



**Australian Government**  
**Department of Defence**

**Information System Audit**  
**Guide**

**VERSION 11.1**  
**January 2012**

**TABLE OF CONTENTS**

**1. INTRODUCTION TO ACCREDITATION.....4**

**2. THE INFORMATION SYSTEM AUDIT – CHECKLIST .....7**

2.1. WHAT IS AN INFORMATION SYSTEM AUDIT? .....7

2.2. WHY IS AN INFORMATION SYSTEM CERTIFICATION NEEDED?.....7

2.3. ASSESSING AN INFORMATION SYSTEM’S SECURITY RISKS .....7

2.4. SELECTING AN INFORMATION SYSTEM’S SECURITY CONTROLS .....7

**3. PURPOSE OF THE CHECKLIST.....8**

**4. HOW TO USE THE CHECKLIST.....8**

4.1. THE CHECKLIST STRUCTURE .....8

4.2. SECURITY OBJECTIVES.....9

4.3. GUIDANCE FOR IRAP ASSESSORS.....9

4.4. INFORMATION SYSTEM COMPLIANCE ..... 10

**5. GUIDANCE FOR IRAP ASSESSORS.....10**

**6. THE CHECKLIST .....11**

6.1. THE INFORMATION SECURITY POLICY & RISK MANAGEMENT ..... 11

6.2. INFORMATION SECURITY ORGANISATION ..... 14

6.3. INFORMATION SECURITY DOCUMENTATION ..... 17

6.4. INFORMATION SECURITY MONITORING ..... 20

6.5. CYBER SECURITY INCIDENTS ..... 22

6.6. PHYSICAL & ENVIRONMENTAL SECURITY ..... 24

6.7. PERSONNEL SECURITY FOR INFORMATION SYSTEMS ..... 26

6.8. PRODUCT & MEDIA SECURITY ..... 27

6.9. SOFTWARE, NETWORK & CRYPTOGRAPHIC SECURITY ..... 30

6.10. ACCESS CONTROL & WORKING OFF-SITE SECURITY..... 33

**APPENDIX A – ACCREDITATION GOVERNANCE.....36**

THE ISM & CERTIFICATION ..... 36

COMPLIANCE LEVELS..... 37

COMPLIANCE REPORT ..... 37

COMPLIANCE COMMENTS ..... 37

AUDIT DOCUMENTATION SUBMISSIONS ..... 38

**APPENDIX B – STANDARDS .....39**

## **For Additional Information & Assistance**

Point of Contact: IRAP Manager

Phone: 1300 292 371

Email: [assist@dsd.gov.au](mailto:assist@dsd.gov.au)

© Australian Government 2011

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the *Copyright Act 1968*, all other rights are reserved.

