



Australian Government
Department of Defence
Defence Signals Directorate



**Gateway/Cross Domain Solution Audit
Guide**

VERSION 10
August 2011

Table of Contents

TABLE OF CONTENTS	2
1. INTRODUCTION TO CERTIFICATION	4
2. THE GATEWAY CERTIFICATION CHECKLIST	5
2.1. WHAT IS A GATEWAY CERTIFICATION?	5
2.2. WHY IS A GATEWAY CERTIFICATION NEEDED?	5
2.3. ASSESSING GATEWAY SECURITY RISKS	5
2.4. SELECTING GATEWAY SECURITY CONTROLS	5
3. PURPOSE OF THIS CHECKLIST	6
4. HOW TO USE THE GATEWAY AUDIT CHECKLIST	6
4.1. THE GATEWAY AUDIT CHECKLIST STRUCTURE	6
4.2. SECURITY OBJECTIVES	7
4.3. GUIDANCE FOR ASSESSORS	7
4.4. GATEWAY COMPLIANCE	7
5. GUIDANCE FOR ASSESSORS	7
6. GATEWAY CERTIFICATION PROCESS	8
7. THE GATEWAY AUDIT CHECKLIST	10
7.1. GATEWAY RISK ASSESSMENT	10
7.2. GATEWAY POLICY FRAMEWORK	12
7.3. GATEWAY DESIGN METHODOLOGY	15
7.4. GATEWAY SECURITY MANAGEMENT	19
8. APPENDIX A – COMMERCIAL GATEWAY CERTIFICATION	23
9. APPENDIX B – STANDARDS	24
10. APPENDIX C – SECURITY REQUIREMENTS SUMMARY	25

For Additional Information & Assistance

Point of Contact: DSD Assist

Phone: (02) 6265 0197

Email: 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

Organisation:

Gateway Name:

Contact:

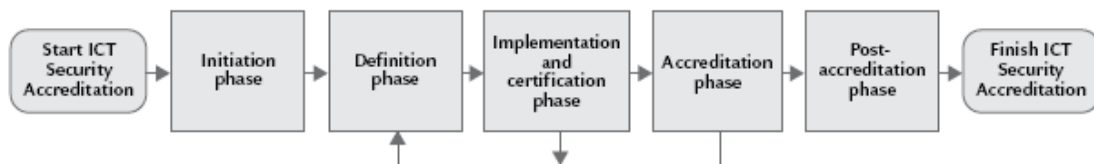
Assessor:

1. Introduction to Certification

Australian Government agencies are required by 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 (DSD) 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 and associated organisations.

The ISM provides an organisation with a blue print for the establishment of an information security management system (ISMS). An information security assessment is conducted as part of the wider accreditation process. The aim of an information security assessment is to review the information system architecture (including the information security documentation), assess the actual implementation and effectiveness of controls for a system (an information security certification) and to report on any residual security risks relating to the operation of the system to the accreditation authority.



The implementation of system controls, as outlined in the System Security Plan (SSP), must be certified by the assessor to determine whether they have been implemented and are operating effectively.

The ISM requires that all agencies must obtain information security accreditation for each of their systems prior to being put into operation.

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

2. The Gateway Certification Checklist

The Cyber and Information Security Division of DSD has identified a continuing need for perimeter security or gateway protection in addition to effective and appropriate internal security controls. This protection is essential when an organisation connects to an untrusted network such as the internet or a partner organisation.

DSD's 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 individual gateway infrastructure.

2.1. What is Gateway Certification?

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 often 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 Gateway Certification needed?

Obtaining certification for its information system(s) provides an organisation with the 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 Gateway 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 Gateway 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.

3. Purpose of this Checklist

The Gateway Audit Checklist is designed to serve as a reference source for the implementer; it details the security objectives, an approach to securing a gateway and guiding references to the ISM. The checklist also identifies the areas of concern and their context within a gateway infrastructure and the management processes that support it.

It provides a lead for assessors who must evaluate an organisations gateway architecture, infrastructure and management processes and procedures, based upon the organisations context, their identified risk, their risk appetite and preferred or strategic treatment approach.

It will also allow organisations to establish the scope, funding and resource requirements prior to undertaking a gateway certification. A gap analysis is made possible using the checklist as a baseline to compare existing controls and additional measures against.

