

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3



Australian Government
Department of Defence

Defence Signals Directorate

Gateway Certification Checklist

VERSION 2.2.3

Point of Contact: Computer Network Vulnerability Team

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

Organisation: _____

Assessor: _____

© Australian Government 2007

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.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

Document Change Record

Version	Changed By	Date	Changes
2.2	Advice and Assistance	July 05	Policy and consistency check.
2.2.1	Advice and Assistance	October 05	Update for September 2005 ACSI 33 and PSM 2005.
2.2.2	Advice and Assistance	March 06	Update for March 2006 ACSI 33 and consistency. Incorporate minor changes.
2.2.3	Computer Network Vulnerability Team	March 07	Update for September 2006 ACSI 33 and consistency. Incorporate minor changes.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

Table of Contents

1. Introduction 4

1.0 Gateway Risk Assessment..... 10

2.0 Gateway Policy Development..... 10

 2.1 Access Policy..... 10

 2.2 Security Policy 10

 2.3 Contingency Policy 12

 2.4 Incident Detection and Response Policy..... 12

3.0 Gateway Design Methodology..... 14

 3.1 Gateway Major Components 14

 3.2 Mandatory Design Criteria 14

 3.3 Risk Based Security Design Criteria 15

 3.4 Critical Security Configuration 17

 3.5 Design Documentation 17

4.0 Gateway Security Management 17

 4.1 Security Administration Tasks 17

 4.2 Proactive Security Checking Tasks 19

 4.3 Proactive Security Audit Tasks..... 21

 4.4 Contingency Plan 22

 4.5 Incident Detection and Response Plans and Procedures..... 22

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

1. Introduction

1.1. Purpose

1. The following checklist is designed to assist assessors in the conduct of a Gateway Certification to Defence Signals Directorate (DSD) standards. This document can be used by I-RAP assessors, DSD, and Australian Government agencies undertaking a certification or review.

1.2. Related Documentation

2. Related documentation for assessors to seek further guidance include:
 - Protective Security Manual (PSM) 2005, Attorney General's Department;
 - Australian Government Information & Communications Technology Security Manual (ACSI 33) September 2006, Information Security Group, Defence Signals Directorate; and
 - Gateway Certification Guide (GCG) V3.4.3, Information Security Group, Defence Signals Directorate.

Note: a working level familiarity with these documents is assumed.

1.3. Keywords

3. The table below defines the keywords used within this document to indicate the compulsory requirements for certification.

Keyword	Interpretation
MUST	The item is mandatory for compliance.
MUST NOT	Non-use is mandatory for compliance.
SHOULD	Valid reasons to deviate from the requirement may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by an authorised organisation security representative. Note: Organisations deviating from a SHOULD , MUST document the reason(s) for doing so.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

	be approved by an authorised organisation security representative. Note: Organisations deviating from a SHOULD NOT , MUST document the reason(s) for doing so.
RECOMMENDS RECOMMENDED	A recommendation or suggestion. Note: Organisations deviating from a RECOMMENDS or RECOMMENDED , are encouraged to document the reason(s) for doing so.

1.4. Definitions

4. Organisation, or any of its derivations, is used to refer to any Government Agency or Department as well as any Service Provider seeking to provide Internet services to the Australian Government.
5. Please refer to the glossary in ACSI 33 for a comprehensive list of additional technical definitions.

2. Requirements for Certification

6. I-RAP assessors **MUST** forward the following documents to the DSD I-RAP Manager once an assessment is completed:
 - completed checklist;
 - additional requirements;
 - checklist comments;
 - certification report; and
 - certification letter.
7. The DSD I-RAP Manager's details are as follows:

The I-RAP Manager
Information Security Group
Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

3. Checklist Guidance

8. This section provides guidance upon answering items within the checklist and provides some detail upon the obligations of the assessor.
 - Checklist requirements **MUST NOT** be scoped out during a review.
 - The titles of the documents given in this checklist are guidelines; organisations may title their policies sections/documents as appropriate.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

3.1. Requirements

9. The checklist consists of requirements, designated as a bolded capital 'R' followed by an outline number. The complete requirement consists of:
- the requirement number;
 - the requirement; and
 - a checkbox.

