

UNCLASSIFIED

Gateway Certification Guide V4.0.0



Australian Government
Department of Defence

Defence Signals Directorate

Gateway Certification Guide

VERSION 4.0.0

Point of Contact: Computer Network Vulnerability Team

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

© Australian Government 2008

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.

Page 1

UNCLASSIFIED

© Commonwealth of Australia 2008

UNCLASSIFIED

Gateway Certification Guide V4.0.0

Document Change Record

Version	Changed By	Date	Changes
4.0.0	Computer Network Vulnerability Team	April 08	Update for September 2007 ACSI 33. Gateway certification policy brought into line with ACSI 33 and the PSM.

Table of Contents

1.0 Gateway Risk Assessment.....	7
2.0 Gateway Policy Development.....	8
2.1 Access Policy.....	8
2.2 Remote Access Policy.....	8
2.3 Security Policy.....	9
2.4 Contingency Policy.....	12
2.5 Incident Detection and Response Policy.....	12
3.0 Gateway Design Methodology.....	13
3.1 Gateway Devices.....	13
3.2 Cryptographic Devices.....	14
3.3 Gateway Components.....	15
3.4 Network Configuration.....	15
3.5 Critical Security Configuration.....	15
3.6 Risk Based Security Criteria.....	16
4.0 Gateway Security Management.....	18
4.1 Security Administration Tasks.....	18
4.2 Intrusion Detection	19
4.3 Proactive Security Audit.....	20
4.4 Incident Detection and Response Plan and Procedure.....	22

Introduction

Australian Government agencies are required by the Protective Security Manual (PSM) to consider the security of their electronic information systems and to implement safeguards designed to adequately protect these systems. The degree of protection for these systems must be commensurate with the risk.

The Information Security Group of the Defence Signals Directorate (DSD) has identified a continuing need for perimeter security (or gateway) protection in addition to effective and appropriate internal security controls. This protection is essential when an organisation connects to an untrusted network. The number of threats to systems, data and applications, and the high level of threat likelihood, dictates that appropriately managed safeguards are required to minimise the risk of intrusion or compromise.

Purpose

The Gateway Certification process aims to provide agencies or Australian Government service providers with an independent assessment from DSD or through I-RAP that their gateway has been configured and managed to Australian Government standards, and that appropriate safeguards are implemented and operate effectively.¹ This assurance provides clients using the gateway with a reasonable level of trust in the service provided. This document is designed to assist organisations seeking or renewing certification.

This document serves as a reference detailing the areas of specific concern to the assessors conducting a certification and allows organisations to scope, cost and resource the security requirements in advance of the certification process itself. Accordingly, this document provides a reference for verification of any gateway.

This document should be used in conjunction with the Australian Government Information and Communications Technology Security Manual (ACSI 33) produced by DSD. The Gateway Certification Checklist found with this guide on the DSD website (<http://www.dsd.gov.au>) can also assist preparation for certification.

Related Documentation

Related documentation for assessors to seek further guidance includes:

- Protective Security Manual (PSM) 2005, Attorney General's Department;
- Australian Government Information & Communications Technology Security Manual (ACSI 33) September 2007, Information Security Group, Defence Signals Directorate;
- Gateway Certification Checklist V3.0.0, Information Security Group, Defence Signals Directorate.

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

Keywords

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

Keyword	Interpretation
MUST	The item is mandatory for certification. Government agencies deviating from a MUST , MUST follow the process outlined in ACSI 33 1.1.25 and Part A of the PSM. Private entities seeking to deviate from a MUST , MUST seek approval for the proposed deviation directly from DSD.
MUST NOT	Non-use is mandatory for certification. Government agencies deviating from a MUST NOT , MUST follow the process outlined in ACSI 33 1.1.25 and Part A of the PSM. Private entities seeking to deviate from a MUST NOT , MUST seek approval for the proposed deviation directly from DSD.

¹ The Infosec Registered Assessors Program (I-RAP) is a DSD initiative designed to register suitably qualified information security assessors to conduct work to Australian Government standards.

SHOULD	<p>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.</p> <p>Note: Organisations deviating from a SHOULD, MUST document (ACSI 33 1.1.26):</p> <ul style="list-style-type: none"> • the reasons for the deviation; • an assessment of the residual risk resulting from the deviation; • the acceptance of the risk by a responsible authority; • a date by which to review the decision; • the IT Security Adviser's (ITSA's) involvement in the decision; and • management's approval. <p>DSD RECOMMENDS that ITSAs retain a copy of all deviations.</p>
SHOULD NOT	<p>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 an authorised organisation security representative.</p> <p>Note: Organisations deviating from a SHOULD NOT, MUST document (ACSI 33 1.1.26):</p> <ul style="list-style-type: none"> • the reasons for the deviation; • an assessment of the residual risk resulting from the deviation; • the acceptance of the risk by a responsible authority; • a date by which to review the decision; • the ITSA's involvement in the decision; and • management's approval. <p>DSD RECOMMENDS that ITSAs retain a copy of all deviations.</p>
RECOMMENDS RECOMMENDED	<p>A recommendation or suggestion.</p> <p>Note: Organisations deviating from a RECOMMENDS or RECOMMENDED, are encouraged to document the reason(s) for doing so.</p>

Definitions

Organisation, or any of its derivations, is used to refer to any Government Agency or Department or any private entity seeking certification.