## **Assessment Details**

**Agency Name:** \_\_\_\_\_

**Agency ITSA:** \_\_\_\_\_

**IRAP Assessor:** \_\_\_\_\_

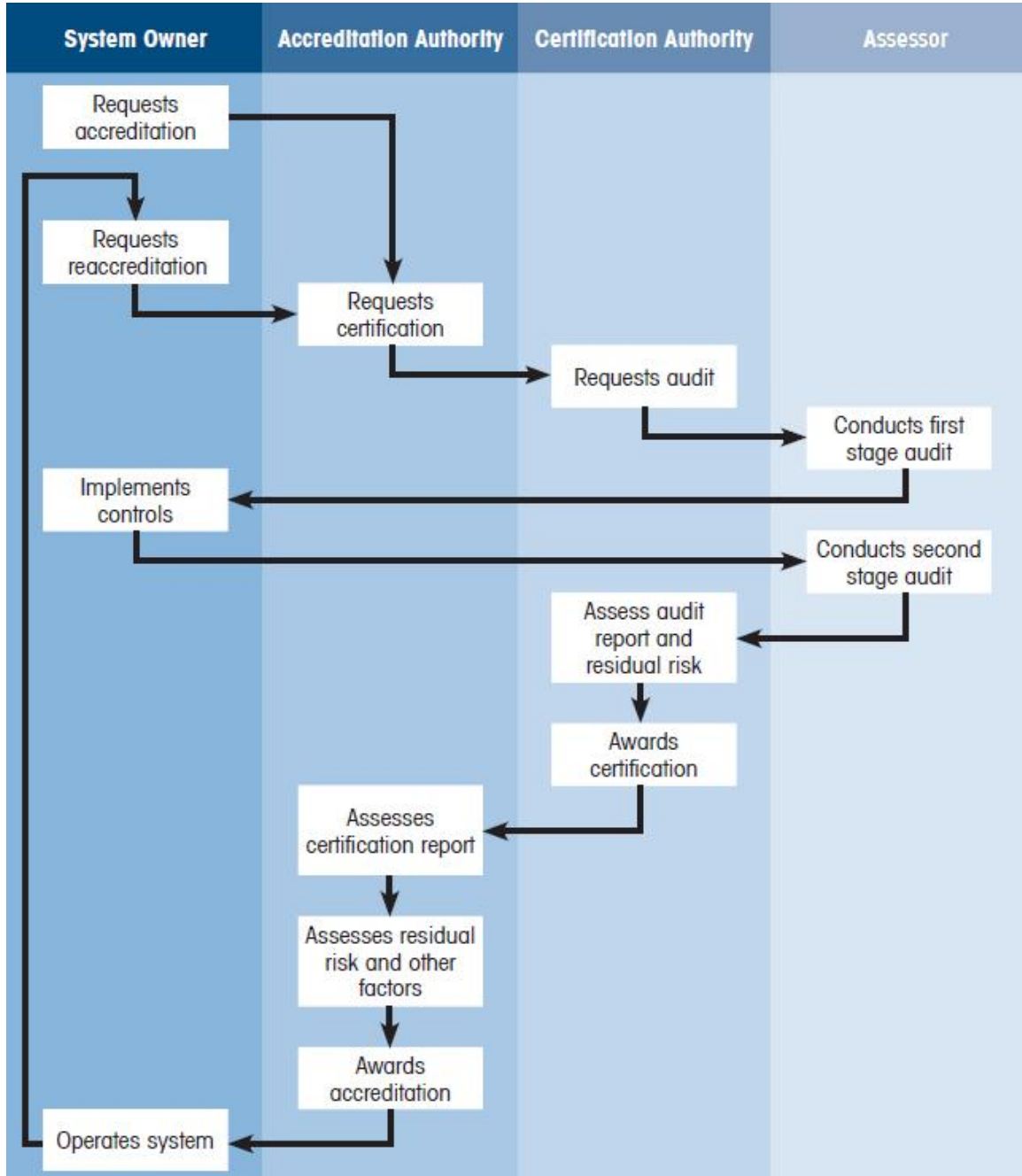
**Date of IRAP Audit:** \_\_\_\_\_

## 1. Introduction to Accreditation

Government Agencies are required under the Protective Security Policy Framework (PSPF) to consider the security of their electronic information systems and to implement safeguards designed to adequately protect these essential systems.

The Defence Signals Directorate regularly issues the Australian Government Information Security Manual (ISM). This manual defines the Australian Government's information security best practices and is designed to provide assistance with information security to State & Federal Government agencies.

An information security audit is conducted as part of the wider accreditation process. The aim of an information security audit is to review the information system architecture (including the information security documentation), assess the actual implementation and effectiveness of controls for a system and to report on any observed operational risks relating to the operation of the system to the certification authority.



The Information System Audit is conducted in two distinct stages. In Stage 1, the Assessor reviews all available documentation to assess the **completeness** and **appropriateness** of the controls selected through the Statement of Applicability and defined in the System Security Plan (SSP).

The second stage of the audit is conducted to assess whether the controls documented in the SSP have been **implemented** and are operating **effectively**.

The Certification Authority will receive the Compliance Report from the Assessor and make a judgement based on the findings of the review to determine if any residual risk is present in the manner in which the controls are operated. The Assessor should provide detailed information regarding the operation of controls if they are found to be ineffective or partially effective to enable the Certification Authority to make this assessment.

A requirement of the ISM is that Agencies **must** obtain accreditation for each of their systems and **must** obtain certification for these systems prior to the awarding of accreditation.

**It should be noted that the certification process does not provide any guarantee that the System or any connected networks cannot or will not be compromised.**

## **2. The Information System Audit – Checklist**

The ISM defines processes and controls to assist agencies with security for all ICT systems. This checklist focuses on the ISM's processes and controls allowing an organisation to concentrate on an individual information system. Controls defined in the SOA that originate from the System Risk Management Plan should be assessed in conjunction with these ISM controls.

### **2.1. What is an Information System Audit?**

The purpose of the information security certification is to determine whether the documented security controls within the SSP, as approved by the system owner and reviewed during the information system architecture review stage, have been implemented and are operating effectively. The outcome of this process is a certificate confirming that the system was certified as being compliant with its SSP. In addition, the controls that are reviewed are wider than those contained in the SSP and extend across the contents of the ISM so a recommendation can be made to the organisation for the system's suitability for being accredited.

### **2.2. Why is Information System Certification needed?**

Obtaining certification for an information system(s) provides an organisation with the needed assurance that their Information systems are compliant with DSD's best practice information security guidelines. The certification process forms part of the system's accreditation as defined in the ISM.

### **2.3. Assessing an Information System's Security Risks**

Security requirements are identified by methodically assessing the security risks faced by the organisation and its' systems. The subsequent implementation of appropriate and measured controls to reduce the potential consequence or likelihood mitigates these risks and reduces the organisations overall risk profile.

### **2.4. Selecting an Information System's Security Controls**

An organisation, having decided to treat a risk, must then select and implement an appropriate control/s to reduce the risk to a level the organisation deems acceptable. The selection of controls should be based on the organisations context and risk profile, and subject to all relevant national and international legislation and regulations.

Not all the controls listed in the ISM will be applicable to every information system. A Statement of Applicability **should** be created and it is **recommended** that it be annexed to the SSP to identify which controls in the ISM and from the SRMP will be applied to the system.

### 3. Purpose of the Checklist

The Information System Audit Checklist is designed to serve as a reference source for the IRAP Assessor. It details the security objectives, an approach to reviewing the security of a system and possible guiding references within the ISM. The checklist identifies the key areas of concern and their context within an information system and the management processes that support it.

It provides a lead for IRAP Assessors who must evaluate an organisation's Information System's components, configuration, architecture, management processes and procedures, based upon the organisational context, their identified risk, their risk appetite and preferred or strategic treatment approach.

It will also allow System Owners to establish the scope, funding and resource requirements prior to undertaking an information system certification. A gap analysis is made possible using the Information System Audit Checklist as a baseline to compare and review existing controls.

### 4. How to Use the Checklist

The Information System Audit Checklist is designed to meet 2 functions:

Provide guidance to IRAP Assessors as to the appropriate audit steps and assist with the evaluation of the ISM security controls that have been implemented.

Provide the implementer with guidance on how information systems will be assessed and to provide context for ISM controls and the certification process.

#### 4.1. The Checklist Structure

As can be seen below, the checklist is structured in line with the ISM and broken into 10 main sections which groups together related security controls under a single heading.