For example:

R1 Organisations **MUST** keep records. (ACSI 33 2.8.26)

R2 Organisations **MUST** have a Business Continuity plan (ASCI 33 2.8.11)

Bolded, capitalised words are key words, as described above. Key words stipulate a condition upon the requirement, and must be considered when deciding whether a requirement has or has not been met by an organisation.

10. Assessors should either tick or cross a requirement to indicate that either an organisation has succeeded, or failed, in answering the requirement. The assessor should record any comments using the comments table that is attached at the end of this checklist. Comments must be submitted with the checklist documentation.
11. Bracketed information towards the end of a requirement's wording implies a reference. The material that is referenced should be examined for further detail or for justification of a requirement.
12. DSD may prescribe requirements beyond the minimum stated in ACSI 33 in order to achieve greater granularity for the certification context, especially where requirements are drawn from the range of reference materials.

3.2. Sub-requirements

13. Some requirements are broken into sub-requirements. Sub-requirements are designated with a two-level number, and a parent requirement from which all sub-requirements stem.

For example:

R2 Organisations **MUST**:

R2.1 keep records; and

R2.2 examine each record.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

14. The key word in the parent item '**MUST**' applies to all sub-requirements. Organisations **MUST** achieve a tick in each sub-requirement box in order to satisfy the parent requirement.

Consider another example:

R3 Organisations **SHOULD**:

R3.1 perform audits annually; and

R3.2 report upon audit results.

15. The key word in the parent item '**SHOULD**' applies to all sub-requirements, just like the first sub-requirement example. Organisations must achieve a tick in each sub-requirement box in order to satisfy the parent requirement. This statement should be considered in light of the guidance provided in 'When to tick or cross'.

3.3. When to tick or cross

16. Ticks are given where the key word of the requirement is satisfied.
17. For a '**MUST / MUST NOT**' you should tick when:
- The requirement is complied with explicitly.
18. For a '**SHOULD / SHOULD NOT**' you should tick when:
- The requirement is complied with explicitly; or
 - Valid reasons exist for non-compliance and these reasons are documented.
19. For a '**RECOMMENDS**' or any of its derivations you should tick when:
- The requirement is complied with explicitly; or
 - Valid reasons exist for non-compliance and these reasons are provided to the certifying authority.
20. You should mark a requirement with a cross in all other situations.

3.4. Additional Requirements

21. Additional requirements may arise from an organisation's Risk Assessment. Such requirements **MUST** be documented and submitted to the Certifying Authority. See ACSI 33 Part 2 Chapter 7 for the definition and responsibilities of the Certifying Authority.

3.5. Checking the implementation

22. Assessors **MUST** verify consistency between policy, plans, and procedures. In order to verify that procedures mentioned within policy documentation are operational, assessors must have the organisation's IT Security Advisor (ITSA),

Page 7

UNCLASSIFIED (RECLASSIFY after first entry)

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

IT Security Manager (ITSM), or an authorised substitute demonstrate that the procedure is in use.

3.6. Comments

23. Provision is made at the back of the checklist for assessors to provide their comments against individual requirements.
24. Assessors **MUST** comment upon individual requirements within the checklist. Comments **MUST** provide justification of how well an organisation complies with each requirement.

3.7. Certification Levels

25. For further information on any of the certification levels please refer to ACSI 33 Part 2 Chapter 7.
26. **Full Certification** is awarded to gateways that are compliant with all the requirements for gateway certification based on a comprehensive evaluation.
27. **Provisional Certification** is awarded to gateways that are lacking compliance in some non-critical aspect(s) of design, policy or management. It does not preclude the gateway from operating, but does mandate that the provisions be corrected within a specified timeframe.
28. **Recertification** should be undertaken on all certified gateways at least every 12 months or at initiation of a major change. See the GCG for the definition of a major change.