Please refer to the glossary in ACSI 33 for a comprehensive list of additional technical definitions.

Gateway Certification Process

Gateway Certification is a process to verify that a gateway is being managed to Australian Government standards. **The certification process does not provide any guarantee that the gateway or any connected networks will not be compromised**; rather that its design, management and operation is appropriate to the assessed level of risk. Checks will provide a degree of assurance that management processes are satisfactory for the continued, secure operation of the gateway.

The certification process can be broken down into five stages. ACSI 33 2.7.34 provides more details.

Conditions of Certification

Levels of Certification

The different levels of certification are:

- **Full Certification:** This is awarded to gateways that are compliant with all the requirements

for gateway certification based on a comprehensive evaluation.

- **Provisional Certification:** This 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:** This should be undertaken on all certified gateways at least every 12 months, and also at initiation of a major change that could alter the integrity of the security of the gateway (ACSI 33 2.7.43). Examples of events that meet this definition can be found in ACSI 33 2.7.43.

Certification Letter

As part of the certification letter, any specific conditions of certification will be stated. Failure to meet conditions of the certification letter may result in withdrawal of the certification. The broad conditions include but are not limited to:

- advice to DSD on major changes to key policy, process or technical components, before these changes are implemented; and
- discussion with DSD on any changes to the analysed threat level.

Reporting

Certified gateways **MUST** provide a report to DSD at intervals not exceeding three months detailing any suspicious or unusual traffic detected by the gateway. These reports should be by exception, and include only those events that indicate a potential compromise of gateway or Australian Government customer security.

Advertising

Any advertisement mentioning DSD by name **MUST** be made available for review by DSD prior to publication.

Gateway Development Process

The development process focuses on a number of related issues, specifically a review of:

- risk assessment;
- security policies;
- gateway design;
- installation and configuration; and
- security management plans and procedures.

The titles of the documents given in this guide are guidelines; organisations may title their policy sections and documents as appropriate. To assist the certification process, DSD **RECOMMENDS** that a document providing a map between the titles given in this document and the titles used by the organisation be submitted during certification.

As part of the certification process, the assessor needs to specifically look for adherence to minimum standards, gaps and inconsistencies, mapping of the results of the risk assessment to the design and operation of the gateway, and realistic and achievable plans and procedures.

The assessor needs to also verify that threats are identified, assessed and addressed appropriately, and that the stated controls are working effectively.

1.0 Gateway Risk Assessment

Organisations **MUST** have security risk assessments, policies and plans that cover gateway systems (ACSI 33 2.4.4).

The gateway **SHOULD** be covered by a comprehensive Security Risk Management Plan (SRMP) (ACSI 33 2.4.6).

2.0 Gateway Policy Development

The Gateway Policy comprises high-level statements that describe the functional requirements and the protections for the gateway. Assessors undertaking a certification of the gateway need to look for realistic policies that are implemented as part of the gateway management and operation.

Gateway Policy has a number of components including Access, Security, Contingency, Incident Detection and Response, and Configuration Control.

2.1 Access Policy

Organisations **MUST** (ACSI 33 3.6.2):

- develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering user:
 - 1) identification;
 - 2) authentication;
 - 3) authorisation; and
- make users aware of these policies, plans and procedures.

All system users **MUST** be (ACSI 33 3.6.6):

- uniquely identifiable; and
- authenticated on each occasion that access is granted to the system.

As a minimum, all privileged users **MUST** (ACSI 33 2.1.25):

- comply with the relevant policies, plans and procedures for the system they are using;
- possess a security clearance at least equal to the highest classification of information processed on the system;
- protect the authenticators for privileged accounts at the highest level of information it secures; Example: Passwords for root and administrator accounts.
- not share authenticators for privileged accounts without approval;
- be responsible for all actions under their privileged accounts;
- use privileged access only to perform authorised tasks and functions; and
- report all potentially security-related information system problems to the ITSA.

Organisations **MUST** (ACSI 33 2.1.26):

- restrict privileged access to the minimum required to fulfil designated roles; and
- closely audit privileged access.

Access Policy **SHOULD** ensure that (ACSI 33 3.6.21):

- administrators are assigned an individual account for the performance of their administration tasks;
- privileged accounts are kept to a minimum; and
- privileged accounts are used for administrative work only.

Organisations **SHOULD** (ACSI 33 3.7.19):

- maintain a secure log of all authorised users, their user identification and who provided the authorisation and when; and
Note: In many cases this could be achieved by retaining the account application form filled in by the user and/or their supervisor.
- maintain the log for the life of the system.

DSD **RECOMMENDS** that multiple methods are combined for authenticating users (ACSI 33 3.6.7).