4. How to Use the Gateway Audit Checklist

The checklist is designed to meet 2 functions:

1. To provide guidance to assessors as to the appropriate audit steps and assist with the evaluation of the ISM security controls that have been implemented; and
2. To 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 Gateway Audit Checklist Structure

The checklist is structured in line with the ISM and is broken down into 4 main sections designed to demonstrate the gateway development process:

Item	Gateway Security Control Processes
7.1	Risk Assessment - Ascertain organisational risks
7.2	Policy Framework - Ensure policy addresses organisational risk
7.3	Design Methodology - Ensure technical design and controls implement policy
7.4	Security Management - Ensure solution operation supports control design

Each section is then broken into subsections, each assisting the assessor with the specific requirements for each phase. The assessor must ensure that these “requirements” are met by the gateway that is being reviewed.

4.2. Security Objectives

This component identifies some general security objectives associated with each section. The objectives have been drawn from the ISM with some reference to AU/NZS ISO27001:2006 Information Security Management Systems.

In observing the requirements of the ISM, each organisation through their Security Risk Management Plan (SRMP) identifies their own security objectives and it is these objectives that the selected controls will need to achieve.

4.3. Guidance for 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.

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

4.4. Gateway Compliance

This indicates the minimum certification requirements (eg: R1, R2) and allows the assessor to indicate compliance and provide appropriate comment. It provides reference(s) to the 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 Assessors

The following assessment guidance is provided to assessors:

- To recommend certification, an assessor must verify consistency between the controls implemented for the gateway under review and the organisations policies, plans, and procedures. In order to verify that procedures detailed within policy documentation are operational, assessors should request the organisation’s IT Security Advisor (ITSA), IT Security Manager (ITSM), or an authorised delegate to demonstrate that procedures are in use.
- This checklist’s requirements must not be scoped out during a review, unless it is demonstrated that a specific requirement may not be applicable to a particular system or scenario type.

- The titles of the documents given in this guide are guidelines only; individual organisations may title their policy and documents to best meet the organisation's needs. To assist the certification process, DSD recommends that a document matrix provide a mapping between the titles given in this document and the titles used by the organisation be available to assist during certification.
- The assessor needs to 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 audit process, the assessor needs to specifically look for adherence to the ISM's minimum standards and identify any gaps and/or inconsistencies. This is achieved by mapping the results of the risk assessment to the design and operation of the information system, and the establishment of realistic and achievable policies, plans and procedures.
- Assessors shall 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.
- Awarding assessment ratings:
 - Effective: The essential elements of the requirement have been satisfied. The relevant controls from the SSP and ISM have been implemented and will achieve the results intended.
 - Partially Effective: All relevant controls have not been implemented, or implemented in such a way that the intended results are only partly achieved, or the available evidence only permits a partial assessment to be made.
 - Not Effective: Significant controls have not been implemented, or implemented in such a way that the intended results are not achieved, or the necessary assessment evidence could not be observed.

Comments: Comments are required in support of ratings to highlight noteworthy observations – either positive or negative – and to highlight areas for future assessment continuity.

6. Gateway Certification Process

The ISM provides detail on the certification process. The table below indicates the review process and the content or evidence that the assessor will be expecting to find.

Stages	Reviewing	Verifying
1	ICT Security Policy	Policies have been developed or identified by the agency to protect its ICT assets
2	SRMP	That the SRMP is in accordance with the ICT Security requirements and the comprehensiveness and appropriateness of the identified controls.
3	Design Documentation	The documents have been developed and meet ICT security requirements. Design documents used for audit can include the: <ul style="list-style-type: none"> • logical/infrastructure diagram; • concept of operations; • list of mandatory requirements; • risk based requirements; and • list of critical configurations.
4	SSPs and SOPs	That the ICT security documents meet the ICT security requirements and include: <ul style="list-style-type: none"> • security administrative tasks; • proactive security checking tasks; • proactive security auditing tasks; and • a contingency plan.
5	Current System Configuration	The configuration checking of critical components and the tools in use meet the requirements and are functional.

7. The Gateway Audit Checklist

The following sections, 7.1 to 7.4, form the “Gateway Audit Checklist” and will need to be completed and submitted by the assessor to DSD as described in Appendix A.

