Australian Government

Digital Transformation Office

Third Party Identity Services Assurance Framework

Information Security Registered Assessors Program Guide

Version 2.0 November 2015

Digital Transformation Office

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the *It's an Honour* website (http://www.itsanhonour.gov.au)

Contact us

Enquiries or comments regarding this document are welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

Contents

1. Guide Management

1.1 Change Log

This is the first published edition of the *Third Party Identity Services Assurance Framework* (Assurance Framework) Information Security Registered Assessors Program (IRAP) Guide (‘*The Guide*’).

1.2 Review Date

This document will be reviewed regularly and updated in line with changes to the relevant government protective security policies, manuals and frameworks.

1.3 Conventions

This guide adopts the following conventions:

- **MUST** indicates a mandatory requirement that a Service Provider is to satisfy in order to obtain accreditation. This convention is also used to describe actions or activities to be undertaken by an IRAP Assessor.
- **MUST NOT** indicates something that if practiced, exercised or implemented will breach an accreditation requirement.
- **SHOULD** indicates something that is not mandatory but is recommended which either supports a mandatory obligation or is considered best practice.
- **COMPLIANCE** is an assessment outcome which indicates a Service Provider satisfies a control listed in this guide for accreditation.
- **NON COMPLIANCE** is an assessment outcome which indicates a Service Provider does not meet a mandatory control listed in this guide for accreditation. Non-compliance severity ratings are listed at Annex A: Non-Compliance Ratings. A template for recording non-compliance is provided at Annex B: Non-Compliance Template.
  - Service Providers may seek a waiver for a NON COMPLIANCE with any mandatory control listed in this Guide from their Accreditation Authority. The Accreditation Authority for Agencies is their Agency Head or their delegated representative. For commercial organisations the Accreditation Authority is a person or committee with the necessary authority to grant such a waiver.
  - Service Providers seeking accreditation are to meet all mandatory controls in this Guide unless they obtain a waiver for a NON COMPLIANCE from their Accreditation Authority.
  - Service Providers seeking a waiver for a NON COMPLIANCE with any mandatory control listed in this Guide MUST document the justification for NON COMPLIANCE, alternative mitigation measures to be implemented (if any) and an assessment of the residual security risk.
  - Service Providers MUST retain a copy of all decisions to grant a waiver for any mandatory control listed in this Guide.

1.4 Terms and Definitions

The terms and definitions used in this document are defined in the *Identity and Access Management Glossary*.

1.5 Advice on this Guide

Advice on the IRAP Guide or suggestions for amendment is welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

1.6 Document Structure

This document is structured in the following manner:

- Section 2 provides an introduction to the IRAP Guide.
- Section 3 outlines the IRAP Assessment process.
- Section 4 summarises the protective security controls covered by this Guide.
- Sections 5 through 8 list the documentation, physical, logical and personnel controls to be met by Service Providers.
- Annex A: Non-Compliance Ratings lists the severity rating definitions to distinguish between degrees of non-compliance.
- Annex B: Non-Compliance Template contains a template that IRAP Assessors can use to record their findings for areas of non-compliance.

2. Introduction

2.1 Purpose

The Assurance Framework operates within a risk management context and aligns with the *Australian Government Protective Security Policy Framework* (PSPF) and the *Australian Government Information Security Manual* (ISM).

- The PSPF defines a series of core policies and mandatory requirements with which applicable Commonwealth agencies and bodies must demonstrate their compliance. These requirements cover protective security governance, personnel security, information security and physical security.
- The ISM is designed to assist Australian government agencies in applying a risk-based approach to protecting their information and systems. The ISM includes a set of information security controls that, when implemented, will help agencies meet their compliance requirements for mitigating security risks to their information and systems.

Service Providers who apply for Assurance Framework Accreditation undergo rigorous evaluation of all aspects of their operations, including compliance with relevant Australian Government protective security requirements outlined in the PSPF and ISM. Service Providers are required to undergo an Information Security Registered Assessors Program (IRAP) by an IRAP Assessors[1] in order to obtain Assurance Framework Accreditation.

This document provides IRAP Assessors with guidance to enable them to assess the implementation, appropriateness and effectiveness of information security controls within a Service Provider's operating environment.

Once accreditation is granted by the Assurance Framework Competent Authority, a Service Provider may require an additional IRAP Assessment if their operating environment is changed in a manner which may result in significant impacts to protective security. If such circumstances occur the Assurance Framework Competent Authority will advise the Service Provider in writing of the requirement for them to carry out an additional IRAP Assessment.

Security and privacy are interlinked. Subsequent iterations of this document will consider the relationship between particular PSPF/ISM controls and the requirements of the Australian Privacy Principles.

As this document is primarily written for Government agencies it contains references to security classifications and security domains, which may or may not be applicable to some commercial service providers. The applicability of such controls within unclassified networks and systems should be addressed with the DTO initially and reflected in the Statement of Applicability (see Section 3.1).

[1] The full list of endorsed IRAP Assessors is available here: http://www.asd.gov.au/infosec/irap/assessors.htm

3. IRAP Assessment

3.1 What is an IRAP Assessment?

An IRAP Assessment is a review by an IRAP Assessor of the implementation, appropriateness and effectiveness of the protective security controls within a Service Provider's operating environment.

An IRAP Assessment is achieved through a two-stage audit which encompasses documentation reviews, a site visit and interviews with key personnel. The outcome of the IRAP Assessment is a Findings Report which is sent to the Assurance Framework Competent Authority for consideration.

Stage 1 Audit

In a Stage 1 Audit and IRAP Assessor:

- Defines the Statement of Applicability in consultation with the Service Provider;
  - The IRAP Assessor **MUST** determine if the information system under evaluation is operational or not.
  - If elements of the information system are not yet operational but would have been considered within the statement of applicability if they were operational, the IRAP Assessor **MUST** note that these elements are subject to review as part of the Service Provider's first Assurance Framework Compliance Audit. Such a situation **MUST NOT** adversely impact the outcome of the IRAP Assessment.
- Gains an understanding of the Service Provider's operating environment;
- Reviews system architecture and information security documentation;
- Seeks evidence of compliance with Australian Government protective security requirements and recommendations; and,
- Highlights the effectiveness of protective security controls and recommends actions to address or mitigate non-compliance.

The outcome of a Stage 1 Audit is a Findings Report which is used as an input for the Stage 2 Audit.

Stage 2 Audit

In the Stage 2 Audit an IRAP Assessor looks deeper into the system's operation, focusing on seeking evidence of compliance with and the effectiveness of security controls. The IRAP Assessor will conduct a site visit where they will:

- Conduct interviews with key personnel;
- Investigate the implementation and effectiveness of security controls in reference to the information security documentation suite; and,
- Sight all relevant protective security certifications and waivers.
  - Where a waiver has been granted in relation to any aspect of a Service Provider's operating environment, the IRAP Assessor **MUST** sight the document and make allowance for the waiver in their evaluation and indicate this in the relevant section of the assessment against this Guide and in the Findings Report.

The outcome of a Stage 2 Audit is a Findings Report to the Assurance Framework Competent Authority that:

- Describes areas on compliance and non-compliance;
- Suggests remediation actions; and,

- Make a recommendation to the Assurance Framework Competent Authority.