Item	Information System Security Control Processes
6.0	Information Security Policy & Risk Management
	<b>Information Security Governance</b>

Item	Information System Security Control Processes
6.1	Information Security Organisation - Roles & Responsibilities
6.2	Information Security Documentation
6.3	Information Security Monitoring
6.4	Information Security Incidents
	<b>Physical Security</b>
6.5	Physical & Environmental Security
	<b>Personnel Security</b>
6.6	Personnel Security for Information Systems
	<b>Information Technology Security</b>
6.7	Product & Media Security
6.8	Software, Network & Cryptographic Security
6.9	Access Control & Working Off-Site Security

Each section is then broken into subsections, which identifies a system security requirement<sup>1</sup>. The IRAP Assessor must ensure that these “Requirements” are met by the system via compliance with some or all of the ISM controls identified along side the security requirement.

## 4.2. Security Objectives

This component identifies some general security objectives associated with each section. The objectives have been drawn from the ISM and ISO27001:2007 Information Security Management Systems and should only be references as a guide to assist control selection.

Each organisation through their SRMP identifies their security objectives and it is these objectives that the selected controls will need to achieve.

## 4.3. Guidance for IRAP Assessors

This section provides an introductory level of detail as to how the objective(s) may be achieved and guidance as to the selection of available security controls.

---

<sup>1</sup> Within the Checklist under the compliance heading are the Requirements denoted by a reference number and title ie “R1 ICT Security Policy”

It also describes what evidence the IRAP Assessor may look for to confirm that the appropriate controls have been applied and are mitigating risk effectively.

#### **4.4. Information System Compliance**

This section indicates the minimum certification requirements (eg: R1, R2) and allows the IRAP Assessor to indicate compliance and provide appropriate comment. It provides reference(s) to the ISM's pertinent control principles and the relevant security controls as defined in the ISM. For the system to be compliant with the requirement, the implemented controls must address the security objective and have reduced the identified risk to an acceptable level, whilst meeting the organisation's stated goal/s.

### **5. Guidance for IRAP Assessors**

The following assessment guidance is provided to IRAP Assessors:

- In order to verify that procedures discussed within policy documentation are operational, IRAP Assessors **MUST** request a demonstration to see that procedures are in use.
- This checklist's requirements **MUST NOT** be scoped out during a review, unless it is indicated that a specific requirement may not be applicable to a particular system or scenario type.
- The IRAP Assessor **MUST** also verify that threats are identified, assessed and addressed appropriately, and that the stated controls are working to effectively mitigate the risk to an acceptable level.
- As part of the certification process, the IRAP Assessor **MUST** specifically look for adherence to the applicable ISM's standards and identify any gaps and/or inconsistencies.
- IRAP Assessors **MUST** review operational audit trails, action plans, meeting minutes, etc. to demonstrate that sufficient inspection of controls has taken place to evaluate and determine operational effectiveness.

## 6. The Checklist

The following sections, 6.1 to 6.9, form the “Information System Audit Checklist” and if appropriate will need to be completed and submitted by the IRAP Assessor to the IRAP Manager as described in Appendix A.

### 6.1. The Information Security Policy & Risk Management

| [Risk Assessment](#) | [Security Risk Management Plan](#) | [Information Security Policy](#)

#### 6.1.1. Security Objective

##### ***Risk Management***

*A System Owner shall attempt to identify, quantify, analyse and evaluate risks to their information assets. The System Owner will select appropriate risk treatments and plan the implementation of controls designed to reduce the identified risks to a level acceptable to Australian Government.*

##### ***Information Security Policy***

*Information systems & ICT security are built on stable policy foundations, as such; an organisation should establish an Information Security Policy thereby providing the organisation with management direction and support for the secure establishment and operation of Information Systems & ICT infrastructure, along with its management and operational processes and procedures.*

#### 6.1.2. Guidance for IRAP Assessors

Effective Risk Management involves 2 main Tasks:

1. Assessing Risk, which involves:
  - Establishing the objective and context for the risk assessment;
  - Identification of risks based on valid threats and vulnerabilities;
  - Analysis of the risks and their impact; and
  - Evaluation of risk for likelihood and consequence to the organisation.
2. Treating Risk, which involves:
  - Identify the treatment approach (Reduce, Transfer, Avoid, Accept); and
  - If reducing the risk, the selection of effective and appropriate controls.

The IRAP Assessor **MUST** ensure that;

- The System Owner has conducted a Threat & Risk Assessment and developed an SRMP utilising the Defence risk management framework or a suitable Risk methodology;
- The Accreditation Authority has authorised the implementation of the SRMP and the acceptance of all identified residual risk;
- The SRMP may indicate existing controls and their maturity, and if required the selection of any additional controls based on the scope and context of the assessment; and
- The System Owner’s records show that the SRMP has been reviewed and updated at appropriate intervals or following significant events within the organisation, and ensure that appropriate action/s have occurred.

The IRAP Assessor **MUST** review an organisation’s TRA, SRMP, implementation approvals and the organisation’s Risk Management Framework to assess the consistency between the methodology, policies, plans, and procedures.

### 6.1.3. Risk Management Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System’s Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls
<b>R1. Risk Assessment</b>	Effective <input type="checkbox"/>	ITSM	0760.
	Partially Effective <input type="checkbox"/>	ITSO	0777
	Not Effective <input type="checkbox"/>	Identification & Authentication	0413
		Detecting CS Incidents	0121
		Managing CS Incidents	0916
		Product Installation & Configuration	0291
<b>Comments:</b>			
<b>R2. Security Risk Management Plan</b>	Effective <input type="checkbox"/>	CISO	0721, 0726, 0727
	Partially Effective <input type="checkbox"/>	ITSM	0019
	Not Effective <input type="checkbox"/>	System Owners	0040
		Documentation Fundamentals	0788
		Security Risk Management Plans	

**Comments:****6.1.4. Guidance for IRAP Assessors**

A policy document MUST provide and define:

- Scope, objective and context for the particular policy;
- Policy statements which clearly articulate the organisation's intent and/or requirements;
- Processes and procedures that support the policies implementation and operation;
- Roles and responsibilities for the policy's implementation, operation and maintenance;
- Guidance on policy interpretation and external references; and
- Consequences of policy violation, reporting and assistance contacts.