7.1. Gateway Risk Assessment

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

7.1.1. Security Objective

An organisation shall attempt to identify, quantify, analyse and evaluate risks to their gateway and the information assets it protects. The organisation will select appropriate risk treatments and plan the implementation of controls, designed to reduce the identified risks to a level acceptable to the organisation.

7.1.2. Guidance for Assessors

Effective Risk Management involves two main tasks:

1. Assessing risk, which involves:
 - establishing the objective and context for the risk assessment;
 - identifying risks based on valid threats and vulnerabilities; and
 - analysing risks including their likelihood and consequences.
2. Treating risk, which involves:
 - identifying the treatment approach (reduce, transfer, avoid, accept); and
 - if reducing the risk, selecting effective and appropriate controls.

These tasks take the path described below:

- The organisation shall conduct a Threat & Risk Assessment (TRA) and develop a SRMP utilising their organisation’s risk management framework or methodology;
- The organisation’s management shall authorise 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
- An organisation’s management records will 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.

An assessor shall review an organisation’s TRA, SRMP, implementation approvals



7.2. Gateway Policy Framework

| [Information Security Policy](#) | [Access Policy](#) | [Remote Access Policy](#) | [Cryptographic Control Policy](#) | [Contingency Policy](#) | [Incident Detection and Response Policy](#) |

7.2.1. Security Objective

Information & ICT security are built on stable policy foundations. An organisation should establish a policy framework which provides management direction and support for the establishment and operation of ICT infrastructure, along with its management and operational processes and procedures.

The policies need to reflect business objectives and be appropriately authorised, endorsed, implemented, enforced and maintained at all levels of the organisation and thereby minimise the risk of system compromise or failure and the subsequent loss of information confidentiality, integrity and availability.

7.2.2. Guidance for Assessors

A policy document should as a minimum provide and define:

- scope, objective and context for the particular policy;
- policy statements which clearly articulate the organisations 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;
- give guidance on interpretation and external references; and
- consequences of policy violation, reporting and assistance contacts.

Gateway policy may exist at both an administrative level; comprising high-level statements that describe the gateway's functional requirements, and at the operational level; defining the protection required, both technical and procedural, and the implementation of controls for the gateway.

Assessors undertaking an audit of the gateway shall look for realistic policies at each level that are implemented and enforced as part of the gateway's operation and management.

Policy at all levels should be approved and endorsed by management. Management

should assign security roles and co-ordinate and review the implementation of security for the gateway in line with all other systems and functions.

Notes to R3 & R4: Organisations must use the classification scheme defined in the PSPF Section 5.2 and must comply with physical security requirements as details in the PSPF Section 6 with Non Government organisations obtaining ASIO T4 Physical Security certification.

Note to R7: The PSPF section 4.11 requires organisations to determine availability requirements for their systems.

Note to R8: A security incident, in ICT Terms, is an event that impacts on the confidentiality, integrity and availability of a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction.

7.2.3. Gateway Policy Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the security objective and gateway certification requirements:

Requirements	Assessment	ISM Chapter	ISM Controls
R3. Information Security Policy	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals	39-44, 46-48, 786-787, 1153-1154
Comments:			
R4. Access Policy	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	System Users Identification & Authentication Authorisations, Security Clearances & Briefings Privileged Access Event Logging & Auditing Gateways	33-34, 406 413-431, 853, 976 404, 407, 432, 434-435, 440-443 444-448, 450 109, 580, 585-586 628-629, 631, 634-635, 637, 598, 605, 607-613, 616-617, 619-620, 622, 624
Comments:			
R5. Remote Access Policy	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Secure Shell Remote Access	484-489 706, 709, 858
Comments:			

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

R6. Cryptographic Control Policy

Effective
Partially Effective
Not Effective

Reporting Cyber Security Incidents
Network Infrastructure
Product Patching & Updating

123-124, 139-143
152, 156-157
297-298, 300, 303-304, 940-941, 1143-1144

Comments:

R7. Contingency Policy

Effective
Partially Effective
Not Effective

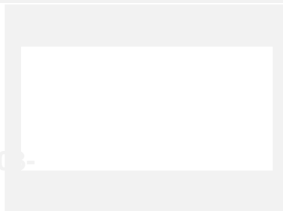
Business Continuity and Disaster Recovery

118-119

Comments:

R8. Incident Detection and Response Policy

PoliT740t20 -



7.3. Gateway Design Methodology

[| Gateway Major Components](#) | [Gateway Components](#) | [Asset Identification and Classification](#) | [Network Security](#) | [Critical Security Configuration](#) | [Risk Based Security Criteria](#) | [Cryptographic Security](#) |

7.3.1. Security Objective

Gateway design must ensure that identified risks to the gateway and the information assets it protects, are treated in accordance with the SRMP and based on approved administrative and operational policy.