2.2 Remote Access Policy

If remote access is used, organisations **SHOULD** provide an organisation accredited device for remote access if the remote worker is able to access sensitive information (ACSI 33 3.10.48).

Organisations **SHOULD** disable split tunnelling when using VPN technology to connect remotely to the gateway (ACSI 33 3.10.50).

Organisations **SHOULD** authenticate each user and device prior to allowing remote connection to gateway services that are not intentionally anonymous (ACSI 33 3.10.51).

Organisations **SHOULD** implement additional security controls for devices used to connect remotely to the gateway (ACSI 33 3.10.52).

Organisations **SHOULD** consider the following additional controls when implementing remote access systems (ACSI 33 3.10.52):

- Appropriate Use policies and procedures;
- user training and education;
- storage and transit encryption;
- application white listing;
- host intrusion detection systems;
- network access control;
- host based personal firewalls;
- device-level authentication;
- enhanced user-level authentication e.g. two factor authentication; and
- a hardened standard operating environment.

DSD **RECOMMENDS** that organisations do not allow the use of privileged access remotely (ACSI 33 3.10.53).

Please see ACSI 33 3.10.54 for additional information relating to remote access for HIGHLY PROTECTED gateways.

Organisations **MUST** ensure that the standards for the use of DSD Approved Cryptographic Protocols (DACPs) are met when using Secure Shell (SSH) (ACSI 33 3.9.25).

ACSI 33 3.9.25 – 3.9.27 contain further information that **SHOULD** be followed when using SSH.

2.3 Security Policy

Security Policy needs to detail the management of various security aspects of the gateway.

Gateways **MUST** be covered by an ICT Security Policy document (ICTSP) (ACSI 33 2.4.5).

ACSI 33 2.3.8 provides a recommended process for developing an ICTSP.

Gateways **SHOULD** be covered by a System Security Plan (SSP) (ACSI 33 2.4.7).

ACSI 33 2.5.8 provides a recommended process for developing an SSP.

Organisations **SHOULD** ensure that the SRMP, ICTSP, SSP and Standard Operating Procedures (SOPs) are logically connected and consistent for each system (ACSI 33 2.4.12).

All ICT security documents **SHOULD** be formally approved and signed off by an appropriate person (ACSI 33 2.4.15).

Organisations **MUST** use the classification scheme defined in the PSM Part C.

Access Control:

Organisations **MUST** specify the level of security clearance and briefings required for each type of user given system access/accounts (ACSI 33 3.2.13).

Physical Security and Media Control:

Server and communications equipment **SHOULD** be secured in accordance with the area, room and container standards as shown in ACSI 33 3.1.17.

PSM Part E 7.34 and ACSI 33 2.7.33 outline physical security certification requirements. Non-government organisations seeking gateway certification **MUST** obtain ASIO T4 physical security certification.

DSD **RECOMMENDS** that organisations contact T4 for advice prior to the design and construction of a secure room/facility (ACSI 33 3.1.12).

Removable media containing classified information **MUST** be stored in accordance with the PSM requirements for information of that classification (ACSI 33 3.1.46).

ACSI 33 3.1.24 provides the physical security requirements for the operation and secure storage of workstation media. These requirements **MUST** be complied with.

ACSI 33 3.1.35 provides the physical security requirements for network infrastructure carrying unencrypted information. These requirements **MUST** be complied with.

All patch panels, fibre distribution panels, and all structured wiring enclosures **SHOULD** be located within locked spaces that prevent casual access by general users (ACSI 33 3.1.33). DSD **RECOMMENDS** that the ITSA control the keys or equivalent access mechanism to these locked spaces (ACSI 33 3.1.33).

The classification of all media **MUST** be readily visually identifiable (ACSI 33 3.4.18). This **SHOULD** be achieved by labelling media with a protective marking that states the maximum classification and set of caveats applicable to the information stored on the media (ACSI 33 3.4.18). Other methods may be required where the media is small, has no space available for labels, is used in hardware where there are extremes of temperature or could interfere with the operation of the media or its surrounding hardware. In these instances, a colour coding system or the use of indelible markers to label media may be possible. The option to regard all equipment without labels as a particular classification should only be used as a last resort.

Hardware containing media **MUST** be classified at or above the classification of the media (ACSI 33 3.4.10).

Storage media **MUST** be reclassified if (ACSI 33 3.4.16):

- information copied onto that media is of a higher classification; or
- information contained on that media is subject to a classification upgrade.

Organisations **MUST** use an approved method of sanitisation when media is moving from a higher classification to a lower classification (ACSI 33 3.4.26). Approved methods are described in ACSI 33 3.4.25 to 3.4.32.

Repairs and maintenance for hardware containing classified media **SHOULD** be carried out by appropriately cleared and briefed personnel (ACSI 33 3.4.33).

If cleared personnel are not able to perform the work, uncleared personnel may be used (ACSI 33 3.4.34). The uncleared personnel **SHOULD** be escorted (ACSI 33 3.4.35).

