZS 27001 standard. It should also be noted that all “should” statements contained in the controls for 27002 become “shall” or mandatory statements when the 27001 standard is referenced.

4.1.1. Overview of the ISMS quality management lifecycle

The ISMS is a quality management system, using the Plan – Do – Check - Act [PDCA] cycle, also known as the “Deming Cycle”, for business process improvement based upon Total Quality Management [TQM] principles. In the context of Information Security Management, this cycle supports implementation, ongoing management, monitoring and improvement. The ISMS takes a risk management approach, operating within the context of the Responsible Party’s overall business risks. The ISMS’ purpose is to apply appropriate safeguards to reduce the likelihood and/or mitigate the consequences of unacceptable risks with respect to information security management. The ISO/IEC 27001:2013 standard no longer stipulates a particular approach to achieving continual improvement although the Deming Cycle is presented within the ISMF as one such method of achieving this objective.

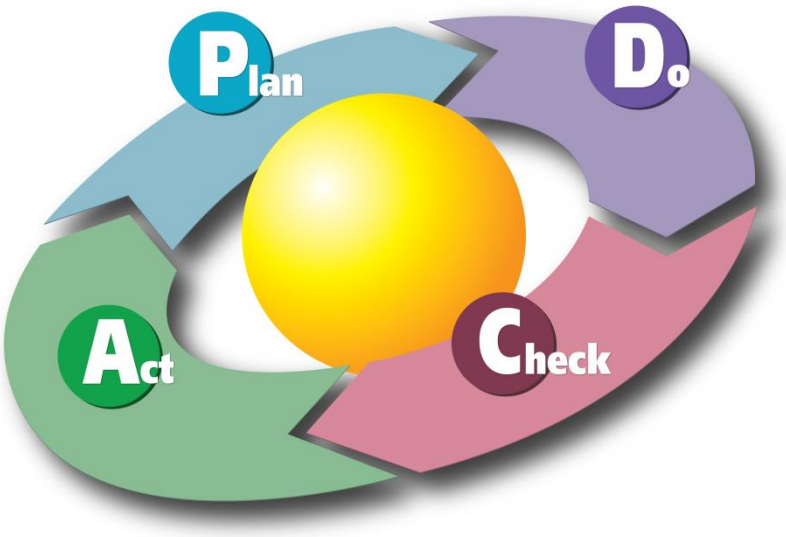


Figure 3: PDCA or Deming Cycle used by ISMS Standards

(Image attributed under Creative Commons BY-3.0 license: ***Karn G. Bulsuk*** *http://karnbulsuk.blogspot.com/)*

The PDCA cycle consists of the following elements, or stages:

- **Plan**

  Establish strategy, policy, objectives, targets[8], processes and procedures to manage risk and improve cyber security in accordance with business needs, strategy, polices and objectives.

- **Do**

  Identify and classify assets, conduct risk assessment, and implement and operate controls to manage cyber security risks in a manner consistent with overall business risks.

- **Check**

  Monitor and review the performance and effectiveness of the ISMS, using objective measurement.

- **Act**

  Review outcomes and performance indicators or benchmarking findings, and act accordingly to continually improve the ISMS.

[8] Strategy, policy, objectives and targets are governance & management responsibilities.

4.1.2. Documentation requirements

Responsible Parties should establish standards documentation for the ISMS as early as possible, akin to other business processes. Responsible Parties must document those parts of their ISMS for which certification is sought or maintained. The AS/NZS ISO/IEC 27001 standard describes minimum documentation standards and requirements for certification purposes and the section entitled 'Information Security Documentation' in the ISM provides useful guidelines and controls to assist Responsible Parties in managing documentation requirements. Further reference information on documentation requirements for ISMS systems may also be found at http://www.iso27001security.com.

Auditors reviewing the ISMS or performing certification audits will require this documentation.

4.1.3. ISMS requirement

Each Responsible Party must develop or have in place an Information Security Management System that **conforms to the principles** of *AS/NZS ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements*. The diagram in *Figure 4* below is based on ISO 27001:2006 requirements and provided for informational and reference purposes only.

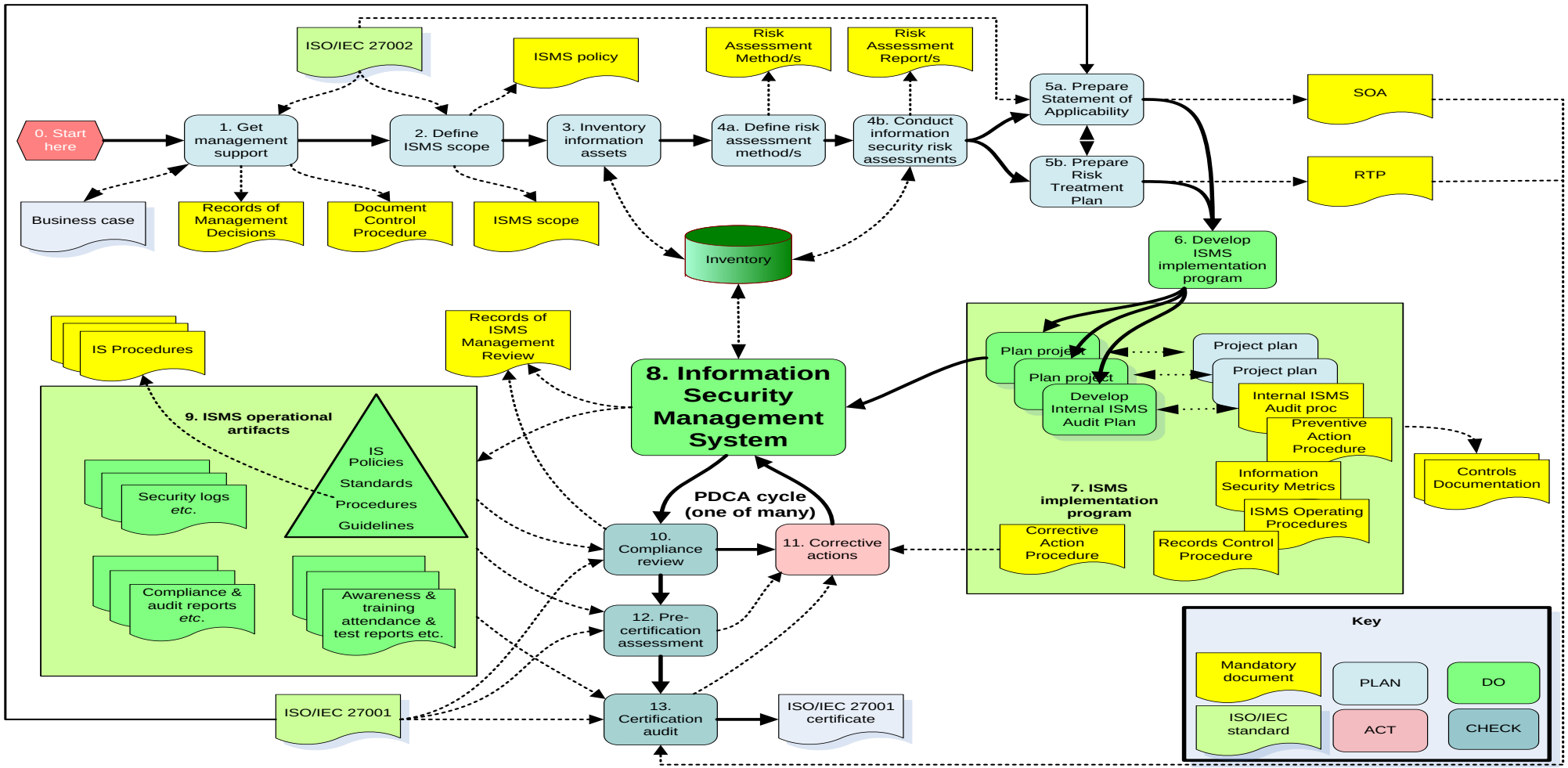


Figure 4: ISMS Implementation and Certification Process for ISO/IEC 27001:2006

(Reproduced and modified with permission: ISO 27k Implementers' Forum http://www.iso27001security.com/)

4.1.4. ISMS certification requirements

Suppliers with contractual obligations as described in section 2.1 of this framework that stipulate an ***ISMS certification requirement*** must obtain and maintain certification that their information security management system conforms to *AS/NZS ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements*.

Agencies should obtain and maintain independent certification from a recognised authority (such as an 'Accredited' certifying body) to the AS/NZS ISO/IEC 27001 standard. Certified compliance of the ISMS provides independent assurance that the Agency's information security management posture is appropriate to executive management, boards, ministers, parliament and the public.

Each Agency has discretion in making the decision to obtain certification for their ISMS, particularly with regard to any cost-benefits findings. For example:

- Agencies may decide that the relatively low value of their information assets and/or the low-impact consequences of security failures do not warrant Certification. In all cases, such Agencies must conduct a risk assessment in accordance with this framework and maintain all associated documentation leading to the decision not to seek certification.

- An Agency may decide to certify only part of its ISMS, even though it believes the whole ISMS to be compliant. Components may be deemed an acceptable risk, such as an application that has operated unchanged for many years without incident. Similarly a cost-benefit analysis may determine there is limited value in certifying all sites where the ISMS operates; for example, a small regional shop front might be excluded.

Management decisions concerning certification of all, part or none of the ISMS must be recorded as part of the ISMS documentation, in accordance with AS/NZS ISO/IEC 27001 "documentation requirements".

4.2. Assurance of cyber security measures

Executive management within Agencies must satisfy themselves that information security measures are adequate. SA Government recommends that Responsible Parties should reference an appropriate assurance model such as the IT Assurance Guide using COBIT, available from http://www.isaca.org.

4.3. Compatibility with other management systems

The quality management system defined in AS/NZS ISO/IEC 27001 (or ISO/IEC 27001:2013) is intended "*to support consistent and integrated implementation and operation with related management standards.*" Agencies should pursue such consistency with any other standards-based management systems that they operate such as the organisational risk management system. Suppliers may also elect to pursue consistency with any other standards-based management systems that they operate.

5. INFORMATION SECURITY RISK MANAGEMENT

5.1. Risk management

Policy Statement 2

Each Responsible Party shall develop and use information security risk management processes as outlined in section 5.1 of the PSMF. The risk assessment process shall include the identification and assessment of security risks for information assets, a summary of the Agency's response to these risks and provide ongoing monitoring and review of the risks and the potential security exposure(s).

Standards

5.1.1. Risk identification and assessment

The objective of a risk assessment is to gain an understanding of the value of and the security risks associated with an information asset and to agree on what controls are appropriate to reduce the level of risk or to lessen the impact of a security breach.

ISMF Standard 1 (Risk identification and assessment)

Key information security risks shall be identified, documented and assessed for all information assets (ISMF Standard 16) within the scope of the ISMS, in accordance with the ISO/IEC 27005 standard and/or the AS/NZS ISO 31000 standard.

Business Controls

The guidance below is provided to assist Responsible Parties in development of their controls in compliance with the above ISMF Standard. It should be considered in association with a risk assessment of the relevant information assets. High-level guidance on risk assessment and treatment is described in clause 4 of the AS/NZS ISO/IEC 27002:2006 standard. (There is no equivalent guidance provided in the ISO/IEC 27002:2013 standard).

The following guidance applies regardless of the classification levels of the information assets:

S1.1. Responsible Parties shall implement an Information Security Risk Management methodology that is based on or compatible with the ISO/IEC 27005 standard and/or the AS/NZS ISO 31000 standard

S1.2. Responsible Parties should consult the AS/NZS ISO 31000 standard (formerly AS/NZS 4360) as necessary to ensure that the Information Security Risk Management applied is in alignment with the broader organisational Risk Management process

R1.3 *Part B, section 2 of the PSM is a useful resource for describing security risk management principles*

S1.4. The Business Owner is responsible for ensuring that risk identification is undertaken and that appropriate input is obtained from information custodians and information users. Security risks must consider key threats and vulnerabilities of the information asset together with any business initiatives potentially impacting the security of the information asset.

S1.5. The risk identification should summarise the key potential risks to achieving the required level of security for the information asset in relation to each of the three security objectives (confidentiality, integrity and availability), and supporting the classification requirements for the information asset (Policy Statement 8).

S1.6. In identifying risks to the integrity, confidentiality and availability of information assets, consideration should be given to the following:

- including references or pointing to the PSMF and ISMF on an Agency's risk and/or compliance register
- physical location and environment;
- extent of use and transmission;
- attractiveness to theft or change (potential value to employees or third parties);
- potential for error;
- nature of computer operations tasks;
- network environment and structure;
- transactional integrity requirements (including evidentiary weight);
- known or previous incidents;
- extent and nature of system or application changes;
- source of data and nature of data entry;
- nature of access and use of information, including the identity of those who access and use the information.

S1.7. An assessment of risk for the three security objectives for each information asset (or grouping of like-assets) should be performed giving consideration to:

- the business impact likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information asset, and;
- the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

S1.8. The Business Owner should review the security risk rating and either:

- accept and monitor the security risk; or
- identify further actions necessary to control, manage, transfer or monitor the security risk.

S1.9. The risk identification and assessment outcome and the actions already taken should be documented in a security Risk Profile for the Responsible Party. This report should clearly identify the selected management action that has been applied to the identified risk, namely:

- Treatment : control(s) have been applied to reduce the risk's likelihood of occurring

- Transfer : the management of the risk has been transferred to another Responsible Party
- Tolerate : the risk falls with acceptable thresholds or the identified business impact is unlikely and/or minimal
- Terminate : the risk has been eliminated or a decision has been made to cancel or eliminate the activity giving rise to the identified risk

S1.10. The overall risk assessment and proposed actions should be reviewed and approved by the Principal Officer (involving executive management, specifically the Agency Security Executive). For all proposed actions, responsibility should be allocated and a date for completion set. Monitoring processes should then be established to ensure satisfactory completion by the relevant date. Typically, this is achieved by having the Principal Officer sign off on the ISMS annually or whenever significant changes occur.

S1.11. The risk assessment should be updated on an annual basis or if any event occurs which may materially impact an existing risk assessment and the controls in place, e.g. change in location / use of information assets, major system implementation (application, operating environment or hardware), change in personnel, contracting or sourcing arrangements, changes in business or objectives.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

1. SECURITY POLICY

6.1. Information security policy

Policy Statement 3

Agencies must establish a documented Information Security Policy and demonstrate their ongoing support for and commitment to information security incorporating ongoing review and improvement, as required, of the information security policy across the organisation.

Standards

6.1.1. Information security policy document

ISMF Standard 2 (Information security policy document)

Each Agency must establish and maintain an Information Security Policy document that is approved by executive management (namely the CE and/or ASE), which states management commitment and sets out the Agency's approach to managing information security. The policy must, at a minimum implement the control(s) described in A.5 of the AS/NZS ISO/IEC 27001 standard. Suppliers are required to comply with Agency Information Security Policies if their contractual requirements require them to do so.

Business Controls

The guidance below is provided to assist Responsible Parties in developing their controls in compliance with the above-listed ISMF Standard. It should be considered in association with a risk assessment of the relevant information assets, maintain accordance with business relevance and objectives and adhere to relevant laws and regulatory compliance requirements.

The following general guidance applies regardless of the classification levels of the information assets.

S2.1. The policy should, at a minimum, incorporate the implementation guidance described in clause 5.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 5.1.1 of the ISO/IEC 27002:2013 standard).

S2.2. Information Security Policy that is developed by an Agency must be aligned with SA Government policy as defined within this document.

S2.3. Additional guidelines for consideration in policy formulation are described under the section entitled 'Contents of Information Security Policies' on page 25 of the ISM.

S2.4. Agency specific standards, procedures and controls that will implement the policy should be established for all of the relevant areas under the guidance provided, as well as all whole-of-government standards.

S2.5. Agencies should establish the relevance of each standard (and associated procedures and controls) based on the classification of the information assets at risk, as well as a formal assessment of risks relevant to the specific circumstances of the Responsible Party.

S2.6. Information security policies (as distinct from standards and controls) must comply with the Australian Government Information Security Manual [ISM]

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[R] Restricted [C] Confidential [S] Secret [TS] Top Secret	S2.7. Information security policies that deal with National Security classified information or other highly sensitive information based upon classification must be restricted to audiences on a "need-to-know" basis.

6.1.2. Policy ownership and review

ISMF Standard 3 (Policy ownership and review)

Responsible Parties must nominate an owner of their information security policy. The owner of this policy must have approved management authority for the development, maintenance and evaluation of the security policy.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets.

S3.1. The policy evaluation and review process should, at a minimum, incorporate the implementation guidance described in clause 5.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 5.1.2 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7. SECURITY ORGANISATIONAL STRUCTURE

7.1. Internal organisation

Policy Statement 4

Responsible Parties must establish a management framework for governance and oversight of initiation and control of the information security implementation across the organisation.

Standards

7.1.1. Executive management oversight and support for Information Security

ISMF Standard 4 (Executive management oversight)

Executive Management shall ensure that there is clear direction and visible management support for information and asset security initiatives within the Agency.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S4.1. All levels of management within each Responsible Party should adopt the implementation recommendations described in clause 6.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer chapter 5 of the ISO/IEC 27001:2013 standard).

S4.2. A multi-disciplinary approach to information security should be encouraged

S4.3. One executive in each Agency (i.e. the ASE as described in the PSMF) must have designated responsibility for all security related activities.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.1.2. Information security coordination

ISMF Standard 5 (Security coordination)

Responsible Parties shall ensure that information security activities are undertaken in a coordinated manner, spanning multiple roles and responsibilities within the enterprise.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets.

S5.1. Agencies must adopt the implementation recommendations described in clause 6.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 5).

S5.2. Suppliers should adopt the implementation recommendations described in clause 6.1.2 of the AS/NZS ISO/IEC 27002:2006 standard

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.1.3. Information security roles and responsibilities

ISMF Standard 6 (Security roles and responsibilities)

Agencies shall assign roles and responsibilities to appropriate personnel for the protection and management of information assets in accordance with clause 4 of the PSMF. Each Responsible Party must have documented assigned roles and responsibilities in matters pertaining to the ownership, custodianship and protection of information.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S6.1. Agencies shall, at a minimum, assign the roles and functions described in clause 4 of the PSMF.

S6.2. Agencies shall adopt the implementation recommendations described in clause 6.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.1.1 of the ISO/IEC 27002:2013 standard) and should apply the guidelines for security roles and responsibilities described in the Australian Government PSPF.

S6.3. The ISM (Roles and Responsibilities) further elaborate these requirements with respect to cyber security management functions. ISMF Guideline 4b characterises the ITSA function in the context of the South Australian public sector.

S6.4. Suppliers must implement the control(s) and should adopt the implementation recommendations described in clause 6.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.1.1 of the ISO/IEC 27002:2013 standard)

S6.5. Responsible Parties shall ensure that the workforce management function must, with the assistance of the information security administration function, ensure that:

- potential employees (including contractors and temporary staff) are suitably screened prior to assignment in Positions of Trust, and that when applicable, ongoing screening is conducted at regular intervals;

- all employees, contractors and consultants are aware of the Responsible Party's Information Security Policy, Standards and/or procedures;
- information classification, handling and awareness training and induction programs are implemented;
- all employees, contractors and consultants are notified formally of their information security responsibilities under applicable policies and sign a formal acknowledgement thereof;
- controls are in place to ensure that all access to information and systems is revoked simultaneously with any termination of an employee, contractor or consultant's services.

S6.6. All managers of personnel within Agencies shall:

- ensure that personnel in their area of responsibility comply with established procedures relating to access, confidentiality and availability of information and ICT systems;
- ensure that adequate security is maintained consistently over the information systems and associated data for which they are responsible;
- make all personnel aware of their responsibilities in relation to information security, including the section entitled Handling Official Information as described on page 12 of the Code of Ethics for the South Australian Public Sector;
- take appropriate disciplinary steps should they become aware of a violation of the policy or the underlying standards and procedures;
- ensure that responsibility is allocated and adequate training is provided for all critical ICT functions to be performed effectively when the person primarily responsible is not available;
- ensure that segregation of conflicting ICT responsibilities is achieved wherever practical.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.1.4. Segregation of duties

ISMF Standard 49 (Segregation of duties)

Responsible Parties shall segregate conflicting duties to reduce the risk of accidental or deliberate system misuse in alignment with the controls described in the AS/NZS ISO/IEC 27001 standard.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S49.1. Responsible Parties should implement the control(s) and guidance described in clause 10.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.1.2 of the ISO/IEC 27002:2013 standard).

S49.2. Agencies should consider separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorised modification or misuse of information or services.

S49.3. Agency management should ensure that conflicting duties are segregated within the business areas. For example, activities, which require collusion in order to defraud (i.e. raising a purchase order and verifying that goods have been received), should be separated.

S49.4. Where permissible, personnel assignment rotation may be implemented as an aid to identifying possible inappropriate activities, promoting knowledge transfer and assisting business operations continuity.

Additional controls based on DLMs and protective markings

The following table identifies additional guidance specific to the classification levels of the information assets:

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S49.5. There should be split control for highly sensitive information or access to highly sensitive IT assets, so that no single person ever knows or possesses all components. For example, two people might each know half of a sensitive password, half of a cryptographic key or possess one of two keys required to gain access to an area or to activate a device. Where such controls are implemented, secure back-up arrangements should exist to cover personnel absences.
[I4] Integrity 4	S49.6. Application systems should be developed to enforce dual authorisation for sensitive business functions or unusual transactions.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

7.1.5. Authorisation process for Information Processing Facilities

ISMF Standard 7 (Authorisation processes for facilities)

Management authorisation processes should be established for new Information Processing (i.e. hosting) Facilities.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S7.1. Implementation of ISMF Standard 7 meets the requirements described by control 6.1.4 of the AS/NZS ISO/IEC 27001:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 7).

S7.2. Responsible Parties must ensure that when the establishment of a new Information Processing Facility has implications for across Government services delivery, an approval for that facility has been formalised.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.1.6. Incident response and contact with authorities

ISMF Standard 9 (Incident response)

Responsible Parties shall adopt a cooperative approach in responding to and sharing information on security incidents, with the aim of improving the timeliness and efficiency of security incident response across government. Responsible Parties must comply with ISMF Standard 140 - Notifiable Incidents and must maintain procedures stipulating when and by whom Authorities such as law enforcement and other regulatory authorities are to be contacted in relation to information security incidents.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S9.1. Responsible Parties should adopt the implementation recommendations described in clause 6.1.6 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.1.3 of the ISO/IEC 27002:2013 standard)

S9.2. Responsible Parties should contact the Privacy Committee of South Australia for further advice and guidance if an incident involves a breach of personal information

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.1.7. Security industry and sector collaboration

ISMF Standard 10 (Security industry and sector collaboration)

Responsible Parties should establish criteria for and encourage participation in relevant Professional Associations, Special Interest Groups and Information Security Forums. Responsible Parties should ensure that procedures exist for information gathering and dissemination resulting from participation in such forums.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S10.1. Responsible Parties may adopt the implementation recommendations described in clause 6.1.7 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.1.4 of the ISO/IEC 27002:2013 standard)

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.1.8. Projects and project management

ISMF Standard 142 (Projects and project management)

Responsible Parties shall address information security and information security management considerations in all projects irrespective of the specific nature of the undertaking.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S142.1. Responsible Parties must factor information security objectives, including the classification requirements of the information being managed, in to project and program objectives. The Agency ITSA (or equivalent) should be consulted as required.

S142.2. Implementation of ISMF Standard 142 satisfies the requirements and objectives of control A6.1.5 when undertaking an ISO/IEC 27001:2013 certification review.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.2. External organisations (third parties)

Policy Statement 5

Access to information processing facilities by third parties must be controlled and such controls must be agreed to and defined by way of contractual obligation with the external organisation.

Contracts conferring tertiary access (e.g. A supplier who utilises sub-contractors or outsourced suppliers in the fulfilment of their contractual obligations and/or service agreement) should include allowances for designation of deemed eligible participants and the conditions for their access.

Standards

7.2.1. Risk identification associated with external organisations

ISMF Standard 12 (Risk assessment of external organisations)

Responsible Parties must conduct a thorough risk assessment in accordance with Section 5.1 of the PSMF prior to granting access to information and/or information processing facilities by any External Organisation.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S12.1. Responsible Parties must implement the controls described in clause 6.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 15.1.1 of the ISO/IEC 27002:2013 standard) prior to granting access to information and/or information processing facilities by any External Organisation.

S12.2. Responsible Parties should consult the StateNet Conditions of Connection as appropriate.

S12.3. Responsible Parties may embed the use of an assessment tool as a component of the selection process for external organisations, such as the Third Party Security Assessment Tool [TPSAT] available to *Information Security Forum* members.

Cloud computing and Software-as-a-Service (SaaS) implementations:

Agencies need to consider a multitude of factors when considering the adoption of cloud-based services. Business Owners should conduct a risk assessment for third party suppliers in concert with the Agency ITSA that encompasses the following considerations:

1. ***Legislative and jurisdictional risks***

   What legislation governs the service?
   (e.g. what country is the information housed in? under what legislation is the provider bound to adhere? Foreign corporations are often subject to foreign laws)

   Where is the service physically located?
   (e.g. US based services or those that transit via the US are subject to various provisions in US Law)

   Does Privacy legislation exist in that jurisdiction? If so, what are the provisions?

2. ***Terms and conditions of service***

   Do the terms and conditions confer ownership of the information to the provider?
   Do the terms and conditions provide a 'cooling-off period' when changes to terms occur?
   Under what law and jurisdiction are the terms governed?

3. ***User and Identity Management***

   How is identity managed and by whom?
   Who has access to the User and Account Management functions and features of the service?
   Is the user identity dedicated to a particular function and role or is it used for multiple purposes? (note: particularly combined private/public activities)

4. ***Access and Connectivity***

   Is the level of system availability and accessibility acceptable?
   How is connectivity achieved? Is it encrypted? Does it have redundancy? Does it traverse particular jurisdictions such as the United States and/or Singapore, China etc?

5. ***Change Control***

   Does the Agency have a remediation plan in place as a result of:
   - Adverse or undesirable changes to the terms and conditions of use?
   - Change of ownership, tertiary provider or merger & acquisition activity?
   - Changes to foreign and/or Australian legislation (particularly telecommunications, interception and privacy)?
   - Changes in Software/User interfaces/Technical characteristics or access policies from the provider?
   - Discontinuation and/or sudden non-availability of the service resulting from legal proceedings, bankruptcy, non-competition etc. on the part of the provider?

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.2.2. Access controls applied to third parties

ISMF Standard 13 (Access controls applied to third parties)

Access provided to third parties (including customers, contractors etc.) should be controlled based on the specific business requirements of the Responsible Party.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S13.1. Responsible Parties should implement the applicable controls described in the ISM prior to granting access to information and/or information processing facilities by any Third Party.

S13.2. Responsible Parties should implement the controls described in clause 6.2.2 of the AS/NZS ISO/IEC 27002:2006 standard as a generally accepted Industry Practice, prior to granting access to information and/or information processing facilities by any Third Party. (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 13).

S13.3. Part A, paragraph 1.9 of the PSM states that "Contractors to agencies must be provided with relevant sections of the PSM by the agency holding the contract to allow them to meet their contractual obligations". Critical infrastructure owners and operators are also described in this clause. In certain instances contractors may still require access to selected parts of the PSM for ongoing support of legacy systems.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

7.2.3. Security requirements in third party contractual agreements

ISMF Standard 14 (Contractual agreements)

Arrangements involving third party access to Agency information processing facilities shall be based on a formal contract containing, or referring to, all of the security requirements to ensure compliance with the Responsible Party's security policies, standards and obligations.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S14.1. Agencies must implement the controls described in clause 6.2.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 15.1.2 of the ISO/IEC 27002:2013 standard)

S14.2. Agencies must align Third Party Contract Agreements with ISMF Standard 139

S14.3. Suppliers should implement the controls described in clause 6.2.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 15.1.2 of the ISO/IEC 27002:2013 standard)

S14.4. Third parties and their employees, including sub-contracted service providers, who require access to security classified information must be security cleared to the appropriate level. Utilising a Third Party Contract Agreement, the service provider must be required to implement security procedures that ensure that access to Official information assets is restricted to those employees who require access to perform their function.

S14.5. Responsible Parties should establish individual confidentiality agreements with the staff of contractors. Depending on the risk assessment findings and sensitivity of information assets or systems, the Responsible Party may wish to undertake a police records/fingerprint check of an individual or elect to use a vetting process for sensitive Positions of Trust.

S14.8. Responsible Parties should implement the guidance described under controls 15.1.1 and 15.1.3 of the ISO/IEC 27002:2013 standard

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[C] Confidential	S14.6. All personnel must be subject to a security vetting process. Refer to *Authorisations, Security Clearances and Briefings section of the ISM* for further guidance.
[P] Protected [SC] Sensitive: Cabinet	S14.7. All personnel should be subject to a security vetting process in accordance with Personnel Security Protocol of the PSPF. Personnel must be subject to this process when accessing Australian Government information.
Note: for each classification level, controls from lower classifications are retained	

7.3. Security requirements in procurement and sourcing

Policy Statement 6

Access to Agency and Australian Government information provided to prospective Suppliers during tendering and/or procurement processes shall be limited on a need-to-know basis and commensurate with the applicable controls to the information's classification.

Agencies must stipulate and account for security considerations and controls as defined in the PSMF and ISMF and their subordinate documents during all phases of the procurement process.

Standards

7.3.1. Security in procurement and sourcing activities

ISMF Standard 15 (Procurement and sourcing)

Responsible Parties must include and consider the security controls required by the PSMF and ISMF as part of their procurement procedures. Information classification controls must be applied during all phases of the tender and/or procurement process.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S15.1. Agencies must include the requirements of the PSMF and the ISMF in their procurement procedures and should select only those subsets of controls and procedures required according the scope and nature of the project(s) and/or services, products and materials being considered

S15.2. Where a contract requires the service provider to access security classified information, additional matters must be addressed in the evaluation criteria. All tenderers must meet the following requirements:

- a *Conflict of Interest Declaration* must be completed to disclose any potential conflict of interest that would impact on security in the performance of functions or services on behalf of the South Australian Government
- service provider employees requiring access to security classified information must be cleared to the appropriate level
- service provider premises and facilities must be suitable for the storage and handling of security classified information up to and including the nominated level, and

- the service provider must have systems able to meet designated information security standards for the electronic processing, storage, transmission and disposal of security classified information.

S15.3. Suppliers that intend to procure services, products and/or materials via a third party shall obtain written authorisation from the relevant Agency if any classified information needs to be shared with or otherwise released to the third party as part of the Supplier's procurement process.

S15.4. Significant risks identified in the procurement cycle should be reflected in the organisation's risk register and the treatment and/or mitigation strategy should be identified as part of the organisational risk management procedures

R15.5. Responsible Parties shall note the requirements of the PSM as a SECURITY-IN-CONFIDENCE document during procurement procedures, in particular part A paragraph 1.8 of the PSM which states:

*"…where a tender process is being run by an agency, and applicants need to take the cost of compliance with relevant PSM standards into account in their tender, the agency running the tender **must** ensure applicants have access to the sections of this Manual that are relevant to that tender, but not the whole document…"*

S15.6. Responsible Parties may choose to include a generic requirement for information security standards compliance as outlined below during the early stages of procurement such as at the EOI/RFI phase of a tender (more detailed information on specific security and information handling requirements could subsequently be provided to short-listed candidates on a "need-to-know" basis):

"*The ISMF is a whole of Government framework designed to closely align with the AS/NZS ISO/IEC 27002 code of practice for information security controls which leverages the information security objectives of the AS/NZS ISO/IEC 27001 standard.*

Respondents shall state their capability to implement each of the controls contained in the AS/NZS ISO/IEC 27001 standard (Information Technology - Security techniques - Information security management systems - Requirements). If the respondent is not able to implement (or varies their implementation of) any single control contained in AS/NZS ISO/IEC 27001, they shall identify those controls which are modified or excluded and provide a brief statement for each item therein.

