Australian Government
Department of Defence

Defence Signals Directorate

GATEWAY CERTIFICATION CHECKLIST

VERSION 2.2.1

Point of Contact: Advice and Assistance Team

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

Organisation: _____

Assessor: _____

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.

Table Of Contents

Introduction 4
Certification 5
1.0 Gateway Risk Assessment 9
2.0 Gateway Policy Development 9
2.1 Access Policy 9
2.2 Security Policy 9
2.3 Contingency Policy 11
2.4 Incident Detection and Response Policy 11
3.0 Gateway Design Methodology 13
3.1 Gateway Major Components 13
3.2 Mandatory Design Criteria 13
3.3 Risk Based Security Design Criteria 14
3.4 Critical Security Configuration 15
3.5 Design Documentation 16
4.0 Gateway Security Management 16
4.1 Security Administration Tasks 16
4.2 Proactive Security Checking Tasks 18
4.3 Proactive Security Audit Tasks 20
4.4 Contingency Plan 21
4.5 Incident Detection and Response Plans and Procedures 21

Introduction

Purpose

The following checklist is designed to assist assessors in the conduct of a Gateway Certification to DSD standards.

Related Documentation

Assessors are strongly encouraged to seek further guidance from the following companion documents:

- The Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2005.
- The Gateway Certification Guide (GCG), V3.4.1.
- Protective Security Manual (PSM), 2005.

Please note a working level familiarity with these documents is assumed.

Key Words

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 certification.
MUST NOT	Non-use is mandatory for certification.
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 the certifying authority during the certification process. **Note:** Agencies 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 be approved by the certifying authority during the certification process. **Note:** Agencies deviating from a **SHOULD NOT**, **MUST** document the reason(s) for doing so.
RECOMMENDS **RECOMMENDED**	A recommendation or suggestion. **Note:** Agencies deviating from a **RECOMMENDS** or **RECOMMENDED**, are encouraged to document the reason(s) for doing so.

Definitions

Organisation, or any of its derivations, is used to refer to any Government Agency or Government Department as well as any Service Provider seeking to provide services to Australian Government.

Please refer to the glossary in ACSI 33 for a comprehensive list of technical definitions used within this document.

Certification

I-RAP assessors MUST forward the following documents to the DSD I-RAP Manager once the assessment is completed:

- completed checklist;
- additional requirements;
- comments;
- certification report; and
- certification letter.

DSD I-RAP Manager Information:

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

Checklist Guidance

This section provides guidance upon answering items within the checklist and provides some detail upon the obligation of the assessor.

Checklist components must not be scoped out during a review.

The titles of the documents given in this guide are guidelines; organisations may title their policies sections/documents as appropriate.

Requirements

Each 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 itself, and a checkbox.

For example:

R1 Organisations **MUST** keep records. (ACSI 33 2.8.12) ☐

Bolded, capitalized 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.

Assessors should either tick or cross a requirement to indicate that an organisation has succeeded or failed in answering the requirement. The reviewer 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.

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.

DSD prescribes further minimum requirements in order to achieve greater granularity where the requirement is drawn from a range of reference material.

Sub-requirements

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 from.

For example:

R2 Organisations **MUST**:	
R2.1 keep records; and	☐
R2.2 examine each record.	☐

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.	☐

The key word in the parent item '**SHOULD**' applies to all sub-requirements, just like the first sub-requirement example given above this 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'.

When to tick or cross

Ticks need only be given where the key word of the requirement is properly addressed.

For a '**MUST / MUST NOT**' you should tick when:

- The requirement is complied with explicitly.

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.

For a '**RECOMMEND**' or any of its derivations you should tick when:

- The requirement is complied with explicitly.

You should mark a requirement with a cross in all other situations.

Supplying comments

Assessors must supply comments using the table supplied at the back of this checklist. Specific guidance upon using the comments section is provided just prior to the comments table.

The comments table allows you to register comments against an individual requirement or sub-requirement.

Checking the implementation

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

Certification Levels

For further information on any of the certification levels please refer to ACSI 33 Part 2, Chapter 7.