DSD **RECOMMENDS** that support contracts do not require the return of classified defective media (ACSI 33 3.4.33).

Organisations **MUST** have a documented process for the disposal of hardware (ACSI 33 3.4.39).

Organisations **MUST** (ACSI 33 3.4.36):

- sanitise and declassify, or destroy media containing classified material before disposal; and
- use approved methods to declassify or destroy media.

ACSI 33 3.4.19 and 3.4.23 contain extra information for HIGHLY PROTECTED media.

Organisations **MUST** perform the destruction of classified material under the supervision of an officer cleared to the highest level of media being destroyed (ACSI 33 3.4.42).

The officer **MUST** (ACST 33 3.4.42):

- supervise the handling of the material to the point of destruction; and
- ensure that the destruction is complete.

Cryptographic Security:

Organisations **SHOULD** develop a Key Management Plan (KMP) where they have implemented a configurable cryptographic system in hardware or software (ACSI 33 3.9.71).

Please see ACSI 33 3.9.72 for requirements relating to HIGHLY PROTECTED gateways.

The level of detail included with the KMP **MUST** be consistent with the criticality and classification of the information to be protected (ACSI 33 3.9.73).

ACSI 33 3.9.73 describes the minimum contents which **SHOULD** be documented in the KMP.

Organisations **SHOULD** be able to readily account for all transactions relating to cryptographic system material including identifying hardware and software, and who has been issued with the equipment (ACSI 33 3.9.66).

Audits of cryptographic system material **SHOULD** be conducted (ACSI 33 3.9.67):

- on handover/takeover of administrative responsibility for the system;
- on change of individuals with access to the cryptographic system; and
- at least annually.

Change Management:

Organisations **SHOULD** ensure that (ACSI 33 2.8.7):

- the change management process defined in ICT security documentation is followed;
- proposed changes require approval by the documented authority;
- any proposed change that may impact the security of the ICT system is submitted to the Accreditation Authority for approval; and
- all associated system documentation is updated to reflect changes.

The change management process **SHOULD** define appropriate actions to be followed before and after urgent changes are implemented (ACSI 33 2.8.7).

Education and Training:

Organisations **MUST** (ACSI 33 3.2.7):

- ensure that all personnel who have access to ICT systems have sufficient training; and
- provide ongoing ICT security training and awareness for staff on topics such as responsibilities, potential security risks and countermeasures.

The degree and content of security training **SHOULD** be aligned to user responsibilities (ACSI 33 3.2.9).

2.4 Contingency Policy

PSM Part B 5.67 - 5.68 and Part C requires organisations to determine availability requirements for their systems. Once these have been determined, organisations **MUST** implement appropriate measures to support these requirements (ACSI 33 2.8.13).

Such measures may include:

- information backups;
- remote storage;
- remote processing;
- redundant ICT systems; and
- redundant environmental systems.
Example: Uninterruptible Power Supply (UPS).

Organisations **SHOULD** (ACSI 33 2.8.14):

- backup all information identified as critical;
- store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the standards for the classification of the information; and
- test backup and restoration processes regularly to confirm their effectiveness.

Movement of classified information to and from remote storage **MUST** be done in accordance with the PSM Part C.

2.5 Incident Detection and Response Policy

These policy statements could have been covered either by the Security or Contingency Policy. However, DSD **RECOMMENDS** that it be addressed separately to reflect its importance in the management of a secure gateway. A security incident, in ICT terms, is an event that impacts on the confidentiality, integrity or availability of a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction.

Organisations **MUST** develop, implement and maintain tools and procedures, derived from a risk assessment, covering the detection of potential security incidents, incorporating (ACSI 33 2.8.17):

- countermeasures against malicious code;
- intrusion detection strategies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

Organisations **SHOULD** use the results of the risk assessment to determine the appropriate balance of resources allocated to prevention versus detection (ACSI 33 2.8.17).

Organisations **MUST** (ACSI 33 3.5.69):

- develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering how to:
 - 1) minimise the likelihood of malicious code being introduced into the system(s);
 - 2) detect any malicious code installed on the system(s);
- make users aware of the policies, plans and procedures; and
- ensure that all instances of detected malicious code outbreaks are handled according to the procedures.

ACSI 33 2.8.30 provides a **RECOMMENDED** set of steps to follow when malicious code is detected.

DSD **RECOMMENDS** that systems infected with malicious code be re-built from trusted sources.

Organisations **SHOULD** (ACSI 33 2.8.24):

- encourage staff to note and report any observed or suspected security weakness in, or threats to, systems or services;
Examples: unexpected dialog boxes or excessive processing.
- establish and follow procedures for reporting software malfunctions;
- put mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored; and
- deal with the violation of organisational security policies and procedures by employees through a formal disciplinary process.

Organisations **MUST** detail security incident responsibilities and procedures in the SSP and in the SOPs (ACSI 33 2.8.22).

Staff **MUST** be directed to report security incidents to the ITSA as soon as possible after the incident is discovered (ACSI 33 2.8.23).