Respondents that have attained certification to the AS/NZS ISO/IEC 27001 standard should provide evidence of the currency and scope of their ISMS certification."

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[C] Confidential	S15.7. All personnel (including respondents) must be subject to a security vetting process. Refer to *Authorisations, Security Clearances and Briefings section of the ISM*.
[P] Protected [SC] Sensitive: Cabinet	S15.8. All personnel (including respondents) should be subject to a security vetting process in accordance with Personnel Security Protocol of the PSPF. Personnel must be subject to this process when accessing Australian Government information.
Note: for each classification level, controls from lower classifications are retained	

7.3.2. Security in an outsourced environment

ISMF Standard 139 (Security in an outsourced environment)

Responsible Parties shall ensure that contracts with external service providers specify agency-approved information security policies and procedures and must contain provisions to indemnify the Government of South Australia and its agencies against the outcomes of violations to the aforementioned policies and procedures. While the service provider is entrusted with the management of government data, the government continues to own the data and the agency retains the responsibility of custodianship of the data.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S139.1. Responsible Parties must familiarise themselves with ISMF Ruling 2 in matters contemplating the storage or processing of information outside of South Australia.

S139.2. Responsible Parties should consider the guidance described under control 15.1.3 of the ISO/IEC 27002:2013 standard.

S139.3. Contracts must:

- Identify the obligations of the supplier to prevent a breach of security occurring, in line with Government of South Australia ICT security policies, standards and guidelines and,
- Provide remedies for the Government of South Australia in the event of damage to assets belonging to the government, and the unauthorised access to, use of, or release of information which relates to:
    - the enforcement of a law of the Commonwealth or of a State or Territory
    - the personal affairs of any person
    - the protection of public safety
    - trade secrets and commercial information the disclosure of which could cause advantage or disadvantage to any person
    - any other information that would be exempted under the *Freedom of Information Act 1991* from release.
- Include a requirement to propagate and promote any Agency or governmental information security requirements to their supply chain (as deemed necessary, and amended from time to time),
- Incorporate the requirements described in ISMF Standard 14

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

8. ASSET MANAGEMENT

8.1. Accountability for assets

Policy Statement 7

Information assets must be accounted for and have a nominated Business Owner. Responsibility for implementing and maintaining any controls may be delegated, but accountability remains with the nominated Business Owner.

Standards

8.1.1. Asset inventory

ISMF Standard 16 (Asset inventory)

Responsible Parties must be able to identify their information assets and the relative value and importance of these assets in order to provide commensurate levels of protection:

a) Agencies must compile and maintain an inventory of their ICT assets. The inventory must identify any assets that are components of State Government Critical Information Infrastructure [SGCII]. Each asset shall be clearly identified and its ownership and security classification must be agreed and documented, together with its current location (important when attempting to recover from loss or damage). The purpose of the inventory process is to identify discrete assets, their associated owners and to ensure security controls reflect the classification of the asset.

b) An Agency's asset inventory should be reviewed and signed off by the Principal Officer (in consultation with executive management, specifically the Agency Security Executive). Responsibility for maintaining and updating the asset inventory may be delegated. The asset inventory should be formally reviewed, updated and approved by the Principal Officer on an annual basis.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S16.1. Responsible Parties should implement the controls described in clause 7.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.1.1 of the ISO/IEC 27002:2013 standard)

S16.2. Agencies should implement the guidance described in clause 7.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.1.1 of the ISO/IEC 27002:2013 standard)

S16.3. The primary business use for each information asset should be identified and described. Where applicable, this will include identifying applications (and supporting databases) residing on the hardware domains. For items solely used to transmit information, the business use should reflect this.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

8.1.2. Asset ownership

ISMF Standard 17 (Asset ownership)

Each information asset must have a designated Business Owner, being the person or group that is ultimately responsible for an information asset.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S17.1. A **"Business Owner"** represents the person or group that is ultimately responsible for an information asset. This person or group is distinct from an information custodian, who may take responsibility for the ongoing management of the information (such as a CIO or system administrator). Individual business units own business critical information, rather than information technology or information security departments (they are custodians, not owners). The manager of the business unit responsible for the creation of any information and / or the business unit directly impacted by the loss of the information is usually the Business Owner. A Business Owner or group of Business Owners must be identified for each information asset. For the purpose of ISO 27001 certification, the 'risk owner' is synonymous with the term Business Owner contained in this framework.

S17.2. Information assets may collectively include the logical groupings of information residing on the hardware domains that have a common business use or purpose.

S17.3. An information asset may be a service consisting of multiple assets, in which case a Business Owner must be designated against the service offering.

S17.4. The party most impacted by the loss of confidentiality, integrity or availability of Information is typically the Business Owner.

S17.5. Responsible Parties should implement the guidance described in clause 7.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.1.2 of the ISO/IEC 27002:2013 standard)

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

9. CLASSIFICATION

9.1. Classification requirements

Policy Statement 8

Information must be classified to suitably reflect its importance, degree of sensitivity and protection requirements and such classification should be periodically reviewed.

Once assigned a classification, the information must be appropriately handled to adhere to protection controls for confidentiality, integrity and availability as well as any other special handling measures applicable to the defined classification of the information.

Standards

9.1.1. Classification of information and associated assets

ISMF Standard 19 (Classification)

Each information asset (or logical grouping of like-assets) identified by an Agency shall have a designated Business Owner. The designated Business Owner shall make decisions about the classification of the Agency's information assets.

a) The classification of each information asset must be documented in accordance with the entirety of the *Asset Management* section of the ISMF. This documentation should also align with clause 6.6.2 of the AS ISO/IEC 20000.2 standard encompassing service management.

b) Business Owners must ensure that information is classified to satisfy appropriate handling controls encompassing confidentiality in Table 1 and/or Table 2 of the ISMF (as applicable), and integrity and availability in Table 3 of the ISMF. The decision to classify information for confidentiality purposes must be based solely on the guidelines provided in the ISMF and the Australian Government Information Security Management Guidelines and for no other reason as described in Australian Government Information Security Management Protocol. Business Owners should refer to the State Chief Information Security Officer [CISO] for assistance in classification matters related to National Security classified assets.

c) The information classification should be reviewed and approved by the Principal Officer (in consultation with executive management, including the Agency Security Executive) as part of the review and approval of the information asset inventory. Classification reviews should consider the guidance described in Australian Government Information Security Management Guidelines.

d) Each Agency must have an information classification procedure defined in accordance with the requirements identified in Section 5.2 of the PSMF.

e) Responsible Parties must protect information received from another Agency or other Australian jurisdiction according to the protective markings (classification) applied by the originating Agency or jurisdiction, regardless of media.

f) Responsible Parties must not alter, remove or otherwise modify the protective markings (classification) applied to Information originating from another Agency or other Australian jurisdiction without the express written permission of the Business Owner (or equivalent) from the originating Agency/jurisdiction. This requirement cannot be waived by the receiving Responsible Party.

Table 1. Dissemination Limiting Markers

South Australian Dissemination Limiting Markers [DLMs]

		Implementation Guidance		
Marking	**Description**	**Portable Storage Devices**	**Remote Access**	**Media Sanitisation and Re-use**
Public	Information authorised for unlimited public access and circulation, such as agency publications and web sites. Such information should still be accompanied by Integrity and Availability classifications.	Labelling or colour-coding of devices according to classification is recommended per controls 0332-0336 in the ISM.	No special controls applicable	No special controls applicable.
For Official Use Only	Information is only available for official use by South Australian or Australian Government personnel (including authorised contractors). The public release of this information may be authorised by an agency head or agency policy.	PSDs shall only be connected to systems with an equal or greater classification per control 0337 in the ISM. Password control plus basic encryption shall apply. Additional mechanisms for Information marked as Protected should include use of strong ciphers and additional key files. Cryptographic controls and guidance are described in the ISM.	Dual phase password control (Remote Access login and system login) plus transmission encryption as described in the ISM.	Media should be wiped in alignment with ISMF Standard 60. Post sanitisation media classifications for non-volatile magnetic media and for non-volatile flash memory are described in the ISM.
Sensitive (legislation cited) **Sensitive: Personal**	Compromise could cause limited damage to the State, the Government, an agency, commercial entities or members of the public. (refer control S19.13 in the ISMF)		Responsible Parties shall observe the authentication requirements described by ISMF Standard 86 Cryptographic (encryption) mechanisms must be enabled in alignment with the *Cryptography* chapter in the ISM.	
Sensitive: Legal **Sensitive: Commercial** **Sensitive: Medical**	Compromise could cause moderate damage to the State, the Government, commercial entities or members of the public.			
Sensitive: SA Cabinet **Sensitive: Cabinet**	Compromise could cause significant damage to the State, the Government, commercial entities or members of the public. **Sensitive: Cabinet** materials received from the Australian Government must be classified as [P] Protected.	PSD use not permitted without formal exemption process and authorisation by Agency Chief Executive.		Secure wipe per ISM *or* destruction of media per the relevant sections of the ISM.

Dissemination Limiting Markings [DLMs] **must** be applied to documents that are not intended for general public consumption (Public) and are not security classified (PROTECTED and higher). They **may** also be applied to security classified information that uses protective markings. Responsible Parties that use ICT equipment to store, process or communicate National Security classified information must also comply with the Australian Government Information Security Manual [ISM].

Table 2. Security Classifications (Protective Markings)

Classification	Description
[P] Protected	The PROTECTED security classification is used when the compromise of the information could cause damage to the Australian Government including states and territories, commercial entities or members of the public. For instance, where compromise could: • endanger individuals and private entities • work substantially against national finances or economic and commercial interests • substantially undermine the financial viability of major organisations • impede the investigation or facilitate the commission of serious crime, or • seriously impede the development or operation of major government policies.
[C] Confidential	Compromise of the information could cause damage to national security. For instance: • damage diplomatic relations (that is, cause formal protest or other sanction) • damage the operational effectiveness or security of Australian or allied forces • damage the effectiveness of valuable security or intelligence operations • disrupt significant national infrastructure • damage the internal stability of Australia or other countries.
[S] Secret	Compromise of the information could cause serious damage to national security. For instance, compromise could: • threaten life directly • seriously prejudice public order • raise international tension • substantially damage national finances or economic and commercial interests • seriously damage relations with other governments • seriously damage the operational effectiveness or security of Australian or allied forces • seriously damage the continuing effectiveness of highly valuable security or intelligence operations • shut down or substantially disrupt significant national infrastructure • seriously damage the internal stability of Australia or other countries.
[TS] Top Secret	Compromise of the information could cause exceptionally grave damage to national security. For instance, compromise could: • threaten directly the internal stability of Australia or other countries • lead directly to widespread loss of life • cause exceptionally grave damage to the effectiveness or security of Australian or allied forces • cause exceptionally grave damage to the effectiveness of extremely valuable security or intelligence operations • cause exceptionally grave damage to relations with other governments • cause severe long-term damage to the Australian economy.

Table 3. South Australian Government Availability and Integrity Classifications

SOUTH AUSTRALIAN GOVERNMENT AVAILABILITY CLASSIFICATION SCHEME

Classification	Description
A4	ABSOLUTE requirement, meaning that the business would be crippled by the loss and recovery must be virtually instantaneous (no longer than a few minutes).
A3	HIGH requirement, meaning that loss would cause major disruption to the business and recovery must be achieved within a period measured in hours (typically same business day).
A2	MODERATE requirement, implying the loss would have a significant impact and recovery must be achieved within a period measured in days (typically three business days or less).
A1	LOW requirement, meaning that loss of the data would have only a minor impact on the business for an extended period (i.e. “best-effort” recovery).

SOUTH AUSTRALIAN GOVERNMENT INTEGRITY CLASSIFICATION SCHEME

Classification	Description
I4	ABSOLUTE requirement, implying that no inaccuracies or omissions can be tolerated
I3	HIGH requirement, meaning that a loss of integrity would cause significant embarrassment and disruption and might be difficult to detect.
I2	MODERATE requirement, meaning that the Agency would be somewhat affected by a loss of integrity, but the situation could be easily detected and recovered.
I1	LOW requirement, such that there would be minimal impact if the data was inaccurate or incomplete

South Australian integrity and availability classifications should be considered for major ICT assets and critical infrastructure, including public systems and services.

The ISMF describes various information classification controls that apply based on confidentiality, integrity and/or availability classifications.

Integrity and availability markings for information originating from other jurisdictions must be maintained in accordance with the originator’s specifications/scheme.

Business Controls

The following general guidance applies regardless of the classification level applied to information assets:

S19.1. Notwithstanding that the designated Business Owner shall make decisions about the classification of the Agency's information assets, such decisions should be made in conjunction with and after consultation with the Agency ITSA and/or ASA when appropriate to do so.

S19.2. Official Information consists of two types, being:

- material intended for public consumption, and
- information requiring increased security to protect its confidentiality provisions.

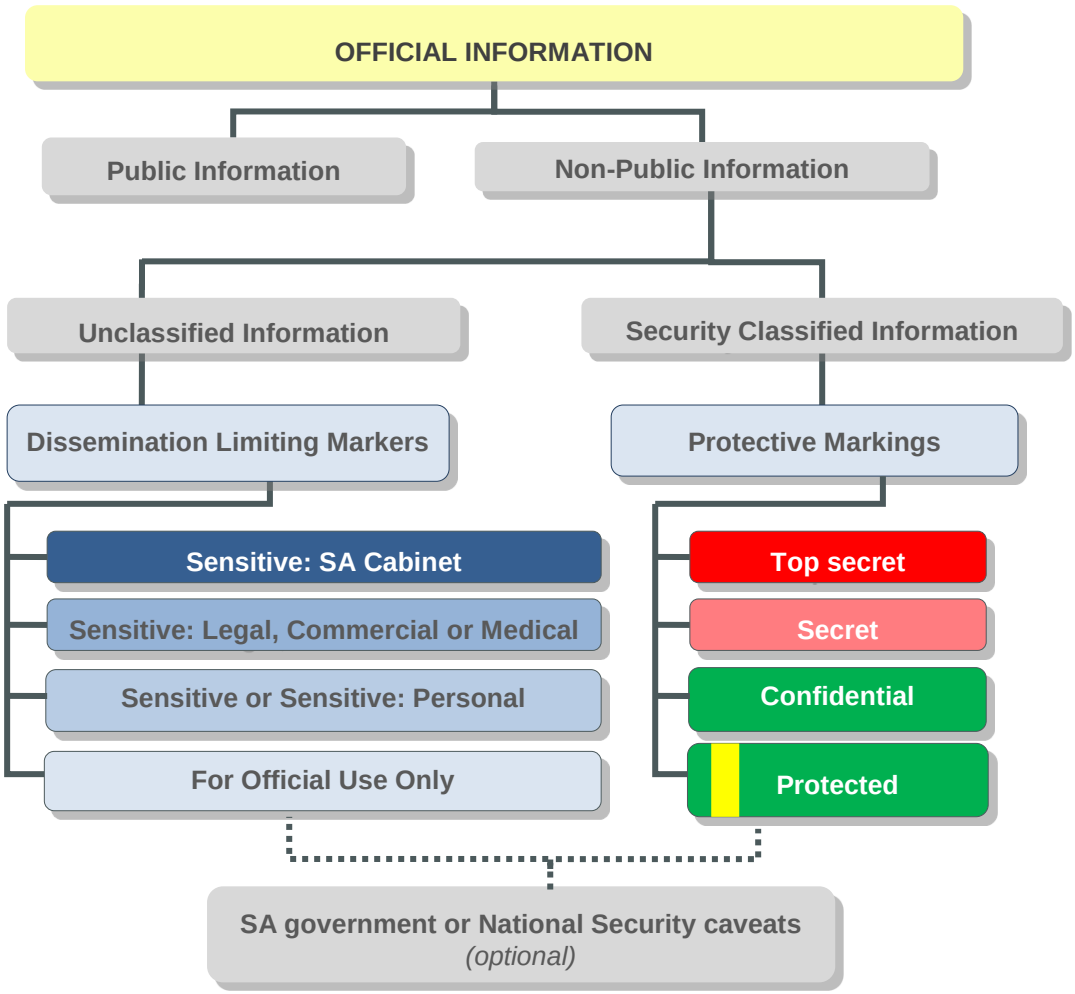


Figure 5: Australian Government Information Classifications and Types

(Image concept derived from Queensland Government Information Security Classification Framework v1.0.1)

S19.3. Public domain material is Official Information that has been authorised for public access or circulation, such as agency publications or web sites. Even if information is

intended for public release or publication, it could have confidentiality requirements before release (e.g., Budget papers). In this case, the point at which the information will be entered in the public domain should also be specified (via the use of caveats). When this information ceases to need confidential treatment, agencies must continue to consider ongoing availability and integrity requirements.

S19.4. All Official Information and information assets not in the public domain must be considered to be 'for official use only' and the 'need-to-know' principle must be applied. This principle means a person must have a legitimate need to access the classified information assets to carry out their official duties. Other justifications, such as position of authority, or the desire to enter controlled areas or access information for the sake of convenience, are not valid.

S19.5. Official Information requiring a protective marking for confidentiality reasons is information that could result in harm or damage to the nation, the State, the public interest, the Government, private entities or individuals through compromise or misuse. Under this security management framework, the selection of controls by each Agency will be based on the classification of information assets at risk. In addition, the specific circumstances of the Agency and their assessment of associated risks may have a significant impact on the controls that should be implemented.

S19.6. Classification and/or dissemination limiting marking(s) [DLMs] may alert accredited Freedom of Information Officers to consider the reasons a particular document has been given a particular classification, when considering it for access under the provisions of the *Freedom of Information Act 1991*. Special consideration should be given to the use of the 'Sensitive' DLM, in which instances the applicable and corresponding sections of legislation must be cited.

S19.7. There are two types of Official Information that require DLMs and/or confidentiality classifications:

- Unclassified information is any official resource (including equipment) that requires moderate levels of protection and does not meet the definitions for 'security classified information'. Most often this information will pertain to:
  - government or agency business, whose compromise could affect the government's capacity to make decisions or operate, the public's confidence in government, the stability of the market place and so on;
  - commercial interests, whose compromise could affect the competitive process and provide the opportunity for unfair advantage;
  - law enforcement operations, whose compromise could hamper or inhibit crime prevention strategies or particular investigations or adversely affect personal safety
  - personal information that is required to be protected under the provisions of Premier and Cabinet Circular No. 12, the *Freedom of Information Act 1991* or other legislation (such as healthcare enactments, legal-professional privilege etc.).
- Security classified information is any official resource (including equipment) that records information about or is associated with Australia's (including states and territories):
  - security from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference

- defence plans and operations
- international relations, significant political and economic relations with international organisations and foreign governments and
- national or state interests, that relate to economic, scientific or technological matters vital to Australia's stability and integrity.

S19.8. Responsible Parties must comply with the ISM in circumstances where information classified for National Security is stored, processed or communicated.

S19.9. Where an Agency considers an information asset to be classified above the PROTECTED level (i.e. CONFIDENTIAL, SECRET and TOP SECRET), they should consult with DPC about appropriate controls to be applied.

S19.10. Where a protective marking is not incorporated to denote specific confidentiality provisions, the information asset is considered to be **For Official Use Only**. Existing Unclassified Official Information may remain unlabelled, however newly created content or content that is modified on or after 1st May 2012 that is considered to be Unclassified must be marked with an appropriate 'dissemination limiting marker' as described in figure 5 of the ISMF. When personal information is involved, any release must comply with any legislative and South Australian Government privacy requirements.

S19.11. Suppliers may adopt the implementation guidance and general principles contained in clause 7.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.2.1 of the ISO/IEC 27002:2013 standard).

S19.12. Agencies shall note that the use of protective markings and/or DLMs is determined by the information (or content) rather than the object type or artefact (e.g. a poster, a letter or a database). In general terms, such markings are conveyed on any document/dataset that contains records management information pursuant to the *State Records Act 1997*, such as file number, folder references etc.

S19.13. Use of the 'Sensitive' DLM (i.e. not predefined as Personal, Medical etc.) must cite the section of legislation or enactment that warrants the use of this DLM and associated handling.

S19.14. Agency implementation of the Availability classifications and the corresponding obligations and controls conveyed by the ISMF satisfies control objective 17.2.1 of the ISO/IEC 27001:2013 standard.

Generally-Accepted Industry Practice:

Not all information assets need to be classified for confidentiality. Information assets must only be classified if the compromise could cause damage. Further information on the issues associated with over classification can be found in section 3.7 of the Australian Government Information Security Management Guidelines*. Integrity and availability requirements should be considered as part of the classification process.*

Introduction of DLMs, revised protective markings and caveats

Revised Australian Government Confidentiality Classifications

On 26 July 2011, the Australian Government announced a new confidentiality classification scheme which was subsequently approved by the Government of South Australia for use in ICT systems on 12 October 2011. Notably, the X-IN-CONFIDENCE, HIGHLY PROTECTED and RESTRICTED classifications have been retired and several 'dissemination limiting markers' were introduced. Further guidance, including a translation between the former scheme and the revised scheme are contained in Annex B of this document.

National Security Protective Markings

The bulk of the work in classifying the confidentiality of information in the work of the South Australian Government can be expected to lie in the non-national security domain. However, there will be some occasions, such as when classifying information about critical infrastructure protection or counter-terrorism activities and the like, where the use of national security markings is applicable. National Security protective markings include CONFIDENTIAL, SECRET and TOP SECRET. These markings are described in Table 2 of the ISMF.

There are strict handling requirements for national security information and these are documented in the PSPF and ISM.

Most national security information handled by the State would be adequately protected by the procedures associated with a protective marking of CONFIDENTIAL. The RESTRICTED marking is retained in the ISMF for legacy treatment purposes but has been retired at the federal level and within South Australia.

The TOP SECRET classification will be used very rarely and only by Agencies with national security requirements.

Responsible Parties must comply with the ISM in circumstances where information classified for National Security is stored, processed or communicated.

Caveats

Australian Government caveats have been in use for several decades and remain largely unchanged. Applicable caveats for Responsible Parties that receive or use Australian Government information are described in section 3.6 of the Australian Government Information Security Management Guidelines.

Version 3.1 of the Information Security Management Framework introduced **South Australian government caveats** which may be applied to Official Information. The primary function of South Australian government caveats is to readily identify an 'audience' (i.e. recipients) for which information is intended or to establish 'currency' of information (such as an embargo date before information becomes publicly releasable, as often used with press releases or budget papers, or conversely to establish an expiration date by which information should no longer be used or released to the public, a typical example of which would be information associated with incidents and/or emergency management events.

A caveat is a warning that the information has special requirements in addition to those indicated by the DLM or protective marking. Caveats are not classifications in their own right and are not to appear without the appropriate DLM or protective marking. Those people who need to know will be adequately cleared and briefed about the significance of this type of information. Other people are not to have access to such information.

Caveats should typically be used sparingly and in limited circumstances.

Table 4. South Australian Government Caveat Descriptors

SOUTH AUSTRALIAN GOVERNMENT INFORMATION CAVEATS

Caveat	Description
Eyes only (EO)	The **Eyes Only** marking indicates that access to information is restricted to select individuals, functions or workgroups for instance: • Committee EO: Only Committee members • Agency EO: Only Agency personnel Information must only be shared on a strict need-to-know basis and membership to a given agency and/or committee does not convey an automatic entitlement.
Permission required	Express written consent is required by the originator of the information prior to it being republished or communicated to any other party.
When completed	Predominately used for forms and templates, this conditional caveat indicates that an accompanying DLM or protective marking takes effect only when the form/template has been completed.
DO NOT release until	Information may only be released AFTER a specific date, time or specified event. *(This caveat may also be used with Public Information, particularly with respect to major announcements or initiatives.)*
DO NOT release after	Information must only be released PRIOR to a specific date, time or specified event. *(This caveat may also be used with Public Information, particularly with respect to emergency management information.)*

9.1.2. Marking and handling appropriate to classification scheme

ISMF Standard 20 (Classification based handling and marking)

Responsible Parties should implement a procedure for labelling and handling all media containing information. These procedures should reflect different requirements based on the classification of the information being stored, displayed or otherwise manipulated. Storage and handling of information must be in accordance with the South Australian Government PSMF.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S20.1. Suppliers may adopt the implementation guidelines described in clause 7.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.2.2 of the ISO/IEC 27002:2013 standard).

S20.2. Agencies must adopt information marking and handling procedures that conform to the Australian Government Information Security Management Protocol (and guidelines). (Implementation of these procedures fulfils the requirements of control 8.2.3 in the ISO/IEC 27002:2013 standard).

Generally-Accepted Industry Practice:

Where the labelling of content is not feasible or practical an alternative method of indicating the classification should be utilised, such as by establishing a file-naming standard or by utilising the extended file properties available with contemporary operating systems.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

9.1.3. Release of public information

ISMF Standard 70 (Release of public information)

Agencies are accountable for the integrity of electronically published information that is released to the public domain and must implement controls to prevent unauthorised modification or disclosure of information that breaches privacy laws, which could harm the reputation of the publishing organisation. Responsible Parties must maintain and adhere to Agency controls for the management and administration of publicly available information.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S70.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.9.3 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 70).

S70.2. Agencies should assess the requirements for traditional copyright of information versus releasing publicly-accessible information into creative commons by way of the Australian Government Open Access and Licensing framework

S70.3. Information that is released into the public domain cannot be controlled readily in terms of duplication and alteration, whether authorised or unauthorised duplication and alteration takes place. For this reason, a single reference location or description of the original source of information must be described in the publication/document.

S70.4. Information released in the public domain may be replicated across multiple domains and sites thus relieving some availability aspects for information in a single location, however a “single source of the truth” should be stipulated in all copies to assist with the aspects of integrity and relevancy of information. Such documents may be coupled with version control or version identification information, such as the publication date, to ensure relevancy.

S70.5. Public registers should not be published on an Agency website, without due consideration by the Agency Chief Executive. If there is a legislative requirement to publish a register that contains personal information it should be limited to search functions from within that website only (i.e. such a register cannot be searched or otherwise accessible via a global search engine).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[I3] Integrity 3	S70.6. Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, such as digital signatures, watermarking or other forms of Digital Rights Management [DRM]
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

10. WORKFORCE MANAGEMENT SECURITY

10.1. Pre-employment

Policy Statement 9

Security responsibilities shall be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment.

Candidates shall be adequately screened (ISMF Standard 22), commensurate to the sensitivity of information being handled. All employees and third party users shall sign a confidentiality (non-disclosure) agreement.

Standards

10.1.1. Including security in job and person specifications

ISMF Standard 21 (Security in job and person specifications)

Responsible Parties should define security roles and responsibilities in accordance with their information security policy. Agencies must allocate security roles and responsibilities in accordance with Clause 4 of the PSMF.

Responsible Parties shall ensure that information security policies are readily accessible and formally communicated to all personnel on a periodic basis.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S21.1. Some roles which should be defined include:

- responsibilities for general personnel, including contractors and volunteers, in relation to implementing or maintaining security in line with whole-of-government and Agency policies;
- specific responsibilities for the protection of particular assets, including critical infrastructure, or for the execution of particular security processes or activities.

S21.2. Agencies shall communicate the requirement for personnel to report security events and incidents (actual or perceived) and uphold the requirement to report other security risks that are identified.

S21.3. Implementation of ISMF Standard 21 and the corresponding controls satisfies the control described in clause 8.1.1 of the AS/NZS ISO/IEC 27002:2006 standard. (The

removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 21).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

10.1.2. Personnel screening

ISMF Standard 22 (Personnel screening)

When employing personnel, the Responsible Party shall perform appropriate security and / or reference checks to verify their credentials in accordance with the Australian Government personnel security core policy, and the AS/NZS ISO/IEC 27002 code of practice.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S22.1. Responsible Parties must adopt the controls and implementation guidance described in clause 8.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.1.1 of the ISO/IEC 27002:2013 standard).

S22.2. A security clearance is defined in alignment with the Australian Government PSPF as "*An administrative determination by competent authority that an individual is eligible and suitable, from a security stand-point, for access to security classified resources*"

S22.3. Responsible Parties shall adhere to the minimum requirements defined in the Australian Government Personnel Security Protocol

S22.4. Responsible Parties should implement controls that support the objective(s) of the 'Authorisations, Security Clearances and Briefings' section in the ISM and must implement all applicable controls described in the ISM for information that is classified in National Security interests

S22.5. Baseline vetting for access to South Australian Government Information must be in accordance with the AS 4811-2006 standard.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet	S22.6. Australian Government vetting in accordance with the Australian Government PSPF must be undertaken for access to Australian Government Information at [P] Protected and higher classifications. Information for prospective security clearance applicants is available in the PSPF Security clearance subjects guidelines

CLASSIFICATION	ADDITIONAL CONTROLS
	S22.7. All personnel should be subject to a security vetting process in accordance with Personnel Security Management Core Policy of the PSPF. Personnel must be subject to this process when accessing Australian Government information.
[I4] Integrity 4 [A4] Availability 4	S22.8. Police security checks should be performed on all applicants (permanent and contractors) for sensitive positions.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S22.9. Appropriate checks (e.g. Police security checks) should be carried out upon appointment or promotion to a position where the applicant will have access to sensitive Information Processing Facilities, (e.g. financial information or critical infrastructure). For personnel holding positions of considerable authority these checks should be repeated regularly.
Note: for each classification level, controls from lower classifications are retained	

10.1.3. Contractual obligations, terms and conditions of employment

ISMF Standard 23 (Employment obligations, terms and conditions)

All Agency employees including contractors, temporary staff, board and/or committee members should sign confidentiality or non-disclosure agreements as part of their initial terms and conditions of employment. Such agreements should give notice to users of the Agency's policies, rights, obligations and responsibilities in relation to access to information assets.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S23.1. Responsible Parties should implement the controls and adhere to the guidelines described in clause 8.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.1.2 of the ISO/IEC 27002:2013 standard).

S23.2. Agencies must adhere to the requirements described in the Australian Government Personnel Security Protocol

S23.3. Confidentiality, non-disclosure and/or contractual agreements should also be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave an Agency or contracts are due to expire (refer ISMF Standard 8)

S23.4. Agencies may note that all personnel employed under the auspices of the *Public Sector Act 2009* are adequately bound to the confidentiality and non-disclosure

requirements of that legislation thus alleviating the requirement for additional non-disclosure undertakings.

S23.5. Punitive and/or remedial action(s) to be taken if the employee disregards security requirements should also be clearly described in the terms and conditions. Such measures must be aligned with a formally documented disciplinary process

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[FOUO] Official Use Only [SOUO] Sensitive	S23.6. Casual staff and third party users (such as volunteers) not already covered by an existing contract (containing the confidentiality agreement) should also be required to sign a confidentiality agreement prior to being given access to information processing facilities or Agency information assets. S23.7. Establish agreements with equipment repairers to safeguard the confidentiality of information (and data) on equipment undergoing repair.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

10.2. During employment

Policy Statement 10

Responsible Parties shall demonstrate commitment to ongoing Information Security Awareness to ensure that all employees including contractors and temporary staff are equipped to support Agency security policies and objectives.