3.8. Certification Report

29. A certification report based upon the requirement components as detailed in this document **MUST** be provided.
30. The certification 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.
31. The certification report provides any recommendations based on non-mandatory best practice guidelines that have not been demonstrated by the organisation.
32. Where the checklist requirements have not been met the result is a fail and the organisation **MUST** be awarded NO certification.

3.9. Certification Letter

33. The certification letter, as a minimum, **MUST** include:

- whether certification has been achieved;
- the level of classification of the system;
- the type of certification for the system;
- the requirement to inform DSD of any new or existing consideration that may render a previously certified system non-compliant;
- the requirement to provide regular advice to DSD on significant changes to any analysed threat level; and
- conditions for maintaining certification.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

1.0 Gateway Risk Assessment

The requirements contained in the following section are derived from PSM Part B, Gateway Certification Guide Chapter 1 and ACSI 33 Part 2 Chapter 2 and 4.

- R1.** The organisation **MUST** conduct a Risk Assessment (RA) on the gateway environment.
- R2.** The RA **MUST** contain:
- R2.1.** analysis of the risk;
 - R2.2.** prioritisation of the identified risks against target risk levels/predetermined standards; and
 - R2.3.** risk treatments.
- R3.** The RA **MUST** have been signed by the CEO or delegate of the organisation confirming they have read and accepted the RA, including any identified residual level of risk.

2.0 Gateway Policy Development

These requirements are derived from the Gateway Certification Guide, Chapter 2.

Access Policy

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 2 and ACSI 33 Part 3 Chapter 6.

- R4.** Access Policy **MUST** ensure that:
- R4.1.** all services are denied by default unless expressly permitted;
 - R4.2.** all gateway users (including groups), clients, or any subset are identified;
 - R4.3.** all services allowed through the gateway are identified;
 - R4.4.** user responsibilities within the gateway and their training requirements are documented; and
 - R4.5.** policies defining user account permissions and administration (including privileged users) are documented.
- R5.** Access Policy **SHOULD** ensure that:
- R5.1.** access between networks, especially those networks that are owned by different organisations, are detailed; and
 - R5.2.** changes to the Access Policy results in a review of the RA.

Security Policy

The requirements contained in the following section are derived from Gateway Certification Guide, Chapter 2 and ACSI 33 Part 2 Chapters 2, 3, 8 and Part 3 Chapters 1, 2, 4, 6 and 9.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R6.** There **MUST** be a clear correlation between the RA and the Security Policy.
- R7.** Security Policy **MUST** include:
- R7.1.** user administration policy (ACSI 33 Part 3 Chapter 6);
 - R7.2.** personnel security policy (ACSI 33 Part 3 Chapter 2);
 - R7.3.** physical security policy (ACSI 33 Part 3 Chapter 1);
 - R7.4.** key management policy (ACSI 33 Part 3 Blocks 3.9.38 to 3.9.53);
 - R7.5.** hardware security policy (ACSI 33 Part 3 Chapter 4); and
 - R7.6.** change management policy (ACSI 33 Part 2 Blocks 2.8.6 to 2.8.10).
- R8.** User administration policy **MUST** ensure that:
- R8.1.** the classification scheme is defined as per the definitions in the PSM;
 - R8.2.** the maximum classification of data handled or accessed by users and clients is identified; and
 - R8.3.** the data owner(s) are identified.
- R9.** Personnel security policy **MUST** ensure that:
- R9.1.** users' security clearance requirements are documented; and
 - R9.2.** records of the status of users' security clearances are kept.
- R10.** Personnel security policy **SHOULD** ensure that any legal conditions obligated on employees and contractors are documented.
- R11.** Physical security policy **MUST** ensure that:
- R11.1.** all server rooms have a physical security certification to the appropriate server room standard for the system classification (ACSI 33 Block 3.1.19);
 - R11.2.** personnel access restrictions to the gateway premises are documented;
 - R11.3.** server room certification is performed by a suitable Certification or Accreditation Authority;
 - R11.4.** personnel access restrictions to server rooms are documented; and
 - R11.5.** servers and any associated communication equipment are separated from general users (ACSI 33 Block 3.1.17).
- R12.** Key management policy **MUST** ensure that the cryptography used to protect classified information and systems is:
- R12.1.** approved by DSD; and
 - R12.2.** used in accordance with the standards outlined in ACSI 33.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R13.** Hardware security policy **MUST** ensure the:
- R13.1.** requirements for classification labelling and registering of hardware are documented (ACSI 33 Blocks 3.4.15/16);
 - R13.2.** requirements for the secure maintenance and disposal of hardware are documented (ACSI 33 Part 3 Chapter 4); and
 - R13.3.** requirements for media sanitisation and destruction are documented (ACSI 33 Part 3 Chapter 4).
- R14.** Change management policy **SHOULD** ensure that:
- R14.1.** authorities for approving changes are documented;
 - R14.2.** the accreditation authority is responsible for approving changes that will impact the security of Information and Communications Technology (ICT) systems; and
 - R14.3.** any associated system documentation will be updated to reflect changes to the ICT system.