An organisation's gateway design should reflect a close association between risk management, organisational policy and security control selection.

Effective system planning will assist in minimising the risk of system compromise or failure and the subsequent loss of information confidentiality, integrity and availability.

7.3.2. Guidance for Assessors

The design of the gateway and its components is a critical process in ensuring the security of those services offered as part of the gateway implementation, and to those networks being protected by the gateway.

The environments surrounding gateways differ between organisations. For this reason, organisations need to consider additional requirements identified in the SRMP for their gateway design.

The design considerations should include:

- operational business requirements of the organisation
- organisational culture and policy at all levels
- existing network design and technical service configuration
- skill sets of system managers, administrators and users
- proscribing best practices and their implementation
- industry hardening guides for software & hardware
- security considerations such as data classification, privacy, ecommerce, etc
- product capability, selection and availability requirements for:
 - firewalls
 - routers
 - IDS & IPS

- encryption
- VPN services
- virus control.

The documentation needed to support the gateway design should include:

- policy directives
- network diagrams
- system configuration
- critical configuration lists
- SSPs
- input to the Site Security Plans
- security calendar
- gateway components administration and operation guides.

Once the service and technical designs and configurations have been developed and approved, they need be managed via formal change, configuration and release management practices.

Assessors shall look for a close correlation between the SRMP, the gateway design/implementation and control selection, including procedural and policy controls.

Prior to undertaking the certification stage assessors need to satisfy themselves that the supporting documentation is complete and sufficient to meet the organisation's needs. In addition they need to determine if the documentation is a true and current representation of the gateway's design and that the supporting administrative and operational processes and procedures are in place and effective.

Note to R14: DSD **RECOMMENDS** that services hosted in the gateway be determined by business requirements and the TRA. Subject to the SRMP, the following are examples of common services that may need to be protected by application level security measures:

- DNS: Name server on the DMZ with no knowledge of the organisation's internal network addresses
- NTP: NTP server will synchronise with a trusted time source regularly and be the central source of time for the environment
- Email: Only known required file types will be permitted through the gateway. Determining file types will not rely on file extension alone; and
- Web: Potentially malicious active content will be blocked.

7.3.3. Gateway Design Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and Gateway Certification Requirements:

Requirements	Assessment	ISM Chapter	ISM Controls
R9. Gateway Major Components	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	ITSM	742-743, 745-767, 19, 23, 24
		Product Selection & Acquisition	279-280, 282-287, 463-464
		Product Installation & Configuration	289-292
		Product Patching & Updating	297-298, 300, 303-304, 940-941, 1143-1144
		Industry Engagement and Outsourcing	744
Comments:			
R10. Gateway Components	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Gateways	628-629, 631, 634-635, 637, 598, 605, 607-613, 616-617, 619-620, 622, 624
		Data Import & Export	667, 1077, 1156
		Content Filtering	649, 652
		Firewalls	638-639, 641-642
		Diodes	643, 645-648 1157-1158
Comments:			
R11. Asset Identification and Classification	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Standard Operating Procedures	51, 55-57, 789-790
		Servers and Network Devices	150-151, 1053
		Network Infrastructure	153, 156-157
		ICT Equipment	159-163
		Product Classifying & Labelling	293-296
Comments:			
R12. Network Security	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Network Management	513-517, 1006-1008
		VLANs	530, 533, 535, 1138
		Wireless LAN	536, 539-544, 1010-1013, 1081
		Intrusion Detection & Prevention	575, 577-579
		Fax Machines & MFDs	241, 244, 588-590, 1036, 1075, 1092
Comments:			

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

R13. Critical Security Configuration

- Effective
- Partially Effective
- Not Effective

Documentation Fundamentals	39-44, 46-48, 786-787, 1153-1154
Security Risk Management Plans	9, 788
System Security Plans	895, 67
Authorisations, Security Clearances & Briefings	432, 434-435, 440-443, 404, 407, 816