The Assurance Framework Competent Authority uses the Findings Report to:

- Assess the residual risk relating to the operation of the Service Provider's environment;
- Assess any remediation activities the Service Provider has undertaken; and,
- Support a decision on whether to grant accreditation.

3.2 Documents to be reviewed as part of the IRAP Assessment

The following information security documentation **MUST** be reviewed by the IRAP Assessor as part of the IRAP Assessment:

- Protective Security Risk Review;
- Security Risk Management Plan;
- System Security Plan, comprising;
  - Standard Operating Procedures;
- Physical & Environmental Security Plan;
- Personnel Security Plan;
- Incident Response Plan; and,
- Disaster Recovery and Business Continuity Plan.

The suite of Information Security Documentation **MUST** be maintained by all Assurance Framework Accredited Service Providers. These documents address all elements of the Service Provider's protective security arrangements and are used to support the accurate and consistent application of policy and procedure within a Service Provider's operating environment[2].

All documents **MUST** include the title, version number and date and be authorised by an appropriate representative of the Service Provider's organisation.

3.3 Controls, Waivers and Site Visits

A control is satisfied if the IRAP Assessor determines the Service Provider has successfully met the intent of a control. A control is not satisfied if the IRAP Assessor determines the Service Provider has not successfully met the intent of a control.

Where a waiver has been granted in relation to any aspect of a Service Provider's operations, the IRAP Assessor **MUST** sight the document and make allowance for the waiver in their evaluation and indicate this in the Findings Report.

The IRAP Assessor **MUST** comment on each instance of **NON COMPLIANCE**. Comments are to include an indication of the extent to which the Service Provider does not comply with the control under evaluation. The severity ratings of **NON COMPLIANCE** are listed in Annex A: Non-Compliance Ratings. A template for providing comments on areas of non-compliance is outlined in Annex B: Non-Compliance Template.

[2] Hosted or third party environments used by Service Provider as part of their accredited service also need to be covered by the information security documentation.

The IRAP Assessor **MUST** verify consistency between policy, plans, and procedures. In order to verify that procedures mentioned within policy documentation are operational, the IRAP Assessor **SHOULD** have the Service Provider demonstrate that the procedure is in use.

3.4 Failed Evaluations

A failed evaluation is one where, in the opinion of the IRAP Assessor, the Service Provider's implementation of its security policies and procedures, EITHER does not adequately mitigate the threats and risks identified in the Security Risk Management Plan OR does not satisfy the requirements of this Guide.

In reaching this decision the IRAP Assessor **MUST** have due regard to the nature of the service provided by the Service Provider and the importance of maintaining a balance between commercial and security considerations.

This decision is not subject to negotiation with the Service Provider seeking Assurance Framework accreditation.

Where a failed evaluation occurs the Findings Report **MUST** identify remedial action to be undertaken (and a timeframe within which the actions are to be completed) to address a **NON-COMPLIANCE.**

The Findings Report **MUST** include signoff from the Service Provider's Accreditation Authority, stating that to the best of their knowledge, the IRAP Assessor who signed the Findings Report has actively participated in conducting the assessment work.

A copy of the counter-signed Findings Report **MUST** be provided to the Service Provider.

3.5 Findings Report

The IRAP Assessor **MUST**:

- Prepare a Findings Report based on the activities they have undertaken in completing the IRAP Assessment; Identify areas of compliance and non-compliance with the controls listed in this guide;
- Suggest remediation actions to address all areas of non-compliance; and
- Provide a recommendation to the Assurance Framework Competent Authority as to the adequacy of the Service Provider's protective security controls for the environment under evaluation.

The covering letter to the Findings Report **MUST** advise the Assurance Framework Competent Authority, in the view of the IRAP Assessor, whether or not the Service Provider has successfully met the requirements of the Guide. A copy of the counter-signed Findings Report **MUST** be included with the covering letter.

Where the Service Provider has failed the IRAP Assessment, the letter and the report **MUST** specify what remedial action is required to be undertaken by the Service Provider in order to achieve compliance.

A copy of the Covering Letter **MUST** also be provided to the Service Provider.

The IRAP Assessor **MUST** forward the following documents to the Assurance Framework Competent Authority once the assessment is completed:

- Findings Report with covering letter,
- Completed assessment against this guide,

- A complete list of non-compliances including their severity ratings[3], and
- Recommended actions to remediate non compliances.

Completed IRAP Guides are to be send to the following address:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

[3] Annex A defines the non-compliance severity ratings and their associated definitions.

4. Protective Security Controls

The Guide consists of 191 controls which cover the protective security requirements specific for Assurance Framework accreditation. Each control contains four pieces of information:

1. **No**. The control number (1 through 191).
2. **Source**. The source document from where a control is taken (i.e. PSPF, ISM or the Framework itself).
3. **Control**. The control number relative to the source. For example, 'GOV4' is a control from the PSPF; '0040' is a control from the ISM.
4. **Requirement**. The requirement to be met.

Below is an example of a requirement used within the Guide.

No	**Source**	**Control**	
No: 17	**Source:** ISM, PSPF	**Control:** 0040, GOV4, INFOSEC2	
All systems MUST be covered by a Security Risk Management Plan.			

Note: For the purpose of this guide some ISM and PSPF controls have been altered to fit within an accreditation-specific context.

Wherever alterations like this have occurred the source of the control will state both the Framework itself – identified as FW - and either the ISM/PSPF.

4.1 Summary of Protective Security Controls

Below is a summary of protective security controls contained within this Guide.

Section	**Requirement**	**Controls**
	Total Controls	**191**
5	**Documentation Controls**	**53**
5.1	Security Provider Governance	11
5.2	Information Security Documentation	42
6	**Physical Controls**	**46**
6.1	Facilities	6
6.2	Infrastructure	7
6.3	Equipment & Media	26
6.4	Mobile Devices	7

Section	Requirement	Controls
7	**Logical Controls**	**83**
7.1	Strategies to Mitigate Targeted Cyber Intrusions	24
7.6	Access Controls	7
7.7	User Accounts	10
7.8	Standard Operating Environment	5
7.9	Databases	12
7.10	System Monitoring	2
7.11	Approved Algorithms and Protocols	22
7.12	Outsourced Arrangements	1
8	**Personnel Controls**	**9**
8.1	Clearances	3
8.2	Training	2
8.3	Security Awareness	3
8.4	Staff Responsibilities	1

5. Documentation Controls

5.1 Service Provider Governance

No	Source	Control	
No: 1	**Source:** FW	**Control:** FW	
Service Providers MUST be registered with the Australian Business Register and maintain a current Australian Business Number.			
No: 2	**Source:** ISM	**Control:** 1071	
Each system MUST have a system owner who is responsible for the operation of the system.			
No: 3	**Source:** ISM, PSPF	**Control:** 1229, GOV2	
A Service Provider's Accreditation Authority MUST be at least a senior executive with an appropriate level of understanding of the security risks they are accepting on behalf of the Service Provider.			
No: 4	**Source:** ISM, PSPF	**Control:** 768, GOV3	
Service Providers MUST appoint at least one expert, commonly referred to as an ITSA (or an equivalent position), in administering and configuring a broad range of systems as well as analysing and reporting on information security issues.			
No: 5	**Source:** ISM, PSPF	**Control:** 741, GOV2	
Service Providers MUST appoint at least one executive, commonly referred to as an ITSM (or an equivalent position), to manage the day-to-day operations of information security within the Service Provider, in line with the strategic directions provided by the CISO or equivalent.			

