

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0



Australian Government
Department of Defence

Defence Signals Directorate

Information System Review Checklist

VERSION 4.0.0

Point of Contact: Computer Network Vulnerability Team

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

Organisation: _____

Assessor: _____

© 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 (RECLASSIFY after first entry)

© Australian Government 2008

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

Document Change Record

Version	Changed By	Date	Changes
4.0.0	Computer Network Vulnerability Team	July 08	Update for September 2007 ACSI 33. ISR checklist brought into line with ACSI 33 and the PSM.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

Table of Contents

1	Introduction.....	4
2	Components for Compliance.....	6
3	Checklist Guidance.....	6
1.0	Security Documentation.....	10
1.1	Risk Management Plan (RMP).....	10
1.2	ICT Security Policy.....	10
1.3	System Security Plan (SSP).....	11
1.4	Standard Operating Procedures (SOPs).....	11
1.5	Policy Consistency.....	13
2.0	Security Organisation.....	14
2.1	Information Technology Security Adviser (ITSA).....	14
3.0	Asset Classification.....	15
3.1	Information Classification.....	15
4.0	Personnel Security.....	17
4.1	Security in Job Definition and Resourcing.....	17
4.2	User Training.....	17
4.3	Responding to Security Incidents and Malfunctions.....	17
5.0	Physical and Environmental Security.....	21
5.1	Security Environment.....	21
5.2	Equipment Security.....	21
5.3	General Controls.....	24
6.0	Communications and Operations Management.....	25
6.1	Operational Procedures and Responsibilities.....	25
6.2	Operation Management.....	25
6.3	Information System Management.....	26
6.4	Media Handling and Security.....	34
6.5	Exchanges of Information and Software.....	35
7.0	Access Control.....	38
7.1	Business Requirement for Access.....	38
7.2	User Access Management.....	38
7.3	User Responsibilities.....	39
7.4	Proactive Security Audit.....	40
8.0	Portable Computers, Portable Electronic Devices (PEDs) & Teleworking.....	42
8.1	Portable Computers and Portable Electronic Devices (PEDs).....	42

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

1 Introduction

1.1 Purpose

1. The following checklist is designed to assist assessors in the conduct of an Information System Review, to ensure an Information Communications and Technology (ICT) system is compliant with Defence Signals Directorate (DSD) standards. Infosec-Registered Assessor Program (I-RAP) assessors, DSD, and Australian Government agencies undertaking a review can use this document.
2. The checklist is intended for use with non-national security systems up to HIGHLY PROTECTED and national security systems up to RESTRICTED.

1.2 Related Documentation

3. Related documentation for assessors to seek further guidance include:
 - Protective Security Manual (PSM) 2005, Attorney General's Department; and
 - Australian Government Information & Communications Technology Security Manual (ACSI 33) September 2007, Information Security Group, Defence Signals Directorate.

1.3 Key Words

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

Keyword	Interpretation
MUST	Compliance with the MUST keyword should be seen in the context of maintaining the integrity of the security model used in ACSI 33. Failure to comply with MUST statements will usually require the implementation of risk management strategies that will achieve a comparable level of assurance, and may also require organisations to follow the waiver requirements outlined in Part A of the PSM if an ACSI 33 or PSM MUST is not being met. (ACSI 33 1.1.4 and 1.1.25).
MUST NOT	Compliance with the MUST NOT keyword should be seen in the context of maintaining the integrity of the security model used in ACSI 33. Failure to comply with MUST NOT statements will usually require the implementation of risk management strategies that will achieve a comparable level of assurance, and may also require organisations to follow the

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

	waiver requirements outlined in Part A of the PSM if an ACSI 33 or PSM MUST is not being met. (ACSI 33 1.1.4 and 1.1.25).
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>

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

1.4 Definitions

5. 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 services to the Australian Government.
6. Please refer to the glossary in ACSI 33 for a comprehensive list of additional technical definitions.