Contingency Policy

The requirements contained in the following section are derived from Gateway Certification Guide, Chapter 2 and ACSI 33 Part 2 Chapter 8.

- R15.** There **MUST** be a clear correlation between the RA and the Contingency Policy.
- R16.** The Contingency Policy **MUST** ensure that the critical management objectives for a contingency plan are documented.
- R17.** The Contingency Policy **MUST** ensure that the following is documented (ACSI 33 Block 2.8.13):
- R17.1.** definitions of outages, and identify the appointment responsible for declaration of each grade of outage;
 - R17.2.** recovery time objectives, for the various grades of outages;
 - R17.3.** testing regime objectives and status reporting of backup systems; and
 - R17.4.** on-line and off-line redundancy.

Incident Detection and Response Policy

The requirements contained in the following section are derived from Gateway Certification Guide, Chapter 2 and ACSI 33 Part 2 Chapter 8.

- R18.** Incident Detection and Response Policy **MUST** document the definition of a "Security Incident", and identify the authority responsible for declaration of a security incident.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R19.** Incident Detection and Response Policy **SHOULD** include the following components:
- R19.1.** detecting security incidents (ACSI 33 Block 2.8.16);
 - R19.2.** managing security incidents (ACSI 33 Block 2.8.22);
 - R19.3.** reporting of incidents (ACSI 33 Block 2.8.23); and
 - R19.4.** incident response plan (ACSI 33 Blocks 2.8.40-44).
- R20.** Incident Detection and Response Policy **SHOULD** ensure that, for detecting security incidents, definitions on the types of incidents that are likely to be encountered are documented.
- R21.** Incident Detection and Response Policy **MUST** ensure that for managing security incidents:
- R21.1.** the process for internal reporting of security incidents is documented;
 - R21.2.** incidents are recorded and logged;
 - R21.3.** possible data spillage is minimised (ACSI 33 Block 2.8.27); and
 - R21.4.** malicious code is mitigated against (ACSI 33 Block 2.8.29).
- R22.** Incident Detection and Response Policy **MUST** ensure that for the reporting of security incidents:
- R22.1.** DSD and all connected gateway customers are addressees on off-line, analytical reports;
 - R22.2.** analytical reports are sent at least quarterly to DSD and connected gateway customers;
 - R22.3.** reports sent to DSD list all connected gateway customers;
 - R22.4.** in accordance with the requirements of ISIDRAS, DSD is notified as soon as practicable of all Category 3 or higher incidents;
 - R22.5.** DSD is informed of any ICT security incidents that require formal investigative action; and
 - R22.6.** users and clients are regularly informed on how to report security incidents to their ITSA or equivalent in accordance with organisational procedures.
- R23.** Incident Detection and Response Policy **SHOULD** ensure that for reporting of security incidents:
- R23.1.** timely reporting is done via the ISIDRAS reporting scheme;
 - R23.2.** DSD and connected gateway customers receive incident/analytical reports in the expected timeframe; and
 - R23.3.** if necessary, the report is formally acknowledged or reported to a higher

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

management level.