Standards

10.2.1. Management and supervisory obligations

ISMF Standard 24 (Management and supervisory obligations)

Managers and Supervisors, or those acting in supervisory capacities must ensure that personnel under their direction and control, including contractors and temporary staff, apply security practices in accordance with the Agency's established policies and procedures.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S24.1. Responsible Parties must implement the controls and guidance specified in clause 8.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.2.1 of the ISO/IEC 27002:2013 standard).

S24.2. Responsible Parties may note that the personal circumstances of personnel such as financial problems, changes in their behaviour or lifestyle, recurring absences and evidence of stressful situations or illness may give rise to security implications in the workplace.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

10.2.2. Confidentiality and non-disclosure arrangements

ISMF Standard 8 (Confidentiality and non-disclosure)

Each Responsible Party should ensure that confidentiality and/or non-disclosure agreements are in place for all staff, contractors and/or sub-contractors that seek or have in place access to South Australian Government information, materials and/or intellectual property that is not intended for public access or circulation.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S8.1. Agencies should note that all personnel employed under the auspices of the *Public Sector Act 2009* are adequately bound to the confidentiality and non-disclosure requirements of that legislation thus alleviating the requirement for additional non-disclosure undertakings.

S8.2. Responsible Parties should adopt the implementation recommendations described in clause 6.1.5 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.2.4 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

10.2.3. Information security awareness and education

ISMF Standard 25 (Ongoing security awareness)

Agencies shall provide appropriate training in Agency information security policy, standards and procedures to employees and, where necessary, to contractors and other temporary personnel prior to granting access to information assets or services. Agencies must ensure that Information Security Awareness programs inform personnel of the existence of and availability of current versions of the PSMF and ISMF.

Responsible Parties must ensure that employee information security awareness and procedures are reinforced by regular updates.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S25.1. Responsible Parties shall implement the control(s) and should apply the guidance described in clause 8.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.2.2 of the ISO/IEC 27002:2013 standard).

S25.2. Responsible Parties shall implement the controls and guidance described in the ISM

S25.3. Security reminder messages should be posted in secured areas and/or regularly communicated to personnel according to the intended audience and or classification of the notifications

S25.4. A copy of the Agency's information security policies should be issued to all new personnel as they join and to all existing personnel

S25.5. Personnel should be made aware of the security classifications of the information assets that they use, and that they handle them appropriately

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

10.2.4. Disciplinary process

ISMF Standard 26 (Disciplinary process)

A formal disciplinary process shall be established by all Agencies in relation to employees who have violated whole-of-government and/or Agency security policies and procedures (ISMF Standard 23) and, for retention of evidence (ISMF Standard 34).

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S26.1. Responsible Parties must implement the control described in clause 8.2.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.2.3 of the ISO/IEC 27002:2013 standard).

S26.2. Disciplinary processes should aim to be a deterrent to employees who might otherwise be inclined to disregard security policies and procedures.

S26.3. Where it is formally stated that some activity is not allowed, but informally action is not generally taken against the activity (e.g. banning the distribution of jokes via e-mail), any subsequent disciplinary action that is taken in this regard may be subject to legal challenge and may therefore be unenforceable.

S26.4. Where appropriate, discipline should be in line with the relevant employment act conditions. For employees not covered under this, discipline should be in line with contract terms and conditions.

S26.5. Standard No 1 - A Planned Workforce from the Commissioner of Public Employment should be consulted in relation to volunteers within an Agency.

Generally-Accepted Industry Practice:

Disciplinary action should accurately reflect the nature of the breach of policy. Minor infringements are to be expected and should be dealt with through cautions and user security awareness education. Repeated minor infringements may be symptomatic of an inappropriate policy or control, and should entail a re-assessment of its suitability. Repeated minor infringements not due to an inappropriate policy or control, or a major breach of security, may be more suitably dealt with by formal sanctions such as termination of access (temporary or permanent) or legal action. The nature of appropriate disciplinary action should be determined by the workforce management function for the Responsible Party, in consultation with security officers and with legal officers if legal action is contemplated.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

10.3. Cessation or change of employment

Policy Statement 11

Responsible Parties shall implement and maintain a procedure or set of procedures to effectively manage departing employees or the withdrawal of assigned responsibilities for employees, contractors and other third party users.

Standards

10.3.1. Termination responsibilities

ISMF Standard 27 (Departing employees)

Each Responsible Party should have a documented procedure for performing employment termination and/or for the withdrawal of assigned responsibilities resulting from a change in employment status for employees, contractors and other third party users.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S27.1. Implementation of ISMF Standard 27 meets the requirements of control 8.3.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.3.1 of the ISO/IEC 27002:2013 standard).

S27.2. Responsible Parties should implement procedures concerning employment termination, or change of duties in alignment with the implementation guidance described in clause 8.3.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 7.3.1 of the ISO/IEC 27002:2013 standard).

S27.3. Responsible Parties should ensure that important knowledge or operational skills have been transferred to other resources prior to departure of the employee and/or contractor.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

10.3.2. Return of assets

ISMF Standard 28 (Return of assets)

Responsible Parties must ensure that all Agency assets are returned by departing employees, contractors and third-party users.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S28.1. Implementation of ISMF Standard 28 addresses control 8.3.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.1.4 of the ISO/IEC 27002:2013 standard).

S28.2. Responsible Parties must establish procedures and processes to transfer Official Information contained on personal (home office or BYO) devices such as home computers and mobility devices to agency owned information assets. Such procedures shall include a provision for the secure erasure of all Official Information (other than PUBLIC) that is stored on the personal device.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal	S28.3. Responsible Parties shall adhere to the requirements of the ISM with respect to sanitisation and/or disposal of assets prior to reallocating returned equipment to other personnel or for other functions. (For further details consult ISMF Standard 60)
[FOUO] Official Use Only [SOUO] Sensitive	S28.4. Agency assets shall include all instances of information, data, documents etc.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

10.3.3. Removal of access entitlements

ISMF Standard 29 (Removal of access)

Each Responsible Party shall have an established and logged procedure for the withdrawal and/or modification of access rights for departing employees, contractors and third-party users.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S29.1. Implementation of ISMF Standard 29 meets the objectives described by control 8.3.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.2.6 of the ISO/IEC 27002:2013 standard).

S29.2. Agencies must implement procedures for the withdrawal or change of access entitlements in alignment with the implementation guidance described in clause 8.3.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.2.6 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

11. INCIDENT MANAGEMENT

Policy Statement 12

Incidents affecting security must be reported through formal procedures and appropriate management channels as quickly as possible. Responsible Parties shall implement procedures encompassing different incident types (i.e. security breach, threat, weakness or malfunctions) and communicate these procedures to employees and contractors as part of a comprehensive Information Security Awareness Program.

Responsible Parties must familiarise themselves with the requirements of the whole of Government ISMF Standard 140 - Notifiable Incidents *and shall include this standard in their Information Security Awareness Program.*

Responsible Parties shall apply a process of continual improvement to the response, assessment, treatment and overall management of security incidents.

Standards

11.1. Reporting incidents

ISMF Standard 30 (Incident reporting)

A formal procedure for the reporting of security incidents should be established within all Agencies, with the intent of ensuring that incidents are reported to management (both within the Agency and at SA Government level) in a timely manner for appropriate action. Suppliers to Agencies shall comply with any Agency specific reporting procedures and must comply with the requirements of ISMF Standard 140 - Notifiable Incidents.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets.

S30.1. Responsible Parties should implement the control(s) and guidance described in clause 13.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 16.1.2 of the ISO/IEC 27002:2013 standard).

S30.2. Agencies must note the minimum standards for security incidents and investigations contained in the cyber security incidents section of the ISM and PSPF. These requirements are enabled by clause 5.6.4 of the PSMF

S30.3. Reporting and response escalation procedures should incorporate reporting processes such that, where appropriate based on the nature of the incident, action can be taken on a whole-of-government basis, and coordinated through DPC. The role of the Responsible Party that is affected by such incidents is to provide timely advice of the incident in accordance with the specific Government Policy on Information and Communication Technology on notifiable incidents. DPC will be

responsible for the action to be taken in terms of the whole-of-government response (as distinct from the Agency response which may be independently managed)

S30.4. Where an incident involves software malfunction or behavioural anomaly, provisions within the reporting scheme should include space to note on-screen messages, system behaviour etc. Procedural measures must be in place to isolate machines suspected of being infected with malware (i.e. malicious software code or programs) until they can be inspected by suitably qualified personnel. Under no circumstances should individuals attempt to self-patch, repair or otherwise re-attach the system to networks until inspected and authorised by suitably qualified personnel.

S30.5. Agencies shall have due regard for their established occupational health and safety policies in respect of protecting personnel in situations where violence may occur and may consider the use of duress alarms in high-risk circumstances.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

11.2. South Australian Government Notifiable Incidents

ISMF Standard 140 (Notifiable Incidents)

Responsible Parties must note and adhere to the requirements of *ISMF Standard 140 - Notifiable Incidents*.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets.

S140.1. Responsible Parties must include this standard in their respective information security awareness programs.

S140.2. Incorporation of ISMF Standard 140 into procedures and protocols pertaining to security vulnerabilities, events and incidents fulfils the objective of control 16.1.4 in the ISO/IEC 27002:2013 standard.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

11.3. Reporting vulnerabilities

ISMF Standard 31 (Reporting vulnerabilities)

Agencies shall establish a formal procedure for the reporting of security vulnerabilities (i.e. weaknesses), and all employees, contractors and Suppliers shall be made aware of it as part of an overarching Information Security Awareness Program. Suppliers shall adhere to relevant Agency and whole-of-government reporting requirements that encompass security vulnerabilities.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S31.1. Implementation of ISMF Standard 31 fulfils the objectives described by control 13.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 16.1.3 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

11.4. Managing information security incidents

11.3.1. Responsibilities and procedures

ISMF Standard 32 (Incident management)

Incident management, reporting and handling procedures must be defined and should describe relevant roles and responsibilities, including the function of management and/or Agency governance bodies to ensure the effective treatment of and resolution to security incidents.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S32.1. Incident management, classification and treatment processes should be established based on the business impact within the Agency and should consider potential and/or actual implications to whole-of-Government. Responsible Parties should develop documented incident response procedures in alignment with the implementation guidance described in control 16.1.5 of the ISO/IEC 27002:2013 standard.

S32.2. Responsible Parties should implement the guidance and controls described in the 'Cyber security incidents' section of the ISM

S32.3. Responsible Parties should implement the guidance described in clause 13.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 16.1.1 of the ISO/IEC 27002:2013 standard).

S32.4. Regardless of the classification of the information asset that is compromised, there can be significant implications in relation to incident management in that a breach on one computer environment may flow on to other environments. Therefore, all security incidents should be treated seriously and an assessment should be made as to the escalations required in the given circumstances (control 16.1.5 of the ISO/IEC 27002:2013 standard.)

S32.5. Responsible Parties should consider the entirety of section 8.2 of the AS ISO/IEC 20000.2 standard (or its implementations such as ITIL) for further guidance on Incident Management considerations.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

11.3.2. Incident monitoring, review and applied learnings

ISMF Standard 33 (Incident monitoring, review and applied learnings)

Responsible Parties should implement mechanisms to monitor, evaluate and review historical trends in information security incidents for the purposes of ongoing improvement in the organisation's ISMS.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S33.1. Implementation of ISMF Standard 33 fulfils the requirements described by control 13.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 16.1.6 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

11.3.3. Collection of evidence

ISMF Standard 34 (Evidence)

Agencies shall implement procedures to ensure that adequate evidence is available to support an action taken against a person or organisation.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S34.1. Responsible Parties should familiarise themselves with the concepts of: a) admissibility of evidence and b) quality and completeness of evidence

S34.2. The South Australian Evidence Act (1929) Part 6A specifies requirements for admissibility of computer based evidence. In summary, the court needs to be satisfied that the information is accurate and has not been modified after the event for which the data is evidence of. A person suitably qualified or experienced in computer evidence preservation may certify the validity of the data. The certification of validity generally will be accepted by the court in the absence of any contrary evidence.

S34.3. Detailed determination of what is admissible as evidence should be obtained from SA Attorney General's Department prior to the occurrence of any incident that may require the production of computer evidence in court.

S34.4. Responsible Parties should be conversant with the principles of the State Government's Information Privacy Principles Instruction issued as Premier and Cabinet Circular no 12. Any questions or concerns relating the protection of personal information should be directed to the Agency's Privacy Officer or the Privacy Committee of South Australia

S34.5. Responsible Parties must implement the control and guidance described in clause 13.2.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 16.1.7 of the ISO/IEC 27002:2013 standard).

S34.6. When an incident is first detected, it might not be obvious that it will result in possible court action. Therefore, a risk exists that necessary evidence is destroyed accidentally before the seriousness of the incident is realised. In such circumstances, Responsible Parties should seek legal advice on evidence requirements.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

12. PHYSICAL AND ENVIRONMENTAL SECURITY

12.1. Secure areas

Policy Statement 13

Responsible Parties shall establish or elect to use Business information processing facilities (including Hosting Facilities) which are housed in secure areas commensurate with identified risks and protected by a defined security perimeter, with appropriate security barriers and entry controls. Such facilities must include physical protection mechanisms which minimise vulnerability to unauthorised access, damage and interference.

Agencies must comply with the entirety of section 5.4 of the *PSMF and the requirements of the Government of South Australia Protective Security Policy. Responsible parties should consult* physical security section of the *ISM for additional controls and guidance.*

Standards

12.1.1. Physical security perimeter

ISMF Standard 35 (Physical security perimeter)

Each Responsible Party should identify and clearly define the security perimeter(s) around Agency information assets.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S35.1. For the purpose of this standard, a security perimeter is defined as the physical boundary between an area requiring protection at one level and an area requiring protection at another level (relative to the classification level of information available in each area). This perimeter may be around the business premises, and may also surround key areas within the organisation (e.g. information processing facilities) to provide various layers of access controls that protect information assets at levels commensurate with information classification and risk. For example, security perimeters may exist around general office areas (as distinct from customer areas), a locked tape safe located in the general office area and a server room, forming four distinct security perimeters within the premises.

S35.2. Responsible Parties should consult the section entitled 'Physical Security' in the ISM for further controls and guidance related to physical security considerations and to attain compliance with the requirements of the PSMF

S35.3. Responsible Parties should implement the guidance described in clause 9.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2	S35.4. Construction of all external facing structures must be physically sound, and suitably protected to prevent unauthorised access. Additional physical controls should be considered in the case of ground-level and first floor facilities. S35.5. The physical barrier spanning the perimeter should extend from floor to ceiling to prevent unauthorised entry and environmental risks, such as fire or flood.
[A2] Availability 2	S35.6. All fire doors on security perimeter shall be alarmed, monitored and tested to comply with jurisdictional and local regulations. Fire doors must operate in a failsafe manner.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.1.2. Physical access control

ISMF Standard 36 (Physical access control)

Physical access (entry) controls for secure areas shall be established to restrict access to authorised personnel only.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S36.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 9.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.2 of the ISO/IEC 27002:2013 standard).

S36.2. Access rights to secure areas should be reviewed and updated on a regular basis. Documented evidence of the review should be retained. These reviews should be performed at least annually, or more frequently based on a risks assessment that takes into account such factors as the level of turnover of personnel and the classification of the information asset being protected.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S36.3. Any person seen inside the security perimeter without sufficient identification should be escorted immediately to the reception and the Agency should take action as appropriate. S36.4. Dual authentication controls (e.g. Swipe cards plus PIN) should be used to authorise and validate all access.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S36.5. All personnel should wear Photo ID badges.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S36.6. Time of entry and departure of visitors must be logged. Visitors should be supervised, security requirements and emergency procedures should be conveyed to visitors (excepting those who have already been briefed on prior occasion). S36.7. Visitors must be provided with identification, which must be worn clearly. The identification must be collected when visitors leave the premises. S36.8. Authentication controls (such as an access card with PIN) should be employed where feasible and an audit log should be maintained commensurate with the access granted.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.1.3. Securing offices, rooms and facilities

ISMF Standard 37 (Security of offices and facilities)

Offices, rooms and facilities shall be secured in a manner that appropriately protects the information assets stored within the area, relative to its classification and the risk assessment for that information. Responsible Parties shall, at a minimum, take into account protective security measures encompassing:

a. Access to offices, rooms and facilities housing computer infrastructure, which supports sensitive information assets, shall be restricted to authorised personnel.

b. Physical security measures shall take into account the potential for damage from fire, flood and explosion and any other relevant natural or man-made disaster.

c. Physical security measures shall take into account relevant occupational health and safety regulations and standards.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S37.1. Responsible Parties should adopt the guidance described in clause 9.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.3 of the ISO/IEC 27002:2013 standard).

S37.2. A secure area may be a locked office or several rooms inside a physical security perimeter, which may be locked and may contain lockable cabinets or safes.

S37.3. Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.

S37.4. Responsible Parties should consider protecting against external and environmental threats, particularly with respect to data backup, and disaster-recovery planning [DRP] activities. Guidance on this topic is provided in clause 9.1.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.4 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S37.5. Processing facilities managed by the Responsible Party should be segregated physically from those managed by third parties.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S37.6. Intruder prevention and detection systems for physical incursions, including alarms should be installed and regularly tested. S37.7. Locations of sensitive information processing facilities and other areas should not be included on directories and phone books, with special consideration given to publicly accessible directory information such as that located in lobbies, foyers and stairwells.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S37.8. Office equipment and support functions should be situated within the secure area to reduce the likelihood of information being compromised. S37.9. To the extent practicable, site locations should not give indication of the information processing activities and requirements transpiring in situ. Key facilities should be located to avoid or reduce general access by the public.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.1.4. Working in Secure Areas

ISMF Standard 38 (Secure Areas)

Each Agency should enforce controls for working in secure areas and should apply such controls to all personnel or third parties working there, as well as third party activities taking place there. Suppliers and their contractors or representatives must adhere to Agency controls for working in secure areas.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S38.1. Each Responsible Party should implement the guidance described in clause 9.1.5 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.5 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S38.2. Personnel should only be made aware of the presence of a secure area, or the activities conducted within the secure area, on a strict need-to-know basis. Unattended secure areas should be appropriately secured (including physical locks and/or surveillance as determined by the outcome of a risk assessment).
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S38.3. Third party support services personnel should be granted restricted access to secure areas or sensitive information processing locations only when required. This access should be authorised and monitored.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.1.5. Delivery and loading areas

ISMF Standard 39 (Delivery and loading areas)

Agency management and Responsible Parties at hosting facilities shall ensure that the physical security perimeter for information assets cannot be breached via the delivery and loading areas.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S39.1. Implementation of ISMF Standard 39 fulfils the objective stated in control 9.1.6 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.6 of the ISO/IEC 27002:2013 standard).

S39.2. Suppliers and managers of hosting facilities must implement the control(s) described in A9.1.6 of the AS/NZS ISO/IEC 27001 standard.

S39.3. Responsible Parties should implement the guidance contained in clause 9.1.6 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.1.5 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

12.2. Equipment security

Policy Statement 14

Equipment that supports information assets shall be protected from physical and environmental security threats in order to prevent unauthorised access to information and/ or loss or damage.

Standards

12.2.1. Equipment siting and protection

ISMF Standard 40 (Equipment site selection)

Housing for information assets must be secured (Policy Statement 13), and equipment locations must be determined with a view to reducing the risks from environmental threats and hazards, and opportunities for unauthorised access.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S40.1. Responsible Parties should implement the guidance contained in clause 9.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[A3] Availability 3	S40.2. Environmental conditions should be monitored at a minimum to include temperature and humidity that may adversely impact the performance or operation of systems and services.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.2.2. Supporting utilities

ISMF Standard 41 (Supporting utilities)

Protection mechanisms for equipment outages caused by loss of one or more supporting utilities, such as power outages should be determined in correlation with the classification of the information asset, its importance to the business and in alignment with the Business Continuity Plan of the Responsible Party.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S41.1. Responsible Parties may consult clause 9.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.2 of the ISO/IEC 27002:2013 standard) for further guidance.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[A4] Availability 4 [I4] Integrity 4	S41.2. Responsible Parties must implement all guidance described in clause 9.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.2 of the ISO/IEC 27002:2013 standard).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.2.3. Cabling security

ISMF Standard 42 (Cabling)

Interception, interference and damage controls for power, telecommunications, storage and other systems interconnection cabling should be implemented. The level of protection adopted must be based on classification requirements and an assessment of the level of risk involved.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S42.4. Responsible Parties may consult clause 9.2.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.3 of the ISO/IEC 27002:2013 standard) for further guidance.

Generally-Accepted Industry Practice:
Where possible, cabling for highly sensitive systems (red) should be physically separated from non-sensitive cabling (black) by a distance determined to be acceptable after proper threat and risk assessment. Cabling used for sensitive systems should be of a sufficiently contrasting colour and consideration should be given to using multiple cabling routes for sensitive systems in unison with appropriate physical security controls.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[A4] Availability 4	S42.1. Multiple and diverse path routing of cables, network services or transmission media should be available.
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S42.2. Responsible Parties should implement the guidance described in clause 9.2.3f of the AS/NZS ISO/IEC 27002:2006 standard
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S42.3. Utility feeds including power and telecommunications into facilities should be concealed (underground or via alternate and adequate physical protection). Network cabling should be protected from unauthorised interception and damage using conduits and path diversion to avoid routing through publicly accessible areas.
Note: for each classification level, controls from lower classifications are retained	

12.2.4. Equipment maintenance

ISMF Standard 43 (Equipment maintenance)

Equipment should be maintained in accordance with the control(s) and implementation guidance described in clause 9.2.4 of the AS/NZS ISO/IEC 27002:2006 standard.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S43.1. Responsible Parties may consult clause 9.2.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.4 of the ISO/IEC 27002:2013 standard) for further guidance.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S43.2. Clause 9.2.4d of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer item to 11.2.4d of the ISO/IEC 27002:2013 standard) S43.3. Equipment which has been returned from off-site reparations must be isolated and assessed for malicious software or viruses prior to being placed back into the Agency or Supplier production environment.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

12.2.5. Secure disposal or re-use of equipment

ISMF Standard 45 (Secure disposal or re-use)

Agencies shall develop standards and procedures for the safe disposal and/or re-issue of ICT infrastructure that has been used to store Agency information assets.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S45.1. Agency standards and procedures must address the measures to be taken to ensure that media is cleared of sensitive information prior to being used for another purpose.

S45.2. Storage devices containing sensitive information shall be physically destroyed or securely overwritten rather than using the standard ‘delete’ function. Such procedures should incorporate “secure erase or wiping” (versus standard formatting) of hard drives and destruction of floppy diskettes. The determination to secure erase (a.k.a. wipe) storage media versus destruction of the asset must be in accordance with the ISM and is generally determined by the sensitivity and/or classification of the information stored on the device(s).

S45.3. Responsible Parties must implement the guidance described in clause 9.2.6 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.7 of the ISO/IEC 27002:2013 standard) and must adhere to the prescribed assessment and treatment techniques described in pages 131 to 141 of the ISM.

S45.4. Further controls and guidance pertaining to the disposal of storage media (as distinct from general equipment) are provided under ISMF Standard 60.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

12.2.6. Removal of property

ISMF Standard 46 (Removal of property)

Responsible Parties must ensure that information assets, including but not limited to: physical assets including Portable Storage Devices, software and other communications devices are not removed from premises without prior authorisation.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S46.1. In general, the Business Owner or their appointed information custodian should authorise the removal of equipment, information or software. Procedures should be established to facilitate the approval process.

S46.2. Responsible Parties may consult the guidance described in clause 9.2.7 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.5 of the ISO/IEC 27002:2013 standard) noting that implementation of ISMF Standard 46 satisfies the requirements of the corresponding control objective.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13. INTERNAL OPERATIONS AND SERVICE DELIVERY

13.1. Operational procedures and responsibilities

Policy Statement 15

Responsibilities and procedures for the management and operation of all information assets must be established including the segregation of duties where applicable, and development of appropriate operating instructions and incident response procedures.

Standards

13.1.1. Documented operating procedures

ISMF Standard 47 (Documented procedures)

Operating procedures should be documented, maintained and provided to relevant users of information assets. Operating procedures should be treated as formal documents and changes should be authorised by management.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S47.1. Responsible Parties should implement the guidance described in clause 10.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.1.1 of the ISO/IEC 27002:2013 standard).

S47.2. Separate operating procedures should be compiled for privileged users and these should not be made accessible to ordinary users.

S47.3. A printed or secondary offline copy of the operating procedures should be available as electronic copies may not always be available (especially in the case of a system malfunction)

S47.4. Operating procedures and particularly paper documents should be periodically reviewed for relevancy and accuracy

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.1.2. Change management

ISMF Standard 48 (Change management)

Responsible Parties shall ensure that changes, modifications and additions to information processing facilities, systems and capabilities are controlled.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S48.1. Responsible Parties may implement the guidance described in clause 10.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.1.2 of the ISO/IEC 27002:2013 standard).

S48.2. Responsible Parties should implement the guidance described under Control 0912 in the ISM.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.1.3. Separation of test, development, verification and operational environments

ISMF Standard 50 (Separation of test, development and production environments)

Development, test and production operational facilities shall be subject to physical or logical separation to achieve segregation of the processing environments. Transfer of software and information processing facilities from development to operational status should be based upon documented rules and in accordance with established Change Management procedures.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S50.1. Responsible Parties shall implement the guidance described in clause 10.1.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.1.4 of the ISO/IEC 27002:2013 standard).

S50.2. Procedures should be in place to segregate test data from live data. Test data must only be used for testing purposes. The presence of test data in a live (i.e. production) system presents a risk of data corruption (i.e. a risk to data integrity) in live systems.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS	
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S50.3.	Responsible Parties should prevent access to compilers, editors, development tools and systems utilities from operational systems unless specifically granted under an established change management and control process.
[I4] Integrity 4	S50.4.	Different profiles must be established for users of operational and test systems. Menus and contextual login banners should be applied to reduce the risk of operational errors.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S50.5.	Application development personnel should not have open access to operational systems. They should only be given access when required for the support of those systems, and the access should be removed when the support activity has been completed.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.		

13.2. External (third party) service delivery management

Policy Statement 16

Responsible Parties shall implement a program of compliance monitoring, periodic performance review and change (improvement) management for third party service delivery agreements.

ISMF Standard 51 (Security in third party service delivery)

Each Agency shall be responsible for identifying the risks associated with the outsourcing arrangements for their processing facilities and/or service delivery agreements (whether sourced internally or externally to Government), as well as defining the control measures that the contractor or other Third Party is required to implement. At a minimum, controls must include the applicable security controls described in the ISMF, service definitions and delivery expectations such as Service Level Agreements [SLAs] in alignment with ISMF Standard 139.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S51.1. Responsible Parties should implement the control(s) and guidance for Service Delivery described in clause 10.2.1 of the AS/NZS ISO/IEC 27002:2006 standard as well as the periodic monitoring and review of third party services described in clause 10.2.2 (alternately refer control 15.2.1 of the ISO/IEC 27002:2013 standard) and change management considerations for third party services described in clause 10.2.3 (alternately refer control 15.2.2 of the ISO/IEC 27002:2013 standard) of the same standard.

S51.2. Responsible Parties shall note that external (third party) service delivery agreements may include supply agreements sourced from other Agencies and/or service delivery partners (e.g. Shared Services, Service SA, Service Delivery Group etc.).

S51.3. Management of information processing facilities by contracted service providers could introduce potential security exposures, including but not limited to compromise, damage, or loss of data at the Third Party's site(s). Particular attention must be paid to risks where the site or service is designated as critical infrastructure [SGCII] to the State or nationally.

S51.4. The removal of an equivalent control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 51.

13.3. System planning and acceptance

Policy Statement 17

Agencies must determine, document and subsequently test the operational requirements of new systems prior to their acceptance and use in production (i.e. live) environments. Anticipated capacity requirements must be forecast, to reduce the likelihood of system overload including capacity for ancillary services such as video, voice and data transmission capacities and capabilities.

Standards

13.3.1. Capacity management

ISMF Standard 52 (Capacity management)

Responsible Parties should ensure that capabilities, resources and services are monitored, optimised and projections for demand particularly during peak usage periods (whether calendar or event driven) are factored into the service delivery plan.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S52.1. Capacity planning and management activities should be incorporated into Agency Business Continuity [BCP] and Disaster Recovery Plans [DRP] and should include the overflow capabilities for supporting assets and/or services such as communication transmission links for voice, video and data networks or network attached storage devices.

S52.2. Implementation of ISMF Standard 52 satisfies the objectives described in control 12.1.3 of the ISO/IEC 27002:2013 standard (or alternately clause 10.3.1 of the AS/NZS ISO/IEC 27002:2006 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[A4] Availability 4 [A3] Availability 3	S52.3. Responsible Parties must incorporate services and platforms classified at Availability 3 or Availability 4 into a documented capacity management plan.

13.3.2. System acceptance

ISMF Standard 53 (System acceptance)

Responsible Parties shall implement provisions for acceptance testing of new ICT systems, services, upgrades and releases.

Business Controls

S53.1. Responsible Parties shall initiate initial acceptance testing in a segregated manner so as not to place the production environment at risk. Subsequent testing (such as user acceptance testing) may be extended to a subset of users in the production environment.

S53.2. Capacity planning and management activities should be included in the testing procedure(s).

S53.3. Implementation of ISMF Standard 53 satisfies the objectives described in control 14.2.9 of the ISO/IEC 27002:2013 standard (or alternately clause 10.3.2 of the AS/NZS ISO/IEC 27002:2006 standard).

S53.4. Responsible Parties must not initiate user acceptance testing until such time that the Business Owner has confirmed acceptance of any residual risks arising from security testing activities (refer control 14.2.8 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.4. Protection against malicious software and scripts

Policy Statement 18

Responsible Parties shall undertake an active role in protecting information assets from exposure to malicious software and scripts including but not limited to: implementing controls to prevent and restrict the proliferation of virus and trojan software, educating personnel in the risks associated with the use and/or introduction of unauthorised software products, and, where appropriate, introducing custom controls to detect or prevent its introduction.

Standards

13.4.1. Controls against malicious software

ISMF Standard 54 (Malware and virus prevention)

Each Responsible Party shall implement standards and procedures for the prevention, early identification of, and response to malicious software. This strategy shall incorporate use and regular/frequent maintenance of approved virus scanning tools, as well as a user awareness program that will assist users in understanding their roles and responsibilities in relation to malicious software. Only authorised copies of software shall be resident on computer systems and all software licensing requirements must be adhered to.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S54.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.4.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.2.1 of the ISO/IEC 27002:2013 standard).

S54.2. Agencies should implement a strategy for scanning or otherwise monitoring ongoing compliance with licensing requirements.

S54.3. Agencies should establish a formal process for the authorisation of software purchases such that records are appropriately maintained and unauthorised software can be identified and actioned.

S54.4. Anti-virus detection and repair software should be installed to scan computers and media on a regular basis. This software should be updated in a timely manner as enhanced versions become available.

S54.5. Client firewall software should be installed or otherwise configured to grant/deny unauthorised outbound and inbound connection attempts by applications that have not been authorised for use by an Agency.

S54.6. Any files on electronic media of uncertain or unauthorised origin or files received over non-trusted networks should be checked for viruses, malware and other malicious code and scripts before use.

S54.7. Electronic mail attachments and downloads should be checked for malicious software before use. This check may be carried out at different places, (e.g. at electronic mail servers, on client computers or when entering the network of the organisation).

S54.8. Procedures should be established that clearly state responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks (Incident Management Procedures).