2 Components for Compliance

7. I-RAP assessors **MUST** forward the following documents to the DSD I-RAP Manager once the assessment is completed:
 - completed checklist;
 - additional requirements;
 - checklist comments (including rationale for decisions);
 - review report; and
 - compliance letter.
8. 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

9. This section provides guidance on answering items within the checklist and provides some detail on the obligations of the assessor.
10. DSD **RECOMMENDS** that the rigour of a review be commensurate with the risk environment and the highest level of classified information that is involved (ACSI 33 2.9.10).
11. Depending on the scope and subject of the review, DSD **RECOMMENDS** considering in the review current information about areas such as (ACSI 33 2.9.9):
 - agency priorities;
 - business requirements;
 - threat data;
 - likelihood and consequence estimates;
 - effectiveness of existing countermeasures;
 - other possible countermeasures; and

Page 6

UNCLASSIFIED (RECLASSIFY after first entry)

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- best practice.
12. The titles of the documents given in this guide are guidelines; organisations may title their policy documents/sections as they choose.

3.1 Requirements

13. 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** have security risk assessments, policies and plans that cover ICT systems (ACSI 33, 2.4.4).

R2 All ICT security documents **SHOULD** be formally approved and signed off by an appropriate person (ACSI 33 2.4.15).

14. 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.
15. Assessors should either tick or cross a requirement to indicate that either an organisation has succeeded, or failed in addressing 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. The comments should indicate the rationale for the decision, including any information not conveyed by the checklist.
16. Bracketed information towards the end of a requirement's wording implies a reference. The material that is referenced can be examined for further detail or for justification of a requirement.
17. Some requirements have a "Not Applicable" (N/A) checkbox. This indicates that a requirement may not apply to some information systems or in some circumstances. Assessors need to explain why a requirement is not applicable in their comments.

3.2 Sub-requirements

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

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

For example:

R41 Organisations with classified information **MUST** (PSM Part D):

R41.1 have a security clearance process;

R41.2 enforce the need-to-know principle; and

R41.3 monitor and periodically review clearances.

19. 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:

R12 Security SOPs **SHOULD** exist for each of the following roles (ACSI 33 2.6.5):

R12.1 ITSA;

R12.2 System Manager;

R12.3 System Administrator; and

R12.4 System Users.

20. 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

21. Ticks are given where the key word of the requirement is satisfied.

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

- The requirement is complied with explicitly; or
- Valid reasons exist for non-compliance and the deviation process outlined above has been completed.

23. For a '**SHOULD / SHOULD NOT**' you should tick when:

- The requirement is complied with explicitly; or
- Valid reasons exist for non-compliance and the deviation process outlined above has been completed.

24. For a '**RECOMMEND**' 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.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

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

3.4 Checking the implementation

26. Assessors **MUST** verify consistency between policy, plans, and procedures. In order to verify that procedures mentioned within policy documentation have been implemented, assessors should have the organisation's IT Security Advisor (ITSA), IT Security Manager (ITSM), or an authorised delegate demonstrate that the procedure is in use where possible.

3.5 Comments

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

28. Assessors **MUST** comment upon individual requirements within the checklist. Comments **MUST** provide justification of how well an organisation complies with each requirement.

3.6 Review Report

29. Please develop a compliance report based on the materials used for assessment.

30. Provide any recommendations based on non-mandatory guidelines that have not been demonstrated by the organisation. Comments on non-mandatory guidelines that have been implemented are also welcome.

31. The formal I-RAP compliance report must include signoff from the ITSA of the organisation. The statement must stipulate that, to the best of the ITSA's knowledge, the I-RAP assessor who has signed the compliance report has actively participated in conducting the assessment work leading to compliance.

3.7 Letter of Compliance

32. The compliance letter, as a minimum, must include:

- whether compliance has been achieved;
- the level of classification of the system; and
- conditions for maintaining compliance.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

1.0 Security Documentation

Objective: To provide management direction and support for information security.