Comments:

R14. Risk Based Security Criteria

- Effective
- Partially Effective
- Not Effective

Servers and Network Devices	150-151, 1053
Product Selection & Acquisition	279-280, 282-287, 463-464
Standard Operating Environments	380-383, 385-388, 1033, 953-954

Comments:

R15. Cryptographic Security

- Effective
- Partially Effective
- Not Effective

Web Applications	263
Cryptographic Fundamentals	453, 455, 457, 459, 462, 465, 469, 1080, 1150, 1161-1162
DACA	471-477, 479-480, 994, 1054
DACP	481
SSL and TLS	482, 1139
Secure Shell	484-489, 997
S/MIME	490
OpenPGP Message Format	1091
Internet Protocol Security	494-498, 998-1001
Key Management	499-507, 509-511, 1002-1005

Comments:

UNCLASSIFIED (RECLASSIFY after first entry)

7.4. Gateway Security Management

| [Proactive Security Audits](#) | [Data Import & Export](#) | [Media Handling & Security](#) | [Security Administration Tasks](#) | [Change Management](#) | [Business Continuity and Disaster Recovery](#) | [Incident & Intrusion Detection and Response Plan](#) | [Reporting Security Incidents](#) | [General Documentation Controls](#) |

7.4.1. Security Objective

To ensure the correct and secure operation of information processing services and facilities.

The administration and operation of a gateway infrastructure and the services it provides are often key controls within a secure gateway environment, therefore comprehensive operating processes and procedures need to be developed and documented.

A documented procedure is one that is established, documented, implemented and maintained.

7.4.2. Guidance for Assessors

The ongoing security of a gateway is based on its administration, operation and maintenance. To ensure that all administrative activities are completed appropriately, it is essential to provide personnel with documented procedures identifying their roles and responsibilities within the overall operation of the gateway. Assessors will be looking for evidence that all documentation is being followed.

As a minimum standard the gateway will need:

- Standard Operating Procedures (SOPs) for the:
 - ITSM
 - ITSO
 - System Administrator
 - System Users
- a SSP to ensure alignment between SRMP, ICTSP and the gateway's operation
- a Site Security Plan to ensure all physical security task and measures are implemented and maintained.

Other specific documentation that is essential for effective operations of a gateway is;

- work instruction or procedures detailing proper completion of tasks
- incident detection strategy

- incident response plans and procedures
- security calendar to schedule periodic security related tasks
- an audit program (internal & external).

In addition to the above documentation the assessor will be looking for the gateway to be included in normal service delivery practices such as change and configuration management, capacity planning, incident and problem management all of which enables efficient, effective and secure service delivery management.

The assessor will also look to ensure that the documentation is accessible for all that need it and is reviewed and updated regularly or when changes to the gateway occur.

Many technical implementations are supported by service delivery functions such as a number of the ITIL practices. The assessor may also review key service components including the change and configuration management documentation along with incident and problem management records.

Note to R22 & R23: 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.

Contact details for reporting incidents to DSD are:

Email: incidents_@_dsd.gov.au Phone: 02 6266 0009 (24x7)

7.4.3. Gateway Security Management Compliance

The organisation has demonstrated effective implementation of appropriate processes and procedures, as listed below, to meet the Security Objective and Gateway Certification Requirements:

Requirements	Assessment	ISM Chapter	ISM Controls
R16. Proactive Security Audits	Effective <input type="checkbox"/>	Standard Operating Environments	386, 954
	Partially Effective <input type="checkbox"/>	Privileged Access	444, 446-448, 450, 982, 984
	Not Effective <input type="checkbox"/>	Event Logging & Auditing	580, 585-586, 859, 109
Comments:			

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

R17. Data Import & Export	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Data Import & Export	667, 1077, 1156
Comments:			
R18. Media Handling & Security	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Media Handling Media Usage Media Sanitisation Media Destruction Media Disposal	322-323, 325, 330-334 337-338, 341-344, 347, 831-832 348, 350-354, 356-360, 1065-1068 361-366, 368, 370-373, 838-840, 1160 374-375, 378, 329
Comments:			
R19. Security Administration Tasks	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	ITSM ITSO System Owners System Users Documentation Fundamentals Standard Operating Procedures Email Infrastructure Vulnerability Management Information Security Awareness & Training Event Logging & Auditing Industry Engagement and Outsourcing	742-743, 745-767, 19, 23, 24 108, 768-785 27-28, 1071-1072 33-34, 406 39-44, 46-48, 786-787, 1153-1154 51, 55-57, 789-790 568 911, 105, 909, 112-113 251-253, 255, 257, 922 109, 580, 585-586, 859 744
Comments:			
R20. Change Management	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Change Management	115, 117, 912, 809
Comments:			
R21. Business Continuity and Disaster Recovery	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Business Continuity and Disaster Recovery	118-119, 913-914