No	Source	Control	
No: 6	**Source:** ISM	**Control:** 7	
Service Providers undertaking system design activities for in-house or out-sourced projects MUST use the latest release of the ISM for security requirements.			
No: 7	**Source:** ISM	**Control:** 710	
Service Providers seeking approval for non-compliance with any control MUST document: • the justification for non-compliance, • a security risk assessment, • the alternative mitigation measures to be implemented, if any.			
No: 8	**Source:** ISM, FW	**Control:** 3, FW	
Service Providers MUST retain a copy of decisions to grant non-compliance with any Assurance Framework specific control from the ISM.			
No: 9	**Source:** ISM	**Control:** 876	
Service Providers MUST review decisions to grant non-compliance with any control, including the justification, any mitigation measures and security risks, at least annually or when significant changes occur to ensure its continuing relevance, adequacy and effectiveness.			
No: 10	**Source:** PSPF	**Control:** GOV10	
Service Providers MUST adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Australia is a party.			
No: 11	**Source:** ISM	**Control:** 137	
Service Providers considering allowing intrusion activity to continue under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.			

5.2 Information Security Documentation

5.2.1 Protective Security Risk Review

No	Source	Control	
No: 12	**Source:** FW	**Control:** FW	
Threats to information systems, assets and business processes MUST be outlined in the Protective Security Risk Review and Security Risk Management Plan documents as part of the Service Provider's Information Security Documents.			

5.2.2 Security Risk Management Plan

No	Source	Control	
No: 13	**Source:** ISM, PSPF	**Control:** 40, GOV4, 5 & 6, INFOSEC2	
All systems MUST be covered by a Security Risk Management Plan.			
No: 14	**Source:** ISM	**Control:** 1208	
Service Providers MUST document identified information security risks, as well as the evaluation of those risks and mitigation strategies, in their Security Risk Management Plan.			
No: 15	**Source:** ISM	**Control:** 1203	
Service Providers MUST identify and analyse security risks to their information and systems.			
No: 16	**Source:** ISM	**Control:** 1204	
Security risks deemed unacceptable MUST be treated.			

No	Source	Control	
No: 17	**Source:** FW	**Control:** FW	
Assets to be protected MUST be identified in the Risk Assessment.			
No: 18	**Source:** ISM	**Control:** 1205	
Service Providers MUST incorporate the relevant controls contained in the current version of the ISM in their security risk management processes. The relevant controls are those listed in this IRAP Guide.			
No: 19	**Source:** ISM, PSPF	**Control:** 1354, GOV5 & GOV6, INFOSEC 2	
Service Providers MUST adopt a risk–management approach and implement alternative security controls for: • technologies which lack available software to enforce the mandatory controls; and • scenarios or circumstances which prevent enforcement of the mandatory Top 4 Strategies.			
No: 20	**Source:** FW	**Control:** FW	
Security risks deemed acceptable by a Service Provider MUST be formally accepted by the System Owner.			

5.2.3 System Security Plan

No	Source	Control	
No: 21	**Source:** ISM	**Control:** 41	
All systems MUST be covered by a System Security Plan (SSP).			

No	Source	Control	
No: 22	**Source:** ISM, PSPF	**Control:** 895, INFOSEC 5 & 6	
Service Providers MUST select controls from the current version of the ISM to be included in the SSP based on the scope of the system with additional system specific controls being included as a result of the associated SRMP.			
No: 23	**Source:** ISM	**Control:** 432	
Service Providers MUST specify in the SSP any authorisations necessary for system access.			
No: 24	**Source:** FW	**Control:** FW	
All server and workstation security objectives and mechanisms MUST be documented in the relevant SSP.			
No: 25	**Source:** ISM	**Control:** 580	
Service Providers MUST develop an event log strategy covering: • logging facilities including availability requirements and the reliable delivery of event logs to logging facilities; • the list of events associated with a system or software component to be logged; and • Event log protection and archival requirements.			
No: 26	**Source:** ISM	**Control:** 586	
Event logs MUST be protected from modification and unauthorised access, and whole or partial loss within the defined retention period.			
No: 27	**Source:** ISM	**Control:** 1405	
Service Providers MUST implement a secure centralised logging facility.			

No	Source	Control	
No: 28	**Source:** ISM	**Control:** 1344	
Service Providers MUST ensure systems are configured to save event logs to the secure centralised logging facility.			

5.2.4 Standard Operating Procedures

No	Source	Control	
No: 29	**Source:** ISM, FW	**Control:** 123, 130, FW	
Standard Operating Procedures for all personnel with access to systems MUST include the requirement to notify the ITSM: • of any cyber security incident as soon as possible after the cyber security incident is discovered, and • access to any data that they are not authorised to access.			
No: 30	**Source:** ISM	**Control:** 322	
Service Providers MUST document SOPs for the reclassification and declassification of media and equipment.			
No: 31	**Source:** ISM	**Control:** 348	
Service Providers MUST document SOPs for the sanitisation of media and equipment.			
No: 32	**Source:** ISM	**Control:** 363	
Service Providers MUST document SOPs for the destruction of media and equipment.			
No: 33	**Source:** ISM	**Control:** 374 /313	
Service Providers MUST document SOPs for the disposal of media and equipment			

No	Source	Control	
No: 34	**Source:** ISM	**Control:** 1082	
Service Providers MUST develop a policy governing the use of mobile devices.			

5.2.5 Physical & Environmental Security Plan

No	Source	Control	
No: 35	**Source:** PSPF	**Control:** PHYSEC3	
Service Providers MUST prepare a Physical & Environmental Security Plan.			

5.2.6 Personnel Security Management Plan

No	Source	Control	
No: 36	**Source:** FW	**Control:** FW	
Service Providers MUST implement a Personnel Security Management Plan.			

5.2.7 Vulnerability Management

No	Source	Control	
No: 37	**Source:** ISM	**Control:** 112	
Service Providers MUST analyse any vulnerabilities to determine their potential impact on their operations and determine appropriate mitigations or other treatments. Evidence of these mitigations and treatments MUST appear in the Service Provider's Information Security Documentation.			

No	Source	Control	
No: 38	**Source:** ISM	**Control:** 113	
Service Providers MUST mitigate or otherwise treat identified vulnerabilities as soon as possible.			

5.2.8 Incident Response Plan

No	Source	Control	
No: 39	**Source:** ISM, PSPF	**Control:** 43, PHYSEC7	
Service Providers MUST develop, maintain and implement an Incident Response Plan and supporting procedures.			
No: 40	**Source:** ISM	**Control:** 58	
Service Providers MUST include, as a minimum, the following content in their IRP: • broad guidelines on what constitutes a cyber security incident • the minimum level of cyber security incident response and investigation training for users and system administrators • the authority responsible for initiating investigations of a cyber security incident • the steps necessary to ensure the integrity of evidence supporting a cyber security incident • the steps necessary to ensure that critical systems remain operational • how to formally report cyber security incidents.			
No: 41	**Source:** ISM	**Control:** 131	
Service Providers MUST document procedures for dealing with data spills[4] in their IRP.			

[4] Where a data spill involves personal information as defined in the Privacy Act, Service Providers MUST advise the Office of the Australian Information Commissioner (OAIC).