S54.9. User awareness and training (Information Security Awareness programs) should be periodically undertaken to inform users of the risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.4.2. Controls for scripting and remote execution code

ISMF Standard 55 (Remote execution code and scripts)

Each Responsible Party should implement controls preventing unauthorised scripts and remote execution code (i.e. mobile code such as JavaScript) from running on information assets in accordance with Agency defined security policies.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S55.1. Implementation of ISMF Standard 55 fulfils the objectives described by clause 10.4.2 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 55).

S55.2. Agencies should implement procedures for regular maintenance and patching of remote code execution runtime libraries and applets to reduce the likelihood of security exploits and associated vulnerabilities of using out of date or unlatched software.

S55.3. Agencies should ensure that remote code execution is undertaken using non-Administrative user account(s) to limit the impact of unauthorised remote code execution on an information asset.

S55.4. User awareness and training should be periodically undertaken to inform users of the risks associated with obtaining files and software, including scripts and remote execution code, either from or via external networks, or on any other medium, including middleware applications, indicating what protective measures should be taken.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.4.3. Endpoint protection

ISMF Standard 141 (Endpoint protection)

Agencies must establish and maintain security measures that ensure proportionate protection of endpoint devices relative to the confidentiality, integrity and availability classification of information being accessed or processed on such devices.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S141.1. Agencies must consult the full text of ISMF Standard 141 to satisfy themselves of appropriate protection and security management of endpoint devices in their operating environment(s). Refer http://www.digital.sa.gov.au/resources/topic/secuirity for current detailed control set.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S141.9. Endpoint devices must not be connected to public internet WiFi hotspots (irrespective of whether they are free or for fee services). S141.10. Endpoint devices must not be connected to Internet Kiosks and other generally accessible public facilities.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.5. Information back-up, archival and retrieval

Policy Statement 19

Responsible Parties shall implement demonstrably consistent procedures for undertaking information back-ups and/or archives according to Agency requirements and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

Standards

13.5.1. Information back-up and archiving

ISMF Standard 56 (Archives and backups)

Essential business information and software must be backed up regularly and information integrity checks should be conducted at random intervals to ensure that backed up information is accurate, available and relevant for recovery following a Notifiable Incident (such as disaster, media failure or system errors that have affected information integrity).

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S56.1. Implementation of Policy Statement 19 and ISMF Standard 56 satisfies the requirements described in clause 10.5.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.3.1 of the ISO/IEC 27002:2013 standard).

S56.2. Agency employees are responsible for backing up all data stored on workstations that are not connected to the network (e.g. portables used outside the office) and they should be made aware of this responsibility. Guidance may need to be provided regarding requirements and back-up methods to be used in these circumstances. For example, backups may be performed to suitable directories on the LAN server provided Agency management approval is obtained. Where backups are created to stand alone media (i.e. not to network servers), the media (diskettes or other) should be stored securely. (Note: Data stored on the network servers should be backed up centrally - refer to standards for contingency and recovery measures).

S56.3. Back-up information may need to be encrypted according to the sum of its classification, sensitivity and/or importance to the business. It should be noted that multiple instances of information at one classification and being stored in aggregate (for example on a given type of media such as a hard drive or portable media) may result in an elevation of classification for that asset.

S56.4. Responsible Parties must classify storage media according the highest classification of information stored (or intended to be stored) on that media per control 0323 in the ISM.

S56.5. Transportation of backup media between locations should adhere to ISMF Standard 64.

S56.6. Recommended media lifespan should be observed and media that has suffered from temporary recording errors should be replaced.

S56.7. Procedures should ensure that appropriate backups are stored off-site and are capable of restoring the system's files to a state that satisfies the terms of the service level agreements with the business units.

S56.8. Responsible Parties may adopt a strategy based on full, differential or incremental backups. In either case, the off-site back-up storage strategy will need to allow for the recovery of all relevant data.

S56.9. Back-up processes should incorporate a check for errors encountered during backup creation. In addition, the processes should ensure that the problem is resolved and the backups are retaken.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[A3] Availability 3	S56.10. Appropriate point-in-time backups of application files, as specified by the Agency, should be taken as a part of the application's processing schedule.
[A2] Availability 2	S56.11. Data should be stored in an appropriate location on a network server rather than on the local drive to facilitate automated backup processes. S56.12. At least three generations or cycles of back-up information should be retained for important business applications. S56.13. A catalogue of the backup media stored off-site should be established and maintained. Copies of this listing should always be available in hard-copy form, both on-site and off-site.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.6. Network management

Policy Statement 20

Appropriate security management shall be applied to networks and supporting infrastructure, including those that span organisational boundaries. Controls must be applied to protect sensitive information transmission that accesses or uses public networks.

Standards

13.6.1. Network controls

ISMF Standard 57 (Network security)

Procedures and controls shall be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S57.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.6.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.1.1 of the ISO/IEC 27002:2013 standard).

S57.2. Controls for external network connections are described in Network Access Control section of this framework.

S57.3. State Net Conditions of Connection is a controlled document that identifies specific implementation requirements including network controls for Responsible Parties that connect or seek to connect to the Government of South Australia State Net infrastructure. State Net Conditions of Connection must be consulted in such circumstances.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet	S57.4. Sensitive messages or individual fields should be encrypted during transmission over shared communications networks.
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S57.5. When encryption is used, rigorous cryptographic key management procedures, including secure means of generation, dissemination, custody, storage, destruction and backup should be implemented (15.3 Cryptographic Requirements).

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal	S57.6. Management approval should be required each time network monitoring a device is used. S57.7. Access to network management information such as topology, configuration and connections should be restricted.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S57.8. The attachment of devices and workstations to the network should be controlled to ensure that only authorised devices are connected (14.4 Network Access Control).
[FOUO] Official Use Only [SOUO] Sensitive	S57.9. The connection of network monitoring devices and access to their recordings of network traffic should be controlled S57.10. Fixed network connections such as LAN ports should be disabled in public areas, and in locations where they are not being used for prolonged periods of time
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.6.2. Network services

ISMF Standard 58 (Network services)

Agreements for network services whether provided in-house or externally sourced must include security controls, service level expectations and metrics for measuring performance of the service. Contractual agreements for network services should include a “right to audit” or “right to access log information” provision.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S58.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.6.2 of the of AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.1.2 of the ISO/IEC 27002:2013 standard).

S58.2. State Net Conditions of Connection is a controlled document that identifies specific implementation requirements including network controls for Responsible Parties that connect or seek to connect to the Government of South Australia State Net infrastructure. State Net Conditions of Connection must be consulted in such circumstances.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.7. Media handling and security

Policy Statement 21

All forms of media and storage devices, including Portable Storage Devices and other information storage and processing mechanisms must be controlled and physically protected.

Standards

13.7.1. Management of Portable Storage Devices and removable media

ISMF Standard 59 (Portable Storage Devices)

Procedures shall be established for the secure management and recovery of Portable Storage Devices.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S59.1. Responsible Parties should implement the guidance described in clause 10.7.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.3.1 of the ISO/IEC 27002:2013 standard).

S59.2. Where removable storage media is kept off-site it should be physically controlled and restricted to authorised personnel. The level of control should be equivalent to that applied at the primary site.

S59.3. Responsible Parties shall document and implement recovery procedures for the return of assets including Portable Storage Devices as described in ISMF Standard 28 (Return of Assets).

S59.4. Disposal of storage media should be carried out in line with ISMF Standard 60 (Sanitisation and/or disposal of media).

S59.5. Portable Storage Devices [PSDs] that are to be used outside of the standard office environment or primary site should be protected according to classification markings described in this framework. In general, only Public information should be stored on PSDs in an unencrypted and/or non-password controlled method. Agencies must adhere to the requirements described in ISMF Standard 101 in such instances.

S59.6. Responsible Parties should implement the techniques described by controls 0332 to 0336 in the ISM

S59.7. Responsible Parties must implement controls 0337 and 0338 in the ISM

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [A3] Availability 3	S59.8. When not in use, PSDs or other removable media containing backups or other information should be stored in secure rooms or cabinets on the Responsible Party's premises. S59.9. Responsible Parties must implement controls 0831 and 0832 in the ISM.
[FOUO] Official Use Only [SOUO] Sensitive [A2] Availability 2	S59.10. PSDs shall be encrypted and/or password protected according to Agency information security policies S59.11. If no longer required, the previous contents of any re-usable media that are to be removed from the organization should be securely erased using wiping methods described in pages 131 to 141 of the ISM. S59.12. Authorisation should be granted for media removal from the premises (i.e. regular organisational operating environment) and a record should be maintained to establish an effective audit trail of media removal(s). S59.13. Certain removable media should be physically secured during transportation to off-site locations (ISMF Standard 64).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.7.2. Sanitisation and/or disposal of media

ISMF Standard 60 (Sanitisation and/or disposal of media)

Agencies must implement formal procedures, including Supplier obligations for adherence to such procedures, for the sanitisation and/or secure and safe disposal of media that is no longer required, in alignment with the technical controls described in the current edition of the Australian Government ISM.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S60.1. Media may include any form of information asset that contains information or has previously contained information including but not limited to: paper documents, magnetic media, PSDs, non-volatile RAM, solid state disks, memory cards etc.

S60.2. Agencies should implement formal procedures for secure and safe disposal of media in alignment with the Media Security section of the ISM.

S60.3. Agencies shall observe the requirements for the disposal of Official Records in accordance with a records disposal schedule approved by State Records pursuant to section 23(1) of the *State Records Act* 1997.

S60.4. Responsible Parties shall implement the technical controls and adhere to the guidance described in the Media Security section of the ISM.

S60.5. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.7.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.3.2 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet	S60.6. Disposal of information assets must be logged.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal	S60.7. Where re-use after media sanitisation is impractical, information assets must be disposed of in a secure manner (e.g. secure destruction and/or incineration).
[FOUO] Official Use Only [SOUO] Sensitive	S60.8. All information and software should be removed totally (i.e. secure-erased (a.k.a. "wiped") or overwritten, not just deleted from data storage media (e.g. hard drives, discs, PSDs), which are to be disposed of by the Agency. S60.9. When equipment is sold, or otherwise disposed of, data on any storage devices should be effectively erased using the methods described in the Media Security section of the ISM.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.7.3. Information handling procedures

ISMF Standard 61 (Information handling)

Agencies should implement documented handling and storage procedures for information to reduce the likelihood of unauthorised disclosure or misuse. Agencies should maintain information handling procedures and communicate these to Suppliers and prospective Suppliers. Responsible Parties shall include applicable documented information handling procedures as a component of their comprehensive Information Security Awareness program(s) to relevant personnel, including contractors.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S61.1. Responsible Parties should implement the guidance described in clause 10.7.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.2.3 of the ISO/IEC 27002:2013 standard).

S61.2. Personnel should be made aware of the security classifications of the ICT assets that they use, especially the data and documents they deal with, and that they handle them appropriately.

S61.3. Responsible Parties must ensure that documented information handling procedures are communicated to employees and contractors or sub-contractors as part of a comprehensive Information Security Awareness program, including the requirements described in the section entitled *Handling Official Information* on page 12 of the Code of Ethics for the South Australian Public Sector.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.7.4. Securing system documentation

ISMF Standard 62 (Security in system documents)

System documentation should be securely stored according to its sensitivity and classification.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S62.1. Responsible Parties may implement the guidance described in clause 10.7.4 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 62).

S62.2. System documentation may contain a range of sensitive information that requires appropriate protection. Such information may include descriptions of applications processes, procedures, data structures and authorisation processes.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S62.3. The Business Owner should grant the application owner responsibility for maintaining an access list to documentation on a 'need-to-know' basis.

13.8. Exchange of information and software

Policy Statement 22

Exchanges of information and software between organisations shall be compliant with all applicable legislation and controlled via the implementation of commercial agreements or memorandums of understanding [MOUs]. Additional control mechanisms from both a business and security standpoint shall be applied to electronic data interchange, electronic commerce and electronic messaging deployments.

Standards

13.8.1. Agreements for the exchange of software and information resources

ISMF Standard 63 (Software and information exchange)

Each Responsible Party should implement formal agreements for the exchange of information and software between organisations and must consider the classification of the information being exchanged and the handling procedures therein.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S63.1. Responsible Parties should implement the guidance contained in clause 10.8.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.2.1 of the ISO/IEC 27002:2013 standard).

S63.2. When dealing with third parties and other external entities, Responsible Parties should implement the guidance described in clause 10.8.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.2.2 of the ISO/IEC 27002:2013 standard).

S63.3. Incorporation of both ISMF Standard 68 and ISMF Standard 63 by Responsible Parties fulfils the objective of control 13.2.1 in the ISO/IEC 27002:2013 standard.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical	S63.4. Agencies should establish software escrow agreements where the purchased software is critical to business operations. Where such agreements are put in place, they should incorporate a mechanism that will ensure that escrowed source code is appropriately maintained, in order to protect the interests of the Agency as code is updated over time (through

CLASSIFICATION	ADDITIONAL CONTROLS
[SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	tailoring to Agency requirements or through general product upgrades).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.8.2. Security of media in transit

ISMF Standard 64 (Media in transit)

In instances where information processing requirements dictate that media is transported externally from the processing centre or Responsible Party (e.g. for off-site backup), measures shall be taken to protect these information assets appropriate to the classification of the information and the Agency's assessment of risk.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S64.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.8.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.3.3 of the ISO/IEC 27002:2013 standard).

S64.2. Responsible Parties must implement the guidance described in clause 10.8.3d of the AS/NZS ISO/IEC 27002:2006 standard.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S64.3. Clause 10.8.3e of the AS/NZS ISO/IEC 27002:2006 standard
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S64.4. A log should be maintained at both the point of collection and at the destination, to record the time of collection and delivery. In addition, the individual responsible for "receipt" of the media (at the time of collection and at delivery) should be required to formally sign-off the log to complete the audit trail.
[FOUO] Official Use Only [SOUO] Sensitive	S64.5. Responsible Parties should establish procedures to validate/verify the identity of couriers.

CLASSIFICATION	ADDITIONAL CONTROLS
[I2] Integrity 2	
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.8.3. Electronic messaging (including e-mail)

13.8.3.1. Security risk management for messaging and social networking

ISMF Standard 65 (Messaging and social networking)

Responsible Parties shall implement controls to reduce security risks arising from the use of electronic messaging systems, such as email, electronic data interchange, instant messaging and social networking sites.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S65.1. Responsible Parties must implement the control(s) and guidance described in clause 10.8.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.2.3 of the ISO/IEC 27002:2013 standard).

S65.2. Responsible Parties may elect to include the SA Government Social Media – Guidance for Agencies and Staff as part of their comprehensive Information Security Awareness program(s)

S65.3. Where the identified risks have implications for other Agencies (e.g. risks relating to worms and viruses), DPC will determine the minimum standards to be applied by all Agencies in this regard, in consultation with each Agency.

S65.4. Some security risks which may need addressing include:

- vulnerability to unauthorised access to and/or interception of messages within the Agency, within StateNet (inter-Agency messaging) or within the Internet (external messaging);
- vulnerability of messages to unauthorised modification or denial of service;
- vulnerability to errors related to incorrect addressing, mail misdirection, unauthorised forwarding and distribution to external entities, and the general reliability and availability of the service;
- vulnerability to misuse by internal parties (e.g. harassment, distribution of objectionable material, chain letters);
- vulnerability to misuse by external parties (e.g. inappropriate use of mail relay services, electronic messaging and social networking worms and distribution of viruses or trojans that may compromise internal network security);

- liability issues relating to misuse of electronic messaging services that result in loss for other parties;
- impact of a change of communication media on business processes, (e.g. the effect of increased speed of dispatch or the effect of sending formal messages from person to person rather than company to company);
- legal considerations, such as the potential need for proof of origin, dispatch, delivery and acceptance (ISMF Standard 111);
- implications of publishing externally accessible personnel lists;
- controlling remote user access to electronic messaging accounts.

S65.5. Responsible Parties should give consideration to the use of mail proxies, secure messaging appliances and/or services that address common electronic messaging issues such as:

- preventing inappropriate inbound and outbound messages by filtering mail based on content (both presence or absence of words)
- quarantining messages for closer investigation (policies and procedures need to address the process to follow for quarantined messages)
- limiting the message size (including attachments) to prevent un-necessary resource waste (e.g. Storage and network capacity)
- limiting the number of recipients for a message to prevent un-necessary resource waste
- including a disclaimer on outbound messages.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.8.3.2. Policy on electronic messaging

ISMF Standard 66 (Email and messaging policy)

Agencies should clearly define policies regarding electronic messaging and make such policies readily available and communicated to all employees.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S66.1. Responsible Parties shall note that all e-mail made or received in the conduct of Agency business are considered 'Official Records' under the *State Records Act 1997* and must be handled as such. Further information is contained in the State Records Guideline: Management of Emails as Official Records

S66.2. Agencies should establish policies governing the use of electronic messaging that at a minimum encompasses the following considerations:

- Acceptable use policy for electronic messaging

- Guidance on email classifications and marking based on sensitivity and importance of electronic messaging content
- Guidance on cryptographic controls (where applicable)
- Message retention policy
- Message retraction (i.e. revocation) procedures

S66.3. Responsible Parties should promote and provide guidance on the use of archiving facilities to assist with the management and retention of employee e-mail while limiting mailbox size.

Generally Accepted Industry Practice:

Employees should not use e-mail systems as a database. Employees should regularly move important information from e-mail message files to word processing documents, databases, and other files. E-mail systems are not intended for the archival storage of important information. Stored e-mail messages may be expunged by systems administrators, mistakenly erased by users, and otherwise lost when system problems occur.

S66.4. Agency controls should clearly define Agency management's rights and responsibilities in relation to monitoring of message traffic and the intended purpose of this monitoring (if and when it occurs). Although it may not be intended to actually undertake regular monitoring of Internet or e-mail usage, it is important for Agency management to establish the explicit right to monitor user activity to minimise the risk of legal challenge in the event that action is taken in response to user activity recorded in these logs.

S66.5. Personnel should be made aware of attacks or potential issues relating to electronic mail services, (e.g. viruses, and interception) on both an ongoing basis and at the time a specific incident may be relevant.

Implementation Guidance:

Personal use of e-mail facilities by employees may be permitted within the guidelines of the Commissioner for Public Employment on ethical conduct, but must be prohibited for inappropriate activities, such as the promotion of business ventures, political or religious beliefs, harassment etc. Employees should be made aware that any permitted personal use is a privilege, not a right.

S66.6. Personnel should be made aware of issues regarding the retention of messages as Government records on the basis of any applicable charters, South Australian Government policies and legislation. They should also be aware of their ability to be retrieved in case of litigation. In addition to supporting an Agency's case, personnel should be mindful that e-mail may be subject to legal discovery and therefore may be used against the Agency.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S66.7. Facilities and guidance should be provided to Agency personnel for the protection of electronic mail and attachments. This may include the use of cryptographic techniques to protect the confidentiality and integrity of electronic messages (15.3 Cryptographic Requirements).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.8.4. Business information systems

ISMF Standard 67 (Business information systems)

Agency policies, standards and guidelines should be prepared and implemented to control the business and security risks associated with electronic office systems/business information systems. These requirements should be communicated to Responsible Parties.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S67.1. Business Information Systems include facilities such as:

- calendar and diary management systems (electronic or otherwise);
- bulletin boards and other information/knowledge sharing systems;
- Electronic Document Records Management Systems [EDRMS] (see Document and Records Management System Standard issued by State Records of South Australia)
- office communication systems including telephones and telephone systems, faxes, multi-function devices, voice mail systems, multimedia systems used for information dissemination
- other office equipment, such as photocopiers and whiteboards with communication or memory capabilities (excluding electronic messaging and Portable Storage Devices which are treated separately within this framework).

S67.2. Responsible Parties should implement the guidance described in clause 10.8.5 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 67).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.8.5. Miscellaneous information exchanges

ISMF Standard 68 (Miscellaneous information exchange)

Procedures and controls should be in place to protect the exchange of information, particularly in public locations, and encompassing the use of voice, facsimile and video communications facilities.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S68.1. Responsible Parties should implement controls and procedures reminding employees and subcontractors of their obligations and responsibilities when communicating in public places, either over the phone or in general conversations

S68.2. Responsible Parties may elect to include the SA Government Social Media – Guidance for Agencies and Staff as part of their comprehensive Information Security Awareness program(s)

S68.3. Handling procedures and policies should be implemented for information which has disseminated in error (e.g. Misdialled faxes, emails sent to incorrect recipients etc.)

R68.4 Responsible Parties may consult clause 8.7.7 of the AS/NZS ISO/IEC 17799:2000 standard for guidance

S68.5. Agencies shall communicate their relevant policies and procedures to personnel and Suppliers on the transfer requirements of information based upon its sensitivity and corresponding classification requirements. Incorporation of both ISMF Standard 68 and ISMF Standard 63 by Responsible Parties fulfils the objective of control 13.2.1 in the ISO/IEC 27002:2013 standard.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.9. Electronic commerce security

ISMF Standard 69 (E-commerce)

Information used in Electronic Commerce shall be protected from fraudulent activity, misuse, breach of privacy and unauthorised access. Responsible Parties should establish contractual agreements with providers and partners to minimise the risk of potential disputes and should give consideration to PCI DSS compliance for large online transaction based systems that rely on credit and/or debit card transactions.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S69.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 10.9.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.1.2 of the ISO/IEC 27002:2013 standard).

S69.2. Responsible Parties should protect information involved in online transactions using the control(s) and implementation described in clause 10.9.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.1.3 of the ISO/IEC 27002:2013 standard).

S69.3. Liability for fraudulent and erroneous E-Commerce transactions should be risk assessed and may be mitigated through the use of strong Authentication, Authorisation, Non-Repudiation, Integrity and Confidentiality controls.

S69.4. Security and control measures that are adopted by Agencies should also take into account the implications of bad publicity that may result from failed security measures that compromise confidential information, or the provision of incorrect or misleading information on the Agency web site.

S69.5. Agencies are advised to seek legal advice regarding electronic commerce arrangements they may be considering.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.10. Monitoring and event logs

Policy Statement 23

Responsible Parties shall actively monitor information assets for conformance to access control standards and other measures and shall implement event-logging mechanisms to provide evidence in case of security incidents.

Standards

13.10.1. Event logs

ISMF Standard 71 (Event logs)

Information security events, exceptions and major operator/administrator or user activities should be recorded and retained for an agreed timeframe for investigative, diagnostic and access control monitoring.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S71.1. Responsible Parties should implement the control(s) and may implement the guidance described in clause 10.10.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.4.1 of the ISO/IEC 27002:2013 standard).

S71.2. System use activities and monitoring should in implemented in alignment with the control(s) and guidance described in clause 10.10.2 of the AS/NZS ISO/IEC 27002:2006 standard

S71.3. The ISM provides additional guidance on information security monitoring.

S71.4. When allocating responsibility for log review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S71.5. Responsible Parties should implement a process of real-time alerts and immediate response to potential security incidents.

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S71.6. Where relevant to the circumstances of the Agency, the data retention and archiving strategy should take into account any issues relating collection and handling of evidence as it relates to audit logs (*Compliance*).
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2	S71.7. Logging should be activated for security related events that are aligned with the minimum standard defined by the Agency and the level of risk (as assessed by the Agency). S71.8. Log data should be retained for an appropriate period (as determined by each Agency).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.10.2. Protecting system monitoring information and logs

ISMF Standard 72 (Audit and system log protection)

Investigative, diagnostic and access control monitoring information, including audit and system logs should be protected from unauthorised access and from tampering or alteration. Information marked for retention or evidence purposes should be stored in accordance with the retention and evidence collection/storage policies of the Agency.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S72.1. Responsible Parties should implement the guidance described in clause 10.10.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.4.2 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.10.3. Administrator and operator logs

ISMF Standard 73 (Administrator and operator logs)

Logging and activity monitoring must be enabled for all operations and systems support personnel, including system administrators and users in Positions of Trust.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S73.1. Responsible Parties should implement the control(s) and guidance contained in clause 10.10.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.4.3 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

13.10.4. Fault logging

ISMF Standard 74 (Logging of faults)

Faults should be reported prior to undertaking corrective action. There should be clear documented rules for handling of reported faults.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S74.1. Responsible Parties may implement the guidance described in clause 10.10.5 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 74).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S74.2. Fault logs should be reviewed for a period of time upon remediation to ensure that the fault has been corrected and that such corrective action has been effective. S74.3. Review of corrective actions undertaken to ensure that other controls have not been compromised during the process of remediation. Such a review should also ascertain that any

CLASSIFICATION	ADDITIONAL CONTROLS
	systems or services changes have been made with relevant approvals.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

13.10.5. System timestamp (clock) synchronisation

ISMF Standard 75 (System clock synchronisation)

System timestamps or clocks should be set to an agreed standard, (e.g. universal co-ordinated time (UTC) or local standard time) to ensure that logging information accurately reflects the time at which logged events occurred.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S75.1. Responsible Parties should implement the control(s) and may implement the guidance described in clause 10.10.6 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.4.4 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14. ACCESS CONTROL

14.1. Business requirement for access control

Policy Statement 24

Responsible Parties shall establish controls for access to information and business processes that reflect business and security requirements including policies for information dissemination and authorisation.

Standards

14.1.1. Access control policy

ISMF Standard 76 (Access Control)

Agencies shall establish and document their business requirements using policies and guidelines that implement access control mechanisms for their information assets. Protection of information assets should reflect the value of these assets to the Agency. Suppliers shall implement access controls to Agency information in alignment with Agency policies, guidelines and procedures.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S76.1. Responsible Parties shall implement the control(s) and should implement the guidance described in clause 11.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.1.1 of the ISO/IEC 27002:2013 standard).

S76.2. Responsible Parties shall consider the requirements described in the StateNet Conditions of Connection when establishing and documenting access control policies and guidelines

S76.3. A clear statement of the business requirements to be met by access controls through this policy and associated whole-of-government and Agency Controls should be communicated to personnel, Suppliers and contractors.

S76.4. Access controls shall be implemented such that users are only provided with the level of access required to perform their job function.

S76.5. Where information classification may change over time (such as time when a confidential document has been released to the public), access control systems may be required to reflect that change automatically, or it may more appropriate to only allow such a change to be initiated at the discretion of a user.

S76.6. Agency access controls should be included as part of a comprehensive Information Awareness Program and communicated periodically to remind personnel and other parties of their obligations and responsibilities in meeting Agency and whole-of-government information security requirements.

S76.7. Responsible Parties must periodically review their access control policies.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.2. User access management

Policy Statement 25

Responsible Parties shall establish and maintain procedures to control the allocation of access rights to information systems and services encompassing the user-access lifecycle (i.e. establishment to retirement of access privileges) and the requirement to strictly control and monitor the use of privileged accounts.

Standards

14.2.1. User registration

ISMF Standard 77 (User registration)

Formal registration and de-registration procedures should be implemented for granting and revoking access to all information systems and services.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S77.1. Responsible Parties should implement the guidance contained in clause 11.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.2.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S77.2. Procedures should ensure that user IDs are not reissued to other users, to limit the potential for unauthorised access being inadvertently granted.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S77.3. Periodically scan for duplicate/redundant user IDs or accounts and remove or block access until resolved.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.2.2. Privilege management

ISMF Standard 78 (Management of privileges)

Privileges must be restricted and controlled and a formal authorisation process should be implemented for granting and denying access to information resources.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S78.1. Responsible Parties shall implement the control(s) and should implement the guidance described in clause 11.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.2.3 of the ISO/IEC 27002:2013 standard).

S78.2. Wherever common platforms are used across SA Government, standards for allocation of privileged access should be commonly applied. Consideration should be given to implementing “Sudo”, “Run as…” or an equivalent product to define and manage access to the ‘root’ (superuser) account. This product removes the need to share the ‘root’ password between those requiring that level of access, as well as allowing access to be defined only to the specific functions required in order to meet job responsibilities.

S78.3. Where possible default administrative accounts such as Administrator (Windows), root (UNIX), sa (SQL Server) should be disabled and alternate accounts created to carry out the same functions. The alternate accounts should be issued individually to privileged users to maintain accountability.

S78.4. Default accounts should have their passwords changed (even if they are subsequently disabled) irrespective of the default access rights or privileges associated with that account.

S78.5. Agencies shall define and enforce policies and/or procedures defining what (if any) software may be installed by non-privileged accounts (such as user accounts). Such measures should factor in the relative value versus risk of permitting user accounts to install security patches and updates to existing software that is present on the information asset(s). Implementation of this control S78.5 and ISMF Standard 78 satisfies the requirements and objectives described by control 12.6.2 of the ISO/IEC 27002:2013 standard.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S78.6. Unique IDs should be deployed for privileged access versus regular or normal business usage.

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S78.7. All use of privileged accounts should be monitored and audited on a regular basis. S78.8. Clauses 11.2.2a, b and c of the AS/NZS ISO/IEC 27002:2006 standard
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.2.3. User password management

ISMF Standard 79 (User passwords)

Responsible Parties should develop standards to manage the allocation of user passwords.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S79.1. Responsible Parties must implement the control(s) and should implement the guidance contained in clause 11.2.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.2.4 of the ISO/IEC 27002:2013 standard).

S79.2. User passwords include all forms of secret authentication information (such as group authentication or individual user id authentication information) for the purposes of this standard.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S79.3. Additional technologies for user identification and authentication, such as biometrics and/or hardware tokens, should be considered.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S79.4. Guidelines on the selection of strong passwords should be included in security awareness briefings and as part of a comprehensive Information Security Awareness Program.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.2.4. Review of user access rights

ISMF Standard 80 (User access review)

Responsible Parties shall conduct periodic reviews of users' access rights so as to maintain effective control over access to data and information services.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S80.1. Responsible Parties should implement the control(s) and guidance described in clause 11.2.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.2.5 of the ISO/IEC 27002:2013 standard).

S80.2. The frequency of the review process and the depth to which it is performed should be relevant to the specific Agency risks as they relate to obsolete access (e.g. the nature of the user access, particularly for privileged users, the turnover of personnel, the level of personnel that leave on poor terms, the length of time since the last comprehensive review). In addition, timing may be driven by the classification of the information asset to be protected. In some circumstances, a sample basis may be able to provide an acceptable indication of the effectiveness of procedures for the removal of access. In other cases, a full review of user access will be required each period.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S80.3. Access rights should be reviewed more frequently and more comprehensively in relation to privileged access, relative to general user access rights.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.3. User responsibilities

Policy Statement 26

Responsible Parties shall inform personnel of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of Agency information assets for which they are responsible and shall incorporate these requirements into their Information Awareness Program(s).

Standards

14.3.1. Password use

ISMF Standard 81 (Password use obligations)

Responsible Parties shall inform users of their responsibilities with respect to password selection and use, and in accordance with password management standards (ISMF Standard 79) and the rules of the password management system (ISMF Standard 95).

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S81.1. Responsible Parties should implement the guidance described in clause 11.3.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.3.1 of the ISO/IEC 27002:2013 standard).

S81.2. All passwords used to gain access to an information system should be treated as though they are classified at least at the same level as the classification of the system they are used to access.

S81.3. Passwords include all forms of secret authentication information assigned to a user (such as group authentication or individual user id authentication information) for the purposes of this standard.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.3.2. Unattended user equipment

ISMF Standard 82 (Unattended equipment)

Agency personnel and Suppliers should ensure that unattended information assets are protected from unauthorised access and/or misuse.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S82.1. Responsible parties should implement the control(s) and guidance contained in clause 11.3.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.8 of the ISO/IEC 27002:2013 standard) for further guidance.