Policy pertaining to information systems may exist at both an Administrative level; comprising high-level statements that describe the systems functional requirements, and at the Operational level; defining the protection required, both technical and procedural, and the implementation of controls for all information systems.

Assessors SHOULD look for realistic policies that have been approved and endorsed at the appropriate management level, which are implemented and enforced as part of the system's operation and management.

**6.1.5. ISP Compliance**

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Principle	ISM Controls
<b>R3. Information Security Policy</b>	Effective <input type="checkbox"/>	Documentation Fundamentals	0039, 0044
	Partially Effective <input type="checkbox"/>	Information Security Policies	0890
	Not Effective <input type="checkbox"/>		

**Comments:**

## 6.2. Information Security Organisation

| Security Management Forum | Chief Information Security Officer | IT Security Adviser | IT Security Manager | IT Security Officer | System Owner | System Users |

### 6.2.1. Security Objectives

1. To ensure the management of information security within the organisation.
2. To define the information security roles and responsibilities for the organisation and the information systems, thereby to assist in ensuring all security issues receive appropriate attention and control.

### 6.2.2. Guidance for IRAP Assessors

The assessor MUST look for evidence of a security management framework, required by the ISM, which actively promotes and supports information security by setting clear and visible direction via the establishment and endorsement of appropriate security roles and responsibilities.

This is achieved by the allocation of specific security tasks and responsibilities to particular roles:

- Agency Head
- Chief Information Security Officer
- Agency Security Adviser
- IT Security Adviser
- IT Security Managers
- IT Security Officers
- System Owners
- System Managers
- System Users
- Other roles as defined in the SSP.

A key role of the ITSMs and System Owners is to collaborate on and ensure the development, implementation, maintenance and endorsement of essential information system security documentation for the system's secure configuration(s), operations and other key components for system certification.

### 6.2.3. Security Organisation Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls & Guidance
<b>R4. Security Management Forum</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	The Agency Head CISO ITSM	0011, 0012 0725 0767
<b>Comments:</b>			
<b>R5. Chief Information Security Officer</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	CISO	0714, 0716, 0719, 0721, 0723 0725, 0728-0730, 0734
<b>Comments:</b>			
<b>R6. IT Security Advisor</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	ITSA	0013
<b>Comments:</b>			
<b>R7. IT Security Manager</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	ITSM	0741, 0016, 0024, 0747-0750, 0023, 0019, 0753, 0754, 0758
<b>Comments:</b>			
<b>R8. IT Security Officer</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	ITSO	0768, 0770-0782
<b>Comments:</b>			
<b>R9. System Owner/s</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	System Owners	0027
<b>Comments:</b>			
<b>R10. System User/s</b>	Effective <input type="checkbox"/>	System Users	0033

**UNCLASSIFIED (RECLASSIFY after first entry)**

Information System Audit Guide

Requirements	Assessment	ISM Reference	ISM Controls & Guidance
	Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>		
<b>Comments:</b>			

**UNCLASSIFIED (RECLASSIFY after first entry)**

## 6.3. Information Security Documentation

| Documentation Framework | Information Security Policy | Security Risk Management Plan | System Security Plan | Standard Operating Procedures | Incident Response Plan | General Controls |

### 6.3.1. Security Objectives

- 1. A documentation framework will assist an organisation to develop ICT security documentation in a manner that allows for easy creation, use, reference and maintenance.*
- 2. Ensuring ICT security documentation is developed by skilled practitioners will assist the organisation to develop a strong ICT security baseline from which systems can be maintained and developed.*

### 6.3.2. Guidance for Assessors

The assessor MUST review the following documentation set to ensure it is appropriate, complete and meets the required standard for certification:

- Information Security Policy;
- Security Risk Management Plan;
- System Security Plan;
- Standard Operating Procedures;
- Incident Response Plan; and
- General controls.

Other documents that may reflect the effective control, development and operations of a system's security are:

- Statement of Applicability (Controls);
- Site Security Plan;
- Procedures detailing proper completion of tasks;
- Logical /Infrastructure Architecture diagram/s;
- List of critical configurations;
- Security Calendar to schedule security related tasks; and
- An established audit programs/schedule (Internal & External).

### 6.3.3. Security Documentation Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls
<b>R11. Documentation Framework</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals	0044, 0786, 0787, 0047, 0885
<b>Comments:</b>			
<b>R12. Information Security Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Information Security Policy	0039 0049
<b>Comments:</b>			
<b>R13. Security Risk Management Plan</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Security Risk Management Plan	0040 0788
<b>Comments:</b>			
<b>R14. System Security Plan</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals System Security Plan Authorisations, Security Clearances & Briefings Conducting Audits	0041 0895, 0067 0432 0800, 0802
<b>Comments:</b>			
<b>R15. Standard Operating Procedures</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Standard Operating Procedures Conducting Audits	0042 0051, 0789, 0790, 0055, 0056 0800
<b>Comments:</b>			
<b>R16. Incident Response Plan</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Incident Response Plans	0043 0058, 0059
<b>Comments:</b>			

**UNCLASSIFIED (RECLASSIFY after first entry)**

**Information System Audit Guide**

Requirements	Assessment	ISM Reference	ISM Controls
<b>R17. General Documentation Controls</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals	0046
		Emergency Procedures	0062
		Conducting Accreditation	0791
		Conducting Audits	0799, 0800
		Product Selection & Acquisition	0282 0313
		Product Sanitisation & Disposal	0322 0348
		Media Handling	0363
		Media Sanitisation	0374
		Media Destruction	0400
		Media Disposal	0413
		Software Development Environments	0580
		Identification & Authentication	0471
		Event logging & Auditing	0510
		Using DACAs	0588
		Key Management	
		Fax Machines & MFDs	
		<b>Comments:</b>	

**UNCLASSIFIED (RECLASSIFY after first entry)**

## 6.4. Information Security Monitoring

Vulnerability Management | Change Management | Business Continuity & Disaster Recovery |

### 6.4.1. Security Objective

To ensure:

1. The agency is responding to the latest risk environment and that systems are configured in accordance with current ICT security documentation.
2. That as new vulnerabilities are identified and published; agencies reassess the information security of their systems.