No	Source	Control	
No: 42	**Source:** ISM	**Control:** 132	
Service Providers MUST treat any data spillage as a cyber security incident, and follow the IRP to mitigate the incident.			
No: 43	**Source:** ISM	**Control:** 129	
When a data spill occurs Service Providers MUST assume that the information has been compromised and report the details of the data spill to ASD and as appropriate the OAIC.			
No: 44	**Source:** ISM	**Control:** 133	
When a data spill occurs, Service Providers MUST report the details of the data spill to the information owner.			
No: 45	**Source:** ISM, FW	**Control:** 139, FW	
Service Providers MUST report cyber security incidents to ASD and the Assurance Framework Competent Authority.			
No: 46	**Source:** ISM	**Control:** 142	
Service Providers MUST notify all communications security custodians of any suspected loss or compromise of keying material.			
No: 47	**Source:** ISM	**Control:** 141	
Service Providers that outsource their ICT services and functions to a third party MUST ensure that the third party consults with them when a cyber security incident occurs.			

5.2.9 Change Management

No	Source	Control	
No: 48	**Source:** ISM, FW	**Control:** 1211, FW	
Service Providers MUST have a formal change management process in place.			
No: 49	**Source:** ISM	**Control:** 117	
The change management process MUST define appropriate actions to be followed before and after urgent or emergency changes are implemented.			
No: 50	**Source:** ISM	**Control:** 115	
Service Providers MUST ensure that for routine and urgent changes: • the change management process is followed; • the proposed change is approved by the relevant authority; • any proposed change that could impact the security of a system is submitted to the accreditation authority for approval; and • all relevant Information Security Documentation is updated to reflect the change.			
No: 51	**Source:** ISM, FW	**Control:** 809, FW	
When a configuration change impacts the security of a system, and is subsequently assessed as having changed the overall security risk for the system, the system MUST undergo reaccreditation.			

5.2.10 Disaster Recovery and Business Continuity Plan

No	Source	Control	
No: 52	**Source:** PSPF, FW	**Control:** GOV11, FW	
Service Providers MUST develop a Disaster Recovery Business Continuity Plan.			
No: 53	**Source:** ISM, PSPF	**Control:** 118, GOV11	
Service Providers MUST determine availability requirements for their systems and implement appropriate security measures to support these requirements.			

6. Physical Controls

6.1 Facilities

No	Source	Control	
No: 54	**Source:** ISM, PSPF	**Control:** 865, PHYSEC4 & 6	
Service Providers MUST ensure that any facility(s) containing systems or assets (including a mobile device or removable media) meet the requirements in the Australian Government Physical Security Management Protocol.			
No: 55	**Source:** PSPF, FW	**Control:** PHYSEC6, FW	
Service Provider systems MUST be housed within a secure environment and have restrictive physical access controls to ensure only authorized and trained staff have access.			
No: 56	**Source:** ISM	**Control:** 813	
Service Providers MUST NOT leave server rooms, communications rooms or security containers in an unsecured state.			
No: 57	**Source:** ISM	**Control:** 1074	
Service Providers MUST ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers or rooms are appropriately controlled and audited.			

No	Source	Control	
No: 58	**Source:** ISM	**Control:** 150	
Where a Service Provider uses a No-Lone Zone (NLZ), this area MUST: • be suitably sign-posted; and • have all entry and exit points appropriately secured.			
No: 59	**Source:** ISM, PSPF	**Control:** 1053, INFOSEC 6, & 7, PHYSEC 6	
Service Providers MUST ensure that servers and network devices are secured in either security containers or rooms as specified in the Australian Government Physical Security Management Protocol.			

6.2 Infrastructure

No	Source	Control	
No: 60	**Source:** ISM	**Control:** 1304	
Default network device accounts MUST be disabled, renamed or have their passphrase changed.			
No: 61	**Source:** ISM	**Control:** 1383	
Service Providers MUST ensure that all administrative infrastructure including, but not limited to, privileged workstations and jump boxes are hardened appropriately.			

No	Source	Control	
No: 62	**Source:** ISM	**Control:** 1388	
Service Providers MUST ensure that jump boxes are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.			
No: 63	**Source:** ISM	**Control:** 1296	
Adequate physical measures MUST be provided to protect network devices, especially those in public areas, from physical damage or unauthorised access.			
No: 64	**Source:** FW	**Control:** FW	
Service Providers MUST use a firewall as part of their traffic flow filter.			
No: 65	**Source:** ISM	**Control:** 639	
Service Providers MUST use a firewall between networks of different security domains (eg between its network and the public Internet)			
No: 66	**Source:** ISM	**Control:** 1194	
The requirement to use a firewall as part of gateway infrastructure MUST be met by both parties independently; shared equipment does not satisfy the requirements of both parties.			

6.3 Equipment & Media

No	Source	Control	
No: 67	**Source:** ISM, PSPF	**Control:** 294, INFOSEC6 & 7	
Service Providers MUST clearly label all ICT equipment capable of storing information, with the exception of High Assurance products, with the appropriate protective marking.			
No: 68	**Source:** ISM, PSPF	**Control:** 323, INFOSEC6 & 7	
Service Providers MUST classify media to the highest classification stored on the media since any previous reclassification.			
No: 69	**Source:** ISM, PSPF	**Control:** 325, INFOSEC6 & 7	
Service Providers MUST classify any media connected to a system the same sensitivity or classification as the system, unless either: • the media is read-only • the media is inserted into a read-only device • the system has a mechanism through which read-only access can be assured.			
No: 70	**Source:** ISM	**Control:** 333	
Service Providers MUST ensure that classification of all media is easily visually identifiable.			
No: 71	**Source:** ISM, PSPF	**Control:** 334	
When using non-textual protective markings for media due to operational security reasons, Service Providers MUST document the labelling scheme and train personnel appropriately.			

No	Source	Control	
No: 72	**Source:** ISM, PSPF	**Control:** 161, INFOSEC6 & 7	
Service Providers MUST ensure that ICT equipment and media with sensitive (or classified) information[5] is secured in accordance with the requirements for storing sensitive or classified information in the Australian Government Physical Security Management Protocol.			
No: 73	**Source:** ISM	**Control:** 832	
Service Providers MUST encrypt media with at least an ASD Approved Cryptographic Algorithm if it is to be transferred through an area not certified and accredited to process the sensitivity or classification of the information on the media.			
No: 74	**Source:** ISM	**Control:** 418	
Authentication information MUST be stored separately to a system to which it grants access.			
No: 75	**Source:** ISM	**Control:** 1402	
Authentication information stored on a system MUST be protected.			
No: 76	**Source:** ISM	**Control:** 462	
When a user authenticates to ICT equipment storing encrypted information, it MUST be treated in accordance with the original sensitivity or classification of the equipment.			
No: 77	**Source:** ISM, PSPF	**Control:** 159, INFOSEC6 & 7	
Service Providers MUST account for all sensitive and classified ICT equipment and media.			

[5] The majority of commercial identity service and digital mailbox service providers will hold personal information as opposed to security classified information. All such information holdings should be regarded as “sensitive” in the generally understood meaning of the term. Where a service provider holds information that is defined as sensitive under the Privacy Act, additional security controls may be required.