Standard procedures for all personnel with access to the system **SHOULD** include the requirement to notify the ITSA of (ACSI 33 2.8.28):

- any data spillage; and
- access to any data classified above that for which they are authorised.

When a data spill occurs, organisations **SHOULD** assume that the information has been compromised (ACSI 33 2.8.28).

Organisations **MUST** treat any such spillage as an incident, and follow the Incident Response Plan to deal with it (ACSI 33 2.8.28).

Please see ACSI 33 2.8.29 for additional requirements for HIGHLY PROTECTED gateways.

Organisations **SHOULD** ensure that all security incidents are recorded in a register. The purpose of the register is to highlight the nature and frequency of the incidents and breaches so that corrective action may be taken (ACSI 33 2.8.26).

By recording all ICT security incidents and breaches, the register may then be used as a reference for future risk assessments.

The recorded information **SHOULD** include, at a minimum (ACSI 33 2.8.26):

- the date the incident was discovered;
- the date the incident occurred;
- a description of the incident, including the people and locations involved;
- the action taken; and
- to whom the incident was reported.

Organisations **MUST** report significant ICT security incidents to DSD (ACSI 33 2.8.36).

Reporting of incidents to DSD **SHOULD** be undertaken using the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) (ACSI 33 2.8.34).

3.0 Gateway Design Methodology

The design of the gateway is important to the security of those services offered as part of the gateway implementation, and to those networks being protected by the gateway.

1. This section details the minimum design requirements for a gateway. The environments surrounding gateways differ between organisations. For this reason, organisations have to consider additional requirements identified in the risk assessment of their gateway design.

3.1 Gateway Devices

To enforce a security function related to the protection of official information and systems, organisations **SHOULD** select products from the Evaluated Products List (EPL) that have been evaluated against this security functional requirement, as identified in the Security Target,

Certification Report, and DSD Consumer Guide (ACSI 33 3.3.7).

Organisations **SHOULD** ensure that products are installed and configured in a manner consistent with the evaluated configuration of the product (ACSI 33 3.3.17).

Firewalls **MUST** meet the minimum levels of assurance outlined in ACSI 33 3.10.34 – 3.10.35.

Organisations **SHOULD**, when possible, ensure that known security vulnerabilities in EPL products are corrected through a vendor-recommended patch or upgrade process (ACSI 33 3.3.19).

DSD **RECOMMENDS** that prior to patching EPL products, organisations consider (ACSI 33 3.3.19):

- the necessity of the patch;
- the testing of the patch;
- the environment in which the product is used; and
- any new functionality the patch may include.

When choosing a product, organisations **MUST** document (ACSI 33 3.3.9):

- the desired degree of assurance in the product's key functions;
- the actual degree of assurance provided by the chosen product, based on the level of evaluation it has received for its key functions;
- justification for any decisions to drop to the next level in the defined selection order of preference (the order of preference is found in ACSI 33 3.3.8); and
- acknowledgement and acceptance of any risk introduced by the use of a product of lower assurance than desired, particularly if using a product that has not, and may never, complete all relevant evaluation processes.

Organisations **SHOULD** (ACSI 33 3.5.14):

- monitor relevant sources for information about new vulnerabilities, patches and hardening methods in software and hardware used by the organisation;
- take corrective action when vulnerabilities that could affect gateway systems are discovered;
- follow their documented change management procedures when applying patches or hardening systems, including the testing of patches and updates prior to their application to live systems; and
- replace obsolete software and hardware with products for which ongoing support is available.

Organisations **SHOULD** ensure that any leasing agreements for ICT equipment take into consideration the (ACSI 33 3.3.16):

- difficulties that may be encountered when the equipment requires maintenance; and
- sanitisation of the equipment prior to its return.

3.2 Cryptographic Devices

If using encryption to reduce the requirements for transmitting classified information over networks of a lower classification than that of the information, organisations **MUST** use encryption products that meet the minimum level of assurance, as shown in ACSI 33 3.9.7.

Before using an unevaluated product that implements a DSD Approved Cryptographic Protocol (DACP), organisations **MUST** (ACSI 33 3.9.15):

- ensure that the minimum requirements as stated in ACSI 33 3.9.7 will be met; and
- consider and accept the risks.

When using an unevaluated product that implements a DACP, organisations **MUST** ensure that only DSD Approved Cryptographic Algorithms (DACAs) are used (ACSI 33 3.9.17).

The Secure Hashing Algorithms (SHA) family of hashing algorithms **SHOULD** be used wherever hashing is required (ACSI 33 3.9.12).

Symmetric encryption using AES or 3DES **SHOULD NOT** use Electronic Codebook (ECB) Mode (ACSI 33 3.9.13).

If IPsec is used, it **SHOULD** be used in tunnel mode (ACSI 33 3.9.39).

If Internet Security Association Key Management Protocol (ISAKMP) is used, Aggressive Mode **SHOULD** be disabled (ACSI 33 3.9.46).