UNCLASSIFIED (RECLASSIFY after first entry)

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

Comments:

R22. Incident & Intrusion Detection and Response Plan	Effective <input type="checkbox"/>	Documentation Fundamentals	43
	Partially Effective <input type="checkbox"/>	Incident Response Plans	58-59
	Not Effective <input type="checkbox"/>	Detecting Cyber Security Incidents	120-121
		Managing Cyber Security Incidents	122, 125-126, 129-138
		Intrusion Detection & Prevention	575-579

Comments:

R23. Reporting Security Incidents	Effective <input type="checkbox"/>	Managing Cyber Security Incidents	122, 125-126, 129-138
	Partially Effective <input type="checkbox"/>	Reporting Cyber Security Incidents	123-124, 139-143
	Not Effective <input type="checkbox"/>		

8. Appendix A – Commercial Gateway Certification

The objective of the Gateway/CDS Audit Guide is to assist IRAP Assessors to evaluate a gateway configuration and to recommend certification. There are also accreditation requirements that are relevant to both “system” and “gateway”. If you require a copy of the Information System Audit Guide please contact the IRAP Manager.

A commercially provided gateway providing services to multiple entities including a government agency, classified up to SECRET can be assessed for compliance by an information security registered assessor and certified by DSD.

Recertification: This should be undertaken on all certified gateway systems every 12 months, and also at initiation of a major change that could alter the integrity of the security of the gateway.

The audit report must include signoff by the assessed organisation. The statement must stipulate that, to the best of the ITSA/ITSM’s knowledge, the assessor who has signed the certification report has actively participated in conducting the assessment work leading to certification.

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

IRAP assessors **MUST** contact the DSD IRAP Manager and forward the audit report once an assessment is complete. This will instigate certification activities by DSD, which will result in a Statement of Compliance letter. The DSD IRAP Manager’s details are as follows:

I-RAP Manager
C/O Melissa Osborne
Information Security Operations
Defence Signals Directorate
PO BOX 5076
KINGSTON ACT 2604

9. Appendix B – Standards

Australia Government Information Security Manual ISM 2010 (release August 2011)

Protective Security Policy Framework PSPF January 2010

AS/NZ ISO/IEC 27001:2006 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/IEC 27005 Information Security Risk Management

AS/NZ HB4360:2004 Risk Management Guidelines

10. Appendix C – Security Requirements Summary

Requirements	Assessment	ISM Chapter	ISM Controls
R1. Security Risk Assessment	Effective <input type="checkbox"/>	ITSM	741-743, 745-767, 19, 23, 24
	Partially Effective <input type="checkbox"/>	ASA	737,738
	Not Effective <input type="checkbox"/>	ITSO	108, 768-785
		Identification & Authentication	413-431, 853, 976
		Detecting Cyber Security Incidents	120-121
		Managing Cyber Security Incidents	122, 125-126, 129-138
		Reporting Cyber Security Incidents	123-124
		Product Patching & Updating	297-298, 300, 303-304, 940-941, 1143-1144
		Gateways	628-629, 631, 634-635, 637, 598, 605, 607-613, 616-617, 619-620, 622, 624
		Industry Engagement and Outsourcing	744
R2. Security Risk Management Plan	Effective <input type="checkbox"/>	CISO	714-736, 1064
	Partially Effective <input type="checkbox"/>	ITSA	739, 740
	Not Effective <input type="checkbox"/>	ITSM	741-743, 745-767, 19, 23, 24
		System Owners	27-28, 1071-1072
		Documentation Fundamentals	39-44, 46-48, 786-787, 1153-1154
		Security Risk Management Plans	9, 788
R3. Information Security Policy	Effective <input type="checkbox"/>	Documentation Fundamentals	744
	Partially Effective <input type="checkbox"/>		39-44, 46-48, 786-787, 1153-1154
R4. Access Policy	Not Effective <input type="checkbox"/>		
	Effective <input type="checkbox"/>	System Users	33-34, 406
	Partially Effective <input type="checkbox"/>	Identification & Authentication	413-431, 853, 976
R5. Remote Access Policy	Not Effective <input type="checkbox"/>	Authorisations, Security Clearances & Briefings	404, 407, 432, 434-435, 440-443
		Privileged Access	444-448, 450
		Event Logging & Auditing	109, 580, 585-586
		Gateways	628-629, 631, 634-635, 637, 598, 605, 607-613, 616-617, 619-620, 622, 624
	Effective <input type="checkbox"/>	Secure Shell	484-489
	Partially Effective <input type="checkbox"/>	Remote Access	706, 709, 858
Not Effective <input type="checkbox"/>			