- R24.** Incident Detection and Response Policy **MUST** ensure that the incident response plan:
- R24.1.** is based on the incident grading definitions;
 - R24.2.** the response procedures are realistic, achievable, and include the category of incident to be reported on a timely basis; and
 - R24.3.** agencies archive incident logs for no less than 12 months.
- R25.** Archived logs **SHOULD** be stored securely off-site.

3.0 Gateway Design Methodology

These requirements are derived from the Gateway Certification Guide, Chapter 3.

Gateway Major Components

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 3 and ACSI 33 Part 3 Chapter 3 and 10.

- R26.** The mandatory firewall **MUST** be a product from the Evaluated Products List (EPL) (ACSI 33 Block 3.3.3)
- R27.** The mandatory firewall **SHOULD** be configured in accordance with the security target and certification report.
- R28.** Functionality required to provide interface separation **SHOULD** be a part of the evaluation of that firewall.
- R29.** The protection of services provided by the gateway **SHOULD** be based on:
- R29.1.** the function of the service;
 - R29.2.** the classification of the data;
 - R29.3.** the data the service could have access to (such as other networks); and
 - R29.4.** known vulnerabilities of the service that could be exploited and the impact of their exploitation.

Mandatory Design Criteria

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 3; ACSI 33 Part 2 Chapter 7 and Part 3 Chapter 10.

- R30.** Network traffic to any device on either the internal network or within the DMZ **MUST** be denied by default.
- R31.** Access to services between multiple internal networks (if any) using the firewall **MUST** be denied by default.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R32.** All traffic traversing between networks **SHOULD** be routed through the gateway (including firewall(s)).
- R33.** Organisations **MUST** demonstrate an understanding of the risks associated with all external connections and have documented strategies to treat such risks.
- R34.** All implementations of cryptographic services within the gateway required by ACSI 33 or the GCG, including those for confidentiality, authentication, non-repudiation or data integrity **MUST** be included within the scope of the gateway certification.
- R35.** Any cryptographic products required in the gateway environment by ACSI 33 or the GCG **MUST** use a DSD Approved Cryptographic Protocol (DACP) or be a product from the EPL appropriate to the classification level of the gateway used in an evaluated configuration.
- Note: A maximum certification level of Provisional may be granted for gateways using products from the EPL that are in evaluation.
- R36.** All communication links between the internal network components and the firewall, where the communications path is not physically controlled by organisation and/or contractor staff, **MUST** be protected by a DSD approved cryptographic method.
- R37.** Firewall management **MUST** be provided via a secure path.
- R38.** If a remote management feature is used, it **SHOULD** have been included within the scope of the product's evaluation.
- R39.** Services **SHOULD NOT** be passed directly from the outside network to the inside network.
- R40.** The internal and external border router(s) **SHOULD NOT** be solely relied upon for access control.

Risk Based Security Design Criteria

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 3 and ACSI 33 Part 3 Chapters 7 and 10.

- R41.** There **MUST** be a clear correlation between the RA and the gateway design.
- R42.** Protocol specific security services available on gateway servers **SHOULD** be determined by business requirements and the RA.
- R43.** The business continuity strategy for the gateway **MUST** be based on the contingency policy.
- R44.** Audit log backups **SHOULD** be handled appropriately if evidence/forensic capabilities for the data contained in these logs is required.
- R45.** Archive, storage and management of audit logs **SHOULD** reflect the requirements of the Incident Detection and Response Policy/Plan.
- R46.** The outcome of the Contingency Policy discussed in Chapter 2 **SHOULD** be used to determine availability requirements, especially the balance between on-line and offline

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

redundancy.