3.3 Gateway Components

Organisations **SHOULD** ensure that gateways (ACSI 33 3.10.23):

- are the only communications routes into and out of internal networks;
- by default, deny all connections into and out of the network;
- allow only explicitly authorised connections;
- are managed via a secure path;
- provide sufficient audit capability to detect gateway security breaches and attempted network intrusions; and
- provide real-time alarms.

3.4 Network Configuration

Organisations **SHOULD** keep the network configuration under the control of a central network management authority (ACSI 33 3.10.5).

Organisations **SHOULD** commit to regularly reviewing the configuration to ensure it conforms to the documented configuration (ACSI 33 3.10.5).

Organisations **MUST** have (ACSI 33 3.10.6):

- a high level diagram showing all connections into the gateway; and
- a logical network diagram showing all network devices.

These diagrams **SHOULD** (ACSI 33 3.10.6):

- be updated as network changes are made; and
- include a "Current as at <date>" on each page.

For HIGHLY PROTECTED gateways, please see ACSI 33 3.10.7 for further guidance.

3.5 Critical Security Configuration

Security management processes designed to ensure the integrity of the gateway help to achieve the desired level of protection. While the proper configuration of the firewall at installation is important, the business processes used to pinpoint problems, correct errors, detect misconfigurations, respond to changes in threat, cater for maintenance issues and allow for changes in personnel are crucial to the gateway design. Those responsible for drafting the plans and procedures need to be aware of the critical configurations.

The configuration of critical devices used by the gateway needs to be specified in the critical configuration list. The list of items that require strict configuration controls will be determined by the risk assessment process. The list could include, but is not limited to:

- firewall access lists;
- firewall management configuration; and
- network encrypting devices configuration.

As devices are varied in how they produce configuration information, the information required by the assessor will vary with the types of devices used.

3.6 Risk Based Security Criteria

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

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

All server and workstation security objectives and mechanisms **SHOULD** be documented in the relevant SSP or similar document (ACSI 33 3.5.7).

Organisations **SHOULD** reduce potential vulnerabilities on gateway systems by (ACSI 33 3.5.8):

- removing unneeded software;
- removing unused accounts;
- removing unnecessary file shares;
- renaming required default accounts;
- replacing default passwords;
- ensuring patching is up-to-date;
- disabling unused features on installed software and operating systems; and
- disabling access to all unnecessary input/output devices at the BIOS level, which may include CD-ROMS, floppy disks, USB drives or wireless network interfaces. The risk assessment should be used to determine the specific devices that will be disabled.

DSD **RECOMMENDS** that organisations consider seeking and applying additional information on hardening techniques relevant to their specific equipment (ACSI 33 3.5.8).

DSD **RECOMMENDS** that organisations (ACSI 33 3.5.10):

- limit information that could be disclosed about what software is installed;

Examples:

- 1) User Agent on web requests disclosing the web browser type;
 - 2) network and email client information in email headers;
 - 3) email server software headers; and
- implement access controls on relevant objects to limit users and programs to the minimum access required to perform their duties. This may include application whitelisting.

Examples: Objects may include directories, files, programs, databases, and communications ports.

For further information for HIGHLY PROTECTED gateways, please see ACSI 33 3.5.11.

DSD **RECOMMENDS** that organisations develop a hardened Standard Operating Environment (SOE) for workstations, covering the (ACSI 33 3.5.12):

- requirements for hardening during installation;
- implementation of access controls on relevant objects to limit users and programs to the minimum access required to perform their duties;
- installation of workstation firewalls; and
- configuration of either remote logging or the transfer of local event logs to a central server.

For further information for HIGHLY PROTECTED gateways, please see ACSI 33 3.5.13.

DSD **RECOMMENDS** that organisations implement network access controls such as (ACSI 33 3.10.10):

- use of network access control protocols such as 802.1x on all network ports;
- for networks using Dynamic Host Configuration Protocol (DHCP), implement static MAC to IP address assignments; and
- implement port security on network switches to limit access based on MAC address and

disable all unused ports.

For further information for HIGHLY PROTECTED gateways, please see ACSI 33 3.10.11.

Where known vulnerabilities cannot be patched, organisations **SHOULD** use other protective measures as determined from a risk assessment (ACSI 33 3.5.15).

Appropriate protective measures may include:

- controls to prevent attacks from succeeding:
 - 1) email filters that strip potentially harmful content to email clients;
 - 2) web proxy filters that strip harmful content to web browsers;
 - 3) additional access controls on file and configuration settings;
 - 4) firewalls configured to deny by default;
- controls to detect attacks:
 - 1) virus, spyware and malware scanners; and
 - 2) other mechanisms as appropriate for the detection of exploits using the known vulnerability.

Where high risk servers, such as web, email, file and IP telephony servers, have connectivity to public domain networks, organisations **SHOULD** (ACSI 33 3.5.16):

- maintain effective functional separation between servers allowing them to operate independently;
- minimise communications between servers at both the network and filesystem level, as appropriate; and
- limit users and programs to the minimum access required to perform their duties.

Functional separation may be achieved by using dedicated physical machines or using virtualisation technology to create dedicated virtual machines.