### 6.4.2. Guidance for Assessors

The Assessor should review the outcomes and associated actions resulting from relevant Information Security Reviews. The results and any remedial actions associated with relevant Vulnerability Assessments and the defined change management process as identified within the System's SSP.

The Assessor MUST review the systems audit program and/or security calendar to ensure that formal reviews are appropriately scheduled and occur as scheduled.

### 6.4.3. Information Security Monitoring Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls
<b>R18.Vulnerability Management</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Vulnerability Analysis	0105, 0112, 0113
<b>Comments:</b>			
<b>R19.Change Management</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Change Management	0115, 0117, 0809
<b>Comments:</b>			

**R20.Business  
Continuity &  
Disaster Recovery**

Compliant   
NON Compliant

BCP & DRP

0118, 0119

**Comments:**

## 6.5. Cyber Security Incidents

| [Detecting Cyber Security Incidents](#) | [Reporting Cyber Security Incidents](#) |  
[Managing Cyber Security Incidents](#) |

### 6.5.1. Security Objective

- 1. The Organisation should act in a timely and co-operative manner to prevent, detect and respond to information security incidents.*
- 2. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents.*

### 6.5.2. Guidance for Assessors

The Assessor MUST review the procedures for the detection and management of security incidents and ensure Incident Response Plans include and identify:

- What is an information security incident and the various types;
- Who should manage the incident at an operational and technical level;
- The training & skills required to assume these roles;
- The authority that has responsibility for the various actions associated with the investigation of the incident;
- Steps to ensure the integrity of evidence;
- Steps to ensure availability of the systems based on criticality; and
- Formal reporting requirements and procedures.

IRPs MUST to be supported by documented operational procedure that are designed to:

- Detect potential security incidents whether accidental or malicious;
- Establish the cause of any incident that does occur;
- Detail responses to incidents based on the type and severity of the individual incident;
- Formal and Internal incident reporting requirements; and
- Documentation to provide recommendations for security enhancements, tracking of the incidents events, reporting and post incident actions undertaken.

The Assessor MUST review all plans and procedures and ensure that the organisation's objectives for incident management are agreed by management and that those

responsible for incident response understand the organisations objectives.

In addition the assessor MUST review incident registers, minute and outcomes of post incident reviews and the attendees and outcomes of testing & training activities.

**Note to R23 & R24:** DSD **RECOMMENDS** that any requests for DSD assistance are made as soon as possible after the incident is detected, and that no actions which may affect the integrity of the evidence are carried out prior to DSD involvement.

CSOC Contact details for reporting incidents are:

Email: assist@dsd.gov.au Phone: 1300 292 371 (24x7)

### 6.5.3. Incident Response Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Principle	ISM Controls
<b>R21. Incident Response &amp; Detection Policy</b>	Effective <input type="checkbox"/>	Documentation Fundamentals	0043
	Partially Effective <input type="checkbox"/>	Detecting CS Incidents	0139-0141, 0918
	Not Effective <input type="checkbox"/>	Intrusion Detection & Prevention	1032
<b>Comments:</b>			
<b>R22. Incident Detection &amp; Response Plan</b>	Effective <input type="checkbox"/>	Incident Response Plans	0058, 0059
	Partially Effective <input type="checkbox"/>	Detecting CS Incidents	1020, 1021
	Not Effective <input type="checkbox"/>	Managing CS Incidents	0122, 0125, 0126, 0916, 0129-0132, 0134-0136
		Intrusion Detection & Prevention	0575, 0578, 0579
<b>Comments:</b>			
<b>R23. Reporting Security Incidents</b>	Effective <input type="checkbox"/>	Reporting CS Incidents	0123, 0124, 0139-0143
	Partially Effective <input type="checkbox"/>	Managing CS Incidents	0133
	Not Effective <input type="checkbox"/>		
<b>Comments:</b>			

## 6.6. Physical & Environmental Security

| Security Environment | Equipment Security |

### 6.6.1. Security Objective

*With the use of physical security and environmental controls a defense-in-depth strategy is implemented thereby ensuring that information and communications technology assets are being adequately protected and controls enforced.*

- 1. To prevent unauthorised damage, access and interference to business premises and information.*
- 2. To prevent loss, damage or compromise of assets and interruption to business activities*
- 3. To prevent compromise of information and information processing facilities*

### 6.6.2. Guidance for Assessors

As part of the information system's security review the assessor will review the system's physical security, the access control(s) at the data centre and control of equipment, networks and peripherals.

The Assessor MUST review and look for evidence of the effective implementation of:

- The Site Security Plans;
- Standard Operating Procedure; and
- Physical Security Controls.

The security pertaining to the equipment associated with the information system and the acquisition, configuration, maintenance and disposal of the physical components.

The Assessor MUST review and seek evidence of:

- The PSPF's Physical protection requirements have been meet appropriately;
- Cabling controls are appropriate for the connected system's classification; and
- The equipment has appropriate maintenance arrangements and controls.

The organisation SHOULD be asked to demonstrate implementation of effective desktop and system configurations policy for the system's classification, and the appropriate information system relocation, repair and disposal controls and procedures are implemented.