R1 Organisations **MUST** have security risk assessments, policies and plans that cover ICT systems (ACSI 33 2.4.4).

R2 All ICT security documents **SHOULD** be formally approved and signed off by an appropriate person (ACSI 33 2.4.15).

R3 DSD **RECOMMENDS** that (ACSI 33 2.4.15):

R3.1 all high level ICT security documents be approved by the security executive, senior executive manager or organisation head; and

R3.2 all system-specific documents be approved by the owner of the system, the senior executive manager, and/or the security executive.

Note: The role of the security executive is defined in paragraph A4.9 of the PSM.

R4 Organisations **SHOULD** develop a schedule for reviewing all ICT security documents at regular intervals (ACSI 33 2.4.16).

R5 DSD **RECOMMENDS** that (ACSI 33 2.4.16):

R5.1 the interval between ICT security document reviews be no greater than twelve months;

R5.2 reviews be performed in response to significant changes in the environment, business or system; and

R5.3 the date of the most recent review be recorded on each document.

R6 Organisations **MUST** classify their ICT security documentation in accordance with Part C of the PSM (ACSI 33 2.4.17).

1.1 Risk Management Plan (RMP)

R7 Systems **SHOULD** be covered by a Security Risk Management Plan (SRMP) (ACSI 33 2.4.6).

1.2 ICT Security Policy

R8 Organisations **MUST** have an ICT Security Policy (ICTSP) document covering the system under review (ACSI 33 2.4.5).

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

1.3 System Security Plan (SSP)

R9 Organisations **SHOULD** have an SSP that covers the system under review (ACSI 33 2.4.7).

R10 Regular reviews of the SSP **SHOULD** be conducted to determine whether the security objectives have been achieved and the most cost-effective and efficient treatments were used (PSM B 5.83).

1.4 Standard Operating Procedures (SOPs)

R11 Organisations **SHOULD** have SOPs that cover the system under review (ACSI 33 2.4.8).

R12 Security SOPs **SHOULD** exist for each of the following roles (ACSI 33 2.6.5):

R12.1 ITSA;

R12.2 System Manager;

R12.3 System Administrator; and

R12.4 System Users.

R13 The ITSA and System Manager **SHOULD** be familiar with all SOPs (ACSI 33 2.6.5).

R14 Procedures **SHOULD** be documented in the ITSA SOPs for (ACSI 33 2.6.10):

R14.1 instructing new users to comply with ICT security requirements;

R14.2 reviewing system audit trails and manual logs, particularly for privileged users;

R14.3 reviewing user accounts, system parameters and access controls;

R14.4 checking the integrity of system software;

R14.5 testing access controls;

R14.6 inspecting equipment and cabling;

R14.7 managing the review of removable media containing data that is to be transferred off-site;

R14.8 managing the review of incoming media for viruses or unapproved software;

R14.9 labelling, registering and mustering assets, including removable media; and

R14.10 reporting and managing security incidents, including involvement in physical security incident management where the incident could impact on ICT security.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R15 Procedures **SHOULD** be documented in the System Manager SOPs for (ACSI 33 2.6.11):

R15.1 managing the ongoing security and functionality of system software and hardware, including:

R15.1.1 maintaining awareness of current software vulnerabilities;

R15.1.2 testing and applying software patches/updates;

R15.1.3 applying appropriate hardening techniques;

R15.1.4 updating anti-virus software;

R15.2 managing the destruction of unserviceable equipment and media;

R15.3 authorising new system users;

R15.4 approving and releasing changes to the system software or configuration;

R15.5 authorising access rights to applications and data; and

R15.6 recovering from system failures.

R16 Procedures **SHOULD** be documented in the System Administrator's SOPs for (ACSI 33 2.6.12):

R16.1 securing the system out-of-hours if operations are not 24x7;

R16.2 implementing access rights to applications and data;

R16.3 adding and removing users;

R16.4 setting user privileges;

R16.5 cleaning up directories and files when a user departs or changes roles;

R16.6 backing up data, including audit logs;

R16.7 securing backup tapes; and

R16.8 recovering from system failures.

