



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

**Defence Signals Directorate**

# **Gateway/Cross Domain Solution Information Security Assessment Guide**

Incorporating the  
Gateway Certification Checklist

**VERSION 5.0**  
**December 2009**

## **Table of Contents**

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>1. INFORMATION SECURITY WITHIN GOVERNMENT.....</b>	<b>4</b>
<b>2. INFORMATION SYSTEM ACCREDITATION.....</b>	<b>4</b>
<b>3. INFORMATION SECURITY ASSESSMENT .....</b>	<b>4</b>
<b>4. THE GATEWAY/CDS INFORMATION SECURITY ASSESSMENT GUIDE .....</b>	<b>4</b>
<b>5. GUIDANCE FOR ASSESSORS.....</b>	<b>5</b>
<b>6. SECURITY CERTIFICATION REQUIREMENTS CHECKLIST .....</b>	<b>7</b>
6.1. GATEWAY/CDS RISK ASSESSMENT .....	7
6.2. GATEWAY/CDS POLICY FRAMEWORK.....	9
6.3. GATEWAY/CDS DESIGN METHODOLOGY.....	12
6.4. GATEWAY/CDS SECURITY MANAGEMENT .....	17

## **For Additional Information & Assistance**

Point of Contact: DSD Assist

Phone: (02) 6265 0197

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

© Australian Government 2009

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/CDS  
Name:** \_\_\_\_\_

**Description:** \_\_\_\_\_

**Contact:** \_\_\_\_\_

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

## 1. Information security within government

Australian Government agencies are required by the *Australian Government Protective Security Manual* (PSM) to consider the protective security of their information. For information that is processed, stored or communicated by an information system, the PSM prescribes this authority to the *Australian Government Information Security Manual* (ISM).

The Defence Signals Directorate (DSD) issues the ISM. It provides an organisation with a blueprint for the establishment of an information security management system (ISMS) and defines the information security standard for protecting systems that process, store or communicate government information.

The ISM is a publically releasable document and can be obtained from DSD's website at <http://www.dsd.gov.au>.

## 2. Information system accreditation

Accreditation is the process by which an authoritative body, the accreditation authority, gives formal recognition and acceptance of the residual security risk to information processed, stored or communicated by a system.

The formal recognition and acceptance of the residual security risks to the system are a prerequisite for the operation of the system.

To assist the accreditation authority in determining whether the residual security risk to a system is at a suitable level for their risk appetite, an information security assessment is conducted.

## 3. Information security assessment

The aim of an information security assessment is to review the suitability of the information system architecture (including the information security documentation), assess the implementation and effectiveness of controls for the system (an information security certification) and to report on residual security risks relating to the operation of the system to the accreditation authority.

## 4. The gateway/CDS information security assessment guide

This guide aims to assist assessors in undertaking the three stages of an information security assessment for a gateway/CDS. It assumes a detailed knowledge of the ISM and is intended to be used in conjunction with it.

The guide comprises guidance for assessors and a checklist to assist in recording the outcomes of the certification stage of an assessment of a gateway/CDS.

*Note: Previous versions of gateway assessment aids have included guides and checklists that duplicated the ISM and referenced standards. This was shown to foster inconsistency between the ISM and the assessment aids which could be interpreted as competing standards. This version aims to restore the ISM as the definitive standard and simplify the assessment aid for the intended purpose of enabling high quality, complete and repeatable assessments.*

## 5. Guidance for Assessors

The following assessment guidance is provided to Assessors:

- To award certification, an assessor must verify consistency with the controls implemented and the organisation's 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.
- Checklist requirements must not be scoped out unless it is demonstrated that a specific requirement may not be applicable to a particular system.
- The titles of the documents identified in this guide are only guidelines; individual organisations may title their document suite to best meet the organisation's needs. DSD **recommends** that a document matrix provide a mapping between the standardised titles and the titles used by the organisation be available to assist the certification process.
- The assessor needs to verify that applicable 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 assessment 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. Security certification requirements checklist

### 6.1. Gateway/CDS Risk Assessment

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

#### 6.1.1. Security Objective

*An organisation shall identify, quantify, analyse and evaluate risks to their Gateway/CDS 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.*

#### 6.1.2. Guidance for Assessors

Effective Risk Management involves two main tasks:

1. Assessing risk, which involves:
  - establishing the objective and context for the risk assessment;
  - identification of risks based on valid threats and vulnerabilities;
  - analysis of the risks including their likelihood and consequences; and
2. Treating risk, which involves:
  - identifying the treatment approach (Reduce, Transfer, Avoid, Accept); and if reducing the risk
  - the selection of effective and appropriate controls.

These tasks take the path described below:

- The organisation shall conduct a Threat & Risk Assessment and develop a Security Risk Management Plan (SRMP) using 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 and the risk management methodology employed to assess the consistency between the organisations, policies, plans, and procedures.