No	Source	Control	
No: 78	**Source:** ISM, PSPF	**Control:** 293, INFOSEC3 & 7	
Service Providers MUST classify ICT equipment based on the sensitivity or classification of information for which the equipment and any associated media in the equipment are approved for processing, storing or communicating.			
No: 79	**Source:** ISM	**Control:** 310	
Service Providers having ICT equipment maintained or repaired off-site MUST ensure that the physical transfer, processing and storage requirements are appropriate for the sensitivity or classification of the equipment and that procedures are complied with at all times.			
No: 80	**Source:** ISM, PSPF	**Control:** 329, INFOSEC6 & 7	
Service Providers declassifying media MUST ensure that: • the media has been reclassified to an unclassified level either through an administrative decision, sanitisation or destruction • a formal administrative decision is made to release the unclassified media, or its waste, into the public domain.			
No: 81	**Source:** ISM, PSPF	**Control:** 330, INFOSEC6 & 7	
Service Providers wishing to reclassify media to a lower classification MUST ensure that: • the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed. • a formal administrative decision is made to reclassify the media.			
No: 82	**Source:** ISM, PSPF	**Control:** 331, INFOSEC6 & 7	
Media MUST be reclassified if: • information copied onto the media is of a higher classification than the sensitivity or classification of the information already on the media; and • information contained on the media is subjected to a classification upgrade.			

No	Source	Control	
No: 83	**Source:** ISM	**Control:** 375	
Service Providers MUST declassify all media prior to disposing of it into the public domain.			
No: 84	**Source:** ISM, PSPF	**Control:** 311, INFOSEC6 & 7	
Service Providers MUST, when disposing of ICT equipment containing classified media, sanitise the equipment by either: • sanitising the media within the equipment; • removing the media from the equipment and disposing of it separately; or • destroying the equipment in its entirety.			
No: 85	**Source:** ISM	**Control:** 350	
Service Providers MUST destroy the following media types prior to disposal, as they cannot be sanitised: • microform (i.e. microfiche and microfilm) • optical discs • printer ribbons and the impact surface facing the platen • programmable read-only memory • read-only memory • faulty or other types of media that cannot be successfully sanitised.			

No	Source	Control	
No: 86	**Source:** ISM	**Control:** 364	
To destroy media, Service Providers MUST either: • break up the media • heat the media until it has either burnt to ash or melted • degauss the media.			
No: 87	**Source:** ISM	**Control:** 1217	
When disposing of ICT equipment, Service Providers MUST remove labels and markings indicating the classification, code words, caveats, owner, system or network name, or any other marking that can associate the equipment with its original use.			
No: 88	**Source:** ISM	**Control:** 1347	
Where volatile media has undergone sanitisation but sensitive or classified information persists on the media, Service Providers MUST destroy the media, and handle the media at the sensitivity or classification of the information it contains until it is destroyed.			
No: 89	**Source:** ISM, PSPF	**Control:** 370, PERSEC1, PERSEC4, INFOSEC6	
Service Providers MUST perform the destruction of media under the supervision of at least one person cleared to the classification of the media being destroyed.			
No: 90	**Source:** ISM, PSPF	**Control:** 371, PERSEC1, PERSEC4, INFOSEC6	
The person supervising the destruction of the media MUST: • supervise the handling of the material to the point of destruction; and • ensures that the destruction is successfully completed.			

No	Source	Control	
No: 91	**Source:** ISM	**Control:** 378	
Service Providers MUST dispose of media in a manner that does not draw undue attention to its previous sensitivity or classification.			
No: 92	**Source:** ISM, FW	**Control:** 336, FW	
Service Providers MUST register all removable media with a unique identifier in an appropriate register (e.g. removable media register).			

6.4 Mobile Devices[6]

No	Source	Control	
No: 93	**Source:** ISM	**Control:** 864	
Service Providers MUST prevent personnel from disabling security functions on a mobile device once provisioned.			
No: 94	**Source:** ISM	**Control:** 1085	
Service Providers using mobile devices to communicate sensitive or classified information over public network infrastructure MUST use encryption approved for communicating such information over public network infrastructure.			
No: 95	**Source:** ISM	**Control:** 870	
Service Providers MUST ensure mobile devices are carried in a secured state when not being actively used.			

[6] The context for this section is two-fold; 1) the use of mobile devices by Service Provider employees to remotely access networks and systems and, 2) Service Providers that support mobile-based identity proofing capabilities as part of their accredited solution.

No	Source	Control	
No: 96	**Source:** ISM	**Control:** 1087	
When travelling with mobile devices and media, personnel MUST retain control over them at all times, this includes not placing them in checked-in luggage or leaving them unattended for any period of time.			
No: 97	**Source:** ISM	**Control:** 871	
When in use mobile devices MUST be kept under continual direct supervision.			
No: 98	**Source:** ISM	**Control:** 693	
Service Providers permitting personnel to access or store sensitive information using non-Service Provider owned mobile devices MUST implement technical controls to enforce the separation of sensitive information from personnel information.			
No: 99	**Source:** ISM	**Control:** 1200	
If using Bluetooth on a mobile device, Service Providers MUST ensure both pairing devices uses Bluetooth version 2.1 or later.			

7. Logical Controls

7.1 Strategies to Mitigate Targeted Cyber Intrusions (Top 4)[7]

No	Source	Control	
No: 100	**Source:** ISM, PSPF, FW	**Control:** 1353, INFOSEC 4, FW	
Service Providers MUST implement the controls indicated in the following table on all systems that are within the scope of the IRAP Assessment (i.e. within the Statement of Applicability identified in Stage 1 of the audit). *Note: Some controls are duplicated between 'patch applications' and 'patch operating system' as they satisfy both strategies.*			

TOP 4 CONTROLS	
Mitigation Strategy	**ISM Controls**
Application whitelisting	0843, 0846, 0955, 1391, 1392
Patch applications	0300, 0303, 0304, 0940, 0941, 1143, 1144,
Patch operating systems	0300, 0303, 0304, 0940, 0941, 1143, 1144,
Restrict administrative privileges	0405, 0445, 0985, 1175

[7] For Linux based systems use the ASD publication *The Top 4 in a Linux Environment*

7.1.1 Application Whitelisting

No	Source	Control	
No: 101	**Source:** ISM, PSPF	**Control:** 843, 1353, INFOSEC 4	
Service Providers MUST use an application whitelisting solution within the Standard Operating Environments to restrict the execution of programs and Dynamic Link Libraries to an approved set.			
No: 102	**Source:** ISM, PSPF	**Control:** 846, 1353, INFOSEC 4	
Service Providers MUST ensure that users and system administrators cannot temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms.			
No: 103	**Source:** ISM, PSPF	**Control:** 955, 1353, INFOSEC 4	
Service Providers MUST implement application whitelisting using at least one of the following methods: • cryptographic hashes, • publisher certificates, • absolute paths, or • parent folders.			
No: 104	**Source:** ISM, PSPF	**Control:** 1391, 1353, INFOSEC 4	
When implementing application whitelisting using parent folder rules, file system permissions MUST be configured to prevent users and system administrators from adding or modifying files in authorised parent folders.			
No: 105	**Source:** ISM, PSPF	**Control:** 1392, 1353, INFOSEC 4	
When implementing application whitelisting using absolute path rules, file system permissions MUST be configured to prevent users and system administrators from modifying riles that are permitted to run.			