Full Certification is awarded to gateways that are compliant with all the requirements for gateway certification based on a comprehensive evaluation.

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.

Recertification should be undertaken on all certified gateways at least every 12 months or at initiation of a major change.

Additional Requirements

Additional requirements may arise from an organisation's Risk Assessment. These requirements need to be documented and submitted to the Certifying Authority.

Comments

Provision is made at the back of the checklist for assessors to provide their comments against individual requirements.

Assessors must comment upon individual requirements within the following checklist. Comments must provide an indication of how well an organisation complies with each requirement.

Certification Report

Please provide a certification report based upon the Gateway Certification Report template.

The formal 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.

Provide any recommendations based on non-mandatory best practice guidelines that have not been demonstrated by the agency.

Certification Letter

The certification letter, as a minimum, must include :

- advise upon whether certification has been achieved;
- advise the level of certification the system has achieved;
- advise upon the requirement to inform DSD of any new or existing consideration that may render a previously certified system non-compliant;
- advise organisations that they should provide regular advice to DSD on signification changes to any analysed threat level; and
- advise upon the conditions of maintaining certification.

1.0 Gateway Risk Assessment

The requirements contained in the following section are derived from Gateway Certification Guide Chapter 1 and ACSI 33 Part 2, Chapter 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 risks including target risk levels/predetermined standards; and ☐
- **R2.3.** risk treatments. ☐

R3. The RA **MUST** have been signed by the CEO or delegate of the agency confirming they have read and accepted the RA, including the identified residual level of risk. ☐

2.0 Gateway Policy Development

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

2.1 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 gateway users (including groups), clients, or any subset are identified; and ☐
- **R4.2.** all services are denied by default unless expressly permitted. ☐

R5. Access Policy **SHOULD** ensure that:

- **R5.1.** access between networks, especially those networks that are owned by different agencies are detailed; ☐
- **R5.2.** changes to the Access Policy will result in a review of the RA; and ☐
- **R5.3.** changes in business requirements will be reflected in policy and procedures. ☐

R6. There **MUST** be a clear correlation between the RA and the Access Policy. ☐

2.2 Security Policy

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

R7. There **MUST** be a clear correlation between the RA and the Security Policy. ☐

R8. Security Policy **MUST** include:

- **R8.1.** administrative security policy (ACSI 33, Part 3, Chapter 6); ☐
- **R8.2.** personnel security policy (ACSI 33, Part 3, Chapter 2); ☐
- **R8.3.** physical security policy (ACSI 33, Part 3, Chapter 1); ☐
- **R8.4.** key management policy (ACSI 33, Blocks 3.9.35 to 3.9.50); ☐
- **R8.5.** hardware security policy (ACSI 33, Part 3, Chapter 4); and ☐
- **R8.6.** change management policy (ACSI 33 Blocks 2.8.6 to 2.8.12). ☐

R9. Administrative security policy **MUST** ensure that:

- **R9.1.** the maximum classification of data handled or accessed by users and clients is identified; ☐
- **R9.2.** the responsibilities of users within the gateway and the training requirements of those users are established; ☐
- **R9.3.** rules defining user account permissions and administration (including privileged users) are documented; ☐
- **R9.4.** a classification scheme is as per the definitions in the Protective Security Manual; and ☐
- **R9.5.** the data owner(s) are identified ☐

R10. Personnel security policy **MUST** ensure that:

- **R10.1.** users' security clearance requirements are documented; ☐
- **R10.2.** records of the status of users' security clearances are kept; and ☐
- **R10.3.** gateway premises access restrictions on personnel are documented. ☐

R11. Personnel security policy **SHOULD** ensure that legal conditions obligated on employees and contractors are documented. ☐

R12. Physical security policy **MUST** ensure that:

- **R12.1.** all server rooms have a physical security certification to the appropriate server room standard for the system classification; and ☐
- **R12.2.** server room certification is performed by a suitable Certification or Accreditation Authority. ☐