DSD **RECOMMENDS** that organisations, for all servers and workstations (ACSI 33 3.5.70):

- install anti-virus scanners;
- ensure that users do not have the ability to disable the scanner;
- check vendor virus pattern signatures for updates daily;
- apply virus pattern signature updates as soon as possible after vendors make them available; and
- regularly scan all disks.

4.0 Gateway Security Management

The ongoing secure management of the gateway is paramount to ensuring a secure operating environment.

Gateway certifiers need to look for a clear correlation between gateway policy and all the plans and procedures.

The procedures need to be available for operators and administrators to utilise in the event of a gateway system outage or compromise.

4.1 Security Administration Tasks

A site security plan and SOPs **MUST** be developed (ACSI 33 3.1.20).

Information relating to the system-specific roles and responsibilities of IT security advisers, system managers, system administrators and system users **SHOULD** be included in the system documentation (ACSI 33 2.1.2).

Security SOPs **SHOULD** be developed for each of the following roles (ACSI 33 2.6.5):

- ITSA;
- System Manager;
- System Administrator; and
- System Users.

The ITSA, System Manager and System Administrator roles may have some overlap.

The ITSA and System Manager **SHOULD** be familiar with all SOPs (ACSI 33 2.6.5).

Procedures **SHOULD** be documented in the ITSA SOPs for (ACSI 33 2.6.10):

- instructing new users to comply with ICT security requirements;
- reviewing system audit trails and manual logs, particularly for privileged users;
- reviewing user accounts, system parameters and access controls;
- checking the integrity of system software;
- testing access controls;
- inspecting equipment and cabling;
- managing the review of removable media containing data that is to be transferred off-site;
- managing the review of incoming media for viruses or unapproved software;
- labelling, registering and mustering assets, including removable media; and
- reporting and managing security incidents, including involvement in physical security incident management where the incident could impact on ICT security.

Procedures **SHOULD** be documented in the System Manager SOPs for (ACSI 33 2.6.11):

- managing the ongoing security and functionality of system software and hardware, including:
 - 1) maintaining awareness of current software vulnerabilities;
 - 2) testing and applying software patches/updates;
 - 3) applying appropriate hardening techniques;
 - 4) updating anti-virus software;
- managing the destruction of unserviceable equipment and media;
- authorising new system users;
- approving and releasing changes to the system software or configuration;
- authorising access rights to applications and data; and
- recovering from system failures.

Procedures **SHOULD** be documented in the System Administrator's SOPs for (ACSI 33 2.6.12):

- securing the system out-of-hours if operations are not 24x7;
- implementing access rights to applications and data;
- adding and removing users;
- setting user privileges;

- cleaning up directories and files when a user departs or changes roles;
- backing up data, including audit logs;
- securing backup tapes; and
- recovering from system failures.

The System User's SOPs **SHOULD** document (ACSI 33 2.6.14):

- who is responsible for what aspects of security;
- a warning that:
 - 1) users' actions may be audited;
 - 2) users will be held accountable for their actions;
- guidelines on choosing and protecting passwords;
- guidelines on enforcing need-to-know on the system;
- what to do in the case of a suspected or actual security incident;
- the highest level of classified material that can be processed on the system and handling procedures for classified information;
- how to secure the workstation when temporarily absent;
- how to secure the workstation at the end of the day;
- procedures for controlling and sanitising media;
- procedures for labelling, handling and disposing of hardcopy;
- preventing overview of data by visitors; and
- what to do for hardware and software maintenance.

Gateway reviewers need to look for evidence that these SOPs are being followed.

Organisations **MUST** provide guidance to users on their responsibilities relating to ICT security, and the consequences of non-compliance (ACSI 33 2.6.15).

System Users **SHOULD** sign a statement that they have read and agree to abide by the System Users' SOP (ACSI 33 2.6.13).

SOPs **SHOULD** be maintained and updated (ACSI 33 2.6.7). This may be done as:

- a response to changes to the system; and
- part of a regular review of documentation.

Gateway assessors need to check for demonstrated evidence of implementation of the security administration task plans and procedures.

4.2 Intrusion Detection

Organisations **SHOULD** develop, implement and maintain an intrusion detection strategy, based on the results of a risk assessment, that includes (ACSI 33 3.7.5):

- appropriate intrusion detection mechanisms, including network-based IDS (NIDS) and host-based IDS (HIDS) as required;
- the audit analysis of event logs, including IDS logs;
- a periodic audit of intrusion detection procedures;
- user training and awareness programs; and
- a documented incident response procedure.

Organisations **SHOULD** deploy IDSs in all Internet gateways (ACSI 33 3.7.7).

When signature-based intrusion detection is used, organisations **SHOULD** keep the signatures up-to-date (ACSI 33 3.7.7).

DSD **RECOMMENDS** that an IDS be located within the gateway environment, immediately inside the outermost firewall (ACSI 33 3.7.7).

DSD **RECOMMENDS** that organisations deploy tools for (ACSI 33 3.7.10):

- the management and archival of security event information; and
- the correlation of events of interest.