- R47.** Auditing or logging services **MUST** be used to:
- R47.1.** monitor the real level of threat;
 - R47.2.** provide real time alarms to critical events; and
 - R47.3.** monitor the behaviour of privileged users within the gateway.
- R48.** The results of the Incident Detection and Response Policy **SHOULD** drive the requirements for auditing or logging.
- R49.** Logs **SHOULD** be produced/maintained to monitor the administration of the gateway.
- R50.** The information contained in logs **SHOULD** be reviewed within a time frame as described in the IDRP and critical patterns identified to form the basis of exception reporting.
- R51.** The following events **SHOULD** be logged for the firewall, DMZ servers and other critical components, for both successful and unsuccessful attempts:
- R51.1.** logon and logoffs;
 - R51.2.** boot and initialisation;
 - R51.3.** shutdown, and associated details;
 - R51.4.** restart, and associated details;
 - R51.5.** changes to the firewall configuration;
 - R51.6.** policy exceptions;
 - R51.7.** password changes;
 - R51.8.** TCP/UDP/ICMP connection requests; and
 - R51.9.** application connection type and data volume transferred, both inbound and outbound.
- R52.** For each event that is logged, the following information **SHOULD** be logged:
- R52.1.** event name or description;
 - R52.2.** date and time;
 - R52.3.** account Id;
 - R52.4.** command parameter;
 - R52.5.** IP source and destination address;
 - R52.6.** protocol code or description;
 - R52.7.** source and destination port; and

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

R52.8. success/failure of attempt.

Critical Security Configuration

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 3 and ACSI 33 Part 3 Chapter 7.

R53. Critical Security Configurations documentation **SHOULD** include:

R53.1. system backup configuration; and

R53.2. system device configuration.

R54. The system device configuration documentation **SHOULD** include:

R54.1. firewall access lists;

R54.2. firewall management configuration;

R54.3. encrypted modem configuration, including key management issues; and

R54.4. proxy server configuration (if applicable).

Design Documentation

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 3.

R55. The design documentation **MUST** include a:

R55.1. gateway logical/infrastructure diagram;

R55.2. list of design requirements;

R55.3. list of critical security configurations; and

R55.4. detailed configuration document.

4.0 Gateway Security Management

These requirements are derived from the Gateway Certification Guide, Chapter 4.

Security Administration Tasks

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 4 and ACSI 33 Part 2 Chapter 8 and Part 3 Chapters 2, 4, 6 and 9.

R56. The security administration tasks **MUST** include:

R56.1. user accounts administration plan and procedure;

R56.2. privileged user plan (ACSI 33 Part 3 Blocks 3.6.20-27);

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R56.3.** access control plan and procedure (ACSI 33 Part 3 Blocks 3.6.29-36);
- R56.4.** key management plan (ACSI 33 Part 3 Chapter 9);
- R56.5.** user awareness plan (ACSI 33 Part 3 Chapter 2);
- R56.6.** hardware security plan and procedure (ACSI 33 Part 3 Chapter 4); and
- R56.7.** change management plan and procedure (ACSI 33 Part 2 Chapter 8).
- R57.** Accounts administration plan and procedure **MUST** detail:
- R57.1.** a profile of system accounts;
- R57.2.** users allowed an account;
- R57.3.** the process to remove old accounts; and
- R57.4.** an outline of account administration record keeping.
- R58.** Privileged user plan and procedure **MUST** detail:
- R58.1.** all privileged accounts;
- R58.2.** who holds/is allowed to hold privileged accounts;
- R58.3.** how privileged accounts are controlled and accountable;
- R58.4.** rules on privileged accounts (for example, administrators are assigned individual accounts to ensure all admin tasks are accountable); and
- R58.5.** the type of work allowed to be performed on privileged accounts.
- R59.** Access control plan and procedure **SHOULD** detail:
- R59.1.** the users (including user groups);
- R59.2.** allocated/allowed resources;
- R59.3.** how users' access is limited;
- R59.4.** how to perform access control changes; and
- R59.5.** who can authorise access control changes.
- R60.** Key management plan and procedure **MUST** detail:
- R60.1.** how keys are derived;
- R60.2.** how often they are changed for each system;
- R60.3.** users that are allowed access to cryptographic equipment; and
- R60.4.** actions to be taken in event of compromise / replacement or decommissioning of cryptographic equipment.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R61.** Hardware security plan and procedure **SHOULD** detail:
- R61.1.** those systems requiring backup;
 - R61.2.** the frequency of any backup regime;
 - R61.3.** period of storage;
 - R61.4.** media reuse/disposal; and
 - R61.5.** archival of logs or audit trails.
- R62.** User awareness plan **SHOULD** detail:
- R62.1.** processes for the initiation and maintenance of a program to ensure users are aware of their roles and responsibilities;
 - R62.2.** processes that ensure training programs are aligned with user responsibilities; and
 - R62.3.** what constitutes appropriate activities and safe practices for use of the provided services.
- R63.** The change management plan and procedure **MUST** detail:
- R63.1.** all stakeholders in the change process;
 - R63.2.** the responsibilities for approving changes to systems;
 - R63.3.** the process by which changes are approved;
 - R63.4.** the communication of change details to all relevant persons; and
 - R63.5.** record maintenance procedures.
- R64.** There **MUST** be a clear correlation between gateway policy and the security administration task plans and procedures.
- R65.** There **MUST** be demonstrated evidence of implementation of the security administration task plans and procedures.
- R66.** Operators and administrators **SHOULD** utilise hard copies of the procedures to undertake the duties detailed within them.
- R67.** Hard copies of procedures **SHOULD** be readily available in the event of a system outage or compromise.