### 6.6.3. Physical & Environmental Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls
<b>R24. Environment Security</b>	Effective <input type="checkbox"/>	Agency Security Advisor	0738
	Partially Effective <input type="checkbox"/>	Facilities	0810, 0164, 0919
	Not Effective <input type="checkbox"/>	RF & Infrared Devices	0222, 0223
		Escorting Uncleared Personnel	0167
<b>Comments:</b>			
<b>R25. Equipment Security</b>	Effective <input type="checkbox"/>	Servers & Network Devices	1053, 0812, 0813, 1074, 0150, 0151
	Partially Effective <input type="checkbox"/>	Network Infrastructure	0152, 0156
	Not Effective <input type="checkbox"/>	ICT Equipment	0159, 0160-0163
		Tamper Evident Seals	0174, 0175, 0178-0180
<b>Comments:</b>			

## 6.7. Personnel Security for Information Systems

| Information Security Awareness & Training | Security Clearances and Briefings |

### 6.7.1. Security Objective

*To ensure that system users received appropriate information security training and awareness, thereby assisting with the prevention, detection, and reduction of the impact of information security incidents.*

*To ensure that those accessing systems or secure spaces have appropriate security clearance and access*

### 6.7.2. Guidance for Assessors

An assessor must ensure that an appropriate information security training and awareness policy and programme exists within an agency to ensure that all personnel receive and continue to receive, appropriate exposure to:

- their responsibilities as privileged and/or system users;
- the consequences of non-compliance with organisational policies and controls; and
- the risks and vulnerabilities associated with technologies and social engineering.

### 6.7.3. Personnel Security Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Principle	ISM Controls
<b>R26. Information Security Awareness &amp; Training</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	IS Awareness & Training Using the Internet Email applications	0251-0253, 0255, 0257, 0922 0817, 0819, 0820 0269
<b>Comments:</b>			

**R27. Security Clearances and Briefings**

Effective   
 Partially Effective   
 Not Effective

Security Clearances & Briefings  
 Escorting Uncleared Personnel  
 Using the Internet

0432, 0404, 0405,  
 0435  
 0167  
 0818

**Comments:**

**6.8. Product & Media Security**

| [Security Requirements](#) | [Product Selection](#) | [Operations Management](#) | [Security Devices](#) | [Media Handling and Security](#) | [Asset Identification & Classification](#) | [Asset Labeling and Handling](#) |

**6.8.1. Security Objective**

*To ensure that appropriate product selection and acquisition processes provide the agency with a level of assurance that security risks have been reduced.*

*To ensure that the risk associated with products used outside their recommended configuration is managed appropriately*

*To ensure that information and organisational asset receive an appropriate level of protection, an organisation will need to identify, document, manage and control its information assets effectively.*

**6.8.2. Guidance for Assessors**

The assessor MUST review the design and implementation of the information system and review the system acquisition processes to ensure appropriate EPL products have been sourced.

The assessor MUST review the system design documentation based on the system SRMP and the post implementation review documentation.

The assessor MUST seek evidence in support of vulnerability monitoring of all relevant sources and the actions taken pertaining to any identified vulnerabilities.

The assessor MUST ensure that all system changes are appropriately managed and documented to ensure the maintenance of the systems configuration.

Information assets are the focus of an organisation's policy development and risk management activities; hence the assessor MUST review the appropriate identification, classification and labeling of information assets.

An assessor MUST review the organisation's asset register to ensure appropriate

identification, classification, ownership and controls are in place.

An assessor MUST review the SRMP to ensure the asset is receiving the appropriate level of protection.

**Notes to R35 & R36:** Organisations must use the classification scheme defined in the PSM Part C. and must comply with Physical Security requirements as detailed in the PSM Part E with Non Government organisations obtaining ASIO T4 Physical Security certification.

### 6.8.3. Product & Media Security Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls
<b>R28. Security Requirements</b>	Effective <input type="checkbox"/>	ITSM	0747, 0749, 0750
	Partially Effective <input type="checkbox"/>	Product Selection & Acq'tion	0279
	Not Effective <input type="checkbox"/>	Product Installation & Config	0289
<b>Comments:</b>			
<b>R29. Product Selection</b>	Effective <input type="checkbox"/>	ITSM	0751, 0754, 0755
	Partially Effective <input type="checkbox"/>	Product Selection & Acq'tion	0279, 0280
	Not Effective <input type="checkbox"/>	Product Installation & Config	0289, 0291
<b>Comments:</b>			
<b>R30. Operations Management</b>	Effective <input type="checkbox"/>	Product Selection & Acq'tion	0285, 0287
	Partially Effective <input type="checkbox"/>	Product Patching & Updating	0297, 0298, 0300, 0303, 0304, 0940, 0941, 1143, 1144
	Not Effective <input type="checkbox"/>	Product Maintenance & Repairs	0305-0308, 0310, 0943
		Product Sanitisation & Disposal	0311-0319, 0321, 1076
		Privileged Access	0444, 0445, 0790, 0985, 0709, 0986, 0582
<b>Comments:</b>			
<b>R31. Security Devices</b>	Effective <input type="checkbox"/>		
	Partially Effective <input type="checkbox"/>	Product Selection & Acq'tion	0279
	Not Effective <input type="checkbox"/>		

**UNCLASSIFIED (RECLASSIFY after first entry)**

**Information System Audit Guide**

**Comments:**

<b>R32. Media Handling and Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Media Handling	0323, 0325, 0330-0334
		Media Usage	0337, 0338, 0341-0344, 0831, 0832
		Media Sanitisation	0350-0354, 1065-1068, 0356-0362, 0836, 0838
		Media Destruction	0363-0066, 0368, 1160, 0370-0373, 0839, 0840
		Media Disposal	0374, 0375, 0329, 0378