S82.2. Consideration may be given to physically securing portable computer equipment (e.g. using cables and locks) to reduce the risk of theft of such equipment while in the office but unattended.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.3.3. Clear desk and clear screen policy

ISMF Standard 83 (Clear desk and clear screen)

Information on desks and screens should be protected from unauthorised access relative to the classification and findings of a risk assessment for that information.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S83.1. Responsible Parties should implement the guidance described in clause 11.3.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.9 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.4. Network access control

Policy Statement 27

Access controls must be applied and maintained for both internal and external networked services, connection paths and network-attached resources.

Standards

14.4.1. Policy on the use of network services

ISMF Standard 84 (Access to network services)

Access to network services should be established on the basis of Agency business requirements and such access entitlements must be regularly reviewed and controlled to ensure that access is restricted to required services in line with Agency policies and expectations.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S84.1. Agency-specific standards should be consistent with the business access control standard (ISMF Standard 76).

S84.2. Responsible Parties should implement the control(s) and the guidance contained in clause 11.4.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.1.2 of the ISO/IEC 27002:2013 standard).

S84.3. Insecure connections to network services can affect the whole Agency, and potentially other Agencies connected to the SA Government network. On this basis, it is essential that Responsible Parties implement standards that are aligned with SA Government requirements.

S84.4. Additional segmentation between network segments may be introduced to reflect the additional controls that may be required by some Agencies. Responsible Parties should assess their level of risk to determine if such additional controls are warranted by their circumstances.

S84.5. Internet access should be provided through a proxy server (in conjunction with secure gateways) rather than direct to the Internet. This strategy assists in reducing the level of information traffic from external networks regarding the internal network. In addition, it has the potential to simplify firewall rules in that outbound traffic is forwarded to the firewall from a single network address (i.e. that of the proxy server).

S84.6. For shared network infrastructure (e.g. the StateNet and Internet gateway), clear responsibilities and procedures should be established by the network manager to maintain security in a manner that protects the interests of all Agencies that rely on that infrastructure. These procedures should address such issues as:

- maintenance of firewall and router rule sets and authorisation of updates;
- selection of logging options and implementation of intrusion detection and alerting systems;
- requirements in relation to checking network traffic for inappropriate content (e.g. viruses, confidential SA Government information, excessively large data files) – This may be the responsibility of a mail server, however, such a solution will not address data transfers outside the SAGEMS environment (e.g. FTP services);
- responsibilities for actioning reported anomalies and unusual system activity.

S84.7. Standards should be established regarding acceptable use for Internet services (e.g. web, e-mail, news groups) in terms of business versus personal use, as well as consideration of issues regarding objectionable material. Associated with this, the standards need to provide for enforcement of the standards, including notice of management's right to monitor activity and usage. Specialist legal advice should be sought to confirm that the Agency's interests are appropriately dealt with in this regard, given that if formal requirements are over and above what is informally acceptable, the stricter requirements may not be enforceable. In addition, specific issues regarding explicit or implicit acceptance of the standards will also need to be considered in the Agency's context and mindful of the legal implications that follow.

S84.8. The standards should also consider issues that relate to capacity implications for specific types of network traffic. This may include limiting the size of e-mail attachments that are acceptable to the Agency. It may also include limiting or banning streaming audio and video services and any other identified high-bandwidth services that are not required to support authorised business use. In a similar manner, specific types of data download (e.g. MP3 files) may be limited or banned to minimise network impact.

S84.9. In the standards, consideration should also be given to Internet web services and e-mail as a software and virus source, and the potential implications of this in terms of software licensing and network protection in this context.

S84.10. Standards should clearly define responsibility for management and maintenance of the firewall and any other perimeter devices that are in place to protect the internal network. These standards should incorporate the Agency's requirements in relation to:

- Change management processes, particularly in relating to rule-set changes.
- Monitoring and follow up processes, as well as logging and altering configuration settings.
- Procedures for response to a serious security incident, detailing both the technical response and public relations aspects that may arise. The procedures should also consider any special authorities that may apply in order to provide a timely response to the incident (e.g. authority to shut down services to limit damage). The response plan should address incidents that are relevant to the Agency. These may include (but should not necessarily be limited to):
  - An attack on the firewall (to break in or to deny service).
  - An attack or defacement of an Agency web page.
  - E-mail based attack.
  - Computer virus infection.
  - Inadvertent release of confidential information.

S84.11. Agencies should employ Virtual Private Network [VPN] technologies (for example a StateNet certified Remote Access Gateway) to allow for remote access into their network from the Internet.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S84.12. Networks should be designed with security issues in mind in terms of establishing separate logical domains of trust, to appropriately separate segments of the network that store and/or transmit critical information (ISMF Standard 91).
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S84.13. Users should only be provided with direct access to services that they have been specifically authorised to use. This control is particularly important for network connections to sensitive or critical business applications, or to users in high-risk locations (e.g. public or external areas that are outside the Agency's management and control).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.4.2. Dedicated connection paths

ISMF Standard 85 (Dedicated network connection paths)

Dedicated and secured system and network interconnection paths should be established when multiple or unsecured paths would present an unacceptable risk to the security of information.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S85.1. In highly sensitive information processing environments, minimising risk of message interception may be accomplished by restricting the number of alternative routes that are available to users/terminals and/or limiting network traffic to devices that are subject to appropriate physical and logical security. Dedicated connection paths may increase risks related to the availability of services and consideration should be given to implementing a secure diverse route coupling logical and physical access protection mechanisms for those systems and/or services requiring increased availability.

S85.2. Systems and/or network interconnections that require dedicated path access controls must not be attached to wireless LAN and/or public broadband services.

S85.3. Consideration should be given to implementing fibre optic connections between highly sensitive information assets.

S85.4. Remote access devices (e.g. broadband modems and VPN gateways) should be attached via a secure gateway device that provides appropriate filtering and authentication controls commensurate to the classification of the information assets being accessed.

S85.5. Encryption and/or cryptographic controls should be enabled where possible per the guidance and requirements described in this framework.

S85.6. Agencies should locate patch panels, fibre distribution panels and structured wiring enclosures in at least lockable commercial cabinets.

S85.7. Responsible Parties should, based on undertaking the appropriate risk assessments, implement control 0157 in the ISM.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS	
[P] Protected [SC] Sensitive: Cabinet	S85.8.	Unprotected (i.e. unencrypted) network traffic shall be configured to prevent traversal across network segments and/or services that are not physically and logically controlled by the Agency.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S85.9.	Agencies should implement measures that control the network path through which critical and sensitive data traverse, to limit the potential for interception or compromise of such messages.
[TS] Top Secret	S85.10.	Responsible Parties must locate patch panels, fibre distribution panels and structured wiring enclosures in at least lockable commercial cabinets.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.		

14.4.3. User authentication for external connections

ISMF Standard 86 (Authentication of users from external sources)

Access to the Agency network via external connections should be subject to authentication and validation over and above that applied for access to the servers, applications and information on the network.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S86.1. Responsible Parties may implement the guidance described in clause 11.4.2 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 86).

S86.2. Appropriate authorisation should be obtained from the relevant manager (typically the Business Owner) before users can obtain remote access.

S86.3. All external connections to an Agency server or PC have the potential to compromise security of all devices connected to that network, either directly or indirectly, with potential to disrupt services with associated legal liability for such outages. Therefore, standards of controls as they relate to user authentication for external connections should be established on the basis of an Agency risk assessment for these services. In this context, the classification of information assets stored or processed on the specific device may have little relevance in determining the level of control required.

S86.4. Additional considerations for dial-in (a.k.a. "legacy") access include:

- Telephone numbers should only be released to users who are specifically authorised to use external connections.
- Responsible Parties should consult the StateNet Conditions of Connection for further guidance concerning remote access considerations.
- The application of more stringent dial-in controls (refer to controls based on DLMs and protective markings below) may eliminate the need to apply any of the protection measures discussed here.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S86.5. A two factor authentication process at the network perimeter should be adopted for all external connections to an Agency server or PC. For example, the solution may use a challenge response mechanism at the network perimeter, effectively providing authentication that uses a one-time password to allow network access. This process is then followed by normal server or application password authentication in order for the user to obtain access to a service on the network. S86.6. A facility should be implemented that can limit the number of unsuccessful attempts at establishing an external connection before the user identifier is suspended.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S86.7. A simple two-factor password process, with one level of authentication performed at the network perimeter (for example, a VPN client login), followed by standard authentication measures that would normally apply for server or application access. S86.8. During authentication at the network perimeter, there should be no display of a logon banner or other similar information that identifies the Agency or the type of network or device being connected to. However, a banner displaying a message

CLASSIFICATION	ADDITIONAL CONTROLS
	that "*Unauthorised Access is Strictly Prohibited*" and that violators shall be prosecuted is a Generally- Accepted Industry Practice. S86.9. Consideration should be given to restricting access for external connections to specific computer systems and/or from specific locations (sources) as well as restricting the time periods that such connections can be used, as approved by the Agency.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.4.4. Node authentication

ISMF Standard 87 (Authentication of systems from external sources)

Node authentication of remotely connected computer systems may be used to protect the security of information assets on the connected systems.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S87.1. Responsible Parties may implement the control(s) and guidance described in clause 11.4.3 of the AS/NZS ISO/IEC 27002:2006 standard

S87.2. Use of facilities that allow automatic connection from a remote computer should be avoided unless there is no other practical alternative.

S87.3. Node authentication may be used in addition to user authentication mechanisms to provide an additional level of protection.

S87.4. Some examples of techniques for node authentication include:

- IP Address;
- MAC Address;
- Encryption and digital signatures;
- Caller Line Identification (CLID);
- Remote Access Service Call-back.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.4.5. Remote diagnostic/configuration port protection

ISMF Standard 88 (Configuration port protection)

Access to diagnostic and configuration ports shall be securely controlled and where necessary, a key lock and a procedure shall be implemented to ensure that the facility is only accessible by arrangement between the Responsible Party and the support personnel requiring access.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S88.1. Responsible Parties may implement the guidance described in clause 11.4.4 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 88).

S88.2. Supervisory control and data acquisition (SCADA) networks are used to monitor and control key functions in provision of various services and products. Responsible Parties must implement appropriate controls for the protection of SCADA networks as part of the protection of the organisation's overall network infrastructure and should consider additional product and/or feature specific control(s) that may be applied to protect these assets including a combination of physical and logical controls, such as using non-standard virtual port identifiers and dedicated firewalls or remote access devices.

S88.3. Default passwords must be changed and, where applicable, Simple Network Management Protocol (SNMP) and/or Wireless LAN (i.e. Wi-Fi, 3G, GSM etc.) should be disabled on SCADA devices.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S88.4. Hardware that supports remote connections for ad-hoc support (e.g. modems and VPN switches) should be powered off or otherwise disabled, and only enabled when specifically required. S88.5. Where permanent support is required for system diagnostics and support, controls that apply to other remote users should be applied to support personnel including third parties such as contractors and Suppliers (ISMF Standard 86).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.4.6. Network segregation

ISMF Standard 89 (Network segregation)

Networks which extend beyond traditional Agency boundaries shall have controls within the network to segregate groups of information services, users and information systems.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S89.1. Responsible Parties should implement the control(s) and guidance provided in clause 11.4.5 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 13.1.3 of the ISO/IEC 27002:2013 standard).

S89.2. Networks may be segregated either logically, physically or using a combination thereof (e.g. an Agency's internal network domains and external network domains), each protected by a defined security perimeter. The separation of the domains should be based around the level of trust between domains (i.e. Trust Domains). This in turn may be dependent on the level of control that the Agency has over the hardware, software and users, or the confidence the Agency has with the third party responsible for maintaining the relevant network segment.

S89.3. StateNet Conditions of Connection provides detailed information and guidance for the implementation of Trust Domains

Good Practice:

Products from the Australian Signals Directorate Evaluated Products List (EPL) should be given preference due to these products having independently established levels of assurance and security functionality. Physical access to gateway equipment must be restricted as appropriate for the highest classification system.

In the case of software based firewalls, no services or applications should be installed on the underlying platform other than those required by the firewall applications. As the firewall is the point of entry into the network, the likelihood of an attack against the device is high and all reasonable security controls should be applied.

S89.4. Semi-trusted networks (e.g. connections to other state and federal government networks) should be treated as a separate domain of trust from the Agency network, even though it may be treated with a greater level of trust than that of the Internet. In any case, traffic filtering and access control using a firewall or router should be established to limit users to authorised activities.

Generally Accepted Industry Practice:

Access between domains should be restricted by:

- *Protocol or service – only required protocols and services should be allowed to pass between domains. Everything else should be blocked. Accountability can be established by*

logging traffic that passes between domains. Records of which devices are attempting to access resources should be kept. Even if the servers have been hardened so as to not offer services for a protocol, restricting protocol traffic reduces the impact, or risk of compromise, of any unauthorised services. Restricting access to protocols or services also reduces traffic, as attempts to connect to closed ports are blocked before entering the network segment.

- *User credentials – deployment of application proxy type gateways will require users to authenticate prior to attempting to access resources in another domain. Accountability is heightened as there is a now a record of who was attempting access and from where. Access controls may be deployed to gateways to provide granular control of what devices and services authenticated users can access.*

S89.5. Supervisory control and data acquisition (SCADA) networks should be isolated and treated as a unique trust domain.

Generally Accepted Industry Practice:

In addition to the applicable risk management and cyber security practices specified in this framework, operators of SCADA systems should consider the following actions to assist in protecting the functions controlled and monitored by the systems. These include:

- *Implementing the security features provided by device and system vendors including patches for vulnerabilities;*
- *Establishing strong controls over any backdoor or vendor connections since modems, wireless and wired networks used for communications and maintenance can represent a significant vulnerability;*
- *Hardening SCADA networks by removing or disabling unnecessary services;*
- *Conducting technical audits of SCADA devices and networks, and any other connected networks;*
- *Conducting physical security surveys and assessing all remote sites connected to the SCADA network, including access to computer terminals, fibre optic cables, or telephone/communications networks, and exploitable wireless local area network access points or radio and microwave links.*
- *Establishing policies and conduct training to reduce the likelihood that information about the SCADA system design, operations or security controls will be inadvertently disclosed.*

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S89.6. Segmentation should be implemented through the use of a firewall that limits traffic through pre-defined filtering rules (ISMF Standard 90 and ISMF Standard 91). S89.7. Intrusion detection/prevention systems should incorporate real-time alerting and response for significant security incidents.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S89.8. Responsible Parties should implement appropriate controls from the ISM. S89.9. Network access controls should be configured to segment the Agency network based on the level of control of the Agency, or the level of the Agency's trust in management of the network segment by an external party. S89.10. As a minimum, segmentation should be implemented through access control lists within boundary routers, to define filtering rules for network traffic. S89.11. Filtering rules should be designed to block unauthorised access in accordance with the Agency's access control standard (ISMF Standard 76). S89.12. Monitoring and follow-up processes should be established to provide for timely response to significant security incidents.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.4.7. Network connection control

ISMF Standard 90 (Network connection control)

Agency access policy and business requirements in conjunction with a management approval process should determine the network connection capabilities for users either individually and by organisational units or on an Agency wide basis.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S90.1. Responsible Parties should implement the guidance described in clause 11.4.6 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 5).

S90.2. The access policy should document what services should be allowed to pass through the firewall (both inbound and outbound). The access policy should take into account both the functional requirements of the inter-network connection and the risks associated with these requirements (identified and analysed in a risk assessment).

Generally Accepted Industry Practice:

Incoming and outgoing services should be denied by default.

The gateway should deny all network connections to itself. Configuration of the gateway should be performed from a secure console local to the gateway machine(s), with appropriate user identification and user authentication controls. If remote administration is justified, then only encrypted communications (e.g. encrypted VPN tunnel) between the administration machine and the gateway machine should be allowed.

In accordance with least privilege principles, allowed traffic should be restricted to only those objects that require that traffic (e.g. incoming web traffic should only be allowed to the web server, outbound e-mail should only allowed from the mail server, outbound web traffic should be restricted to those users that have been approved to access the Internet).

Policies and procedures adopted for firewall rules should include a "closure procedure" for virtual ports that are no longer used when applications or services are retired.

S90.3. Communications between the network and the gateway should be either physically controlled by the relevant Agency; or appropriately encrypted to reduce the risk of eavesdropping. This will usually be an issue when the network is physically separate from the gateway (e.g. network in building A connects through a firewall in building B – the connection from building A to building B must be secured).

S90.4. All traffic between networks (e.g. public to private networks) or Trust Domains (e.g. StateNet) must pass through the gateway (i.e. there should be no unprotected links).

S90.5. The use of proxy servers is desirable. Proxy servers can perform "sanity checks" on traffic to ensure only legitimate traffic is passed through the gateway.

Good Practice:

If HTTP traffic is allowed, active content (e.g. Java applets, ActiveX controls, scripting) may be blocked where possible (consistent with agency security policies). This will reduce much of the functionality of external web sites, but the risk of damage from malicious content is generally greater than the value of the added functionality.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.4.8. Network routing control

ISMF Standard 91 (Network routing control)

Network routing controls should be implemented by Responsible Parties as necessary to enforce and support the Agency's access control policy.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S91.1. Responsible Parties should implement the guidance contained in clause 11.4.7 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 91).

Good Practice:

SNMP services should be disabled or set to read only with a community string other than "public". Where "write" access is required, the community strings should be set to a string other than "private". Only SNMP queries from known IP addresses (monitoring servers etc) should be processed by a router.

Where possible, restrict hosts that can accept or transmit Routing Information Protocol (RIP) packets.

Restrict the use of trivial file transfer protocol (TFTP). TFTP does not have any security controls built in to it. If TFTP needs to be used, make sure that the TFTP host is secured and that the correct ACLs or file/directory permissions are in place. The TFTP server (if needed) should not run other services, as it may be a source of compromise for those services. Checksums should be placed on all files on the TFTP machine. Also, lock down the hosts from layer 2 (e.g. in UNIX, use the file /etc/ethers to set the MAC address to a specific host).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS	
[A4] Availability 4	S91.2.	Address translation mechanisms must be implemented to isolate the internal network from external networks.
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S91.3.	Address translation mechanisms should be implemented to isolate the internal network from external networks.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S91.4.	Positive source and destination address checking mechanisms should be adopted (to counter IP spoofing attacks).

CLASSIFICATION	ADDITIONAL CONTROLS
	S91.5. Physical and logical access to consoles for all routers should be restricted to only the Network Administrator. S91.6. Privileged modes should be password protected. This helps to ensure that only authorised personnel can make modifications to the router's configuration. S91.7. Advanced authentication mechanisms such as token-based systems, biometrics or X.509 certificates should be enforced when connecting to routing consoles. S91.8. Console sessions should timeout when unattended or after a period of inactivity. *Good Practice:* *An inactivity timeout of 2 minutes is recommended.*
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.5. Operating system access control

Policy Statement 28

Security capabilities at the operating system level shall be enabled to restrict access to electronic information assets to authorised users.

Standards

14.5.1. Authentication techniques for terminals and thin-clients

ISMF Standard 92 (Authentication of terminals and thin-clients)

Responsible Parties should implement procedures for authenticating specific terminals and thin-clients based on user, device descriptor or geographic location in circumstances where it is required that access (including session establishment) can only be initiated from a particular location or device.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S92.1. Physical protective security controls such as the deployment of RFID's and embedded GPS controllers may be suitable for given applications, based on the sensitivity of the applications and information being processed by the Responsible Party.

S92.2. Additional authentication controls such as the use of two-factor authentication techniques may be combined with this technique to provide a higher level of protection for select information assets.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.5.2. Secured login

ISMF Standard 93 (Secure Logon)

Responsible Parties shall implement secure login (logon) procedures designed to minimise the opportunity for unauthorised access to information assets.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S93.1. Responsible Parties should implement the control(s) and guidance described in clause 11.5.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.4.2 of the ISO/IEC 27002:2013 standard).

S93.2. In remote access applications, such as Virtual Private Networks [VPN] applications, Responsible Parties shall implement measures to prevent the use of clear-text password transmission over public networks.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S93.3. Responsible Parties must implement clause 11.5.1e of the AS/NZS ISO/IEC 27002:2006 standard S93.4. Responsible Parties should establish a mechanism to display the time and date of last successful login, coupled with an indication of any failed (unsuccessful) login attempt(s).
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.5.3. User identification and authentication

ISMF Standard 94 (User identification and authentication)

All access to an Agency's networks and computer facilities shall be subject to user identification and authentication. Most commonly, this will rely on a combination of a unique, personal User ID with a password, but may use other methods for this purpose using the principles described in ISMF Standard 81 and ISMF Standard 95 of this framework.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S94.1. Responsible Parties should implement the guidance described in clause 11.5.2 of the AS/NZS ISO/IEC 27002:2006 standard. (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 94).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S94.2. User IDs should not convey the privilege level of that account (e.g. manager, supervisor, administrator, operator etc.). S94.3. During login, a warning message should be displayed to inform users that access is restricted and that activities may be monitored. S94.4. Guest user identities should not be used in any Agency system and should be either removed or disabled.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.5.4. Password management system

ISMF Standard 95 (Password management system)

Responsible Parties shall establish and maintain a password management system to enable the selection of quality passwords by users and to facilitate periodic password changes, established by the user “at will” or enforced by the system at regular intervals as required by the Agency and/or the classification of the information asset.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S95.1. Responsible Parties shall implement the control(s) and should implement the guidance contained in clause 11.5.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.4.3 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3	S95.2. Password syntax checking may be applied for password selection at the discretion of the Agency, particularly where the nature of the information asset being protected warrants an additional level of control. Examples may include a facility that: - enforces a degree of change from one password to the next; - limits the number of repeat characters allowed in a password; - performs dictionary look-ups to verify easily guessed passwords are not selected by users; - maintains a record of previous user passwords in line with Agency requirements to prevent a previous password

CLASSIFICATION	ADDITIONAL CONTROLS	
		from being reused for a stipulated period of time or number of passwords
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2	S95.3.	Temporary passwords should only be valid for a period of five (5) days. For sensitive systems, these temporary passwords should only be valid for twenty four (24) hours.
	S95.4.	Current password should be entered before a user can set a new password.
	S95.5.	Passwords should never be stored on a computer system in an unprotected form. Generally, this protection will be in the form of encryption of password data. This requirement also extends to ensuring that passwords are never stored in clear text in script files.
	S95.6.	Vendor-supplied user identifiers should be deactivated or their passwords changed as soon as practicable.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.		

14.5.5. Use of system utilities

ISMF Standard 96 (Control of system tools and utilities)

Responsible Parties shall identify utility programs and system tools that are capable of overriding system and application controls in each of their processing environments and implement access restrictions to limit use to authorised personnel based on job roles and responsibilities.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

When designing access restrictions for system utilities agencies should consider:

S96.1. Responsible Parties must implement the control(s) and should implement the guidance described in clause 11.5.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.4.4 of the ISO/IEC 27002:2013 standard).

S96.2. System utilities may be stored on removable media. The removable media should be physically secured when not mounted. Physical access to the media should be restricted and monitored. Additional controls may include restrictions on user access to removable media drives (i.e. disallowing ordinary users to mount removable media).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.5.6. Inactivity time-outs

ISMF Standard 97 (Inactive sessions)

Responsible Parties shall ensure that inactive sessions on terminals, computers and remote access devices are automatically disconnected after an agreed period of inactivity as specified by the Agency.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S97.1. Responsible Parties shall implement ISMF Standard 97 in alignment with the guidance described in clause 11.5.5 of the AS/NZS ISO/IEC 27002:2006 standard

S97.2. Determinations to implement session inactivity time-outs may need to account for technical limitations associated with some user activity, where implementation of the time-out may adversely affect day-to-day operations (e.g. disruption of file transfers that are impacted by time-outs, and session time-out features preclude the ability to continue running applications in the background).

S97.3. Responsible Parties may consult appropriate controls of the ISM for further guidance on session termination and locking.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S97.4. Consideration should be given to session inactivity time-out functions that are capable of automatically closing applications and terminating open network connections after a prescribed period of inactivity, as determined by the Agency.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.5.7. Accessibility restrictions

ISMF Standard 98 (System access restrictions)

The duration and/or hours of access to information systems may be limited where this is practical and where such a control will be effective in reducing the risk of unauthorised or fraudulent access.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

R98.1 *Responsible Parties may implement the control(s) and should familiarise themselves with opportunities to implement the guidance described in clause 11.5.6 of the AS/NZS ISO/IEC 27002:2006 standard*

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.6. Information and application access

Policy Statement 29

Security capabilities within applications shall be enabled to restrict access to electronic information assets to authorised users.

Standards

14.6.1. Information access restrictions

ISMF Standard 99 (Legitimate need-to-access / need-to-know)

Entitlement to Agency information must be determined by defined applicability consistent with personnel roles and responsibilities, job requirements, public entitlement and/or right to information and consistent with the Agency's information access policy (ISMF Standard 76).

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S99.1. Responsible Parties should implement the control(s) and guidance described in clause 11.6.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.4.1 of the ISO/IEC 27002:2013 standard).

S99.2. Database schemas should be designed in such a way as to segregate data that requires extra protection. Most large-scale database platforms provide functionality for creation of views. User access can be provided through the database views rather than allowing direct access to the underlying tables. Different views may be created for different classes of database users to aid the segregation of data.

Good Practice:

Sensitive personal information may be stored in two or more tables, one with the identifying data and one with the private or sensitive data: a view can then be created that joins the two tables. Only those users that require access to the private or sensitive data will be given permissions to use the joined table view. All users that require access only to the private or sensitive data will be granted permissions to access a view on the table containing the private or sensitive data.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.6.2. Isolation of sensitive information assets

ISMF Standard 100 (Isolation of computing and processing environment)

An isolated computing and/or Information Processing Environment may be used where an Agency deems an application system to be sensitive enough to warrant the additional expense involved, based on a risk assessment.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets.

S100.1. Responsible Parties may implement the control(s) described in clause 11.6.2 of the AS/NZS ISO/IEC 27002:2006 standard

S100.2. Responsible Parties should implement the guidance described in clause 11.6.2 of the AS/NZS ISO/IEC 27002:2006 standard when an Agency has deemed it necessary to establish and maintain and Isolated Information Processing Environment

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

14.7. Mobility

Policy Statement 30

Security capabilities shall be enabled to restrict access to Portable Storage Devices and other portable information assets including mobility devices and systems. Special controls shall be applied to teleworkers and Agency authorised telecommuting environments.

Standards

14.7.1. Mobile and Portable Storage Devices

ISMF Standard 101 (Mobile and portable storage devices)

Responsible Parties shall implement specific controls for the protection of mobile assets incorporating Portable Storage Devices and other forms of portable telecommunications equipment in recognition of the unique risks these assets introduce.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S101.1. Agencies shall implement formal policies and operating procedures for the use of Portable Storage Devices in alignment with the controls and guidance contained in clause 11.7.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.2.1 of the ISO/IEC 27002:2013 standard).

S101.2. Responsible Parties shall comply with Agency and whole-of-government policies, standards and guidelines in circumstances where Portable Storage Devices are used to process and/or store South Australian Government information that contains classification markings.

S101.3. South Australian Government policies, procedures and standards pertaining to the use of Portable Storage Devices and the general requirement to protect Information used in public places should be included in Agency Information Security Awareness Program(s).

S101.4. Third Parties, including Suppliers and temporary or contract personnel should be informed of Agency and whole-of-government policies, standards and procedures pertaining to the use of Portable Storage Devices.

S101.5. Mobile computing devices such as notebooks, laptops, tablets and netbooks should be labelled with a contact name and phone number in case of loss. Typically the contact name and number should be generic, such as the security desk of the Responsible Party and shall contain no personally identifiable markings.

S101.6. Users should not be permitted to modify a portable device or the software on it without authorisation. Installation of software such as games and entertainment packages should be prohibited.

Good Practice:

Portable Storage Devices and Mobility Devices should not be connected to any official networks without approval. If approval for connection is given, then network authentication credentials should not be cached locally on the device.

Modems should not be operated whilst a portable device is connected to SA Government systems. Modems present an unprotected entry point to the network.

Good Practice:

Laptops should not be left in a car, even if it is locked. When travelling, laptops should be transported as hand luggage rather than in the hold of the plane.

Extra care should be taken when passing through security checkpoints at airports. A common scam that is conducted at airports is one thief (in front of the laptop owner) will deliberately set off the metal detector to delay the laptop owner while an accomplice takes the laptop once it has passed through the X-ray machine.

Hotel accommodation cannot be considered to be safe for storage of valuable items, as they are generally not designed with this in mind. If the equipment is to be left unattended for an extended period of time, where practicable, it should be stored in the hotel's safe (if it has one).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S101.7. Agencies may deem it inappropriate for information classified at this level to be stored on portable equipment that is to be used outside the office. S101.8. Strict encryption and user authentication requirements apply for such information to be deployed in Portable Storage Devices as summarised in Classification chapter of the ISMF.
[FOUO] Official Use Only [SOUO] Sensitive	S101.9. Responsible Parties should ensure that encryption is enabled on Portable Storage Devices (to the greatest extent practicable) and that such encryption is approved for the purpose as described by the current edition of the ISM. S101.10. Agencies must ensure that Portable USB thumb drives (a.k.a. "USB keys") are encrypted using an approved algorithm as described in the current edition of the ISM. S101.11. Responsible Parties should develop procedures and processes to ensure that only copies of information are stored on PSDs. Information stored on encrypted devices may be unrecoverable if passwords and/or cryptographic keys are lost or otherwise corrupted.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.7.2. Telework and telecommuting

ISMF Standard 102 (Telework and telecommuting)

Agencies should develop standards addressing the procedures to control teleworking activities, particularly in terms of requirements for Agency ownership, management and security of equipment and information located outside the office environment.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S102.1. Agencies should implement the guidance contained in clause 11.7.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 6.2.2 of the ISO/IEC 27002:2013 standard).

S102.2. Agencies must develop home based working policies (where home based working is determined to be permissible) in alignment with clause 5.7.3 of the PSMF.

S102.3. Telecommuting must be authorised and controlled by management, and suitable arrangements should be established for this method of working.

S102.4. Procedures must exist to ensure Portable Storage Devices located at the approved telecommuting premises are stored in an appropriate security container for the classification level of the information stored on the items when not in use. Compromises of this requirement must be reported.

S102.5. Procedures should be in place to ensure the revocation of authority, access rights and the return of equipment when the telecommuting activities cease.

S102.6. Communication facilities between the office and the telecommuting site should be subject to controls such that sensitive network traffic is appropriately protected relative to the risks involved.

Good Practice:

There may be Workplace Health and Safety issues involved with working off site. In the case of personnel working from home, the agency's Workplace Health and Safety officer may need to approve the home office to ensure that the agency complies with requirements to provide a safe working environment.

Good Practice:

Subject to the information classification and nature of the work involved, agencies may elect to restrict or limit the use of personal equipment for work based activities. Given that an agency may have no control over the processing environment of home based computers owned by personnel, and the potential security exposures that exist for such equipment (particularly in relation to Internet access through third party ISPs and access by family and friends), such personal equipment should not be used for teleworking activities or other home-based work. In such instances dedicated and controlled equipment should be provided by the employer.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4	S102.7. Information should not be stored on equipment outside the office environment unless an appropriate, robust security solution is installed to protect against both casual access by family or friends and risks associated with theft of the equipment from the staff member's residence. Such security should include encryption of local drives. *R102.8 Agencies should consider prohibiting telecommuting involving any information at this classification.*
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

14.7.3. Security of remote, portable and off premises devices

ISMF Standard 44 (Remote, portable and off premises devices)

The security provided for equipment off-premises shall provide the equivalent level of protection to that for on-site equipment used for the same purpose (in terms of classification of information assets stored on or processed by the device) and taking into account the risks of working away from the premises of the Responsible Party.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S44.1. Information processing equipment includes all forms of personal computers, organisers, mobile phones and media including Portable Storage Devices, paper or other forms, which are held for home working or being transported away from the normal work location.