Requirements	Assessment	ISM References
<p><b>Security Risk Assessment</b></p>	<p>Effective <input type="checkbox"/></p> <p>Partially Effective <input type="checkbox"/></p> <p>Not Effective <input type="checkbox"/></p>	<p>IT Security Managers                      IT Security Officers                      Identification &amp; Authorisation                      Detecting InfoSec Incidents                      Managing InfoSec Incidents                      Product Patching &amp; Updating                      Gateway/CDS</p>
<p><b>Comments:</b></p>		
<p><b>Security Risk Management Plan</b></p>	<p>Effective <input type="checkbox"/></p> <p>Partially Effective <input type="checkbox"/></p> <p>Not Effective <input type="checkbox"/></p>	<p>Chief Information Security Officer                      IT Security Managers                      System Owners                      Documentation Fundamentals                      Security Risk Management Plans</p>
<p><b>Comments:</b></p>		

## 6.2. Gateway/CDS Policy Framework

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

### 6.2.1. 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.*

### 6.2.2. 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 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 interpretation and external references; and
- consequences of policy violation, reporting and assistance contacts.

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

Assessors undertaking a certification of the Gateway/CDS 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/CDS in line with all other systems and functions.

Requirements	Assessment	ISM Reference
<b>Information Security Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Information Security Policies
<b>Comments:</b>		
<b>Access Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	System Users Identification & Authentication Authorisation & System Access Privileged Access Event Logging & Auditing Gateway/CDS
<b>Comments:</b>		
<b>Remote Access Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Secure Shell Remote Access Working Off-Site Fundamentals Working From Home Working Outside the Office
<b>Comments:</b>		
<b>Cryptographic Control Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Reporting InfoSec Incidents Network Infrastructure Product Patching & Updating
<b>Comments:</b>		

Continued on next page

Requirements	Assessment	ISM Reference
<b>Contingency Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Business Continuity & Disaster Recovery
<b>Comments:</b>		
<b>Incident Detection &amp; Response Policy</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Detecting InfoSec Incidents Intrusion Detection & Prevention
<b>Comments:</b>		

### 6.3. Gateway/CDS Design Methodology

[| Gateway Major Components](#) | [Gateway/CDS Components](#) | [Asset Identification & Classification](#) | [Network Security](#) | [Physical Security](#) | [Communications Security](#) | [Critical Security Configuration](#) | [Risk Based Security Criteria](#) | [Cryptographic Devices](#) |

#### 6.3.1. Security Objective

*Gateway/CDS design must ensure that identified risks to the Gateway/CDS and the information assets it protects, are treated in accordance with the Security Risk Management Plan (SRMP) and based on approved administrative and operational policy.*

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

#### 6.3.2. Guidance for Assessors

The design of the gateway/CDS 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/CDS.

The environments surrounding gateways/CDS differ between organisations. For this reason, organisations need to consider additional requirements identified in the SRMP for their Gateway/CDS 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;
- prescribing best practices and their implementation;
- industry hardening guides for software & hardware;
- security considerations such as data classification, privacy, ecommerce, etc; and
- product capability, selection and availability requirements for:
  - firewalls,
  - routers,
  - IDS & IPS,
  - encryption ,
  - VPN services and
  - Virus control.

The documentation needed to support the gateway/CDS design should include:

- policy directives;

- network diagrams;
- system configuration;
- critical configuration lists;
- system security plans;
- input to the site security plans;
- security calendar; and
- gateway/CDS component, 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/CDS design/implementation and control selection, including procedural and policy controls.

Prior to undertaking the certification stage, assessors need to have satisfied themselves that the supporting documentation is complete and sufficient to meet the organisation's needs. This section determines whether that documentation is a true and current representation of the gateway/CDS's design and that the supporting administrative and operational processes and procedures are in place and effective.

Requirements	Assessment	ISM Reference
<p><b>Gateway/CDS Major Components</b></p>	<p>Effective <input type="checkbox"/></p> <p>Partially Effective <input type="checkbox"/></p> <p>Not Effective <input type="checkbox"/></p>	<p>IT Security Managers</p> <p>Product Selection &amp; Acquisition</p> <p>Product Installation &amp; Configuration</p> <p>Product Patching &amp; Updating</p> <p>Product Maintenance &amp; Repairs</p>
<p><b>Comments:</b></p>		

*Continued on next page*

**UNCLASSIFIED (RECLASSIFY after first entry)**

**Gateway/CDS Information Security Assessment Guide**

Requirements	Assessment	ISM Reference
<b>Gateway/CDS Components</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Gateways/CDS Content Filters Firewalls Diodes Peripheral Switches Product Security
<b>Comments:</b>		
<b>Asset Identification &amp; Classification</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Standard Operating Procedures Hardware Products Product Classifying & Labelling
<b>Comments:</b>		
<b>Network Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Network Management VLANs Wireless LANs IP Telephony Email Infrastructure Intrusion Detection & Prevention Multifunction Devices
<b>Comments:</b>		