R17 The System User's SOPs **SHOULD** document (ACSI 33 2.6.14):

R17.1 who is responsible for what aspects of security;

R17.2 a warning that:

R17.2.1 users' actions may be audited;

R17.2.2 users will be held accountable for their actions;

R17.3 guidelines on choosing and protecting passwords;

R17.4 guidelines on enforcing need-to-know on the system;

R17.5 what to do in the case of a suspected or actual security incident;

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- R17.6** the highest level of classified material that can be processed on the system and handling procedures for classified information;
- R17.7** how to secure the workstation when temporarily absent;
- R17.8** how to secure the workstation at the end of the day;
- R17.9** procedures for controlling and sanitising media;
- R17.10** procedures for labelling, handling and disposing of hardcopy;
- R17.11** preventing overview of data by visitors; and
- R17.12** what to do for hardware and software maintenance.
- R18** Organisations **MUST** provide guidance to users on their responsibilities relating to ICT security, and the consequences of non-compliance (ACSI 33 2.6.15).
- R19** Organisations **SHOULD** advise users not to attempt to (ACSI 33 2.6.16):
- R19.1** introduce malicious code into the system;
- R19.2** physically damage the system;
- R19.3** bypass, strain, or test security mechanisms;
- Exception: If security mechanisms must be bypassed for any reason, users must first receive approval from the ITSA.
- R19.4** introduce or use unauthorised software, firmware, or hardware on an information system;
- R19.5** assume the roles and privileges of others;
- R19.6** attempt to gain access to information for which they have no authorisation; or
- R19.7** relocate information system equipment without proper authorisation.
- R20** System Users **SHOULD** sign a statement that they have read and agree to abide by the System Users' SOP (ACSI 33 2.6.13).
- R21** System SOPs **SHOULD** be maintained and updated (ACSI 33 2.6.7).

1.5 Policy Consistency

- R22** The system SRMPs, ICTSPs, SSPs and SOPs **SHOULD** be logically connected and consistent (ACSI 33 2.4.12).

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

2.0 Security Organisation

2.1 Information Technology Security Adviser (ITSA)

Please identify the ITSA(s) in your comments for these criteria.

R23 Organisations **MUST** appoint a person to the role of ITSA (ACSI 33 2.1.8).

R24 It is **RECOMMENDED** that a local ITSA be appointed at each site when the system is spread over multiple geographical locations. However, the primary ITSA retains overall responsibility (ACSI 33 2.1.8).

N/A

R25 Where a government agency has outsourced its ICT, the ITSA **MUST** be independent of the outsourcer (ACSI 33 2.1.9).

N/A

R26 The ITSA **MUST** have security clearance to at least the highest level of classified information processed on the ICT system under review (ACSI 33 2.1.10).

R27 ITSAs and administrative staff may have unrestricted access to large volumes of classified information. DSD **RECOMMENDS** that agencies consider clearing these staff to a higher clearance than that of the system classification (ACSI 33 2.1.10).

R28 DSD **RECOMMENDS** that organisations have an “ITSA e-mail account” set up that can receive security information, security newsletters, and notifications of IT security forums.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

3.0 Asset Classification

3.1 Information Classification

Objective: To ensure that information assets receive an appropriate level of protection.

R29 Organisations **MUST** use the Australian Government security classification system outlined in the PSM Part C.

3.1.1 Information labelling and handling

R30 The classification of all media **MUST** be readily visually identifiable (ACSI 33 3.4.18).

R31 Ready visual identification of media classification **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.

R32 Organisations **MUST** ensure that protective markings are applied to all emails containing classified information that have been written or forwarded by staff (ACSI 33 3.5.53).

R33 Protective markings **SHOULD** be applied to all automatically generated emails (ACSI 33 3.5.53).