R13. Key management policy **MUST** ensure that standards exist for the use and management of cryptographic keys and associated hardware and software. ☐

R14. Hardware security policy **MUST** ensure the:

- **R14.1.** classification labeling and registering of hardware; ☐

R14.2. method for secure disposal and maintenance of hardware is documented; and ☐

R14.3. media sanitisation and destruction requirements are documented. ☐

R15. Change management policy **SHOULD** ensure that:

R15.1. authorities for approving change are documented; ☐

R15.2. accreditation authority approves changes that will impact the security of Information and Communications Technology (ICT) system; and ☐

R15.3. associated system documentation will be updated to reflect changes. ☐

2.3 Contingency Policy

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

R16. There **MUST** be a clear correlation between the RA and the Contingency Policy. ☐

R17. The Contingency Policy **MUST** ensure that the critical management objectives for a contingency plan are documented. ☐

R18. The Contingency Policy **SHOULD** ensure that:

R18.1. a definition of an "incident", and the authority responsible for declaration of an incident are documented; ☐

R18.2. definitions of outages, and the appointment responsible for declaration of each grade of an outage are documented; ☐

R18.3. recovery time objectives, for the various grades of outages are documented; ☐

R18.4. testing regime objectives and reporting of status of backup systems are documented; and ☐

R18.5. on-line and off-line redundancy are documented. ☐

R19. The results of the RA **SHOULD** be used to provide guidance for required recovery times. ☐

2.4 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.

R20. Incident Detection and Response Policy **SHOULD** include the following components:

R20.1. detecting security incidents; ☐

R20.2. managing security incidents; ☐

R20.3. reporting of incidents; and ☐

R20.4. incident response plan. ☐

R21. 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. ☐

R22. Incident Detection and Response Policy **MUST** ensure that for managing security incidents:

R22.1. the process for internal reporting of security incidents is documented; ☐

R22.2. incidents are recorded and logged; ☐

R22.3. possible data spillage is minimized; and ☐

R22.4. malicious code is mitigated against. ☐

R23. Incident Detection and Response Policy **MUST** ensure that for the reporting of security incidents:

R23.1. DSD and connected gateway customers are addressees on off-line, analytical reports; ☐

R23.2. analytical reports are sent at least quarterly to DSD and connected gateway customers; ☐

R23.3. DSD is notified as soon as practicable of all Category 3 or higher incidents (as defined in ISIDRAS); ☐

R23.4. DSD is informed of incidents that require formal investigative action; and ☐

R23.5. users and clients are regularly informed on how to report security incidents to their Information Technology Security Administrator (ITSA) or equivalent in accordance with organisational procedures. ☐

R24. Incident Detection and Response Policy **SHOULD** ensure that for reporting of security incidents:

R24.1. timely reporting is done via the ISIDRAS reporting scheme; ☐

R24.2. DSD and connected gateway customers receive the report in the expected timeframe; and ☐

R24.3. if necessary, the report is formally acknowledged or reported to a higher level. ☐

R25. Incident Detection and Response Policy **MUST** ensure that the incident response plan:

R25.1. is based on the incident grading definitions; ☐

R25.2. the response procedures are realistic and achievable, and include the category of incident to be reported on a timely basis; and ☐

R25.3. agencies keep archives of logs for no less than 12 months. ☐

R26. Archive logs **SHOULD** be stored securely off-site. ☐

3.0 Gateway Design Methodology

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

3.1 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.

R27. The mandatory firewall **MUST** be a DAP. ☐

R28. The mandatory firewall **SHOULD** be configured in accordance with the security target and certification report. ☐

R29. Functionality required to provide interface separation **SHOULD** be a part of the evaluation of that firewall. ☐

R30. The protection of services provided by the gateway **SHOULD** be based on:

R30.1. the function of the service; ☐

R30.2. the classification of the data; ☐

R30.3. the data the service could have access to (eg other networks); and ☐

R30.4. known vulnerabilities of the service that could be exploited and the impact of their exploitation. ☐

3.2 Mandatory Design Criteria

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

R31. Network traffic to any device on either the internal network or the DMZ **MUST** be denied by default. ☐

R32. Access to services between multiple internal networks (if any) using the firewall **MUST** be denied by default. ☐

R33. All traffic traversing between networks **SHOULD** be routed through the gateway (including firewall(s)). ☐

R34. Organisations **MUST** understand the risks associated with all external connections and have documented strategies to treat these risk. ☐

R35. All implementations of cryptographic services in the gateway, including those for confidentiality, authentication, non-repudiation or data integrity **MUST** be included within the ☐

scope of the gateway certification.