7.1.2 Patch Applications

No	Source	Control	
No: 106	**Source:** ISM, PSPF	**Control:** 300, 1353, INFOSEC 4	
High Assurance products MUST only be patched by ASD approved patches using methods and timeframes prescribed by ASD			
No: 107	**Source:** ISM, PSPF	**Control:** 303, 1353, INFOSEC 4	
Service Providers MUST use an approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches as well as the processes used to apply them.			
No: 108	**Source:** ISM, PSPF	**Control:** 304, 1353, INFOSEC4	
Operating systems, applications and hardware devices that are no longer supported by their vendors MUST be updated to a vendor supported version or replaced with an alternative vendor supported version.			
No: 109	**Source:** ISM, PSPF	**Control:** 940, 1353, INFOSEC4	
Service Providers MUST apply all security patches as soon as possible.			

No	Source	Control	
No: 110	**Source:** ISM, PSPF	**Control:** 941, 1353, INFOSEC4	

When patches are not available for vulnerabilities, one or more of the following approaches must be implemented:

- resolve the vulnerability by either:
  - disabling the functionality associated with the vulnerability
  - asking the vendor for an alternative method of managing the vulnerability
  - moving to a different product with a more responsive vendor
  - engaging a software developer to resolve the vulnerability.
- prevent exploitation of the vulnerability by either:
  - applying external input sanitisation (if an input triggers the exploit)
  - applying filtering or verification on output (if the exploit relates to an information disclosure)
  - applying additional access controls that prevent access to the vulnerability
  - configuring firewall rules to limit access to the vulnerability.
- contain exploitation of the vulnerability by either:
  - applying firewall rules limiting outward traffic that is likely in the event of an exploitation
  - applying mandatory access control preventing the execution of exploitation code
  - setting file system permissions preventing exploitation code from being written to disk.
- detect exploitation of the vulnerability by either:
  - deploying an intrusion detection system
  - monitoring logging alerts
  - using other mechanisms for the detection of exploits using the known vulnerability.

No	Source	Control	
No: 111	**Source:** ISM, PSPF	**Control:** 1143, 1353, INFOSEC 4	
Service Providers MUST develop and implement a patch management strategy covering the patching of vulnerabilities in operating systems, applications, drivers and hardware devices.			
No: 112	**Source:** ISM, PSPF	**Control:** 1144, 1353, INFOSEC4	
Vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk MUST be patched or mitigated within two days.			

7.1.3 Patch operating systems

No	Source	Control	
No: 113	**Source:** ISM, PSPF	**Control:** 300, 1353, INFOSEC 4	
High Assurance products MUST only be patched by ASD approved patches using methods and timeframes prescribed by ASD			
No: 114	**Source:** ISM, PSPF	**Control:** 303, 1353, INFOSEC 4	
Service Providers MUST use an approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches as well as the processes used to apply them.			
No: 115	**Source:** ISM, PSPF	**Control:** 304, 1353, INFOSEC4	
Operating systems, applications and hardware devices that are no longer supported by their vendors MUST be updated to a vendor supported version or replaced with an alternative vendor supported version.			

No	Source	Control	
No: 116	**Source:** ISM, PSPF	**Control:** 940, 1353, INFOSEC4	
Vulnerabilities in operating systems, applications, drivers and hardware devices assessed as below extreme risk MUST be patched or mitigated as soon as possible.			
No: 117	**Source:** ISM, PSPF	**Control:** 941, 1353, INFOSEC4	
When patches are not available for vulnerabilities, one or more of the following approaches must be implemented: • resolve the vulnerability by either: – disabling the functionality associated with the vulnerability – asking the vendor for an alternative method of managing the vulnerability – moving to a different product with a more responsive vendor – engaging a software developer to resolve the vulnerability. • prevent exploitation of the vulnerability by either: – applying external input sanitisation (if an input triggers the exploit) – applying filtering or verification on output (if the exploit relates to an information disclosure) – applying additional access controls that prevent access to the vulnerability – configuring firewall rules to limit access to the vulnerability. • contain exploitation of the vulnerability by either: – applying firewall rules limiting outward traffic that is likely in the event of an exploitation – applying mandatory access control preventing the execution of exploitation code – setting file system permissions preventing exploitation code from being written to disk. • detect exploitation of the vulnerability by either: – deploying an intrusion detection system – monitoring logging alerts – using other mechanisms for the detection of exploits using the known vulnerability.			

No	Source	Control	
No: 118	**Source:** ISM, PSPF	**Control:** 1143, 1353, INFOSEC 4	
Service Providers MUST have a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities.			
No: 119	**Source:** ISM, PSPF	**Control:** 1144, 1353, INFOSEC4	
For security vulnerabilities assessed as 'extreme risk', Service Providers MUST, within two days: • apply the security patch, or • mitigate the vulnerability if there is no patch available.			

7.1.4 Restrict Administrative Privileges

No	Source	Control	
No: 120	**Source:** ISM, PSPF	**Control:** 0405, 1353, INFOSEC 4	
Service Providers MUST: • limit system access on a need-to-know basis • have any requests for access to a system authorised by the person's manager • provide personnel with the least amount of privileges needed to undertake their duties • review system access and privileges at least annually and when personnel change roles • when reviewing access, ensure a response from the person's manager confirming the need to access the system is still valid, otherwise access will be removed.			

No	Source	Control	
No: 121	**Source:** ISM, PSPF	**Control:** 445, 1353, INFOSEC 4	
Service Providers MUST restrict the use of privileged accounts by ensuring that: • the use of privileged accounts is controlled and auditable; • system administrators are assigned a dedicated account to be used solely for the performance of their administration tasks; • privileged accounts are kept to a minimum; • privileged accounts are used for administrative work only; • passphrases for privileged accounts are regularly audited to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts); and • privileges allocated to privileged accounts are regularly reviewed.			
No: 122	**Source:** ISM, PSPF	**Control:** 985, 1353, INFOSEC 4	
Service Providers MUST conduct remote administration of systems, including the use of privileged accounts, over a secure communications medium from secure devices.			
No: 123	**Source:** ISM, PSPF	**Control:** 1175, 1353, INFOSEC 4	
Service Providers MUST prevent users from using privileged accounts access to access the Internet and email.			

7.2 Access Controls

No	Source	Control	
No: 124	**Source:** ISM	**Control:** 414	
Service Providers MUST ensure that all users are: • uniquely identifiable • authenticated on each occasion that access is granted to a system.			
No: 125	**Source:** ISM	**Control:** 1173	
Service Providers MUST use multi-factor authentication for: • system administrators, • database administrators, • privileged users, • positions of trust, and • remote access.			
No: 126	**Source:** ISM	**Control:** 1384	
Service Providers MUST ensure that all privileged actions have passed through at least one multi-factor authentication process.			
No: 127	**Source:** ISM	**Control:** 1381	
Service Providers MUST ensure that dedicated workstations used for privileged tasks are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.			

No	Source	Control	
No: 128	**Source:** ISM, PSPF	**Control:** 856, PERSEC1, INFOSEC5	
Users authorisations MUST be enforced by access controls.			
No: 129	**Source:** ISM	**Control:** 382	
Service Providers MUST ensure that users do not have the ability to install, uninstall or disable software.			
No: 130	**Source:** ISM	**Control:** 845	
Service Providers MUST restrict a user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.			