R34 Organisations **MUST** ensure that email protective marking identifies the maximum classification and/or set of caveats for all information in the email, including any attachments (ACSI 33 3.5.53).

R35 Organisations **SHOULD** ensure that all business-originated emails that do not contain any classified information are given a protective marking to indicate this (ACSI 33 3.5.55).

Requirement R35 is a **MUST** for systems at PROTECTED and above (ACSI 33 3.5.56).

R36 Organisations **SHOULD NOT** allow a protective marking to be inserted into user-generated emails without user intervention (ACSI 33 3.5.59).

R37 If a tool that allows users to select from a list of protective markings is used, then the list **SHOULD NOT** include protective markings for which the system is not accredited (ACSI 33 3.5.59).

N/A

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R38 Organisations **MUST** configure systems to block any outbound emails with a valid protective marking indicating that the content of the email exceeds the classification of the path over which the email would be transferred (ACSI 33 3.5.64).

Note: This may need to take into consideration any encryption applied to the email.

R39 Organisations **SHOULD** configure email systems to reject and log inbound emails with protective markings indicating that the content of the email exceeds the accreditation of the receiving system (ACSI 33 3.5.65).

R40 DSD **RECOMMENDS** that the intended recipient be notified of emails that have been blocked (ACSI 33 3.5.65).

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

4.0 Personnel Security

4.1 Security in Job Definition and Resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

R41 Organisations with classified information **MUST** (PSM Part D):

R41.1 have a security clearance process;

R41.2 enforce the need-to-know principle; and

R41.3 monitor and periodically review clearances.

R42 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).

4.2 User Training

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

4.2.1 Information security education and training

R43 Organisations **MUST** (ACSI 33 3.2.7):

R43.1 ensure that all personnel who have access to ICT systems have sufficient training; and

R43.2 provide ongoing ICT security training and awareness for staff on topics such as responsibilities, potential security risks and countermeasures.

R44 The degree and content of security training **SHOULD** be aligned to user responsibilities (ACSI 33 3.2.9).

4.3 Responding to Security Incidents and Malfunctions

Objective: To minimise the damage from incidents and malfunctions, and to monitor and learn from such incidents.

R45 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):

R45.1 countermeasures against malicious code;

R45.2 intrusion detection strategies;

R45.3 audit analysis;

R45.4 system integrity checking; and

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R45.5 vulnerability assessments.	<input type="checkbox"/>
R46 Organisations MUST (ACSI 33 3.5.69):	
R46.1 develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering how to:	
R46.1.1 minimise the likelihood of malicious code being introduced into the system(s);	<input type="checkbox"/>
R46.1.2 detect any malicious code installed on the system(s);	<input type="checkbox"/>
R46.2 make users aware of the policies, plans and procedures; and	<input type="checkbox"/>
R46.3 ensure that all instances of detected malicious code outbreaks are handled according to the procedures.	<input type="checkbox"/>
R47 DSD RECOMMENDS that systems infected with malicious code be re-built from trusted sources.	<input type="checkbox"/>
4.3.1 Detecting security incidents	
R48 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):	
R48.1 appropriate intrusion detection mechanisms, including network-based IDS (NIDS) and host-based IDS (HIDS) as required;	<input type="checkbox"/>
R48.2 the audit analysis of event logs, including IDS logs;	<input type="checkbox"/>
R48.3 a periodic audit of intrusion detection procedures;	<input type="checkbox"/>
R48.4 user training and awareness programs; and	<input type="checkbox"/>
R48.5 a documented incident response procedure.	<input type="checkbox"/>
R49 When signature-based intrusion detection is used, organisations SHOULD keep the signatures up-to-date (ACSI 33 3.7.7).	<input type="checkbox"/>
R50 DSD RECOMMENDS that organisations deploy tools for (ACSI 33 3.7.10):	
R50.1 the management and archival of security event information; and	<input type="checkbox"/>
R50.2 the correlation of events of interest.	<input type="checkbox"/>
R51 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).	<input type="checkbox"/>
R52 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).	<input type="checkbox"/>
R53 The recorded information SHOULD include, at a minimum (ACSI 33 2.8.26):	
R53.1 the date the incident was discovered;	<input type="checkbox"/>
	<input type="checkbox"/> N/A
	<input type="checkbox"/> N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R53.2 the date the incident occurred;

R53.3 a description of the incident, including the people and locations involved;

R53.4 the action taken; and

R53.5 to whom the incident was reported.