*Continued on next page*

Requirements	Assessment	ISM Reference
<b>Physical Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Facilities Servers and Network Devices Network Infrastructure Hardware Products Tamper Evident Seals
<b>Comments:</b>		
<b>Communications Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Cabling Cable Distribution Systems Labelling & Registration Patch Panel, Patch Cables & Fly Leads
<b>Comments:</b>		
<b>Critical Security Configuration</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Documentation Fundamentals Security Risk Management Plan Documentation Fundamentals System Security Plan Standard Operating Environments Security Clearances & Briefings
<b>Comments:</b>		

*Continued on next page*

Requirements	Assessment	ISM Reference
<b>Cryptographic Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	SSL/TLS Filtering Cryptographic Fundamentals DACA DACP SSL and TLS Secure Shell S/MIME OpenPGP Message Format Internet Protocol Security Key Management
<b>Comments:</b>		

## 6.4. Gateway/CDS Security Management

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

### 6.4.1. Security Objective

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

*The administration and operation of a gateway/CDS infrastructure and the services it provides are often key controls within a secure gateway/CDS 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.*

### 6.4.2. Guidance for Assessors

The ongoing security of a gateway/CDS 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/CDS. Assessors will be looking for evidence that all documentation is being followed.

As a minimum standard the gateway/CDS will need:

- Standard Operating Procedures (SOPs) for the:
  - IT Security Manager (ITSM);
  - IT Security Officer (ITSO);
  - System Administrator; and
  - system users
- a System Security Plan (SSP) to ensure alignment between the SRMP, ICTSP and the gateway/CDS operation; and
- a Site Security Plan to ensure all physical security task and measures are implemented and maintained.

Other specific documentation that is essential for effective secure operation of a gateway/CDS includes:

- work instructions or procedures detailing proper completion of tasks;
- incident detection strategy;
- incident response plans and procedures;
- a security Calendar to schedule periodic security related tasks; and

- an audit program.

In addition to the above documentation the assessor will be looking for the gateway/CDS 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/CDS occur.

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

Requirements	Assessment	ISM Reference
<b>Proactive Security Audits</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Privileged Access Event Logging & Auditing
<b>Comments:</b>		
<b>Data Import &amp; Export</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Data Import & Export
<b>Comments:</b>		

*Continued on next page*

Requirements	Assessment	ISM Reference
<b>Media Handling and Security</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Media Handling Media Usage Media Sanitisation Media Destruction Media Disposal
<b>Comments:</b>		
<b>Security Administration Tasks</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	IT Security Managers IT Security Officers System Owners System Users Documentation Fundamentals Standard Operating Procedures Information Security Reviews Vulnerability Analysis InfoSec Awareness & Training Event Logging & Auditing
<b>Comments:</b>		
<b>Change Management</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Change Management
<b>Comments:</b>		

*Continued on next page*

Requirements	Assessment	ISM Reference
<b>Business Continuity</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Business Continuity & Disaster Recovery
<b>Comments:</b>		
<b>Incident &amp; Intrusion Detection + Response Plan</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Incident Response Plans Detecting InfoSec Incidents Managing InfoSec Incidents Intrusion Detection & Prevention
<b>Comments:</b>		
<b>Reporting Security Incidents</b>	Effective <input type="checkbox"/> Partially Effective <input type="checkbox"/> Not Effective <input type="checkbox"/>	Managing InfoSec Incidents Reporting InfoSec Incidents
<b>Comments:</b>		

*Continued on next page*

Requirements	Assessment	ISM Reference
<p><b>General Documentation Controls</b></p>	<p>Effective <input type="checkbox"/></p> <p>Partially Effective <input type="checkbox"/></p> <p>Not Effective <input type="checkbox"/></p>	<p>Documentation Fundamentals</p> <p>Emergency Procedures</p> <p>Conducting Accreditation</p> <p>Information Security Assessment</p> <p>Information Security Reviews</p> <p>Product Selection &amp; Acquisition</p> <p>Product Sanitisation &amp; Disposal</p> <p>Media Handling</p> <p>Media Sanitisation</p> <p>Media Destruction</p> <p>Media Disposal</p> <p>Standard Operating Environments</p> <p>Software Development Environments</p> <p>Identification &amp; Authentication</p> <p>Event logging &amp; Auditing</p> <p>Using DACAs</p> <p>Key Management</p> <p>Multifunction Devices</p> <p>Escorting Uncleared Personnel</p>
<p><b>Comments:</b></p>		