S44.2. Responsible Parties should implement the guidance contained in clause 9.2.5 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 11.2.6 of the ISO/IEC 27002:2013 standard).

R44.3 Further controls and guidance for the protection of mobile equipment is described in the section of this framework entitled Mobility.

S44.4. Management authorisation(s) from an Agency may be implicit in the issuing of Portable Storage Devices, Portable Electronic Devices and/or Mobility devices to staff members, contractors or other third parties, although terms of use for such equipment may limit use off-site for non-work related activities. In such cases, standards should clearly state where implicit and explicit approval is required.

Generally Accepted Industry Practice:

All equipment approved for use off-premises may be recorded in a register, which should be reviewed annually in conjunction with a physical audit of the equipment. The register should record:

- *identifying features (e.g. serial numbers, make, model etc)*
- *maximum classification of data approved for processing and storage on a device*
- *networks that a device is authorised to connect to*
- *current custodian of the equipment*
- *asset numbers.*

To prevent unauthorised disclosure of the information stored on the equipment in the event of theft, suitable controls such as power on passwords, hard disk encryption and use of an operating system that requires user identification and authentication should be considered.

If sensitive information is to be processed outside of the office environment, there shall be procedures in place to ensure the security of any media used for the storage or output of that information. This may be achieved by requiring return of media to the office where there are appropriate facilities for sanitisation and disposal of the media.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15. ACQUISITION, DEVELOPMENT AND MAINTENANCE

15.1. Security attributes

Policy Statement 31

Security requirements shall be identified and agreed upon prior to the development or acquisition of ICT systems. This policy shall also apply to projects relating to infrastructure, business applications, services procurement and user-developed applications.

Standard

15.1.1. Identification of applicable security controls

ISMF Standard 103 (Security in new or enhanced ICT systems)

Requirements documentation for new systems or enhancements to existing systems must include security requirements identification including applicable business and technical controls from the Government of South Australia ISMF.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S103.1. Responsible Parties should implement the guidance contained in clause 12.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.1.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.2. Information integrity attributes and requirements

Policy Statement 32

Sensitive applications and information processing systems shall utilise additional controls, subject to security requirements analysis and risk assessments, including the use of audit trails or activity logs and information integrity checks at all stages of processing.

Standard

15.2.1. Input validation and information integrity

ISMF Standard 104 (Validation of input)

Inbound information (or data), whether input automatically or manually to application systems should be validated to ensure that it is accurate and appropriate.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S104.1. Responsible Parties should implement the guidance described in clause 12.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 104).

S104.2. Input validation testing procedures should incorporate both valid and invalid data entry.

S104.3. Database interface applications should be written to reject any SQL commands submitted as part of user input (unless the user input is expected to be a SQL command – care should be taken in this case to limit the SQL commands that may be executed by the user supplied input).

S104.4. Testing procedures may take into account known hacker methodologies and exploits for application manipulation, particularly the wide-spread use of buffer-overflow and code injection attacks.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[I4] Integrity 4	S104.5. This standard must be applied to all services and platforms at this classification level.

15.2.2. Information corruption prevention

ISMF Standard 105 (Prevention of information corruption)

Responsible Parties may implement processing checks and controls to validate information integrity and to reduce the risks associated with information corruption during internal processing.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S105.1. Responsible Parties may implement the guidance contained in clause 12.2.2 of the AS/NZS ISO/IEC 27002:2006 standard

S105.2. The need for controls and checks in internal processing is determined by the value of the information or data being processed. The value of the data being processed will dictate the number of controls that should be implemented to ensure the integrity of that data. The higher the value will imply a higher number of controls.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[I3] Integrity 3	S105.3. Provide a retention period or expiry date facility for files and storage volumes, and the means to prevent inadvertent modification or destruction of the data within that interval. S105.4. Protect data from inadvertent modification on removable media by enabling any write prevention mechanism provided by the media.
[I4] Integrity 4	S105.5. ISMF Standard 105 must be applied to services and systems requiring absolute integrity of information.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.2.3. Message authenticity and validation

ISMF Standard 106 (Message validation and integrity)

Message validation and integrity checks should be used for applications where there is a security requirement to protect the integrity of the message content and where a risk assessment deems this to be necessary.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S106.1. Responsible Parties may implement the control(s) contained in clause 12.2.3 of the AS/NZS ISO/IEC 27002:2006 standard

S106.2. Message authentication may be used to detect unauthorised changes to, or corruption of, the contents of a transmitted electronic message and is useful in sensitive applications such as financial transactions and commercial contracts.

S106.3. Cryptographic techniques may be used as an additional control to prevent the unauthorised disclosure of messages to third parties and/or external applications.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[I4] Integrity 4	S106.4. Cryptographic techniques should be employed to generate and append a message authentication code (MAC) to every message sent to another party, and to check for a valid MAC on messages received from another party. A cryptographic algorithm endorsed for the purpose in the ISM should be used.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.2.4. Output validation and information integrity

ISMF Standard 107 (Output validation)

Outbound information (or data), including output generated by application systems may be validated to ensure that it is accurate, free of processing errors and appropriate.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S107.1. Responsible Parties may implement the guidance contained in clause 12.2.4 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Agencies from their obligations under ISMF Standard 107).

S107.2. Responsible Parties should define the responsibilities of all personnel involved in the data output process in line with Agency requirements, with appropriate consideration of limitations surrounding the timeliness and effectiveness of the checks that are to be performed.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS	
[I4] Integrity 4	S107.3	ISMF Standard 107 must be applied to services and systems requiring absolute integrity of information.

15.3. Cryptographic requirements

Policy Statement 33

Cryptographic systems and techniques in alignment with the controls and guidance described in Australian Government Information Security Manual must be employed for the protection of information that is considered at risk, and to strengthen complementary controls that require an additional level of protection.

Standard

15.3.1. Policy on the use of cryptographic controls

ISMF Standard 108 (Agency cryptography policy)

Information requiring cryptographic controls and procedures should be complemented by an Agency policy detailing the usage guidelines, requirements, policy exceptions and associated standards for cryptographic controls.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S108.1. Responsible Parties must implement the controls and should implement the guidance described in clause 12.3.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 10.1.1 of the ISO/IEC 27002:2013 standard).

S108.2. Agencies that use encryption and cryptographic techniques for the protection of information must develop policies detailing the implementation guidance, standards and any applicable exceptions to the policy

S108.3. Agencies must communicate policies encompassing the use of cryptographic techniques to relevant personnel and suppliers

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.3.2. Encryption

ISMF Standard 109 (Encryption technology)

Agencies should deploy encryption technologies to protect the confidentiality of sensitive or critical information.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S109.1. For new deployments of encryption technology commencing as of 1st July 2011: Agencies must implement encryption algorithms and cryptographic key lengths based on the recommendations and guidance described in the cryptography section of the most current version of ISM.

S109.2. Encryption algorithm selection and key lengths should be reviewed periodically by Responsible Parties to ensure that the algorithms and keys still adequately protect the Information pursuant to its classification.

S109.3. Suppliers must ensure that their encryption techniques are compatible with the recommendations described in the cryptography section of the ISM and in accordance with Agency controls and cryptographic policies.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet	S109.4. Sensitive messages or individual fields must be encrypted during transmission over public communications networks.
[FOUO] Official Use Only [SOUO] Sensitive	S109.5. Portable Storage Devices should be encrypted and USB thumb drives must be encrypted as described in ISMF Standard 101.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.3.3. Digital signatures

ISMF Standard 110 (Digital signatures)

Responsible Parties that employ the use of Digital signatures to protect the authenticity and integrity of electronic documents shall do so in accordance with the controls stipulated by the Government of South Australia ISMF and the Australian Government ISM.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S110.1. Digital Signatures may be used in electronic commerce applications and e-contracts where there is a need to verify who signed an electronic document and to validate whether the contents of the signed document have been altered or modified. They can be applied to any form of document being processed electronically, e.g. they can be used to sign electronic payments, funds transfers, contracts and agreements.

S110.2. Responsible Parties that employ the use of Digital Signatures must also implement the controls and guidance described by ISMF Standard 111 (Non-Repudiation Services).

S110.3. Digital Signatures that employ cryptographic techniques using a Public/Private Key combination must implement an approved public key algorithm as described in the ISM and furthermore must implement the technical controls for the selected algorithm as described subsequently in the ISM.

S110.4. Private Keys used in Digital Signatures must be kept secret since anyone having access to this key can sign documents, e.g. payments or contracts, thereby forging the signature of the owner of that key. In addition, the integrity of the Public Key must be maintained and these two key pairs shall be maintained in accordance with ISMF Standard 102.

S110.5. Cryptographic keys used for digital signatures should be different from those used for encryption.

S110.6. When using digital signatures, consideration should be given to any relevant legislation that describes the conditions under which a digital signature is legally binding. For example, in the case of electronic commerce it is important to know the legal standing of digital signatures. It may be necessary to have binding contracts or other agreements to support the use of digital signatures where the legal framework is inadequate. Legal advice should be sought regarding the laws and regulations that might apply to the Responsible Party's intended use of digital signatures.

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[I4] Integrity 4	S110.7. Employ cryptographic techniques to generate unique digital signatures that can be used to prove the origin of a message. Append them to messages sent to another party and validate them on messages received from another party. Use a cryptographic algorithm endorsed for the purpose in the current version of Australian Government ISM.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.3.4. Non-repudiation services

ISMF Standard 111 (Non-repudiation)

Responsible Parties shall implement non-repudiation services upon completion of a risk assessment that deems it may be necessary to resolve disputes about occurrence or non-occurrence of an event or action. Non-repudiation services and associated controls must be employed in applications that employ the use of Digital Signatures.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S111.1. Non-repudiation services should provide evidence to substantiate whether a particular event or action has taken place, e.g. when there is a dispute over the use of a digital signature on an electronic contract or payment, or when there is a denial of sending a digitally signed instruction using electronic messaging services.

S111.2. Non-repudiation services require strict implementation of Audit logging and monitoring controls described by this framework including timestamp synchronisation.

S111.3. Responsible Parties that use services such as secure electronic messaging applications or e-commerce shall ensure that the service offering includes Non-Repudiation services, not only from a product feature offering as is included as part of the Contractual agreement associated with the service. (i.e. a service characteristic rather than simply a product feature or attribute).

S111.4. Non-Repudiation services that are based on digital certificates should adhere to the ISO/IEC 13888-1 standard. Mechanisms using symmetric techniques are contained in ISO/IEC 13888-2 and asymmetric techniques are described in ISO/IEC 13888-3.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.3.5. Protection and management of cryptographic keys

ISMF Standard 112 (Cryptographic key management)

A key management system shall be established, based on an agreed set of standards, procedures and secure methods including provisions for protecting cryptographic keys from modification, destruction and unauthorised disclosure.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S112.1. The management of cryptographic keys is essential to the effective use of cryptographic technologies. Any compromise or loss of cryptographic keys may lead to a compromise of the confidentiality, authenticity and/or integrity of information.

S112.2. Responsible Parties must implement the control(s) and guidance described in clause 12.3.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 10.1.2 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.4. Security of system files

Policy Statement 34

Responsible Parties shall implement security measures to maintain the integrity of system files, test and verification data and program source code. Such measures must include the development of procedures to protect these assets from unauthorised access and the removal of personally identifiable information and other sensitive information from test and verification data.

Standard

15.4.1. Control of operational software in production environments

ISMF Standard 113 (Installation and deployment of software)

Responsible Parties shall implement procedures for managing installations and deployment of software on *operational systems*.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S113.1. Responsible Parties should implement the guidance contained in clause 12.4.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.5.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.4.2. Protection of system test data

ISMF Standard 114 (Protection of test data)

Responsible Parties should establish selection criteria for test and system validation data which needs to be protected and controlled in line with the findings of an Agency risk assessment.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S114.1. Responsible Parties should implement the control(s) and guidance described in clause 12.4.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.3.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.4.3. Security of program source code

ISMF Standard 115 (Source code)

Strict control should be maintained over access to program source code and libraries, in order to reduce the potential for corruption of computer programs (ISMF Policy Statement 18).

Business Controls

S115.1. Responsible Parties may implement the control(s) and may implement the guidance described in clause 12.4.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 9.4.5 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[P] Protected [SC] Sensitive: Cabinet [I4] Integrity 4 [A4] Availability 4	S115.2. Program source libraries should not be contained on operational systems at this classification.
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S115.3. Clauses 12.4.3d through 12.4.3g of the AS/NZS ISO/IEC 27002:2006 standard S115.4. Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures. S115.5. A program librarian should be nominated for each application.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S115.6. Access to program source libraries by support personnel should be managed and restricted according to exacting business and operational requirements. S115.7. Programs under development or maintenance should not be held in operational program source libraries.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.5. Security in development and support processes

Policy Statement 35

Responsible Parties shall implement change control procedures and security controls in information processing development and support procedures to reduce the likelihood of compromises to the system and/or the operating environment.

Standard

15.5.1. Change control procedures

ISMF Standard 116 (Change control in development and support)

Formal change control procedures shall be established and enforced so that the risk of corruption and/or disruption to information systems is appropriately controlled.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S116.1. Change control procedures should consider the full system development life cycle. Useful references for further guidance include Configuration Management as described by the AS/NZS ISO/IEC 10007 standard and AS/NZS ISO/IEC 12207 which describes software lifecycle management.

S116.2. Responsible Parties should implement the control(s) and guidance contained in clause 12.5.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.2.2 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S116.3. A change controller should be appointed to coordinate and oversee all aspects of change and configuration management. S116.4. Responsibility for migrating tested changes into production status should be assigned to a person or group with no other role in approving, developing or implementing changes. S116.5. A database of completed changes should be retained for a sufficient period to meet Agency requirements. This requirement is in addition to maintaining a standard audit trail

CLASSIFICATION	ADDITIONAL CONTROLS
	encompassing all change requests, whether or not they have been approved and subsequently actioned. S116.6. Where an emergency change is needed for rapid recovery from critical errors or situations, such changes should be approved by the Business Owner prior to application, and should be documented and reapplied using the normal change management process as soon as practicable.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.5.2. Impact and review of operating system changes

ISMF Standard 117 (Change review)

Business systems and applications shall be reviewed and tested to ensure that there is no adverse impact on operation or security as a result of any changes or upgrades to the underlying operating system.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S117.1. Responsible Parties shall implement the control(s) and should implement the guidance contained in clause 12.5.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.2.3 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

CLASSIFICATION	ADDITIONAL CONTROLS
[SLC] Sensitive: Legal or Commercial [SM] Sensitive: Medical [SP] Sensitive: Personal [I3] Integrity 3 [A3] Availability 3	S117.2. Use only mature, stable operating systems and associated software and defer vendor software maintenance until it has proven to be reliable.
[FOUO] Official Use Only [SOUO] Sensitive [I2] Integrity 2 [A2] Availability 2	S117.3. Only documented and supported techniques should be used to amend the processing or extend the scope of operating system software. These may include the use of exit routines or replaceable programs or commands.

CLASSIFICATION	ADDITIONAL CONTROLS
	S117.4. The function and method of operation of all amendments and extensions should be documented. S117.5. A library of documentation and listings of all amendments and extensions should be maintained and kept current. Ensure that only those IT support personnel who maintain the operating system, and the appropriate management personnel, have access to this library.
Note: Controls begin to apply at the classifications listed and are retained at higher levels.	

15.5.3. Custom modification of software packages

ISMF Standard 118 (Custom modifications to software)

Custom modifications to software packages should be minimised, restricted to essential changes and controlled.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S118.1. Responsible Parties should implement the guidance described in clause 12.5.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 14.2.4 of the ISO/IEC 27002:2013 standard).

S118.2. Reducing the number of modifications minimises the re-work effort required and risks associated with reapplying changes to upgraded software versions as they are released.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.5.4. Prevention of information leakage

ISMF Standard 119 (Covert channels)

Measures and controls should be implemented to protect against unauthorised information disclosure resulting from the presence of embedded covert channels and code exploits (such as Trojans) in applications and systems used to process Agency information. Additionally, all

software products installed on Agency equipment shall be licensed and acquired from a reputable source.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S119.1. Responsible Parties shall implement the control(s) and should implement the guidance described in clause 12.5.4 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 119).

S119.2. ISMF Standard 119 should be applied to include adware and spyware protection methods applied to agency assets. (Refer ISMF Standard 141 for further information)

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.5.5. Outsourced software development

ISMF Standard 120 (Outsourced software development)

Responsible Parties entering into outsourcing arrangements for software development should seek legal advice to ensure that the Agency's rights and interests are protected and should implement the guidance described in the AS/NZS ISO/IEC 27002 code of practice pertaining to outsourced software development.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S120.1. Responsible Parties shall implement the control(s) and guidance described in clause 12.5.5 of the AS/NZS ISOIEC 27002 standard (alternately refer control 14.2.7 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.5.6. Secure development principles

ISMF Standard 143 (Secure development principles)

Responsible Parties shall establish clear rules for security considerations and controls in development of software, services and infrastructure, proportionate to the classification requirements of the information being processed, stored or otherwise transmitted by the service.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S143.1. Responsible Parties should establish clear criteria to support security in all aspects of development and implementation of systems and services. Rules should encompass the guidance contained below:

- control 14.2.1 of the ISO/IEC 27002:2013 standard encompassing development policy
- control 14.2.5 of the ISO/IEC 27002:2013 standard describing secure system engineering principles
- control 14.2.6 of the ISO/IEC 27002:2013 standard for securing the development environment

S143.2 Responsible Parties must consult the Government of South Australia web applications and web server security standards for web server configuration and web application deployment.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

15.6. Vulnerability and threat assessment

Policy Statement 36

Responsible Parties shall establish a procedure to regularly assess risks arising from published technical vulnerabilities and bulletins or other notifications about emerging threats to information assets. Responsible Parties shall enact preventative measures to reduce and/or eliminate vulnerabilities and threats to information assets.

Standard

15.6.1. Controlling technical vulnerabilities

ISMF Standard 121 (Vulnerability management)

Responsible Parties shall implement procedures to regularly obtain information about technical vulnerabilities and emerging threats to Agency information assets and shall undertake preventative measures to reduce and/or eliminate risks to these assets.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

R121.1 Change control procedures should consider the full system development life cycle. Useful references for further guidance include Configuration Management as described by the AS/NZS ISO/IEC 10007 standard and AS/NZS ISO/IEC 12207 which describes software lifecycle management.

S121.1. A typical threat analysis formula should consider the following metrics:

- Desire to cause harm x Expectation of success = Intent
- Resources available to cause harm x knowledge = Capability
- Sum of Intent + Capability = Threat level

S121.2. Responsible Parties may implement the guidance contained in clause 12.6.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.6.1 of the ISO/IEC 27002:2013 standard).

S121.3. The ISM provides additional controls and guidance to Responsible Parties in consideration of threat and vulnerability assessments.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

16. BUSINESS CONTINUITY PLANNING

16.1. Aspects of business continuity management

Policy Statement 37

Responsible Parties shall ensure that risk management and information security management controls and procedures are embedded in their business continuity management process. Business Continuity Plans [BCPs] should be tested, maintained and re-assessed on a regular basis.

Standard

16.1.1. Business continuity management process

ISMF Standard 122 (Business continuity management)

Responsible Parties shall establish a managed process to maintain business continuity throughout the Agency and must incorporate information security considerations and the allocation of responsibilities and resources to appropriately support the business continuity management processes.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S122.1. Responsible Parties shall implement the control(s) and should implement the guidance contained in clause 14.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 122).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

16.1.2. Business impact analysis

ISMF Standard 123 (Business impact analysis)

Responsible Parties should undertake business impact analysis resulting from risk identification and assessments. This process should identify the events that can cause interruptions to business processes and incorporate their probability, scale and acceptable recovery period in a

multitude of scenarios. A strategic plan, endorsed by management, should be developed to determine the overall approach to business continuity.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S123.1. Responsible Parties should implement the guidance contained in clause 14.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 17.1.1 of the ISO/IEC 27002:2013 standard)

S123.2. Responsible Parties must cater for the continuity of information security management functions as part of their business continuity arrangements. Such arrangements should be tested periodically and adjustments or improvements implemented as required (refer controls 17.1.2 and 17.1.3 of the ISO/IEC 27002:2013 standard for further implementation guidance)

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

16.1.3. Establishing continuity plans

ISMF Standard 124 (Business continuity plans)

A documented business continuity plan or set of plans shall be prepared to maintain or restore business operations following interruption to or failure of critical business processes. This plan shall be based around the specific requirements of the Business Owner(s), in terms of the priorities and time scales that are to be met under the plan.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S124.1. Responsible Parties should implement the guidance described in clause 14.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 124).

S124.2. Responsible Parties should familiarise themselves with ISMF Guideline 37a - Critical ICT in order to determine if any assets qualify as being State Government Critical Information Infrastructure [SGCII]

S124.3. In implementing the plan, consideration should be given to preventative measures as well as the action to be taken in response to a significant system outage or disaster event. These may include:

- monitoring systems and processes (e.g. temperature and humidity alarms, fire detection / suppression, power filtering systems);
- system placement (e.g. use of basements);

- computer equipment that incorporates a high degree of internal redundancy and fault tolerance, to permit continuity of operation even when major components have failed;
- operating systems that provide a high degree of tolerance to software and hardware failures;
- alternate routing of critical communications lines via redundant paths isolated to the maximum extent possible;
- redundancy and protection measures within environmental services, to limit the impact of a single point of failure, including;
  - ❖ excess air conditioning and cooling capacity;
  - ❖ implement power filtering, conditioning and/or UPS;
  - ❖ redundant fixed data storage capacity to facilitate recovery from a unit failure.

S124.4. The business continuity plan should include as a minimum:

- the criteria to activate the plan including detection of a disaster and notification of relevant personnel;
- defined maximum tolerable outages (MTOs) for systems and services coupled with recovery time objectives (RTOs);
- defined recovery point objectives (RPOs);
- procedures to implement the recovery strategy and recover all applications;
- the persons/positions responsible for each aspect of the recovery process (within both the Agency and the service provider);
- procedures to revert to normal processing;
- testing procedures;
- the persons/positions responsible for co-ordinating ongoing maintenance of the plan
- coordination with the State's emergency management arrangements, where necessary.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

16.1.4. Business continuity planning framework

ISMF Standard 125 (BCP framework)

Within each Agency, a single framework of business continuity plans should be maintained to ensure that plans across all business units are consistent.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S125.1. Responsible Parties should implement the control(s) and guidance described in clause 14.1.4 of the AS/NZS ISO/IEC 27002:2006 standard (The removal of this control in ISO/IEC 27001:2013 does not absolve Responsible Parties from their obligations under ISMF Standard 125).

S125.2. The business continuity planning framework should also include emergency procedures that describe the actions to be taken following an incident which jeopardises business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities, e.g. police, fire service and local government.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

16.1.5. Validation and continual improvement of business continuity plans

ISMF Standard 126 (BCP review)

Agencies are accountable for the periodic review, testing and maintenance of business continuity plans. Such reviews and tests must incorporate continuity of the information security management function.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S126.1. Responsible Parties may implement the guidance described in clause 14.1.5 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 17.1.3 of the ISO/IEC 27002:2013 standard).

S126.2. Responsible Parties may consult the ISO/IEC 27031 standard (formerly BS 25777) which is a code of practice for ICT continuity management and/or the ISO 22301 standard which describes requirements for Business Continuity Management Systems.

S126.3. ISO/IEC 24762 standard provides guidelines for ICT disaster recovery services.

S126.4. The techniques used for testing and validation should reflect the nature of the specific recovery plan.

S126.5. Business Continuity Plans shall be maintained through periodic review to revisit and reconfirm assumptions and priorities of the plan in light of changes within the Agency, its business operations and/or the technical environment.

S126.6. Instruction and training should be provided to personnel responsible for the execution of the plan. The testing process should involve both the primary personnel and their designated alternatives.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17. COMPLIANCE

17.1. Compliance with legal requirements

Policy Statement 38

Responsible Parties shall implement procedures to monitor and maintain compliance to applicable statutory, regulatory and contractual security requirements. Advice on specific legal requirements should be sought from the Agency's legal advisers, the Crown Solicitor's Office [CSO] or in the case of Suppliers to Government, other suitably qualified legal practitioners.

Standards

17.1.1. Identification of applicable legislation and regulatory requirements

ISMF Standard 127 (Legislative and regulatory requirements)

Responsible Parties shall define, document and maintain their compliance with respect to legislative, statutory, regulatory and contractual conditions and requirements for each identified information asset.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets.

S127.1. Responsible Parties may implement the guidance described in clause 15.1.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.1.1 of the ISO/IEC 27002:2013 standard).

S127.2. Where a Responsible Party is required by legislation to manage information security in a manner contrary to this framework, that legislation must take precedence over this framework. Where legislation mandates a lower level of security than this framework, Responsible Parties should, where applicable, apply the higher level of security.

S127.3. Section 109 of the Australian Constitution provides that if a valid Commonwealth law is inconsistent with a law of a State Parliament, the Commonwealth law operates and the State law is invalid to the extent of the inconsistency.

S127.4. Part A, section 5 of the PSM addresses legislative requirements with respect to implementation of any controls and/or guidance described in the PSM.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.1.2. Intellectual property rights and licensing

ISMF Standard 128 (Intellectual property)

Agencies are accountable for ensuring compliance with legislative, contractual and statutory requirements on the use of material that is the subject of intellectual property rights, such as copyright, design rights or trademarks and software products.

Responsible Parties shall implement procedures to maintain compliance with this standard including the recording of non-compliance(s) and remedial actions that are taken as part of their Incident Management processes.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S128.1. Responsible Parties shall note the obligations and requirements described in the across government Intellectual Property Policy

S128.2. Responsible Parties should implement the guidance contained in clause 15.1.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.1.2 of the ISO/IEC 27002:2013 standard).

S128.3. Compliance with software licence requirements and terms of use therein shall be monitored.

S128.4. Software shall not be copied except for authorised installation and backup purposes. Software shall not be copied for personal use unless it is expressly permitted by the Agency's licensing agreements and approved by senior management.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.1.3. Protection of government records including Data Loss Prevention

ISMF Standard 129 (Protection of government records)

Government records, including information that is stored electronically as data, shall be protected from loss (including theft), destruction and falsification in accordance with relevant statutory, legislative, regulatory and contractual requirements. Responsible Parties shall implement information protection controls commensurate with the importance and sensitivity of the information to the Agency.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S129.1. Responsible Parties should implement the guidance described in clause 15.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.1.3 of the ISO/IEC 27002:2013 standard).

S129.2. Responsible Parties shall implement protection control(s) commensurate with the importance and sensitivity of the information to the Agency. Business Owner(s) are responsible for approving and managing implementation of these controls.

S129.3. In certain circumstances, the identified Business Owner(s) should consult with Agency Security Executives [ASEs] to determine that the control(s) selected are appropriate and adequate to meet Agency or whole-of-government requirements.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.1.4. Data protection and privacy of personal information

ISMF Standard 130 (Privacy and confidentiality)

Responsible Parties shall observe the requirements of the Government's Information Privacy Principle Instruction, secrecy provisions in other legislation and all relevant government policy to ensure the protection of personal information and the protection of SA Government data, during capture, storage and use.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S130.1. Responsible Parties shall note the implementation of ISMF Standard 130 and applicable corresponding controls satisfies the objectives described by clause 15.1.4 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.1.4 of the ISO/IEC 27002:2013 standard).

S130.2. Responsible Parties must define 'Authorised Access' for all data, including who has access, the level of authority required, and the level of access allowed

R130.2 *DPCS4.2 Security – Privacy and Confidentiality* (ISMF Standard 138) describes policy obligations with respect to access to private information on ICT systems

S130.3. In circumstances where information systems are used to solicit information from members of the public (e.g. in an e-commerce or e-government scenario), informative messages should be included at the point of information capture, to make the individual aware of the intended use of the information, who will use the information and any legal authority or requirements to collect the information.

S130.4. Agencies that are involved in transmitting, soliciting and collecting personal information via websites should also have regard for the Privacy Guidelines for SA Government websites available from the Privacy Committee of South Australia.

S130.5. Information that can be used to readily identify an individual should be classified higher than information that has been *de-identified* or '*anonymised*' (e.g. information that does not identify an individual by publicly accessible information such as name, address or telephone number), and appropriate data protection controls should be applied (refer Classification chapter of ISMF).

S130.6. Access control lists for electronically stored personal information should be carefully designed such that only those personnel that have a need-to-know are able to access the information, consistent with the stated purpose of collection and disclosure of the information.

S130.7. Advice should be sought from the Privacy Committee of South Australia or the *Advising Section* of the Crown Solicitor's Office regarding any legislative or government policy obligations for the protection of personal information.

S130.8. The *South Australia Freedom of Information Act (1991)* has provisions regarding the rights of individuals to access records pertaining to their personal affairs and to seek amendment where they believe such records to be incomplete, incorrect, out-of-date or misleading.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.1.5. Acceptable use of information assets

ISMF Standard 131 (Acceptable use of assets)

Agencies should implement an "Acceptable Use" policy or policies and inform all personnel of their responsibilities and obligations surrounding the use of Agency information assets.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S131.1. Agencies should implement the guidance described in clause 15.1.5 of the AS/NZS ISO/IEC 27002:2006 standard

S131.2. Each "Acceptable Use" policy must include a definition and description of what is considered Acceptable Use and what types of usage of information assets by personnel would constitute "unauthorised use" or purpose.

S131.3. Standards for acceptable use of information processing facilities by authorised users shall be clearly defined by each Agency, and implemented through documented guidance for personnel that incorporates processes for monitoring of compliance and disciplinary measures to be applied in the event of non-compliance.

S131.4. In considering requirements for controls over acceptable use of equipment, the Agency should consider both external parties that may attempt to gain unauthorised access to their network and computer systems, as well as unauthorised internal users. Agencies also need to consider internal and external users with authorised access, provided to meet business requirements.

S131.5. A level of personal use of facilities by authorised users may be acceptable (in a manner similar to acceptance of limited personal phone use). Agencies should take care in establishing practical boundaries such that they are both acceptable to Agency management and they can be enforced (i.e. will not be subject to successful legal challenge). Legal advice should be sought in this regard.

S131.6. Responsible Parties should seek to obtain explicit acknowledgement from personnel and authorised users regarding “Acceptable Use” policies, standards and guidelines, as well as management’s monitoring of their activity.

S131.7. Legal implications of system misuse by SA Government personnel should also be determined in consultation with legal advisers. This advice should be communicated to all users so that they are made aware of any possible legal consequences of misuse.

S131.8. Implementation of ISMF Standard 131 satisfies the objectives of control 7.1.3 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 8.1.3 of the ISO/IEC 27002:2013 standard)

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.1.6. Regulation of cryptographic controls

ISMF Standard 132 (Regulatory compliance on encryption and cryptography)

Agencies should allocate responsibility and implement procedures to comply with any agreements, laws, regulations or other instruments relating to access to or use of cryptographic controls.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S132.1. Responsible Parties must implement the guidance contained in clause 15.1.6 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.1.5 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.2. Security policies, standards and technical reviews

Policy Statement 39

Responsible Parties shall undertake regular reviews of information assets to ensure ongoing compliance to applicable security policies, standards and guidelines.