Proactive Security Checking Tasks

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 4 and ACSI 33 Part 3 Chapter 7.

- R68.** The proactive security checking tasks **MUST** detail:

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R68.1.** those responsible for checking the gateway system;
- R68.2.** the components that will be checked and by what means (including what tools are required);
- R68.3.** how often these checks are to be undertaken; and
- R68.4.** the authority that is to receive the reports.
- R69.** The configuration items that require checking and the regularity of checking **MUST** be derived from the critical configuration list and the relevant Security Policy.
- R70.** The proactive security checking tasks **MUST** include:
- R70.1.** firewall configuration checking plan and procedure;
- R70.2.** proxy server configuration checking plan and procedure (if applicable);
- R70.3.** cryptographic configuration checking plan and procedure; and
- R70.4.** physical alarm and access control plan and procedure.
- R71.** The firewall configuration checking plan and procedure **SHOULD** detail:
- R71.1.** items that need to be checked;
- R71.2.** what tool or methodology will be used to check them;
- R71.3.** what checksum algorithm is being used (if any);
- R71.4.** how often the checking will be done;
- R71.5.** how the reporting is to be undertaken;
- R71.6.** the appointment(s) responsible for checking; and
- R71.7.** the recipients for the reports.
- R72.** The proxy server configuration checking plan and procedure **SHOULD** detail (if applicable):
- R72.1.** items that need to be checked;
- R72.2.** what tool or methodology will be used to check them;
- R72.3.** what checksum algorithm is being used (if any);
- R72.4.** how often the checking will be done;
- R72.5.** how the reporting is to be undertaken;
- R72.6.** the appointment(s) responsible for checking; and
- R72.7.** the recipients for the reports.
- R73.** The cryptographic configuration checking plan and procedure **SHOULD** detail:

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R73.1. items that need to be checked;
- R73.2. what tool or methodology will be used to check them;
- R73.3. what checksum algorithm is being used (if any);
- R73.4. how often the checking will be done;
- R73.5. how the reporting is to be undertaken;
- R73.6. the appointment(s) responsible for checking; and
- R73.7. the recipients for the reports.
- R74. The physical alarm and access control plan and procedure **SHOULD** detail:
 - R74.1. items that need to be checked;
 - R74.2. what tool or methodology will be used to check them;
 - R74.3. how often the checking will be done;
 - R74.4. how the reporting is to be undertaken;
 - R74.5. the appointment(s) responsible for checking; and
 - R74.6. the recipients for the reports.
- R75. There **MUST** be a clear correlation between gateway policies and the proactive security checking tasks plans and procedures.
- R76. There **MUST** be demonstrated evidence of implementation of the proactive security checking tasks plans and procedures.