4.3 Proactive Security Audit

Organisations **MUST** develop and document audit requirements reflecting the overall audit objectives, derived from the ICTSP and SRMP, covering (ACSI 33 3.7.26):

- the scope of audits;
- the audit schedule;
- actions to be taken when violations are detected;
- reporting requirements; and
- specific responsibilities.

Organisations **SHOULD** (ACSI 33 3.5.19):

- characterise all devices whose functions are critical, and those identified as being at high risk of compromise;
- store the characterisation information securely;
- update the characterisation information after every legitimate change to the system;
- as part of the ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise or a legitimate but incorrectly completed system modification has occurred;
- perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and
- resolve any detected changes in accordance with the documented incident management procedures.

DSD **RECOMMENDS** that organisations meet the requirement for characterisation using a DACA to perform cryptographic checksums (ACSI 33 3.5.19).

Organisations **MUST** develop and document logging requirements reflecting the overall audit objectives derived from the ICTSP and SRMP, covering (ACSI 33 3.7.12):

- the logging facility, including:
 - 1) log server availability requirements;
 - 2) the reliable delivery of log information to the log server;
- the list of events associated with a system or software component to be logged; and
- event log protection and archival requirements.

For each event identified as needing to be logged, organisations **MUST** ensure that the log facility records at least the following details, where possible (ACSI 33 3.7.16):

- date and time of the event;
- relevant user(s) or process;
- event description;
- success or failure of the event;
- event source (e.g. application name); and
- terminal location/identification.

2.Event logs **MUST** be (ACSI 33 3.7.17):

- protected from modification and unauthorised access;
- archived and retained for future access; and
- protected from whole or partial loss within the defined retention period.

ACSI 33 3.7.14 and 3.7.18 contain additional information for HIGHLY PROTECTED gateways.

The ITSA **SHOULD** be responsible for managing and auditing the event logs (ACSI 33 3.7.25).

A system management log **SHOULD** be used to record the following information (ACSI 33 3.7.20):

- sanitisation activities;
 - system start-up and shutdown;
 - component or system failures;
 - maintenance activities;
 - housekeeping activities;
- Examples: Backup and archival runs.

- system recovery activities; and
- special or out-of-hours activities.

DSD **RECOMMENDS** that organisations maintain system management logs for the life of the system (ACSI 33 3.7.21).

ACSI 33 3.7.22 contains additional information for HIGHLY PROTECTED gateways.

Organisations **SHOULD** ensure that a sufficient number of appropriately trained personnel and tools are available to analyse all logs for potential violations of security policy (ACSI 33 3.7.28).

DSD **RECOMMENDS** that an accurate time source is used consistently throughout the gateway to assist with the correlation of logged events across multiple systems (ACSI 33 3.7.16).

4.4 Incident Detection and Response Plan and Procedure

Organisations **MUST** develop an Incident Response Plan which, as a minimum, defines (ACSI 33 2.8.41):

- broad guidelines on what constitutes an incident;
- the minimum level of training for users and system administrators;
- the authority responsible for initiating investigations of an incident;
- the steps necessary to ensure the integrity of information supporting a compromise;
- the steps necessary to ensure that critical systems remain operational; and
- how to formally report incidents.

The Incident Response Plan **SHOULD** also contain (ACSI 33 2.8.42):

- clear definitions of the types of incidents that are likely to be encountered;
- the expected response to each incident type;
- the authority within the organisation who is responsible for initiating:
 - 1) a formal (administrative) investigation;
 - 2) a police investigation of an incident;
 - 3) an ASIO investigation of national security incidents, in accordance with Part G of the PSM;
- the criteria by which the responsible authority would initiate formal, police or ASIO investigations of an incident;
- references to other related documents;

Examples: Business Continuity Plan, Fraud Control Plan.

- which other organisations or authorities need to be informed in the event of an investigation being undertaken; and
- the details of the system contingency measures, or a reference to these details if they are located in a separate document.

Organisations **SHOULD** develop and maintain procedures supporting the plan to (ACSI 33 2.8.44):

- detect potential security breaches;
- establish the cause of any security incident, whether accidental or deliberate;
- detail the action to be taken to recover and minimise the exposure to a system compromise;
- report the incident; and
- document any recommendations on preventing a recurrence.

It is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

Organisations **SHOULD** (ACSI 33 2.8.32):

- transfer a copy of raw audit trails onto media such as CD-ROM or DVD-ROM for secure archiving, as well as securing manual log records for retention, and
- ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

Organisations may choose to request assistance from DSD for the (ACSI 33 2.8.25):

- analysis of incidents;
- identification of remedial measures to remove exploited vulnerabilities;
- minimisation of the likelihood of compromise; and
- overall assessment of the organisation's system security safeguards.

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

DSD's response will be commensurate with the urgency of the incident; a 24-hour, 7-day service is available if necessary. Contact details for reporting incidents to DSD are:

Email: incidents_at_dsd.gov.au
Phone: 02 6266 0009 (24x7)