4.3.2 Managing security incidents

R54 Organisations **MUST** detail security incident responsibilities and procedures in the SSP and in the SOPs (ACSI 33 2.8.22).

R55 Organisations **MUST** develop an Incident Response Plan and supporting procedures, and ensure users are aware of these (ACSI 33 2.8.22).

R56 When a data spill occurs, organisations **SHOULD** assume that the information has been compromised (ACSI 33 2.8.28).

R57 Organisations **MUST** treat any such spillage as an incident, and follow their Incident Response Plan to deal with it (ACSI 33 2.8.28).

ACSI 33 2.8.29 contains additional requirements for HIGHLY PROTECTED systems.

4.3.3 Reporting security incidents

R58 Organisations **MUST** report significant ICT security incidents to DSD (ACSI 33 2.8.36).

R59 Reporting of incidents to DSD **SHOULD** be undertaken using the Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) (ACSI 33 2.8.34).

Reviewers should examine completed examples of incident response reports, if there have been any incidents on the system.

4.3.4 Incident detection and response plan

R60 Organisations **MUST** develop an Incident Response Plan which, as a minimum, defines (ACSI 33 2.8.41):

R60.1 broad guidelines on what constitutes an incident;

R60.2 the minimum level of training for users and system administrators;

R60.3 the authority responsible for initiating investigations of an incident;

R60.4 the steps necessary to ensure the integrity of information supporting a compromise;

R60.5 the steps necessary to ensure that critical systems remain operational; and

R60.6 how to formally report incidents.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R61 The Incident Response Plan **SHOULD** also contain (ACSI 33 2.8.42):

R61.1 clear definitions of the types of incidents that are likely to be encountered;

R61.2 the expected response to each incident type;

R61.3 the authority within the organisation who is responsible for initiating:

R61.3.1 a formal (administrative) investigation;

R61.3.2 a police investigation of an incident;

R61.3.3 an ASIO investigation of national security incidents, in accordance with Part G of the PSM;

N/A

R61.4 the criteria by which the responsible authority would initiate formal, police or ASIO investigations of an incident;

R61.5 references to other related documents;

Examples: Business Continuity Plan, Fraud Control Plan.

R61.6 which other organisations or authorities need to be informed in the event of an investigation being undertaken; and

R61.7 the details of the system contingency measures, or a reference to these details if they are located in a separate document.

R62 Organisations **SHOULD** develop and maintain procedures supporting the plan to (ACSI 33 2.8.44):

R62.1 detect potential security breaches;

R62.2 establish the cause of any security incident, whether accidental or deliberate;

R62.3 detail the action to be taken to recover and minimise the exposure to a system compromise;

R62.4 report the incident; and

R62.5 document any recommendations on preventing a recurrence.

R63 Organisations **SHOULD** (ACSI 33 2.8.32):

R63.1 transfer a copy of raw audit trails relating to incidents onto media such as CD-ROM or DVD-ROM for secure archiving, as well as securing manual log records for retention; and

R63.2 ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

5.0 Physical and Environmental Security

5.1 Security Environment

Objective: To prevent unauthorised damage, access and interference to business premises and information.

5.1.1 Physical security perimeter

PSM Part E 7.34 and ACSI 33 2.7.33 outline physical security certification authorities.

R64 Site Security Plans and Standard Operating Procedures (SOPs) **MUST** be developed for server rooms (ACSI 33 3.1.20).

R65 Server and communications equipment **SHOULD** be secured in accordance with the area, room and container standards as shown in ACSI 33 3.1.17.