7.3 User Accounts

No	Source	Control	
No: 131	**Source:** ISM	**Control:** 383	
Service Providers MUST ensure that default operating system accounts are disabled, renamed or have their passphrase changed.			
No: 132	**Source:** FW	**Control:** FW	
Administrative rights MUST be removed when no longer required by the user, or when the user leaves the company/Service Provider.			

No	Source	Control	
No: 133	**Source:** ISM	**Control:** 421	
Service Providers using passphrases as the sole method of authentication MUST enforce the following passphrase policy: • a minimum length of 13 alphabetic characters with no complexity requirement; or • a minimum length of 10 characters, consisting of at least three of the following character sets: • lowercase alphabetic characters (a–z) • uppercase alphabetic characters (A–Z) • numeric characters (0–9) • special characters.			
No: 134	**Source:** ISM	**Control:** 417	
Service Providers MUST NOT use a numerical password (or personal identification number) as the sole method of authenticating a user.			
No: 135	**Source:** ISM	**Control:** 1403	
Service Providers MUST ensure accounts are locked after a maximum of five failed logon attempts.			
No: 136	**Source:** ISM	**Control:** 430	
Accounts MUST be removed or suspended the same day a user no longer has a legitimate business requirement for its use. For example, changing duties or leaving the organisation.			

No	Source	Control	
No: 137	**Source:** ISM	**Control:** 1227	
Service Providers MUST ensure reset passphrases are: • random for each individual reset • not reused when resetting multiple accounts • not based on a single dictionary word • not based on another identifying factor, such as the user's name or the date.			
No: 138	**Source:** ISM	**Control:** 976	
Service Providers MUST ensure users provide sufficient evidence to verify their identity when requesting a passphrase reset for their system account.			
No: 139	**Source:** ISM	**Control:** 419	
Authentication information MUST be protected when communicated across networks.			
No: 140	**Source:** ISM	**Control:** 416	
If Service Providers choose to allow shared, non user-specific accounts, another method of attributing actions undertaken by such accounts to specific personnel MUST be implemented.			

7.4 Standard Operating Environment

No	Source	Control	
No: 141	**Source:** ISM	**Control:** 380	
Service Providers MUST remove or disable unneeded operating system accounts, software, components, services and functionality.			
No: 142	**Source:** ISM	**Control:** 1033	
Service Providers MUST ensure that antivirus or internet security software has: • signature-based detection enabled and set to a high level • heuristic-based detection enabled and set to a high level • detection signatures checked for currency and updated on at least a daily basis • automatic and regular scanning configured for all fixed disks and removable media.			
No: 143	**Source:** ISM	**Control:** 1306	
Firmware for network devices MUST be kept up to date.			
No: 144	**Source:** ISM	**Control:** 657	
Data imported to a system MUST be scanned for malicious and active content.			

No	Source	Control	
No: 145	**Source:** ISM	**Control:** 842	
When using a software-based isolation mechanism to share a physical server's hardware, Service Providers MUST ensure that: • the isolation mechanism is from a vendor that uses secure programming practices and, when vulnerabilities have been identified, the vendor has developed and distributed patches in a timely manner; • the configuration of the isolation mechanism is hardened, including removing support for unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism, with the configuration performed and reviewed by subject matter experts; • the underlying operating system running on the server is hardened; • security patches are applied to both the isolation mechanism and operating system in a timely manner; and, • integrity and log monitoring is performed for the isolation mechanism and underlying operating system in a timely manner.			

7.5 Databases

No	Source	Control	
No: 146	**Source:** ISM, PSPF	**Control:** 1250, INFOSEC 4	
Database servers MUST use a hardened SOE.			
No: 147	**Source:** ISM	**Control:** 1262	
Database administrators MUST have unique and identifiable accounts.			
No: 148	**Source:** ISM	**Control:** 1266	
Anonymous database accounts MUST be removed.			

No	Source	Control	
No: 149	**Source:** ISM	**Control:** 1260	
Default database administrator accounts MUST be disabled, renamed or have their passphrases changed.			
No: 150	**Source:** ISM	**Control:** 1263	
Database administrator accounts MUST be used exclusively for administrative tasks with standard database accounts used for general purpose interactions with databases.			
No: 151	**Source:** ISM, PSPF	**Control:** 1249, INFOSEC 4	
Service Providers MUST configure DBMS software to run as a separate account with the minimum privileges needed to perform its functions.			
No: 152	**Source:** ISM, PSPF	**Control:** 1250, INFOSEC 4	
The account under which DBMS software runs MUST have limited access to non-essential areas of the database server's file system.			
No: 153	**Source:** ISM	**Control:** 1252	
Service Providers MUST ensure passphrases stored in databases are hashed with a strong hashing algorithm which is uniquely salted.			
No: 154	**Source:** ISM	**Control:** 1256	
Service Providers MUST apply file-based access controls to database files.			
No: 155	**Source:** ISM	**Control:** 1275	
All queries to database systems from web applications MUST be filtered for legitimate content and correct syntax.			

No	Source	Control	
No: 156	**Source:** ISM	**Control:** 1277	
Sensitive or classified information communicated between database systems and web applications MUST be encrypted.			
No: 157	**Source:** ISM	**Control:** 393	
Databases or their contents MUST be associated with protective markings.			

7.6 System Monitoring

No	Source	Control	
No: 158	**Source:** ISM	**Control:** 859	
Service Providers MUST retain event logs for a minimum of 7 years after action is completed in accordance with the NAA's Administrative Functions Disposal Authority[8].			

[8] Commercial service providers MUST conform the applicability or otherwise of this Authority in relation to their operations.

No	Source	Control	
No: 159	**Source:** ISM	**Control:** 585	
For each event logged, Service Providers MUST ensure that the logging facility records at least the following details: • date and time of the event; • relevant system user(s) or process; • event description; (d) success or failure of the event; • event source (for example application name); and equipment location/identification.			

7.7 Approved Algorithms and Protocols

No	Source	Control	
No: 160	**Source:** FW	**Control:** FW	
Service Providers MUST use encryption products that implement ASD Approved Cryptographic Algorithms			
No: 161	**Source:** ISM, FW	**Control:** 1446, FW	
Service Providers using elliptic curve cryptography MUST select a curve from the NIST standard, FIPS 186-4.			
No: 162	**Source:** ISM	**Control:** 471	
Service Providers using an unevaluated product that implements an AACA MUST ensure that only AACAs can be used			

No	Source	Control	
No: 163	**Source:** ISM	**Control:** 472	
Service Providers using DH for the approved use of agreeing on encryption session keys MUST use a modulus of at least 1024 bits.			
No: 164	**Source:** ISM	**Control:** 1373	
Service Providers MUST NOT use anonymous DH.			
No: 165	**Source:** ISM	**Control:** 474	
Service Providers using ECDH for the approved use of agreeing on encryption session keys MUST use a field/key size of at least 160 bits			
No: 166	**Source:** ISM	**Control:** 998	
Service Providers MUST use HMAC–SHA256, HMAC–SHA384 or HMAC–SHA512 as a HMAC algorithm.			
No: 167	**Source:** ISM	**Control:** 473	
Service Providers using DSA for the approved use of digital signatures MUST use a modulus of at least 1024 bits			
No: 168	**Source:** ISM	**Control:** 475	
Service Providers using ECDSA for the approved use of digital signatures MUST use a field/key size of at least 160 bits			
No: 169	**Source:** ISM	**Control:** 476	
Service Providers using RSA, for both the approved use of digital signatures and passing encryption session keys or similar keys, MUST use a modulus of at least 1024 bits.			