Standard

17.2.1. Compliance with security policies and standards

ISMF Standard 133 (Policy compliance reviews)

Agency managers, particularly Business Owners and ITSAs or the equivalent role(s) within a Supplier, should ensure that all security procedures are carried out correctly, and should regularly review compliance with Agency and whole-of-government security policies and standards.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S133.1. Responsible Parties should implement the control(s) and guidance contained in clause 15.2.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.2.2 of the ISO/IEC 27002:2013 standard).

S133.2. Responsible Parties should support periodic reviews of the compliance of their systems to relevant security policies, standards and controls.

S133.3. Certain instances of non-compliance to Agency and/or whole of government security policies and procedures may trigger a *Notifiable Incident* as described in ISMF Standard 9.

S133.4. The *protective security governance guideline* document entitled 'Agency Security Adviser and IT Security Adviser functions and competencies' describes the role and desirable attributes of ITSA including responsibilities in the area of ICT audit.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.2.2. Technical adherence to security standards and controls

ISMF Standard 134 (Technology compliance reviews)

Responsible Parties shall ensure that information assets and systems are periodically reviewed for compliance with security implementation standards and controls.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S134.1. Responsible Parties should implement the guidance contained in clause 15.2.2 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.2.3 of the ISO/IEC 27002:2013 standard).

S134.2. An internal experienced systems engineer or an external independent trusted expert, such as participants in the Australian Government's Computer Network Vulnerability Assessment Program, should perform system hardening prior to the release into production of any new system or change to a system.

S134.3. There should be documented and planned procedures for the examination of hardware and software to ensure that known security patches and fixes have been implemented. The major weakness in most organisations is the lack of change and configuration control. System documentation should specify a maximum timeframe that security patches have to be applied within, to ensure that the system is not compromised through a vulnerability that has been addressed using either patches or configuration changes recommended by the supplier and/or vendor.

S134.4. Access to tools, utilities and other information or data used in the auditing and compliance checking should be protected as described in ISMF Standard 136

S134.5. The frequency of technical compliance checks depends on the value of the information being stored in that system.

S134.6. An independent trusted expert (e.g. an Internal Auditor from another Agency, or a Supplier who specialises in conducting technical security audits) should perform an external audit of the technical compliance of the technical environment annually. This audit may include a threat and risk assessment and a penetration test.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.2.3. Periodic independent review

ISMF Standard 11 (Independent review)

In addition to periodic self-assessment, each Responsible Party shall be subject to ongoing independent review of Information Security policies, practices and implementation at regular intervals in accordance with the AS/NZS ISO/IEC 27002 code of practice.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S11.1. Responsible Parties should adopt the implementation recommendations described in clause 6.1.8 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 18.2.1 of the ISO/IEC 27002:2013 standard).

R11.2 Responsible Parties may consult the Information Security Reviews section of the 2009 edition ISM for detailed guidance.

S11.2. Agencies may avail the use of the Cyber Security Services Portal of the e-Projects Panel as a means for approaching the market and subsequently obtaining independent reviews from suitably qualified and pre-screened supplier organisations.

S11.3. An information security review may be scoped to cover anything from a single system to an entire agency's systems.

S11.4. Agencies should ensure that the rigour of an information security review is commensurate with the threat environment and if applicable the highest security classification of information that is involved.

S11.5. An agency may choose to undertaken an information security review: a) as a result of a specific information security incident; b) due to a change to a system or its environment that significantly impacts on the agreed and implemented information security architecture and policy, or c) as part of a regular scheduled review.

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.3. Audit planning considerations

Policy Statement 40

Responsible Parties must conduct an internal audit, at least annually, of their information security operating environment and controls. Agencies should provide relevant information security recommendations resulting from Internal Audit(s) to the Department of the Premier and Cabinet.

Safeguards shall be established to preserve the integrity of auditable data and to prevent misuse of audit tools. Additionally, Responsible Parties shall ensure that audits are adequately planned and implement appropriate controls to limit or eliminate possible business disruption.

Standards

17.3.1. Audit planning and controls

ISMF Standard 135 (Internal audits)

Responsible Parties should ensure that Audit activities, scope and requirements are planned accordingly and approved by the Agency Business Owner(s) in order to minimise the risk of disruption to business activities. Responsible Parties must conduct internal audit(s) of their information security environment at least once per year.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S135.1. Agencies should provide information security related internal audit recommendations to the DPC for identification of trends that may impact whole of Government or have implications to Inter-Agency operations.

S135.2. Responsible Parties must implement the control(s) and should implement the guidelines described in clause 15.3.1 of the AS/NZS ISO/IEC 27002:2006 standard (alternately refer control 12.7.1 of the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

17.3.2. Protecting system audit tools and utilities

ISMF Standard 136 (System audit tools)

Responsible Parties should ensure that access to system audit tools and utilities is restricted and that audit data and information is adequately protected to prevent possible misuse or compromise.

Business Controls

The following general guidance applies regardless of the classification levels of the information assets:

S136.1. Responsible Parties must establish procedures for the use of tools and utilities that capture information for auditing purposes

S136.2. Installation and amendment of audit tools and utilities should not be permitted from non-privileged user accounts (Refer ISMF Standard 78)

S136.3. Implementation of ISMF Standard 136 and corresponding controls satisfies the requirements contained in clause 15.3.2 of the AS/NZS ISO/IEC 27002:2006 standard. (There is no corresponding control in the ISO/IEC 27002:2013 standard).

Additional controls based on DLMs and protective markings

There is no additional guidance specific to information asset classification levels.

This page is intentionally left blank.

ANNEX A - BASELINE FOR AGENCIES AND SUPPLIERS

The minimum control set required by all Agencies and Suppliers regardless of the scope of their ISMS implementation(s) consists of applying risk treatment measures (via application of selected ISMF Standards) against all forty (40) Policy Statements contained in the ISMF. Selective application of the ISMF Standards to address each of the forty policy domains sanctioned by Cabinet effectively establishes the cyber security baseline for across government ICT services and operations utilising control objectives derived from the AS/NZS ISO/IEC 27001 standard.

This baseline establishes the *organisational* security posture. Individual projects and undertakings or activities within an organisation may only reference a subset of the requirements below, but need to be rolled up into the holistic security architecture of the organisation. The functional domain field provided in the table below is purely indicated for guidance on the area within an organisation that could maintain and/or administer oversight of the respective ISMF policy requirement.

It should be noted that Business Owners as defined in the ISMF, are equivalent to the term 'risk owner' as introduced in the 2013 publication of the ISO 27001 standard. Conversely, Responsible Parties may treat and manage risks on behalf of a Business Owner. This is commonly the case where an organisation has contracted ICT service delivery to another organisation (whether internal or external to SA Government).

Mandatory ISMF Standards supporting the ISMF Policy Statements are listed below:

Functional domain	ISMF policy domain	ISMF Standards in support of corresponding policy
Governance	**Policy Statement 1**	Establishes the requirement to establish an Information Security Management System [ISMS] in alignment with the principles of AS/NZS ISO/IEC 27001
Business Owners	**Policy Statement 2**	**ISMF Standard 1 (Risk identification and assessment)**
Security	**Policy Statement 3**	**ISMF Standard 2 (Information security policy document)** **ISMF Standard 3 (Policy ownership and review)**
Governance	**Policy Statement 4**	**ISMF Standard 4 (Executive management oversight)** **ISMF Standard 5 (Security coordination)** **ISMF Standard 6 (Security roles and responsibilities)** **ISMF Standard 49 (Segregation of duties)** **ISMF Standard 9 (Incident response)** **ISMF Standard 142 (Projects and project management)**
Procurement	**Policy Statement 5**	**ISMF Standard 12 (Risk assessment of external organisations)** **ISMF Standard 14 (Contractual agreements)**
Procurement	**Policy Statement 6**	**ISMF Standard 15 (Procurement and sourcing)** **ISMF Standard 139 (Security in an outsourced environment)**
Business Owners	**Policy Statement 7**	**ISMF Standard 16 (Asset inventory)** **ISMF Standard 17 (Asset ownership)**
Business Owners	**Policy Statement 8**	**ISMF Standard 19 (Classification)** **ISMF Standard 70 (Release of public information)**

Functional domain	ISMF policy domain	ISMF Standards in support of corresponding policy
Human Resources	**Policy Statement 9**	**ISMF Standard 21 (Security in job and person specifications)** **ISMF Standard 22 (Personnel screening)**
Business Owners	**Policy Statement 10**	**ISMF Standard 24 (Management and supervisory obligations)** **ISMF Standard 25 (Ongoing security awareness)** **ISMF Standard 26 (Disciplinary process)**
Business Owners	**Policy Statement 11**	**ISMF Standard 28 (Return of assets)** **ISMF Standard 29 (Removal of access)**
Business Owners and Security	**Policy Statement 12**	**ISMF Standard 31 (Reporting vulnerabilities)** **ISMF Standard 140 (Notifiable Incidents)** **ISMF Standard 32 (Incident management)** **ISMF Standard 34 (Evidence)**
Building Management	**Policy Statement 13**	**ISMF Standard 36 (Physical access control)** **ISMF Standard 37 (Security of offices and facilities)** **ISMF Standard 39 (Delivery and loading areas)**
Business Owners	**Policy Statement 14**	**ISMF Standard 40 (Equipment site selection)** **ISMF Standard 45 (Secure disposal or re-use)** **ISMF Standard 46 (Removal of property)**
Responsible Parties	**Policy Statement 15**	**ISMF Standard 48 (Change management)** **ISMF Standard 50 (Separation of test, development and production environments)**
Procurement and Security	**Policy Statement 16**	**ISMF Standard 51 (Security in third party service delivery)**
Business Owners	**Policy Statement 17**	**ISMF Standard 53 (System acceptance)**
Responsible Parties	**Policy Statement 18**	**ISMF Standard 54 (Malware and virus prevention)** **ISMF Standard 141 (Endpoint protection)**
Responsible Parties	**Policy Statement 19**	**ISMF Standard 56 (Archives and backups)**
Responsible Parties	**Policy Statement 20**	**ISMF Standard 57 (Network security)** **ISMF Standard 58 (Network services)**
Business Owners	**Policy Statement 21**	**ISMF Standard 59 (Portable Storage Devices)** **ISMF Standard 60 (Sanitisation and/or disposal of media)**
Business Owners	**Policy Statement 22**	**ISMF Standard 64 (Media in transit)** **ISMF Standard 65 (Messaging and social networking)** **ISMF Standard 69 (E-commerce)**
Responsible Parties	**Policy Statement 23**	**ISMF Standard 73 (Administrator and operator logs)**

Functional domain	ISMF policy domain	ISMF Standards in support of corresponding policy
Responsible Parties	**Policy Statement 24**	**ISMF Standard 76 (Access Control)**
Responsible Parties	**Policy Statement 25**	**ISMF Standard 78 (Management of privileges)** **ISMF Standard 80 (User access review)**
Business Owners	**Policy Statement 26**	**ISMF Standard 81 (Password use obligations)**
Responsible Parties	**Policy Statement 27**	**ISMF Standard 88 (Configuration port protection)** **ISMF Standard 89 (Network segregation)**
Responsible Parties	**Policy Statement 28**	**ISMF Standard 93 (Secure Logon)** **ISMF Standard 94 (User identification and authentication)** **ISMF Standard 95 (Password management system)** **ISMF Standard 96 (Control of system tools and utilities)** **ISMF Standard 97 (Inactive sessions)**
Business Owners	**Policy Statement 29**	**ISMF Standard 99 (Legitimate need-to-access / need-to-know)**
Business Owners	**Policy Statement 30**	**ISMF Standard 101 (Mobile and portable storage devices)** **ISMF Standard 44 (Remote, portable and off premises devices)**
Procurement, Security and Responsible Parties	**Policy Statement 31**	**ISMF Standard 103 (Security in new or enhanced ICT systems)**
Business Owners	**Policy Statement 32**	The subordinate ISMF Standards must be applied to systems operating at I4 classification for integrity, and should be applied to I3 systems.
Responsible Parties	**Policy Statement 33**	**ISMF Standard 112 (Cryptographic key management)**
Responsible Parties	**Policy Statement 34**	**ISMF Standard 113 (Installation and deployment of software)**
Responsible Parties	**Policy Statement 35**	**ISMF Standard 116 (Change control in development and support)** **ISMF Standard 117 (Change review)** **ISMF Standard 143 (Secure development principles)**
Responsible Parties	**Policy Statement 36**	**ISMF Standard 121 (Vulnerability management)**
Business Owners	**Policy Statement 37**	**ISMF Standard 122 (Business continuity management)** **ISMF Standard 124 (Business continuity plans)** **ISMF Standard 126 (BCP review)**
Responsible Parties	**Policy Statement 38**	**ISMF Standard 127 (Legislative and regulatory requirements)** **ISMF Standard 128 (Intellectual property)**

Functional domain	ISMF policy domain	ISMF Standards in support of corresponding policy
		ISMF Standard 129 (Protection of government records) **ISMF Standard 130 (Privacy and confidentiality)**
Responsible Parties	**Policy Statement 39**	**ISMF Standard 134 (Technology compliance reviews)** **ISMF Standard 11 (Independent review)**
Business Owners	**Policy Statement 40**	**ISMF Standard 135 (Internal audits)**

Any other controls (incl. ISMF standards) should be accounted for if a given action is considered applicable and being undertaken within the scope of a project, activity or implementation, including service delivery activities.

Care should be taken to ensure that documentation is undertaken for those additional controls that require supporting documents (where indicated that documentation is a requirement).

Where documentation is not indicated as a requirement, *Undocumented Procedures* are those that are:

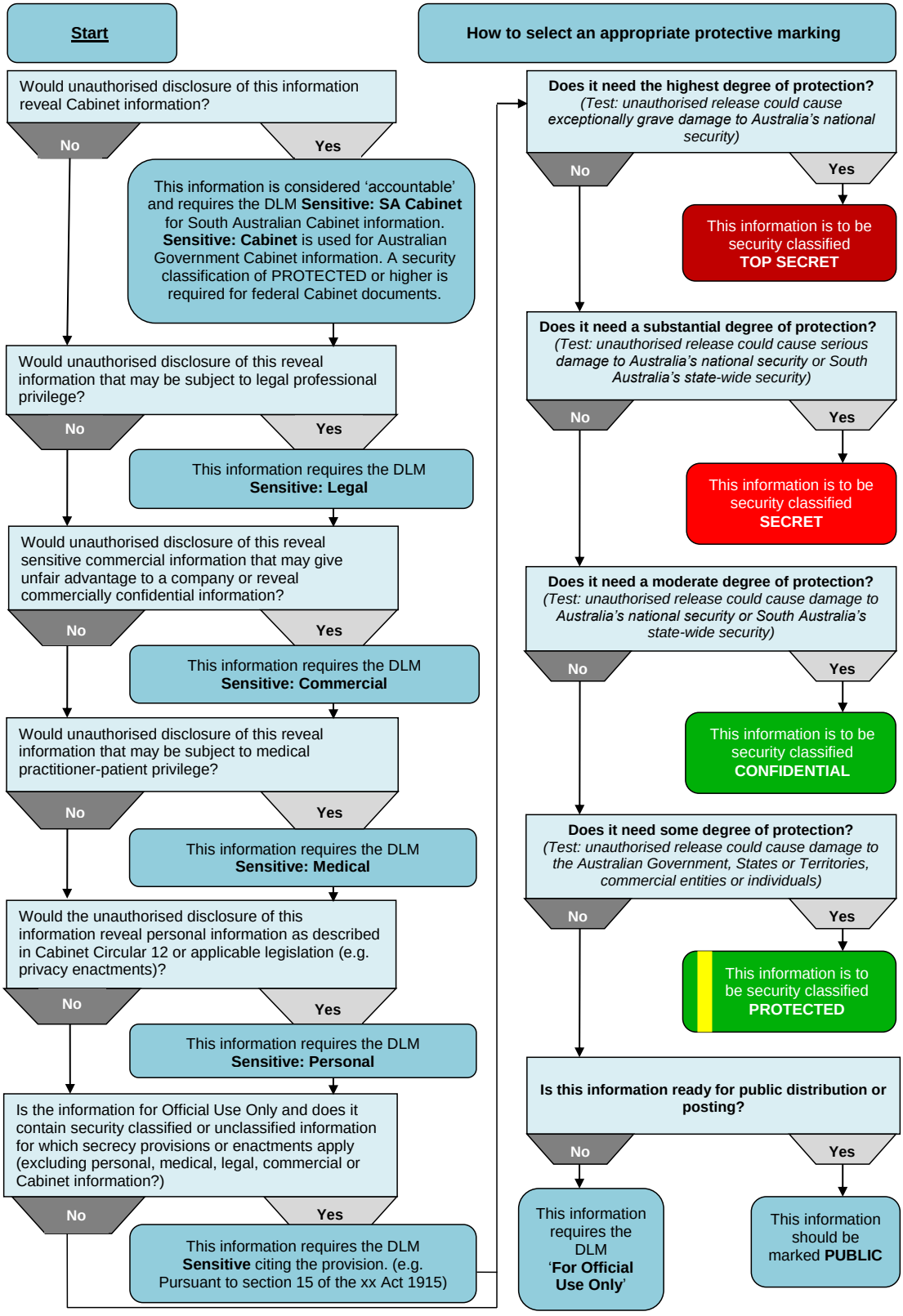
- Communicated
- Understood
- Applied
- Effective (i.e. demonstrable)

In such instances, the applicable Policy Statements from the ISMF may be recognised as a component of the ISMS for the Responsible Party. This shall not absolve the Responsible Party from the above guidance with respect to Undocumented Procedures.

Agencies are strongly encouraged to work collaboratively with their Internal Audit function to identify and remediate any gaps in applying ISMF Standards to Controls to their environments in fulfilling the objectives of the ISMF Policy Statements.

ANNEX B - SELECTING AN APPROPRIATE PROTECTIVE MARKING

Agency personnel should consider the questions posed in both columns to determine an appropriate DLM and/or protective marking for information and information assets.



**Test questions are for guidance purposes only*

*Modified for South Australian Government use and derived from an image attributed under Creative Commons version 3.0 license: Attorney-General's Department, Commonwealth of Australia. The MS-Word® version may be enlarged and edited.

THE REVISED AUSTRALIAN GOVERNMENT CONFIDENTIALITY CLASSIFICATION SCHEME

On 26 July 2011, the Australian Government announced a new confidentiality classification scheme which was subsequently approved by the Government of South Australia for use in ICT systems on 12 October 2011. Notably, the X-IN-CONFIDENCE, HIGHLY PROTECTED and RESTRICTED classifications have been retired and several 'dissemination limiting markers' were introduced. The following table is provided to assist Responsible Parties in mapping former classifications to the new scheme.

Former classifications defined by the Australian Government PSM	Revised scheme aligned to the Australian Government Protective Security Policy Framework [PSPF]
PUBLIC	**PUBLIC** Public information is now considered a dissemination limiting marker [DLM] by the Australian Government. In South Australia, public information may be used as a distinct classification or a DLM. Such information should still be accompanied by Integrity and Availability classifications representing its accuracy and availability requirements to the broader community. Consideration may be given to applying an open licensing arrangement in alignment with AusGOAL
[U] UNCLASSIFIED	**[U] UNCLASSIFIED** Unclassified information must make use of Dissemination Limiting Markers [DLMs]. The DLMSs that may be applied include: **For Official Use Only (FOUO**) may be used on unclassified information only, when its compromise may cause limited damage to government security, Australian government agencies including states and territories, commercial entities or members of the public. For example, an FOUO document might be a tender response. **Sensitive** official use only (SOUO) may be used with security classified or unclassified information: • where the secrecy provisions of enactments may apply, and/or • the disclosure of which may be limited or prohibited under legislation.
[IC] X-in-Confidence	**[U] UNCLASSIFIED** Dissemination Limiting Markers [DLMs] replace the former X-in-Confidence classification in totality. Corresponding DLMSs that may be applied include: **Sensitive: Personal** may be used with security classified or unclassified information that is sensitive personal information. (This aligns with the definition of **sensitive information** in Section 6 of the Australian Government Privacy Act and applicable State legislation and/or principles.)

Former classifications defined by the Australian Government PSM	Revised scheme aligned to the Australian Government Protective Security Policy Framework [PSPF]
	For example: a **Sensitive: Personal** document would protect information such as fact or opinion about an individual including their sexual preference, health status or political beliefs. **Sensitive: Legal** may be used for any information that may be subject to legal professional privilege. **Sensitive: Medical** is a DLM specifically implemented in South Australia and must be used for any information that may be subject to medical practitioner-patient privilege. This DLM must also be applied in place of **Sensitive: Personal** markings where secrecy provisions of healthcare enactments or other medical industry legislation may apply. **Sensitive: Commercial** is a DLM specifically implemented in South Australia to facilitate the rapid reassignment of existing COMMERCIAL-IN-CONFIDENCE classified materials. **Sensitive: SA Cabinet** is a DLM specifically implemented in South Australia to facilitate rapid reassignment of existing CABINET-IN-CONFIDENCE classified materials. It is considered the most sensitive of DLMs that does not require an accompanying protective marking (i.e. security classification).
[P] PROTECTED	**[P] PROTECTED**
[HP] HIGHLY PROTECTED[9]	The PROTECTED security classification is used when the compromise of the information could cause damage to the Australian Government including states and territories, commercial entities or members of the public. For instance, where compromise could: • endanger individuals and private entities • work substantially against national finances or economic and commercial interests • substantially undermine the financial viability of major organisations • impede the investigation or facilitate the commission of serious crime, or • seriously impede the development or operation of major government policies. **Sensitive: Cabinet** is a DLM to be applied to Australian Government (i.e. federal) cabinet information such as: • any document including but not limited to business lists, minutes, submissions, memoranda and matters without submission that is or has been:

[9] Certain elements of the former HIGHLY PROTECTED classification may require elevation to SECRET using the new scheme. The findings of an agency risk assessment including an impact assessment for compromise (loss, damage, theft etc.) of the information should determine if this measure is warranted. Information received by or held on behalf of the Australian Government must be treated as SECRET unless advised otherwise by the originating agency.

Former classifications defined by the Australian Government PSM	Revised scheme aligned to the Australian Government Protective Security Policy Framework [PSPF]
	— submitted or proposed to be submitted to Cabinet, or • official records of Cabinet • any other information that would reveal: — the deliberations or decisions of Cabinet, or — matters submitted, or proposed to be submitted to Cabinet. Any use of the DLM **'Sensitive: Cabinet'** is to be accompanied by a security classification protective marker of at least PROTECTED level.
[R] RESTRICTED	**[C] CONFIDENTIAL**
[C] CONFIDENTIAL	The CONFIDENTIAL security classification should be used when compromise of information could cause damage to national security. For instance, where compromise could: • damage diplomatic relations—in other words, cause formal protest or other sanction • damage the operational effectiveness or security of Australian or allied forces • damage the effectiveness of valuable security or intelligence operations • disrupt significant national infrastructure, or • damage the internal stability of Australia or other countries. Most national security information would be adequately protected by the procedures given to information marked CONFIDENTIAL or by agency specific procedures given to information marked **For Official Use Only**. The majority of RESTRICTED information will be marked '**For Official Use Only**' however such decisions will be made by the document originator in the Australian Government.
[S] SECRET	**[S] SECRET –** No material changes
[TS] TOP SECRET	**[TS] TOP SECRET –** No material changes

ANNEX C - GLOSSARY OF TERMS AND ACRONYMS

The following definitions shall be considered binding and final for the purposes of this framework unless otherwise noted:

Accreditation (Accredited)	Only certifying bodies that issue certifications to individuals and organisations can be Accredited (in order to issue certificates of conformity to individuals or organisations).
ACSI 33	A superseded designation for the Australian Government Information Security Manual [ISM]
Agency	South Australian Government public sector agencies (as defined in the *Public Sector Act 2009*), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Each Agency retains ultimate responsibility for all aspects covered by the Information Security Management Framework [ISMF] as it relates to a particular agency and its information assets.
Agency Critical Infrastructure [ACI]	Systems, Services, Functions, Platforms, Solutions and associated people, processes and technology which are fundamental to the ongoing functioning and survivability of an organisation. Certain ACI may also be critical to the State (refer SGCII).
anonymise	The process of removing all traces of personally identifiable information (such as names, addresses, phone numbers etc.) from a database or other electronic record. This process is typically irreversible.
AS/NZS	Australian Standard/New Zealand Standard
ASA	Agency Security Adviser as defined in the PSMF. The role is appointed by an Agency or organisation for the day-to-day performance of the protective security function.
ASE	Agency Security Executive, as defined in the PSMF. (see also CISO)
asset	Any tangible or intangible thing that has value to an organisation. (see also *information asset* which is the predominate term used in this framework).
Authorised Access	Access to, use of, copying of, or any form of communication with, the information/data owned by an Agency.
BCM	Business Continuity Management.
BCP	Business Continuity Planning.
Bulletin	A document issued by an administrative agency that announces news, policy and guidance. Three classes of Bulletin are possible in the context of the ISMF: ○ *Advisory*: Announcements and informational updates ○ *Alert*: Announcements pertaining to a potential event or series of events causing increased risk(s) to information security, but its occurrence, location or timing remains uncertain ○ *Warning*: Announcements pertaining to an event or series of events causing increased risks(s) to information security is occurring, imminent or extremely likely.

Business Impact Analysis [BIA]	A component of business continuity planning [BCP] that includes an exploratory component to reveal any vulnerability, and a planning component to develop strategies for minimising risk. The result of analysis is a business impact analysis report, which describes the potential risks specific to an organisation. A prime assumption within BIA is that every component of the organisation is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds and/or recovery effort in the wake of a disaster.
Business Owner	The person or group that is ultimately responsible for an information asset. This person or group is distinct from an information custodian, who may take responsibility for the ongoing management of the information (such as a CIO or system administrator). Individual business units own business critical information, rather than information technology or information security departments (they are custodians, not owners). The manager of the business unit responsible for the creation of any information and / or the business unit directly impacted by the loss of the information is usually the Business Owner. For the purpose of ISO 27001 certification, the 'risk owner' is synonymous with the term Business Owner contained in this framework. (e.g. The party most impacted by the loss of confidentiality, integrity or availability of Information is *typically* the Business Owner.)
Caveat	A caveat is a warning that the information has special requirements in addition to those indicated by the DLM or protective marking. Caveats are not classifications in their own right and are not to appear without the appropriate DLM or protective marking. For full details on the usage of caveats, refer to section 9 and table 4 in the ISMF.
C-level	Executive level management
CE	Chief Executive (of an Agency)
Certification	The process by which an Accredited certifying body issues a certificate of conformance to a given Standard to an individual or organisation.
CISO	A defined executive-level role of *Chief Information Security Officer* as described in the ISM. The CISO of an Agency is responsible for coordinating communication between security and business functions as well as overseeing the application of information security controls and security risk management processes within the Agency. The South Australian Government (State) CISO role is located in the Cyber Security and Risk Assurance Group of the Department of the Premier and Cabinet.
classification	The process by which information and/or information assets are labelled according to their business importance and sensitivity. Classification markings are used to indicate the value of the information and that security controls shall apply to it according to its classification level. Such levels govern the protection requirements for this information and/or assets during use, storage, transmission, transfer and disposal.
COBIT	*Control Objectives for Information and related Technology*, which is a set of resources issued by the *IT Governance Institute*. COBIT contains "information for organisations wishing to adopt an IT governance and control framework". Its purpose is to "help optimise IT-enabled investments and assure that IT is used successfully in delivering business requirements"

Control Objectives and Controls	Defined in AS/NZS ISO/IEC 27001*; i.e. "Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security."*
cryptographic information	Information relating to keying material and cryptosystems approved for the protection of information.
Custody (of an asset)	The responsibility for the care of records, archives or other material, usually based on their physical possession. Custody does not always include legal ownership, or the right to control access to records.
cyber security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means. (synonymous with ICT Security)
de-identify	The process of removing personally identifiable information (such as names, addresses, telephone numbers etc.) from a record or dataset. This process is typically reversible by way of re-identifying the record or dataset.
Determination	A position or opinion or judgement reached after consideration of a specific set of facts.
Dissemination Limiting Marker [DLM]	Dissemination limiting markers [DLMs] are markings for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling. The following seven categories of DLM are used: - For Official Use Only - Sensitive - Sensitive: Personal - Sensitive: Medical - Sensitive: Commercial - Sensitive: Legal - Sensitive: SA Cabinet, and - Sensitive: Cabinet.
dual phase login (password control)	As distinct from two factor authentication, dual phase login generally consists of two login stages such as an assigned password or PIN and something the user has assigned or customised. Typical examples would include a remote access client or VPN login to access network resources followed by a system login to gain access to a particular application; or in the case of online banking when a hardware token or physical card has not been provided, it may consist of a user login followed by an image or second security question that has been established by the user.
encryption	A process, which may be irreversible, of transforming information, particularly data, into an unintelligible form.
Endpoint	Any device that is the final interface at the edge of a network and directly used, managed or accessed by a person or persons. These devices may include desktop PCs, laptops, tablets, smartphones, point of sale terminals, thin-client terminals, etc. Sometimes referred to as a 'Human Interface Device' (albeit incorrectly as this may include hardware such as keyboards).

Endpoint Protection	Security measures implemented for user-accessible devices at the edge of a network that may contain, or provide access to, information for an end user. (i.e. the device is readily physically accessible to a user)
EOI	"*Expression of Interest*"
Exemption (ICT Security)	South Australian Government terminology that equates to the term "waiver" in the Australian Government PSM. For the purpose of the SA Government ISMF: *Approval for exclusion from the implementation or use of a mandated whole-of-Government ICT Contract, Standard, Policy, Guideline and/or Notification*. Exemptions shall only be issued in adherence to the provisions described in section 5.8 of the PSMF.
External Organisation	Any organisation that is not a business unit, directorate, branch or other wholly controlled and administered component of the Responsible Party. (also referred to as a Third Party organisation)
framework	A basic conceptual structure used to solve or address complex issues.
Framework	This document: the South Australian Government *Information Security Management Framework*
Goal	A statement defining a desired end-state or result.
governance	The exercising of authority or decision-making processes. Governance may be further described as: *the decision-making processes that define expectations, grant power, or verify performance. It consists either of a separate process or of a specific part of management or leadership processes.*
Guideline	A statement of desired, good or best practice.
Hosting Facility	A facility that is designated for the purpose of housing ICT equipment including the power, cooling, fire, and security systems supporting such equipment. For the purposes of the ISMF, this term is synonymous with *Data Centre*, *Computer Room* and *Information Processing Facilities* when used by the ISO 27002 standard in such context.
ICT	Information and Communication Technology
ICT asset	An information asset that electronically stores, processes or communicates information, including information for which the SA Government (or any of its Responsible Parties) is custodian. Anything that acts upon the ICT asset, including creating, controlling, validating, and otherwise managing the ICT asset throughout the lifecycle of the asset.
ICT Security	See 'cyber security'
incident	Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service and/or the loss or corruption of information resulting in a breach of privacy or security.
information asset	Anything that processes, stores or communicates information of value to the Agency or organisation. Information assets in the South Australian Government are commonly referenced as holistic systems, for example: TRUMPS, LOTS, EMS, Masterpiece etc. This definition is distinct from

	the definition used by the ISO 27000 series standards as the ISMF relates specifically to cyber security. Information assets must have a nominated Business Owner. (see Policy Statement 7)
Information Processing Facilities	Per the AS/NZS ISO/IEC 27002:2006 standard: "*any information processing system, service or infrastructure, or the physical locations housing them*"
information security	Preservation of confidentiality, integrity and availability of information. Additional attributes such as authenticity, accountability, non-repudiation and reliability may also be incorporated.
Information Security Awareness Program(s)	A security awareness program catering to all personnel involved in using and managing ICT resources and designed to help them: ○ Understand their roles and responsibilities related to the organisational mission; ○ Understand the organisation's information security policies, procedures, and practices; and ○ Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the information assets for which they are responsible. The ISMF describes a number of controls which must be included in such programs.
ISM	Australian Government, *Information Security Manual* (formerly designated ACSI 33). The ISMF refers a specific edition of this manual as defined in the pre-requisite documents section. The latest version of ISM is required when handling or dealing with National Security matters and is available from the www.asd.gov.au website.
ISMF	South Australian Government *Information Security Management Framework* ("this document")
ISMF version	Version numbering for the ISMF uses the following sequence: <*major*>.<*minor*>.<*release*> such as ISMF v3.1.1 Major versions are generally approved by Cabinet. Minor revisions are approved through DPC. Release numbers are used to indicate that an existing version of the framework has been released with updated hyperlinks, cosmetic changes and corrections or updated international standard references but do not contain any material changes, additions or removal affecting policies, standards or controls versus the preceding release.
ISMS	An *Information Security Management System* consists of a set of policies, standards, implementation guidelines and procedures for Information Security Management.
ISO/IEC	International Standards Organisation /International Electrotechnical Commission
ITSA	Information Technology Security Adviser is a Position of Trust as defined in the PSMF. This role is appointed by an Agency or organisation to manage the security of information and ICT systems. ISMF Guideline 4b provides information about this role, including guidance on the selection of suitable persons to fill the role.