R66 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).

R67 DSD **RECOMMENDS** that the ITSA control the keys or equivalent access mechanism to these locked spaces (ACSI 33 3.1.33).

R68 Organisations **MUST** ensure that network infrastructure carrying unencrypted information is wholly contained within areas of the appropriate standard as shown in ACSI 33 3.1.35.

R69 DSD **RECOMMENDS** that organisations use “security in depth” or a multi-layered system of protection for information processing facilities. (PSM E 4.16 – E 4.20)

N/A

5.1.2 Client accessible areas

R70 Organisations **SHOULD** prevent unauthorised people from observing ICT equipment, and in particular displays and keyboards (ACSI 33 3.1.43).

R71 DSD **RECOMMENDS** that organisations (ACSI 33 3.1.43):

R71.1 position screens and keyboards so that they cannot be seen by unauthorised people, and/or

R71.2 fix blinds or drapes to the inside of windows.

R72 Organisations **SHOULD** implement measures to protect equipment, including internal components, against theft (ACSI 33 3.1.31).

5.2 Equipment Security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

5.2.1 Equipment availability and protection

R73 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).

R74 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.

R75 ACSI 33 3.1.35 provides the physical security requirements for network infrastructure carrying unencrypted information. These requirements **MUST** be complied with.

5.2.2 Cabling Security

R76 Cabling conduits installed in public or visitor areas **SHOULD** be labelled in a manner that does not attract undue attention by people who may not have the appropriate security clearances or a need-to-know of the existence of such cabling (ACSI 33 3.8.27).

N/A

R77 Site conventions for labelling and registration **SHOULD** be recorded in the SOPs (ACSI 33 3.8.29).

R78 Organisations **SHOULD** maintain a register of cables (ACSI 33 3.8.31).

R79 The cable register **SHOULD** record at least the following (ACSI 33 3.8.31):

N/A

R79.1 cable identification number;

R79.2 classification;

R79.3 source;

R79.4 destination; and

R79.5 floor plan diagram.

R80 Organisations **SHOULD** inspect cables for inconsistencies with the cable register on a regular basis (ACSI 33 3.8.33).

R81 The frequency of the cable inspections **SHOULD** be defined in the SSP (ACSI 33 3.8.33).

5.2.3 Equipment maintenance

R82 Repairs and maintenance for hardware containing classified media **SHOULD** be carried out by appropriately cleared and briefed personnel (ACSI 33 3.4.33).

R83 If appropriately cleared and briefed personnel are not available, classified hardware may be repaired or maintained by a technician without an appropriate security clearance.

Organisations **SHOULD** sanitise media before repair is undertaken by an uncleared technician (ACSI 33 3.4.34).

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R84 DSD RECOMMENDS that support contracts do not require the return of classified defective media (ACSI 33 3.4.33).

R85 DSD RECOMMENDS that equipment be maintained in accordance with manufacturer's instructions.

R86 DSD RECOMMENDS that procedures exist for regular equipment maintenance.

5.2.4 Secure disposal or reuse of equipment

R87 Organisations MUST have a documented process for the disposal of hardware (ACSI 33 3.4.39).

R88 Organisations MUST (ACSI 33 3.4.36):

R88.1 sanitise and declassify, or destroy media containing classified material before disposal; and

R88.2 use approved methods to declassify or destroy media.

ACSI 33 3.4.19 contains extra information for HIGHLY PROTECTED media.

R89 Where the media cannot be effectively accessed or media fails, organisations **SHOULD** repair the equipment to facilitate sanitisation, maintain the media at its highest classification, or destroy the media (ACSI 33 3.4.37).

R90 Storage media **MUST** be reclassified if (ACSI 33 3.4.16):

R90.1 information copied onto that media is of a higher classification; or

R90.2 information contained on that media is subject to a classification upgrade.

R91 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.

R92 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).