**Comments:**

<b>R33. Asset Identification &amp; Classification</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Standard Operating Procedures	0790
		Hardware Products	0159
		Product Classifying & Labelling	0293

**Comments:**

<b>R34. Asset Labeling and Handling</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Standard Operating Procedures	0790, 0056 0294
		Product Classifying & Labelling	0395, 0396
		Databases	1022-1024, 0562-0566, 0875
		Email Infrastructure	

**Comments:**

**UNCLASSIFIED (RECLASSIFY after first entry)**

## 6.9. Software, Network & Cryptographic Security

| SOE | Application Usage | Applications Development | Applications & Database Development | Application Processing | Cryptographic Control Policy | Cryptographic Security | Network Security | Exchange of Information and Software |

### 6.9.1. Security Objective

*To ensure that software security fundamentals are based on hardened SOEs and system software to form a configuration baseline.*

*To ensure that access control listings for applications and services provide an appropriate level of control and security and whilst meeting business.*

*To ensure that Users manage and protect the information contained within email.*

*To ensure that secure Database management practice along with software development and testing procedures are employed*

### 6.9.2. Guidance for Assessors

The assessor MUST review the software design and implementation of the information system and review the security requirements identified and agreed within the planning and design phases of information system acquisition processes.

Design details that need to be reviewed include, but are not limited to:

- System and component acquisition and configuration;
- Data management including input and output validation;
- Internal processing controls and storage requirements;
- Access control for system and application authentication and authorisation;
- Message control and integrity;
- Backup and restore requirements; and
- System fault and vulnerability management.

The assessor MUST review the system design documentation based on the system SRMP and the post implementation review documentation. This will ensure that all cryptographic products and controls are implemented and operated appropriately, ensuring that development and testing environments along with the associated network controls mitigate the identified risks.

### 6.9.3. Software, Network & Cryptographic Security Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System's Certification Requirements:

Requirements	Assessment	ISM Reference	ISM Controls
<b>R35. SOE</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Standard Operating Environments Application Whitelisting	0383, 0385, 0953, 0386-0388, 0954 0843-0851, 0955-0957
<b>Comments:</b>			
<b>R36. Application Usage</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Web Browser Applications Email Applications	0958, 0258, 0260-0263, 1149 0967-0273, 0966, 0852, 0278, 0275, 1089
<b>Comments:</b>			
<b>R37. Applications &amp; Database Development</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Software Application Development Databases	0400, 0401 0395-0399
<b>Comments:</b>			
<b>R38. Application Processing</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Standard Operating Environments Software application Development Databases Email Applications Event Logging & Auditing	0385, 0387, 0953 0399 0966-0968, 0271-0273, 0275, 0278, 0852, 1089 0580, 0582, 0986, 0584-0586, 0859,
<b>Comments:</b>			
<b>R39. Cryptographic Control Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Reporting IS Incidents Network Infrastructure	0142, 0143 0157
<b>Comments:</b>			

**UNCLASSIFIED (RECLASSIFY after first entry)**

**Information System Audit Guide**

Requirements	Assessment	ISM Reference	ISM Controls
<b>R40. Cryptographic Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Cryptographic Fundamentals	0453, 0455, 0457, 0460
		DACA DACP SSL and TLS Secure Shell S/MIME OpenPGP Message Format  Internet Protocol Security Key Management	0473-0477, 0469, 0480 0481 0482, 1139 0486-0489, 0997 0490 1091 0496-0498, 0998-1001 0503-0507, 0509, 1003, 1004, 0511
<b>Comments:</b>			
<b>R41. Network Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Network Management	0513-0517, 1007, 1006
		VLANs Wireless LAN  Intrusion Detection & Prevention  Multifunction Devices	0529, 0530, 0533-0535, 1138 0536, 0538-0544, 0860 0575, 0578, 0579, 1031 0589, 0590
<b>Comments:</b>			
<b>R42. Exchange of Information and Software</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Email Infrastructure	0561-0565, 0875, 1022, 0566, 0569-0572, 0574, 0861, 1151, 1152
		Using the Internet  Internet Protocol Telephony	0817-0823, 1146-1148, 0924, 0923, 0266 0267, 0546-0548, 0551-0559, 1014-1018
<b>Comments:</b>			

**UNCLASSIFIED (RECLASSIFY after first entry)**

## 6.10. Access Control & Working Off-site Security

| Business Requirements for Access | User Access Management | User Responsibilities | System Access | Privileged Access | Remote Access | Working Off-Site |

### 6.10.1. Security Objective

*Appropriate system access control will provides protection against unauthorised access through user identification, authorisation and restricting access to only information and functions needed by staff to undertake their duties.*

- 1. To control access to information*
- 2. To ensure authorised access and to prevent unauthorised access to information systems*
- 3. To prevent unauthorised user access, and compromise or theft of information and information processing facilities*
- 4. To prevent unauthorised access to network services, operating systems, information held within applications*

### 6.10.2. Guidance for Assessors

The assessor MUST review the technical and procedural controls of physical and logical access to the various components of information systems and ensure they support the documented policies and procedures.

The assessor MUST seek evidence supporting the implementation of clear and appropriate policy statements, plans and procedures, for:

- Password policy and management controls;
- User access management including privileged and remote access;
- Registration & de-registration requirements and controls;
- User responsibilities, conditions of use and review of user access rights;
- Network, operating system and application access requirements and controls; and
- Mobile computing & teleworking policy, requirements and controls.

Evidence MUST be sought of the organisation's control mechanisms to authenticate users and subsequently provide appropriate authorisation to the systems assets on a

“need to know” basis.