LAN	Local Area Network (a.k.a. Ethernet or premises/campus network)
Legal Professional Privilege	Legal Professional Privilege is a right at law that protects the confidentiality of communications between a lawyer and client. It is a common law right with specific references pursuant to the Evidence Act (SA) and equivalent Commonwealth and State legislation (as applicable and as modified from time to time). The privilege may normally only be waived by the lawyer's client.
Limiting Marker	Synonymous short form expression for 'Dissemination Limiting Marker' (a.k.a. DLM)
MAN	Metropolitan Area Network (a.k.a. Metro Access Network)
Mobility Device	A portable communications device with embedded information processing (i.e. computing) and communications capabilities. Examples include: laptops, netbooks, smart cards, mobile phones and PDAs. Almost all Mobility Devices are a form of *Portable Storage Device* that contain additional networking and/or communications capabilities, adding an extra dimension of risks that need to be considered.
Non-repudiation	For the intent and purpose of the ISMF, ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement, action or contract. In digital (electronic) transactions, such capabilities ensure: • a service that provides proof of the integrity and origin of data; • an authentication that with high assurance can be asserted to be genuine, to prove that an "event, statement, action or agreement" has transpired. Non-repudiation may be used for legal recourse in electronic business. It is commonly used for digital signatures and electronic signing of agreements.
Notifiable Incident	Notifiable Incidents include, but are not limited to, disruptive events, misconduct, or criminal activity that has occurred, or is likely to occur, resulting in: ○ an adverse impact to the trust and confidence in the government's ICT services; ○ a disruption to Critical ICT that exceeds, or is likely to exceed the recovery time object; ○ a breach of the State's Information Privacy Principles as described in Cabinet Circular No. 12 issued by the Department of Premier and Cabinet. ○ recovery that will, or is likely to, unacceptably exceed recovery time objectives; ○ the belief that, if notified, the CIO will activate the ICT Support Plan; ○ the belief by an Agency or Supplier that a coordinated approach for its resolution is required.
Notification	The official documentation of a Ruling or Determination, for distribution to a community of interest or affected party.
OECD	Organisation for Economic Co-operation and Development

Objective	An aim or intended result of a strategy
Official Information	A term (initially defined by the PSM) as "*any information developed, received or collected by, or on behalf of, the Government, through its agencies and contracted providers*".
periodic (periodically)	An event or action that must occur at prescribed intervals (typically by means of a Standard Operating Procedure, Security Schedule or as part of an Audit calendar) but shall not exceed a period of twelve (12) calendar months.
Policy	A statement of principles and/or values that mandate or constrain the performance of activities used in achieving institutional goals.
Portable Electronic Device	A term defined by the Australian Government ISM and, for the purposes of the ISMF, can be treated as synonymous with a Portable Storage Device [PSD].
Portable Storage Device [PSD]	A term defined by the Australian Government Office of the Privacy Commissioner as a small, lightweight, portable, easy to use device, which is capable of storing and transferring large volumes of data. Common PSDs include portable external hard drives, CDs/DVDs, USB keys, laptops/ notebooks, personal digital assistants (such as Pocket PC, Palm, BlackBerry), and devices with in-built accessible storage (such as MP3 players, iPods, and mobile phones). See also *Mobility Device*.
Position of Trust	A position whose duties involve access to non-national security information to the level of [P] PROTECTED and above classifications or trusted access to significant resources (such as SGCII assets)
Principal Officer	"Principal Officer" means in relation to a Responsible Party: (a) the person holding, or performing duties of, the Office of Chief Executive Officer of the Responsible Party; (b) if the Commissioner for Public Employment declares an office to be the principal office in respect of the agency - the person holding, or performing the duties of, that office; or (c) in any other case - the person who constitutes that Responsible Party or, if the Responsible Party is constituted by two or more persons, the person who is entitled to preside at any meeting of the Responsible Party at which the person is present.
PSM	Australian Government *Protective Security Manual*
PSMF	Department of Premier and Cabinet [DPC] Circular No. 30, entitled *Protective Security Management Framework*.
regular (regularly)	An event or action that should occur at consistent intervals and is typically determined by Standard Operating Procedures or a Security Schedule. The nature of the timeframes and intervals involved should be determined by the Responsible Party in accordance with its risk assessments and policies. For example, regularly updating virus definitions for software would typically occur more frequently than the publication of security bulletins and notifications. Regular events are typically 'event-driven' rather than prescribed. A regular event may include when a significant change occurs.

Removable Media	A term used by the AS/NZS ISO/IEC 27002:2006 standard encompassing tapes, disks, flash disks, removable hard drives, CDs, DVDs and printed media.
residual risk	The remaining level of risk after risk treatment(s) has (have) been undertaken.
Responsible Parties	A term that defines both Agencies and Suppliers who are subject to contractual conditions that require them to comply with the ISMF. Where any ambiguity arises between these entities in relation to adherence to the ISMF, the Agency Controls implemented in the Customer Agreement shall prevail (i.e. The Agency remains the default party and the Customer Agreement is used as the vehicle for setting the scope and requirements for the Supplier to comply with either the entirety of the ISMF or part(s) thereof. The Customer Agreement may also introduce additional Agency-specific controls and policies that the Supplier must comply with).
Responsible Party	A two-context phrase used to address the primary audience of the ISMF, namely: an Agency; or Suppliers who are subject to contractual conditions that require them to comply with the ISMF. When a Supplier has contracted with the State, the provisions of the ISMF will apply to the Supplier either: o under the terms of a Purchasing Agreement for whole of Government contracts and associated Customer Agreements; or o by way of an individual contract with an Agency whereby the Agency has specified the parts of its Information Security Management System (ISMS) for which compliance is sought. It should be noted that Agency Chief Executives retain ultimate accountability for all security matters within their agencies. The application of the ISMF to a Supplier via a contract with the State or Agency shall not absolve the Agency from these obligations and responsibilities.
Risk Profile	An outline of the risks to which an organisation, or business unit within an organisation, is exposed. Most Risk Profiles identify specific risks, associated mitigation strategies and an overall assessment or grading of each risk.
RFI	"*Request for Information*"
RFID	Radio Frequency Identification
Ruling	An official interpretive statement of general applicability issued and published by a recognised authority.
SA	South Australia/South Australian (contextual)
sanitisation	The process of removing certain elements of information that will allow the protective marking that indicates the level of protection required for security classified information to be removed or reduced.
Sensitive [SOUO]	The '**Sensitive**' dissemination limiting marker is considered as applicable to 'Sensitive Official Use Only' content where certain secrecy provisions or enactments limit information dissemination/sharing. It is distinct from other predefined 'Sensitive' DLMs such as **Sensitive: SA**

	Cabinet, **Sensitive: Medical**, **Sensitive: Personal** etc. which are used in specific circumstances and/or for legislative requirements. In South Australia, a SOUO document might be a document which is exempt from disclosure under the FOI Act (SA) or equivalent legislation or information which is confidential under the Whistleblowers Protection Act (SA) or equivalent legislation. When SOUO applies, agencies are required to apply the Sensitive DLM in the header and footer as well as identify the reason the DLM has been applied and any special handling requirements either in the footer or as a cover page. For example: *'This information is subject to the provisions of Section 56 of the Australian Prudential Regulation Authority Act 1998 and may only be accessed by APRA officers.'*
Sensitive: Legal	The '**Sensitive: Legal**' DLM is to be applied to unclassified or classified information that is provided legal professional privilege (held or generated by the South Australian Government). Refer to definition of 'Legal Professional Privilege' in the ISMF.
Sensitive: Personal	Personal information that is required to be protected under the provisions of Premier and Cabinet Circular No. 12, the *Freedom of Information Act 1991* or other legislation. This encompasses **sensitive information** as defined in Section 6 of the Australian Government Privacy Act and applicable State legislation and/or principles. For example: a **Sensitive: Personal** document would protect information such as fact or opinion about an individual including their sexual preference, health status or political beliefs.
Sensitive: Medical	A DLM specifically implemented in South Australia that must be used for any information that may be subject to medical practitioner-patient privilege. This DLM must also be applied in place of **Sensitive: Personal** markings where secrecy provisions of healthcare enactments or other medical industry legislation may apply.
SOA	Statement of Applicability
SOW	Statement of Work (Scope of Works)
State Government Critical Information Infrastructure [SGCII]	State Government Critical ICT Infrastructure upon which '*Critical Services'* are delivered to the community. If the confidentiality, integrity or availability of this ICT infrastructure is compromised then it could significantly impact on the social or economic well-being of the State, the government, commercial entities or members of the public. (*refer* ISMF Guideline 37a)
Statement of Applicability	As defined in AS/NZS ISO/IEC 27001; i.e. "*documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS*".
StateNet	The enterprise communications network that is centrally operated and managed on behalf of SA Government Agencies.
Standard	A formal document that establishes uniform criteria, methods, protocols, processes and practices to meet policy requirements.
Strategy	A long-term plan of action designed to achieve a particular goal.

Supplier (Contracted Provider)	An external to government entity that is typically responsible for compliance with the ISMF by way of a contractual agreement that contains clauses requiring security of Agency information and the regulation of access to an Agency's information assets. The term "Supplier" shall be read as "*Suppliers who are subject to contractual conditions that require them to comply with the ISMF*" unless another intention is apparent.
Trust Domain	A term defined by the StateNet Conditions of Connection as: '*a securely interconnected set of networks, computers and applications that are subject to the same security policies*'.
Two factor authentication	A method of authentication using two separate mutually dependent credentials, typically "something you have" and "something you know". Common two factor authentication systems employ a one-time password (OTP). A common example is in online banking environments where the user has been assigned a hardware token or plastic reference card in addition to using their password to access the system.
Unclassified	Government information that is not 'Security Classified' is considered 'unclassified'. Unclassified information requires the use of a DLM to indicate how it is to be handled and managed from a security perspective. Conversely, security classified information requires associated personnel to have a vetting (i.e. security clearance) to the corresponding classification of the information they need to access or manage. Where the ISMF references controls from the *Australian Government Information Security Manual*, the corresponding notation for unclassified information is [G] which is the short-hand notation for general government information.
Undocumented Procedure	A procedure or technique that is: ○ Communicated ○ Understood ○ Applied ○ Effective (i.e. demonstrable)
User	Anything, including persons and computer systems that access ICT resources.
vetting	Verification and assessment action(s) to develop a realistic and informed evaluation of a person's suitability for security clearance of a specified level and type
waiver	See *Exemption*
WAN	Wide Area Network, sometimes referred to as long haul or regional network.
X-in-Confidence	A former non-national security protective marking (now superseded by DLMs and caveats) that indicates compromise of Official Information could cause limited damage to the State, the Government, commercial entities or members of the public. Typical examples include: *Commercial-in-Confidence* *Security-in-Confidence* *Staff-in-Confidence* *Government-in-Confidence*

Agency-in-Confidence

It should be noted that *Cabinet-in-Confidence* materials vary significantly in their handling and treatment on the basis of security and sensitivity of the content. Early draft documents may be treated with equivalent handling as ***Sensitive*** materials while other more sensitive or confidential topics may be treated as [P] PROTECTED documents as soon as drafting commences. Cabinet-level documents should not be confused with other [IC] In-Confidence materials. South Australian Government Cabinet documents are now identified with the ***Sensitive: SA Cabinet*** dissemination limiting marker when ready for consideration by Cabinet.

ANNEX D - INDEX OF ISMF POLICIES

ANNEX E - INDEX OF ISMF STANDARDS

ANNEX F - MAPPING TO AUSTRALIAN AND INTERNATIONAL STANDARDS

The following table provides a simplified mapping of International, South Australian and Australian Commonwealth legislation, policies, controls and standards as well as listing complementary standards and measures implemented in this framework.

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
Policy Statement 1				**Section 4-8**	**Section 4-10**	ISMF Guideline 1a ISMF Guideline 1b ISM
Policy Statement 2	s5.1 PSMF			**Section 4-8**	**Section 4-10**	ISMF Guideline 2
ISMF Standard 1				*Section 4 (ISO 27002)*	**Section 6**	ISO/IEC 27005 AS/NZS ISO 31000 PSM Part B, s2
ISMF Standard 137	Cabinet Circular 30 Treasurer's Instr. 2			*Refer Other*		
Policy Statement 3				**A.5.1**	**A.5.1**	ISMF Guideline 3
ISMF Standard 2		ISM		A.5.1.1	A.5.1.1	
ISMF Standard 3				A.5.1.2	A.5.1.2	
Policy Statement 4				**A.6.1**	**Section 6**	ISMF Guideline 4a ISMF Guideline 4b
ISMF Standard 4				A.6.1.1	**Section 6**	
ISMF Standard 5				A.6.1.2	(retired)	
ISMF Standard 6		ISM	Governance section	A.6.1.3	A.6.1.1	
ISMF Standard 49				A.10.1.3	A.6.1.2	

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 7				A.6.1.4	(retired)	
ISMF Standard 9				A.6.1.6	A.6.1.3	
ISMF Standard 10				A.6.1.7	A.6.1.4	
ISMF Standard 142				n/a	A.6.1.5	
Policy Statement 5				**A.6.2**	**A.15.1**	ISMF Guideline 5
ISMF Standard 12	s5.1 PSMF			A.6.2.1	A.15.1.1	StateNet Conditions of Connection ISF TPSAT
ISMF Standard 13		ISM	Part A paragraph 1.9	A.6.2.2	(retired)	PSM part A paragraph 1.9
ISMF Standard 14		ISM	Personnel Security Protocol	A.6.2.3	A.15.1.1 A.15.1.2 A.15.1.3	
Policy Statement 6				n/a	n/a	ISMF Guideline 6
ISMF Standard 15		ISM	Personnel Security Protocol	n/a	n/a	PSM part A paragraph 1.8
ISMF Standard 139	*Freedom of Information Act 1991*			n/a	A.15.1.3	ISMF Ruling 2
Policy Statement 7				**A.7.1**	**A.8.1**	ISMF Guideline 7
ISMF Standard 16				A.7.1.1	A.8.1.1	
ISMF Standard 17				A.7.1.2	A.8.1.2	
Policy Statement 8				**A.7.2**	**A.8.2**	ISMF Guideline 8a ISMF Guideline 8b
ISMF Standard 19	s5.2 PSMF Cabinet Circular 12 *Freedom of Information Act 1991* *State Records Act 1997*	ISM		A.7.2.1	A.8.2.1 A.17.2.1	Clause 6.6.2 of the AS ISO/IEC 20000.2 standard Australian Government Information Security Management Guidelines

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 20			PSPF s6.2	A.7.2.2	A.8.2.2 A.8.2.3	
ISMF Standard 70				A.10.9.3	(retired)	
Policy Statement 9				**A.8.1**	**A.7.1**	ISMF Guideline 9
ISMF Standard 21	c.4 of the PSMF			A.8.1.1	(retired)	
ISMF Standard 22		ISM	PSPF s6.1	A.8.1.2	A.7.1.1	PSPF Security clearance subjects guidelines
ISMF Standard 23	*Public Sector Act 2009*		PSPF s6.1	A.8.1.3	A.7.1.2	
Policy Statement 10				**A.8.2**	**A.7.2**	
ISMF Standard 24				A.8.2.1	A.7.2.1	
ISMF Standard 8	*Public Sector Act 2009*			A.6.1.5	A.13.2.4	
ISMF Standard 25		ISM		A.8.2.2	A.7.2.2	
ISMF Standard 26	Commissioner's Standard No 1 - A Planned Workforce			A.8.2.3	A.7.2.3	
Policy Statement 11				**A.8.3**	**A.7.3**	ISMF Guideline 11
ISMF Standard 27				A.8.3.1	A.7.3.1	
ISMF Standard 28		media sanitisation section (ISM)		A.8.3.2	A.8.1.4	
ISMF Standard 29				A.8.3.3	A.9.2.6	
Policy Statement 12				**A.13.1** **A.13.2**	**A.16.1**	ISMF Guideline 12a
ISMF Standard 30		cyber security incidents section (ISM)	PSPF s6.2	A.13.1.1	A.16.1.2	
ISMF Standard 140				n/a	A.16.1.4	
ISMF Standard 31				A.13.1.2	A.16.1.3	

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 32		cyber security incidents section (ISM)		A.13.2.1	A.16.1.1 A.16.1.5	
ISMF Standard 33				A.13.2.2	A.16.1.6	
ISMF Standard 34	*Evidence Act (1929)* Part 6A Cabinet Circular 12			A.13.2.3	A.16.1.7	
Policy Statement 13	s5.4 of the PSMF	ISM Physical security chapter		**A.9.1**	**A.11.1**	
ISMF Standard 35		ISM Physical security chapter		A.9.1.1	A.11.1.1	
ISMF Standard 36				A.9.1.2	A.11.1.2	
ISMF Standard 37				A.9.1.3 A.9.1.4	A.11.1.3 A.11.1.4	
ISMF Standard 38				A.9.1.5	A.11.1.5	
ISMF Standard 39				A.9.1.6	A.11.1.6	
Policy Statement 14				**A.9.2**	**A.11.2**	
ISMF Standard 40				A.9.2.1	A.11.2.1	
ISMF Standard 41				A.9.2.2	A.11.2.2	
ISMF Standard 42				A.9.2.3	A.11.2.3	
ISMF Standard 43				A.9.2.4	A.11.2.4	
ISMF Standard 45		ISM		A.9.2.6	A.11.2.7	
ISMF Standard 46				A.9.2.7	A.11.2.5	
Policy Statement 15				**A.10.1**	**A.12.1**	
ISMF Standard 47				A.10.1.1	A.12.1.1	
ISMF Standard 48		ISM		A.10.1.2	A.12.1.2	
ISMF Standard 50				A.10.1.4	A.12.1.4	
Policy Statement 16				**A.10.2**	**A.15.2**	Covered by ISMF Guideline 39

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 51				A.10.2.1 A.10.2.2 A.10.2.3	(retired) A.15.2.1 A.15.2.2	
Policy Statement 17				**A.10.3**		
ISMF Standard 52				A.10.3.1	A.12.1.3	
ISMF Standard 53				A.10.3.2	A.14.2.8 A.14.2.9	
Policy Statement 18				**A.10.4**	**A.12.2**	ISMF Guideline 18
ISMF Standard 54				A.10.4.1	A.12.2.1	
ISMF Standard 55				A.10.4.2	(retired)	
ISMF Standard 141				*Refer Other*		
Policy Statement 19				**A.10.5**	**A.12.3**	
ISMF Standard 56		ISM		A.10.5.1	A.12.3.1	
Policy Statement 20				**A.10.6**	**A.13.1**	
ISMF Standard 57	StateNet Conditions of Connection			A.10.6.1	A.13.1.1	
ISMF Standard 58	StateNet Conditions of Connection			A.10.6.2	A.13.1.2	
Policy Statement 21				**A.10.7**	**A.8.3**	ISMF Guideline 21
ISMF Standard 59		ISM ISM ISM ISM		A.10.7.1	A.8.3.1	
ISMF Standard 60	*section 23(1) of the State Records Act 1997*	ISM		A.10.7.2	A.8.3.2	
ISMF Standard 61	Code of Ethics			A.10.7.3	A.8.2.3	
ISMF Standard 62				A.10.7.4	(retired)	
Policy Statement 22				**A.10.8**	**A.13.2**	
ISMF Standard 63				A.10.8.1 A.10.8.2	A.13.2.1 A.13.2.2	

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 64				A.10.8.3	A.8.3.3	
ISMF Standard 65				A.10.8.4	A.13.2.3	Social Media – Guidance for Agencies and Staff
ISMF Standard 66	*State Records Act 1997*			*Refer Other*		State Records Guideline: Management of Emails as Official Records
ISMF Standard 67				A.10.8.5	(retired)	
ISMF Standard 68				*Refer Other*		Social Media – Guidance for Agencies and Staff AS/NZS ISO/IEC 17799 clause 8.7.7
Policy Statement 22				**A.10.9**	**A.14.1**	
ISMF Standard 69				A.10.9.1 A.10.9.2	A.14.1.2 A.14.1.3	PCI DSS
Policy Statement 23				**A.10.10**	**A.12.4**	ISMF Guideline 23
ISMF Standard 71		ISM		A.10.10.1 A.10.10.2	A.12.4.1	
ISMF Standard 72				A.10.10.3	A.12.4.2	
ISMF Standard 73				A.10.10.4	A.12.4.3	
ISMF Standard 74				A.10.10.5	(retired)	
ISMF Standard 75				A.10.10.6	A.12.4.4	
Policy Statement 24				**A.11.1**	**A.9.1**	
ISMF Standard 76	StateNet Conditions of Connection			A.11.1.1	A.9.1.1	
Policy Statement 25				**A.11.2**	**A.9.2**	ISMF Guideline 25
ISMF Standard 77				A.11.2.1	A.9.2.1	
ISMF Standard 78				A.11.2.2	A.9.2.3 A12.6.2	
ISMF Standard 79				A.11.2.3	A.9.2.4	

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 80				A.11.2.4	A.9.2.5	
Policy Statement 26				**A.11.3**	**A.9.3**	
ISMF Standard 81				A.11.3.1	A.9.3.1	
ISMF Standard 82				A.11.3.2	A.11.2.8	
ISMF Standard 83				A.11.3.3	A.11.2.9	
Policy Statement 27				**A.11.4**		ISMF Guideline 27
ISMF Standard 84				A.11.4.1	A.9.1.2	
ISMF Standard 85				*Refer ISM and Other*		AS/NZS ISO/IEC 17799
ISMF Standard 86	StateNet Conditions of Connection			A.11.4.2	(retired)	
ISMF Standard 87				A.11.4.3	(retired)	
ISMF Standard 88				A.11.4.4	(retired)	
ISMF Standard 89	StateNet Conditions of Connection			A.11.4.5	A.13.1.3	
ISMF Standard 90				A.11.4.6	(retired)	
ISMF Standard 91				A.11.4.7	(retired)	
Policy Statement 28				**A.11.5**	**A.9.4**	
ISMF Standard 92				*Government Only*		
ISMF Standard 93				A.11.5.1	A.9.4.2	
ISMF Standard 94				A.11.5.2	(retired)	
ISMF Standard 95				A.11.5.3	A.9.4.3	
ISMF Standard 96				A.11.5.4	A.9.4.4	
ISMF Standard 97				A.11.5.5	(retired)	
ISMF Standard 98				A.11.5.6	(retired)	
Policy Statement 29				**A.11.6**	**A.9.4**	Covered by ISMF Guideline 28
ISMF Standard 99				A.11.6.1	A.9.4.1	
ISMF Standard 100				A.11.6.2	(retired)	

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
Policy Statement 30				**A.11.7**	**A.6.2**	ISMF Guideline 30a ISMF Guideline 30b
ISMF Standard 101				A.11.7.1	A.6.2.1	
ISMF Standard 102				A.11.7.2	A.6.2.2	
ISMF Standard 44				A.9.2.5	A.11.2.6	
Policy Statement 31				**A.12.1**	**A.14.1**	
ISMF Standard 103				A.12.1.1	A.14.1.1	
Policy Statement 32				**A.12.2**		
ISMF Standard 104				A.12.2.1	(retired)	
ISMF Standard 105				A.12.2.2	(retired)	
ISMF Standard 106				A.12.2.3	(retired)	
ISMF Standard 107				A.12.2.4	(retired)	
Policy Statement 33				**A.12.3**	**A.10.1**	ISMF Guideline 33
ISMF Standard 108				A.12.3.1	A.10.1.1	
ISMF Standard 109				*Refer ISM*		
ISMF Standard 110				*Refer ISM*		
ISMF Standard 111				*Refer Other*		ISO 13888-1 AS/NZS ISO/IEC 17799
ISMF Standard 112				A.12.3.2	A.10.1.2	
Policy Statement 34				**A.12.4**		
ISMF Standard 113				A.12.4.1	A.12.5.1	
ISMF Standard 114				A.12.4.2	A.14.3.1	
ISMF Standard 115				A.12.4.3	A.9.4.5	
Policy Statement 35				**A.12.5**	**A.14.2**	
ISMF Standard 116				A.12.5.1	A.14.2.2	AS/NZS ISO/IEC 10007

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
						AS/NZS ISO/IEC 12207
ISMF Standard 117				A.12.5.2	A.14.2.3	
ISMF Standard 118				A.12.5.3	A.14.2.4	
ISMF Standard 119				A.12.5.4	(retired)	
ISMF Standard 120				A.12.5.5	A.14.2.7	
ISMF Standard 143	Secure Web Apps Secure Web Servers			n/a	A.14.2.1 A.14.2.5 A.14.2.6	
Policy Statement 36				**A.12.6**	**A.12.6**	
ISMF Standard 121				A.12.6.1	A.12.6.1	AS/NZS ISO/IEC 10007 AS/NZS ISO/IEC 12207
Policy Statement 37				**A.14.1**	**A17.1**	ISMF Guideline 37a
ISMF Standard 122				A.14.1.1	(retired)	
ISMF Standard 123				A.14.1.2	A.17.1.1 A.17.1.2 A.17.1.3	
ISMF Standard 124				A.14.1.3	(retired)	
ISMF Standard 125				A.14.1.4	(retired)	
ISMF Standard 126				A.14.1.5	A.17.1.3	ISO/IEC 27031 ISO 22301 ISO/IEC 24762
Policy Statement 38				**A.15.1**	**A.18.1**	ISMF Guideline 38
ISMF Standard 127			PSM Part A Section 5	A.15.1.1	A.18.1.1	*Section 109 of the Australian Constitution*
ISMF Standard 128	Intellectual Property Policy			A.15.1.2	A.18.1.2	
ISMF Standard 129				A.15.1.3	A.18.1.3	

SOUTH AUSTRALIAN GOVERNMENT		AUSTRALIAN GOVERNMENT		INTERNATIONAL ISO 27001		IMPLEMENTATION GUIDANCE
ISMF Policy Statements and Standards	*Other SA policy, standards and legislation*	*Information Security Manual controls*	*Protective Security Policy Framework (PSPF)*	*ISO 27001:2006 Control Objectives & Controls*	*ISO 27001:2013 Control Objectives & Controls*	*Miscellaneous supporting standards & guidelines and information sheets*
ISMF Standard 130	Cabinet Circular 12 *Freedom of Information Act 1991*			A.15.1.4	A.18.1.4	Privacy Guidelines for SA Government websites
ISMF Standard 131				A.7.1.3 A.15.1.5	A.8.1.3	
ISMF Standard 132				A.15.1.6	A.18.1.5	
Policy Statement 39				**A.15.2**	**A.18.2**	ISMF Guideline 39
ISMF Standard 133				A.15.2.1	A.18.2.1	(PSPF guideline) 'Agency Security Adviser and IT Security Adviser functions and competencies'
ISMF Standard 134				A.15.2.2	A.18.2.2	
ISMF Standard 11				A.6.1.8	A.18.2.1	
Policy Statement 40				**A.15.3**	**A.12.7**	
ISMF Standard 135				A.15.3.1	A.12.7.1	
ISMF Standard 136				A.15.3.2	(retired)	

ANNEX G – RETIRED CONTROL OBJECTIVES IN ISO/IEC 27001:2013

The following control objectives were removed from the ISO 27001:2013 standard publication, and the corresponding ISO 27002:2013 code of practice. Consequently, Responsible Parties seeking to achieve or maintain certification to ISO 27001 shall note that they are no longer included in the context of the certification process (by default, however custom controls can always be applied to any ISMS).

Responsible Parties must also note that the ISMF retains these control objectives for use in management of and treating risks associated with government information and their associated information assets. Selection of suitable and relevant controls, including ISMF Standards, constitute an agency ISMS implementation and are the outcome of a successful risk assessment and management program undertaken by each Agency.

Controls that are removed (citing the AS/NZS 2006 publication, as clauses have been reused or allocated by other meanings in the current 2013 publication):

- 6.1.1 Management commitment to information security
- 6.1.2 Information security coordination
- 6.1.4 Authorisation process for new information processing facilities
- 6.2.2 Addressing security when dealing with customers
- 8.1.1 Roles and responsibilities
- 10.2.1 Service delivery
- 10.4.2 Controls against mobile code
- 10.7.4 Security of system documentation
- 10.8.5 Business information systems
- 10.9.3 Publicly available information
- 10.10.5 Fault logging
- 11.4.2 User authentication for external connections
- 11.4.3 Equipment identification in networks
- 11.4.4 Remote diagnostic and configuration port protection
- 11.4.6 Network connection control
- 11.4.7 Network routing control
- 11.5.2 User identification and authentication
- 11.5.5 Session time out
- 11.5.6 Limitation of connection time
- 11.6.2 Sensitive system isolation
- 12.2.1 Input data validation
- 12.2.2 Control of internal processing
- 12.2.3 Message integrity
- 12.2.4 Output data validation
- 12.5.4 Information leakage
- 14.1.2 Business continuity and risk assessment
- 14.1.3 Developing and implementing business continuity plans
- 14.1.4 Business continuity planning framework
- 15.1.5 Prevention of misuse of information processing facilities
- 15.3.2 Protection of information systems audit tools

ANNEX H – RETIRED ISMF STANDARDS

The following list identifies retired ISMF Standards, and their replacement or amendment as well as the version number of ISMF in which the Standard was de-listed. ISMF Standards number designations are not re-used once retired.

Reference	Title and/or text abstract of standard	Treatment (ISMF version)
ISMF Standard 18	Acceptable use policies encompassing applicable conditions, standards and guidelines must be documented and implemented for information assets.	Replaced in entirety by ISMF Standard 131 (v3.2.0) Control S131.8 added to map to ISO 27002 control objectives.
ISMF Standard 138	Privacy and confidentiality of government data is governed by the *Information Privacy Principles Instruction* (Cabinet Administrative Instruction 1/89) issued as Premier and Cabinet Circular No. 12	Replaced in entirety by ISMF Standard 130 (v3.2.0) Implementation considerations from former standard assigned as control S130.2