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

R6. Cryptographic Control Policy

- Effective
 Partially Effective
 Not Effective

Reporting Cyber Security Incidents 123-124, 139-143
 Network Infrastructure 152, 156-157
 Product Patching & Updating 297-298, 300, 303-304, 940-941, 1143-1144

R7. Contingency Policy

- Effective
 Partially Effective
 Not Effective

Business Continuity and Disaster Recovery 118-119

R8. Incident Detection & Response Policy

- Effective
 Partially Effective
 Not Effective

Documentation Fundamentals 39-44, 46-48, 1153-1154
 Detecting Cyber Security Incidents 120-121
 Managing Cyber Security Incidents 122, 125-126, 129-138
 Intrusion Detection & Prevention 575, 577-579

R9. Gateway Major Components

- Effective
 Partially Effective
 Not Effective

ITSM 742-743, 745-767, 19, 23, 24
 Product Selection & Acquisition 279-280, 282-287, 463-464
 Product Installation & Configuration 289-292
 Product Patching & Updating 297-298, 300, 303-304, 940-941, 1143-1144
 Industry Engagement and Outsourcing 744

R10. Gateway Components

- Effective
 Partially Effective
 Not Effective

Gateways 628-629, 631, 634-635, 637, 598, 605, 607-613, 616-617, 619-620, 622, 624
 Data Import & Export 667, 1077, 1156
 Content Filtering 649, 652
 Firewalls 638-639, 641-642
 Diodes 643, 645-648 1157-1158

R11. Asset Identification & Classification

- Effective
 Partially Effective
 Not Effective

Standard Operating Procedures 51, 55-57, 789-790
 Servers and Network Devices 150-151, 1053
 Network Infrastructure 153, 156-157
 ICT Equipment 159-163
 Product Classifying & Labelling 293-296

R12. Network Security

- Effective
 Partially Effective
 Not Effective

Network Management 513-517, 1006-1008
 VLANs 530, 533, 535, 1138
 Wireless LAN 536, 539-544, 1010-1013, 1081
 Intrusion Detection & Prevention 575, 577-579
 Fax Machines and MFDs 241,244,588-590, 1036, 1075, 1092

R13. Critical Security Configuration

- Effective
 Partially Effective
 Not Effective

Documentation Fundamentals 39-44, 46-48, 786-787, 1153-1154
 Security Risk Management Plans 9, 788
 System Security Plans 895, 67
 Authorisations, Security Clearances 432, 434-435, 440-443,

UNCLASSIFIED (RECLASSIFY after first entry)