No	Source	Control	
No: 170	**Source:** ISM	**Control:** 477	
Service Providers using RSA, both for the approved use of digital signatures and for passing encryption session keys or similar keys, MUST ensure that the key pair used for passing encrypted session keys is different from the key pair used for digital signatures.			
No: 171	**Source:** ISM	**Control:** 480	
Service Providers using 3DES MUST use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.			
No: 172	**Source:** ISM	**Control:** 1161	
Service Providers MUST use an encryption product that implements a AACA if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains sensitive information to an unclassified level.			
No: 173	**Source:** ISM	**Control:** 481	
Service Providers using a product that implements an AACP MUST ensure that only AACAs can be used.			
No: 174	**Source:** ISM	**Control:** 482	
Service Providers MUST NOT use SSL.			
No: 175	**Source:** ISM	**Control:** 1447	
Service Providers MUST use TLS.			
No: 176	**Source:** ISM	**Control:** 1233	
Service Providers MUST NOT use manual keying for Key Exchange when establishing an IPsec connection.			

No	Source	Control	
No: 177	**Source:** ISM	**Control:** 496	
Service Providers MUST use the ESP protocol for IPsec connections.			
No: 178	**Source:** ISM	**Control:** 1162	
Service Providers MUST use an encryption product that implements a AACP if they wish to communicate sensitive information over public network infrastructure.			
No: 179	**Source:** ISM, FW	**Control:** 457, FW	
Service Providers MUST use a Common Criteria-evaluated encryption product that has completed a ACE if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.			
No: 180	**Source:** ISM, FW	**Control:** 465, FW	
Service Providers MUST use a Common Criteria-evaluated encryption product that has completed a ACE if they wish to communicate classified or sensitive information over public network infrastructure.			
No: 181	**Source:** ISM	**Control:** 157	
Service Providers communicating sensitive or classified information over public network infrastructure or over infrastructure in unsecured spaces (Zone One security areas) MUST use encryption approved for communicating such information over public network infrastructure.			

7.8 Outsourced Arrangements

No	Source	Control	
No: 182	**Source:** ISM	**Control:** 71	
If information is processed, stored or communicated by a system not under a Service Provider's control, the Service Provider MUST ensure that the non-Service Provider system(s) has appropriate security measures in place to protect the information. The security measures MUST be adequately reflected in the Service Provider's information security documentation, as listed in Section 3.2 of this Guide.			

8. Personnel Controls

8.1 Clearances

No	Source	Control	
No: 183	**Source:** ISM, PSPF	**Control:** 434, PERSEC 1, 4 & 5	
Service Providers MUST ensure that personnel undergo an appropriate employment screening, and where necessary hold an appropriate security clearance according to the requirements in the Australian Government Personnel Security Management Protocol before being granted access to a system.			
No: 184	**Source:** PSPF	**Control:** PERSEC 6	
Service Providers MUST ensure that personnel holding security clearances advise AGSVA of any significant changes in personal circumstances which may impact on their continuing suitability to access security classified resources.			
No: 185	**Source:** ISM, PSPF	**Control:** 435, PERSEC 1	
Service Providers MUST ensure that personnel have received any necessary briefings before being granted access to a system.			

8.2 Training

No	Source	Control	
No: 186	**Source:** ISM, PSPF	**Control:** 251, GOV1 & 9, INFOSEC 3, PHYSEC2	
Service Providers MUST ensure that all personnel who have access to ICT systems have sufficient information awareness and training.			

No	Source	Control	
No: 187	**Source:** ISM, PSPF	**Control:** 252, GOV1 & 9, INFOSEC 3, PHYSEC2	
Service Providers MUST provide ongoing ICT security training and awareness for personnel on information security policies on topics such as responsibilities, consequences of non-compliance, potential security risks and countermeasures.			

8.3 Security Awareness

No	Source	Control	
No: 188	**Source:** ISM, PSPF	**Control:** 413, GOV1, INFOSEC 3 & 5	
Service Providers MUST develop and maintain a set of policies and procedures covering user identification, authentication, roles, responsibilities and authorisations and make users aware of, and understand the policies and procedures.			
No: 189	**Source:** ISM	**Control:** 122	
Service Providers MUST detail cyber security incident responsibilities and procedures for each system in the relevant SSP, SOPs, and IRP.			
No: 190	**Source:** ISM, PSPF	**Control:** 1083, GOV1, INFOSEC 3 & 5	
Service Providers MUST advise personnel of the sensitivities and classifications permitted for data and voice communications when using mobile devices.			

8.4 Staff Responsibilities

No	Source	Control	
No: 191	**Source:** ISM	**Control:** 661	
Service Providers MUST ensure that system users transferring data to and from a system are held accountable for the data they transfer			

Annex A: Non-Compliance Ratings

Severity Rating	Definition
CRITICAL	An IRAP Assessor's determination that the Service Provider does not comply with essential protective security requirements of the Assurance Framework shall be classified as a critical failure. For example, the inappropriate storage of cryptographic keys, digital certificates or passphrases shall be classified as a critical failure. The cessation of Assurance Framework accreditation activities shall occur until such time as the critical non-compliance is addressed.
MAJOR	An IRAP Assessor's determination that the Service Provider does not comply with significant protective security requirements of the Assurance Framework shall be classified as a major failure. For example, a Service Provider does not have sufficient security awareness training programmes or plans in place shall be classified as a major failure. Escalation of the problem to a critical failure shall be imposed if additional related events impact on the Service Provider's operations simultaneously. Unmitigated failures in this category will result in the Assurance Framework Competent Authority not granting accreditation to the Service Provider until such time as the major non-compliance is addressed.
PARTIAL	An IRAP Assessor's determination that the Service Provider does not comply with important protective security requirements of the Assurance Framework shall be classified as a partial failure. For example Standard Operating Procedures not implemented in a manner consistent with the System Security Plan. Escalation of the problem to a major failure shall be imposed if additional related events impact on the Service Provider's operations simultaneously. Unmitigated failures in this category may result in the Assurance Framework Competent Authority granting conditional accreditation to the Service Provider and request the partial non-compliance be remediated within six months from the accreditation date. Once this time limit is reached the area concerned shall be reviewed for compliance.
MINOR	An IRAP Assessor's determination that the Service Provider does not comply with general requirements of the Assurance Framework shall be classified as a minor failure. For example insufficient linkages between Information Security Documentation. Unmitigated failures in this category may result in the Assurance Framework Competent Authority granting conditional accreditation to the Service Provider and request the minor non-compliance be remediated within twelve months from the accreditation date. The area concerned shall be reviewed as part of the annual Assurance Framework compliance audit.

Annex B: Non-Compliance Template

Section:	**{Documentation, Physical, Logical, Personnel} Controls**				
Total Section Controls:	{number}	Compliant controls:	{number}	Non-compliant controls:	{number}
IRAP Assessor's comments					
No	Severity Rating	Comment			
{requirement #}	{As per Annex A}				
{requirement #}	{As per Annex A}				
{requirement #}	{As per Annex A}				