Proactive Security Audit Tasks

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 4 and ACSI 33 Part 3 Chapter 7.

- R77. The documentation for proactive security audit **MUST** include real-time reporting and off-line or analytical reporting plans and procedures.
- R78. The real-time reporting plan and procedure **MUST** detail:
 - R78.1. who is responsible for checking the audit trails;
 - R78.2. the specific objectives of the checking;
 - R78.3. the tools that will be used for this function (if any);
 - R78.4. how often these checks should be undertaken; and
 - R78.5. the recipients for the reports.

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R79.** The off-line or analytical reporting plan and procedure **MUST** detail:
- R79.1.** who is responsible for checking the audit trails;
 - R79.2.** the specific objectives of the checking;
 - R79.3.** the tools that will be used for this function (if any);
 - R79.4.** how often these checks should be undertaken; and
 - R79.5.** the recipients for the reports.
- R80.** The information required for these tasks **MUST** be derived from the outcomes of the gateway design and the relevant security policy.
- R81.** There **MUST** be a clear correlation between gateway policy and the proactive security audit tasks plans and procedures.
- R82.** There **MUST** be demonstrated evidence of implementation of the proactive security audit tasks plans and procedures.

Contingency Plan

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 4 and ACSI 33 Part 2 Chapter 8.

- R83.** The Contingency Plan **SHOULD** describe the plans and procedures to be followed in event of an actual contingency, including how the plan is to be checked and monitored.
- R84.** There **MUST** be a clear correlation between gateway policies and the contingency plans and procedures.
- R85.** There **MUST** be demonstrated evidence of implementation of the contingency plans and procedures.

Incident Detection and Response Plans and Procedures

The requirements contained in the following section are derived from the Gateway Certification Guide, Chapter 4 and ACSI 33 Part 2 Chapter 8.

- R86.** 132. Organisations **SHOULD** develop and maintain procedures in addition to the incident response plan that: (ACSI 33 Block 2.8.34)
- R86.1.** detect potential security breaches;
 - R86.2.** establish the cause of any security incident, whether accidental or deliberate;
 - R86.3.** detail the action required to recover and minimise the exposure to a system compromise;
 - R86.4.** assist in reporting the incident. (e.g. use of ISIDRAS); and

UNCLASSIFIED (RECLASSIFY after first entry)

Gateway Certification Checklist V2.2.3

- R86.5.** promote the prevention of security incidents and limit recurrences of security incidents.
- R87.** The incident detection and response plan and procedure **MUST** describe the steps to be followed when the proactive security checking tasks and audit tasks identify a security incident.
- R88.** Identified actions (for example, disconnecting the gateway) **SHOULD** map to the incident categories identified in the incident detection and response policy.
- R89.** Incident investigation, reporting, evidence preservation, media control and recording, and system recovery procedures **SHOULD** to be outlined in relation to each category of incident.
- R90.** The appointment(s) responsible for performing incident response **MUST** be clearly identified.

Comments

The following table will assist you to record responses to the IRAP checklists. It is not a substitute for a certification report.

You should enter a response for each check-marked requirement in the checklists, even where you do not wish to record any issues. This will assist in preparing your certification report, and will assist in maintaining appropriate historical records. It will also keep numbering consistent.

Fields

The 'Requirement' field is an auto-numbered field designed to increment each time that you move to a new line. It increments from 'R1' upwards. In order to achieve sub-requirement numbers under the 'Requirement' heading, you need only click on the 'Increase Indent' button – usually in the top-right region of your toolbar. Similarly, to revert to a requirement number from a sub-requirement number, you need only click on the 'Decrease Indent' button.

You should not need to alter the requirement numbering in any fashion as it is automatically configured to increment. This may be the case if you do not enter responses for a particular comment.

The 'Comment' field is a text field for you to record details against the requirement.

Requirement	Comment
R1	
R2	