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

		& Briefings	404, 407, 816
R14. Risk Based Security Criteria	Effective <input type="checkbox"/>	Servers and Network Devices	150-151, 1053
	Partially Effective <input type="checkbox"/>	Product Selection & Acquisition	279-280, 282-287, 463-464
	Not Effective <input type="checkbox"/>	Standard Operating Environments	380-383, 385-388, 1033, 953-954
R15. Cryptographic Security	Effective <input type="checkbox"/>	Web Applications	263
	Partially Effective <input type="checkbox"/>	Cryptographic Fundamentals	453, 455, 457, 459, 462, 465, 469, 1080, 1150, 1161-1162
	Not Effective <input type="checkbox"/>	DACA	471-477, 479-480, 994, 1054
		DACP	481
		SSL and TLS	482, 1139
		Secure Shell	484-489, 997
		S/MIME	490
		OpenPGP Message Format	499
		Internet Protocol Security	1091
		Key Management	494-498, 998-1001
R16. Proactive Security Audits	Effective <input type="checkbox"/>	Standard Operating Environments	499-507, 509-511, 1002-1005
	Partially Effective <input type="checkbox"/>	Privileged Access	386, 954
	Not Effective <input type="checkbox"/>	Event Logging & Auditing	444, 446-448, 450, 982, 984
R17. Data Import & Export	Effective <input type="checkbox"/>	Data Import & Export	580, 585-586, 859 109
	Partially Effective <input type="checkbox"/>		667, 1077, 1156
	Not Effective <input type="checkbox"/>		
R18. Media Handling and Security	Effective <input type="checkbox"/>	Media Handling	322-323, 325, 330-334
	Partially Effective <input type="checkbox"/>	Media Usage	337-338, 341-344, 347, 831-832
	Not Effective <input type="checkbox"/>	Media Sanitisation	348, 350-354, 356-360, 1065-1068
		Media Destruction	361-366, 368, 370-373, 838-840, 1160
		Media Disposal	374-375, 378, 329
R19. Security Administration Tasks	Effective <input type="checkbox"/>	ITSM	742-743, 745-767, 19, 23, 24
	Partially Effective <input type="checkbox"/>	ITSO	108, 768-785
	Not Effective <input type="checkbox"/>	System Owners	27-28, 1071-1072
		System Users	33-34, 406
		Documentation Fundamentals	39-44, 46-48, 786-787, 1153-1154
		Standard Operating Procedures	51, 55-57, 789-790
		Email Infrastructure	568
		Vulnerability Management	911, 105, 909, 112-113
		InfoSec Awareness & Training	251-253, 255, 257, 922

UNCLASSIFIED (RECLASSIFY after first entry)

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway/CDS Audit Guide

		Event Logging & Auditing	109, 580, 585-586, 859
		Industry Engagement and Outsourcing	744
R20. Change Management	Effective <input type="checkbox"/>	Change Management	115, 117, 912, 809
	Partially Effective <input type="checkbox"/>		
	Not Effective <input type="checkbox"/>		
R21. Business Continuity and Disaster Recovery	Effective <input type="checkbox"/>	Business Continuity and Disaster Recovery	118-119, 913-914
	Partially Effective <input type="checkbox"/>		
	Not Effective <input type="checkbox"/>		
R22. Incident & Intrusion Detection + Response Plan	Effective <input type="checkbox"/>	Documentation Fundamentals	43
	Partially Effective <input type="checkbox"/>	Incident Response Plans	58-59
	Not Effective <input type="checkbox"/>	Detecting Cyber Security Incidents	120-121
		Managing Cyber Security Incidents	122, 125-126, 129-138
		Intrusion Detection & Prevention	575-579
R23. Reporting Security Incidents	Effective <input type="checkbox"/>	Managing Cyber Security Incidents	122, 125-126, 129-138
	Partially Effective <input type="checkbox"/>	Reporting Cyber Security Incidents	123-124, 139-143
	Not Effective <input type="checkbox"/>		
R24. General Documentation Controls	Effective <input type="checkbox"/>	Documentation Fundamentals	39-44, 46-48, 786-787, 1153-1154
	Partially Effective <input type="checkbox"/>	Emergency Procedures	62, 1159
	Not Effective <input type="checkbox"/>	Accreditation Framework	64-65, 69-73, 76-78, 86, 791, 793
		Conducting Audits	797
		Email Infrastructure	568
		Product Selection & Acquisition	279-280, 282-287, 463-464
		Media Handling	322-323, 325, 330-334
		Media Sanitisation	348, 350-354, 356-360, 836, 1065-1068
		Media Destruction	361-366, 368, 370-373, 838-840, 1160
		Media Disposal	374-375, 378, 329
		Standard Operating Environments	380-388, 841-842, 953-954, 1033
		Software Application Development	400-403
		Identification & Authentication	408, 413-431 853, 976
		Event logging & Auditing	109, 580, 585-586, 986
		DACAs	471-477, 479-480, 994, 1054
		Internet Protocol Security	494-498
		Key Management	499-507, 509-511, 1002-1005
		Fax Machines and MFDs	588

UNCLASSIFIED (RECLASSIFY after first entry)