R36. Any cryptographic products used in the gateway environment **MUST** be a DACP or a DAP appropriate to the classification level of the gateway. A maximum certification level of provisional may be granted for gateways using DAPs that are in evaluation. ☐

R37. All communication links between the internal network components and the firewall, where the communications path is not physically controlled by agency and contractor staff **MUST** be protected by a DSD approved method. ☐

R38. Firewall management **MUST** be provided via a secure path. ☐

R39. If a remote management feature is used, it **SHOULD** have been part of the product's evaluation. ☐

R40. Services **SHOULD NOT** be passed directly from the outside network to the inside network. ☐

R41. The internal and external border router(s) **SHOULD NOT** be relied upon for access control ☐

3.3 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.

R42. There **MUST** be a clear correlation between the RA and the gateway design. ☐

R43. Protocol specific security services available on gateway servers **SHOULD** be determined by business requirements and the RA. ☐

R44. The business continuity strategy for the gateway **MUST** be based on the policy. ☐

R45. Audit log backups **SHOULD** be treated differently if evidence/forensic capabilities for the data contained in these logs is required. ☐

R46. Archive, storage and management of audit logs **SHOULD** reflect the requirements of the Incident Detection and Response Policy/Plan. ☐

R47. 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 redundancy. ☐

R48. Auditing or logging services **MUST** be used to:

R48.1. monitor the real level of threat; ☐

R48.2. provide real time alarms to critical events; and ☐

R48.3. monitor the privileged users within the gateway. ☐

R49. The results of the Incident Detection and Response Policy (IDRP) **SHOULD** drive the requirements for auditing or logging. ☐

R50. Logs **SHOULD** be provided to monitor the administration of the gateway. ☐

R51. 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. ☐

R52. The following events **SHOULD** be logged for the firewall, DMZ servers and other critical components, for both successful and unsuccessful attempts:

- **R52.1.** logon and logoffs; ☐
- **R52.2.** boot and initialisation; ☐
- **R52.3.** shutdown, and associated details; ☐
- **R52.4.** restart, and associated details; ☐
- **R52.5.** changes to the firewall configuration; ☐
- **R52.6.** policy exceptions; ☐
- **R52.7.** password changes; ☐
- **R52.8.** TCP/UDP/ICMP connection requests; and ☐
- **R52.9.** application connection type, and data volume transferred. ☐

R53. For each event that is logged, the following information **SHOULD** be logged:

- **R53.1.** event name or description; ☐
- **R53.2.** date and time; ☐
- **R53.3.** account Id; ☐
- **R53.4.** command parameter; ☐
- **R53.5.** IP source and destination address; ☐
- **R53.6.** protocol code or description; and ☐
- **R53.7.** source and destination port. ☐

3.4 Critical Security Configuration

R54. Critical Security Configurations **SHOULD** include:

- **R54.1.** system backup configuration; and ☐
- **R54.2.** system device configuration. ☐

R55. The system device configuration **SHOULD** include:

- **R55.1.** firewall access lists; ☐
- **R55.2.** firewall management configuration; ☐

R55.3. encrypted modem configuration, including key management issues; and ☐

R55.4. web proxy server configuration. ☐

3.5 Design Documentation

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

R56. The design documentation **MUST** include:

R56.1. gateway logical/infrastructure diagram; ☐

R56.2. list of requirements; ☐

R56.3. list of critical configuration; and ☐

R56.4. detailed configuration document. ☐

4.0 Gateway Security Management

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

4.1 Security Administration Tasks

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

R57. The security administration task **MUST** include:

R57.1. accounts administration plan and procedure; ☐

R57.2. privileged user plan (ACSI 33 3.6.20); ☐

R57.3. access control plan and procedure(ACSI 33 3.6.30); ☐

R57.4. key management plan (ACSI 33 Part 3, Chapter 9); ☐

R57.5. user awareness plan (ACSI 33 Part 3, Chapter 2); ☐

R57.6. hardware security plan and procedure (ACSI 33 Part 3, Chapters 3 and 4); and ☐

R57.7. change management plan and procedure (ACSI 33 Part 2, Chapter 8). ☐

R58. Accounts administration plan and procedure **MUST** detail:

R58.1. profile of system accounts; ☐

R58.2. users allowed an account; ☐

R58.3. removal of old accounts; and ☐

R58.4. outline of account administration record keeping. ☐

R59. Privileged user plan and procedure **MUST** detail:

R59.1. privileged accounts; and ☐

R59.2. who holds is allowed to hold privileged accounts. ☐

R59.3. how privileged accounts are controlled and accountable; ☐

R59.4. rules on privileged accounts (for example, administrators are assigned individual accounts to ensure all admin tasks are accountable); and ☐

R59.5. definition on type of work allowed to be performed on privileged accounts. ☐

R60. Access control plan and procedure **SHOULD** detail:

R60.1. the users (including user groups); ☐

R60.2. allocated/allowed resources; ☐

R60.3. how users' access is limited; ☐

R60.4. how to perform access control changes; and ☐

R60.5. who can authorise access control changes. ☐

R61. Key management plan and procedure **MUST** detail:

R61.1. how keys are derived; ☐

R61.2. how often they are changed for each system; ☐

R61.3. users that are allowed access; and ☐

R61.4. actions to be taken in event of compromise or replacement. ☐

R62. Hardware security plan and procedure **SHOULD** detail:

R62.1. systems requiring backup; ☐

R62.2. frequency of backup; ☐

R62.3. period of storage; ☐

R62.4. media reuse/disposal; and ☐

R62.5. archival of logs or audit trails. ☐

R63. User awareness plan **SHOULD** detail:

R63.1. processes for initiating and maintaining a program so users are aware of their responsibilities; ☐

R63.2. processes to ensure training programs are aligned with user responsibilities; and ☐

R63.3. the appropriate activities for use of the services and safe practices for use of the services. ☐

R64. The change management plan and procedure **MUST** contain:

R64.1. stakeholders in the change process; ☐

R64.2. the responsibilities for approving changes to systems; ☐

R64.3. the process by which changes are approved; ☐

R64.4. the communication of change details to all relevant persons; and ☐

R64.5. the records to be maintained.

R65. There **MUST** be a clear correlation between gateway policy and the security administration task plans and procedures. ☐

R66. For gateway management there **MUST** be demonstrated evidence of implementation of the security administration task plans and procedures. ☐

R67. Operators and administrators **SHOULD** utilise hard copies of the procedures to undertake the duties detailed in them. ☐

R68. hard copies of procedures **SHOULD** be readily available in event of a system outage or compromise. ☐

4.2 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.

R69. The proactive security checking tasks **MUST** detail:

R69.1. those responsible for checking the gateway system; ☐

R69.2. the components that will be checked and by what means (i.e. whether tools are required); ☐

R69.3. how often these checks are to be undertaken; and ☐

R69.4. the authority that is to receive the reports. ☐

R70. The configuration items that require checking and the regularity of checking **MUST** be derived from the critical configuration list and the relevant Security Policy. ☐

R71. The proactive security checking tasks **MUST** include:

R71.1. firewall configuration checking plan and procedure; ☐

R71.2. proxy server configuration checking plan and procedure; ☐

R71.3. cryptographic configuration checking plan and procedure; and ☐

R71.4. alarm and access control plan and procedure. ☐

R72. The firewall configuration checking plan and procedure **MUST** detail:

R72.1. items that need to be checked; ☐

R72.2. what tool will be used to check them; ☐

R72.3. what checksum algorithm is being used; ☐

R72.4. how often this will be undertaken; ☐

R72.5. how the reporting is to be undertaken; ☐

R72.6. the appointment(s) responsible for checking; and ☐

R72.7. who should receive the reports. ☐

R73. The proxy server configuration checking plan and procedure **MUST** detail:

R73.1. items that need to be checked; ☐

R73.2. what tool will be used to check them; ☐

R73.3. what checksum algorithm is being used; ☐

R73.4. how often this will be undertaken; ☐

R73.5. how the reporting is to be undertaken; ☐

R73.6. the appointment(s) responsible for checking; and ☐

R73.7. who should receive the reports. ☐

R74. The cryptographic configuration checking plan and procedure **MUST** detail:

R74.1. items that need to be checked; ☐

R74.2. what tool will be used to check them; ☐

R74.3. what checksum algorithm is being used; ☐

R74.4. how often this will be undertaken; ☐

R74.5. how the reporting is to be undertaken; ☐

R74.6. the appointment(s) responsible for checking; and ☐

R74.7. who should receive the reports. ☐

R75. The alarm and access control plan and procedure **MUST** detail:

R75.1. items that need to be checked; ☐

R75.2. what tool will be used to check them; ☐

R75.3. what checksum algorithm is being used; ☐

R75.4. how often this will be undertaken; ☐

R75.5. how the reporting is to be undertaken; ☐

R75.6. the appointment(s) responsible for checking; and ☐

R75.7. who should receive the reports. ☐

R76. There **MUST** be a clear correlation between gateway policy and the proactive security checking tasks plans and procedures. ☐

R77. For gateway management there **MUST** be demonstrated evidence of implementation of the proactive security checking tasks plans and procedures. ☐

4.3 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.

R78. The documentation for proactive security audit **MUST** include real-time reporting and off-line or analytical reporting plans and procedures. ☐

R79. The real-time 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 would be used for this function (if any); ☐

R79.4. how often these checks should be undertaken; and ☐

R79.5. the appointment that is to receive the reports. ☐

R80. The off-line or analytical reporting plan and procedure **SHOULD** detail:

R80.1. who is responsible for checking the audit trails; ☐

R80.2. the specific objectives of the checking; ☐

R80.3. the tools that would be used for this function (if any); ☐

R80.4. how often these checks should be undertaken; and ☐

R80.5. the appointment that is to receive the reports. ☐

R81. The information required for these tasks **MUST** be derived from the outcomes of the gateway design and the relevant security policy. ☐

R82. There **MUST** be a clear correlation between gateway policy and the proactive security audit tasks plans and procedures. ☐

R83. For gateway management there **MUST** be demonstrated evidence of implementation of the proactive security audit tasks plans and procedures. ☐

4.4 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.

R84. 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. ☐

R85. There **MUST** be a clear correlation between gateway policy and the contingency plans and procedures. ☐

R86. For gateway management there **MUST** be demonstrated evidence of implementation of the contingency plans and procedures. ☐

4.5 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.

R87. 132. Organisations **SHOULD** develop and maintain procedures in addition to the incident response plan that: (ACSI 33 2.8.34)

R87.1. detect potential security breaches; ☐

R87.2. establish the cause of any security incident, whether accidental or deliberate; ☐

R87.3. detail the action required to recover and minimise the exposure to a system compromise; ☐

R87.4. assist in reporting the incident. (e.g. use of ISIDRAS); and ☐

R87.5. promote prevention of incidents and limit recurrences of incidents. ☐

R88. 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. ☐

R89. Identified actions (eg. disconnecting the gateway) **SHOULD** map to the incident categories identified in the incident detection and response policy. ☐

R90. Incident investigation, reporting, evidence preservation, media control and recording, and system recovery procedures **SHOULD** to be outlined in relation to each category of incident. ☐

R91. The appointment(s) responsible for performing incident response also **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	