### 6.10.3. Access Control Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and this Information System’s Certification Requirements:

Requirements	Assessment	ISM Principle	ISM Controls
<b>R43. Access Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	System Users Identification & Authentication Authorisation, Security Clearances and Briefings Privileged Access Event Logging & Auditing	0033, 0034 0413, 0420, 0421 0404, 0854, 0855 0446-0448 0580
<b>Comments:</b>			
<b>R44. Business Requirements for Access</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Identification & Authentication Event Logging & Auditing	0417-0419, 0974, 0423, 0424 0853, 0427, 0429, 0430 0580, 0582-0587, 0986-0991, 0859, 0109
<b>Comments:</b>			
<b>R45. User Access Management</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Identification & Authentication Authorisation, Security Clearances and Briefings Remote Access	0414, 0416 0407, 0435 0858, 0706, 0985, 0709
<b>Comments:</b>			
<b>R46. System Access</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Authorisation, Security Clearances and Briefings System Access	0404 0854, 0855
<b>Comments:</b>			
<b>R47. Privileged Access</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Authorisation, Security Clearances and Briefings Privileged Access	0407 0444, 0450-0451, 0982

**Comments:**

<b>R48. User Responsibilities</b>	Effective <input type="checkbox"/>	System Users	0033, 0034
	Partially Effective <input type="checkbox"/>		
	Not Effective <input type="checkbox"/>		

**Comments:**

<b>R49. Working Off-Site</b>	Effective <input type="checkbox"/>	Working Off-site Fundamentals	1047, 0693, 0694
	Partially Effective <input type="checkbox"/>	Working From Home	0865, 0685
	Not Effective <input type="checkbox"/>	Working Outside the Office	0866, 0867, 1050, 0700-0702

**Comments:**

## Appendix A – Accreditation Governance

This Appendix provides general information and guidance on Accreditation requirements. It is provided in this checklist as **audit** is part of the wider accreditation process. It also provides instructions to the IRAP Assessor.

The objective of the ISR Checklist is to assist IRAP Assessors to evaluate an agency's system compliance to the relevant and applicable controls in the ISM

This appendix outlines the “**Accreditation Governance**” as stated in the ISM for the information of assessors and implementers. It also provides detail as to the Assessor's role and associated tasks that must be completed by the assessor as part of the agency's certification and accreditation process.

### The ISM & Certification

The relevant ISM controls pertaining to all systems can be found at:

ISM Clause	Control	Keyword
<b>Certification Administration</b>		
Non Compliance	1060	<b>Required</b>
	0001	<b>Must</b>
	1061	<b>Must</b>
Justification for non-compliance	0710	<b>Must</b>
Consultation on non-compliance	0711	<b>Must</b>
	0712	<b>Must</b>
Notification of non-compliance	0713	<b>Must</b>
Reviewing non-compliance	0876	<b>Recommended</b>
Recording non-compliance	0003	<b>Must</b>
Annual compliance reporting	1062	<b>Must</b>
	1063	<b>Must</b>
Accreditation Framework	0791	<b>Must</b>
Accreditation	0064	<b>Must</b>
	0065	<b>Must</b>
	0086	<b>Should</b>
Accrediting systems bearing caveat or compartment	0077	<b>Must</b>
Reaccreditation	0069	<b>Should</b>
	0070	<b>Must</b>
Certification	0795	<b>Must</b>
Accreditation decision	0808	<b>Must</b>

ISM Clause	Control	Keyword
Conducting Certification	1141, 1142, 0807, 0100	<b>Must &amp; Should</b>
Conducting Audits	0902, 0797, 0798, 0799, 0800, 0802, 0904, 0084, 0805, 0806, 0905, 1140,	<b>Must</b>

## Compliance Levels

The identification, implementation, operation and maintenance of effective security controls, designed to mitigate identified risks, is the ultimate objective. Failing to achieve this may result in non-compliance for individual controls. Assessors are referred to pages 1 through 6 for definitions of keyword compliance requirements.

The non-applicability of controls or non-compliance with controls **MUST** be identified within the Compliance Report.

Controls are to be assessed as being Effective, meaning the controls have been fully implemented and are operating as designed.

If the controls has not been implemented or are implemented in a manner that renders the control ineffective, then the Assessor **MUST** find this control as Not Effective.

In certain circumstances, controls can be implemented however its effectiveness is not complete due to operational limitations. The IRAP Assessor may choose to assess this as Partially Effective. Supporting comment will provide the Certification Authority with background information to assess whether there is operational residual risk which may cause the system to be not certified, or to be reported through to the Accreditation Authority as having identified Operational Residual Risk.

## Compliance Report

A compliance report based on the “Requirements” components as detailed in this document **MUST** be provided.

The compliance report **MUST** include signoff by the Assessor.

The compliance report **MUST** provide any recommendations based on non-mandatory best practice guidelines that have not been demonstrated.

## Compliance Comments

IRAP Assessors **MUST** provide their comments against individual requirements in the certification report

IRAP Assessors **MUST** comment on ALL applicable requirements within the checklist.

Comments **MUST** provide details of how well each requirement has been implemented and whether the control is effective.

### **Audit Documentation Submissions**

IRAP Assessors **MUST** forward the audit report to the IRAP Manager once an audit is completed.

The IRAP Manager's details are as follows:

IRAP Manager  
C/o Melissa Osborne  
Information Security Operations Branch  
Defence Signals Directorate  
PO Box 5076  
Kingston ACT 2604

## Appendix B – Standards

Australian Government Information Security Manual, December 2010 **ISM**

Australian Government Protective Security Policy Framework, 2010 **PSPF**

Department of Defence, Defence Security Manual, **eDSM**

AS/NZ ISO/IEC 27001:2007 **Information Technology – Security Techniques - Information Security Management Systems Requirements**

AS/NZ ISO/IEC 27002:2006 **Information Technology – Security Techniques – Code of practice for Information Security Management**

AS/NZ ISO 31000:2009 **Risk Management – Principles and Guidelines**