R93 The officer **MUST** (ACST 33 3.4.42):

R93.1 supervise the handling of the material to the point of destruction; and

R93.2 ensure that the destruction is complete.

R94 Organisations **MUST** perform the destruction of accountable material, as defined in Part C of the PSM, under the supervision of two officers cleared to the highest level of media being destroyed (ACSI 33 3.4.43).

Note: Accountable material includes cabinet documents.

R95 The officers **MUST** (ACSI 33 3.4.43):

R95.1 supervise the handling of the material to the point of destruction;

N/A

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R95.2 ensure that the destruction is complete; and

R95.3 sign a destruction certificate.

5.3 General Controls

Objective: To prevent compromise of information and information processing facilities.

5.3.1 Clear desk and clear screen policy

R96 Organisations **SHOULD** have a clear desk policy (PSM C 7.7 - 7.9).

R97 Organisations **SHOULD** (ACSI 33 3.6.15):

R97.1 configure systems with a screen and/or session lock;

R97.2 configure the lock to activate after a maximum of 15 minutes of user inactivity;

R97.3 configure the lock to completely conceal all information on the screen;

R97.4 ensure the screen does not appear to be turned off while in the locked state;

R97.5 require the user to re-authenticate to unlock the system; and

R97.6 deny users the ability to disable the locking mechanism.

R98 Classified paper and media material **MUST** be appropriately secured when not in use – especially outside of normal working hours. (PSM C 7.42)

5.3.2 Removal of property

R99 Equipment, information or software that is owned by the organisation **MUST NOT** be removed without authorisation (PSM C 7.36).

R100 The organisation **MUST** have procedures for protecting classified information that is removed from the organisation's premises (PSM C 7.35).

R101 For PROTECTED and above materials, the officer responsible for authorising removal **SHOULD** be the manager or equivalent responsible for the material (PSM C 7.36).

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

6.0 Communications and Operations Management

6.1 Operational Procedures and Responsibilities

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

6.1.1 Operational change control

R102 Organisations **SHOULD** ensure that (ACSI 33 2.8.7):

R102.1 the change management process defined in ICT security documentation is followed;

R102.2 proposed changes require approval by the documented authority;

R102.3 any proposed change that may impact the security of the ICT system is submitted to the Accreditation Authority for approval; and

R102.4 all associated system documentation is updated to reflect changes.

R103 The change management process **SHOULD** define appropriate actions to be followed before and after urgent changes are implemented (ACSI 33 2.8.7).

R104 DSD **RECOMMENDS** that organisations retain previous versions of any software required by operational systems.

R105 DSD **RECOMMENDS** that organisations maintain strict control of the operating system environment. This may include having a standard operating environment for all servers and workstations, using a centralised patch management strategy and having a fast response patch testing facility.

R106 DSD **RECOMMENDS** that organisations also have a patch management strategy for applications. Desktop productivity software, e-mail clients, multimedia players, Java virtual machine software, web browsers and PDF viewers are common examples of applications that require security updates.

6.2 Operation Management

Objective: To maintain the integrity and availability of information processing and communication services.

6.2.1 Information backup

R107 Organisations **SHOULD** (ACSI 33 2.8.14):

R107.1 backup all information identified as critical;

R107.2 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

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R107.3 test backup and restoration processes regularly to confirm their effectiveness.

R108 Movement of classified information to and from remote storage **MUST** be done in accordance with the PSM Part C.

N/A

6.2.2 Operator logs

R109 A system management log **SHOULD** be used to record the following information (ACSI 33 3.7.20):

R109.1 sanitisation activities;

R109.2 system start-up and shutdown;

R109.3 component or system failures;

R109.4 maintenance activities;

R109.5 housekeeping activities;

Examples: Backup and archival runs.

R109.6 system recovery activities; and

R109.7 special or out-of-hours activities.

R110 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 systems.

6.3 Information System Management

Objective: To ensure the safeguarding of information in information systems and the protection of supporting infrastructure.

6.3.1 Information system configuration

Please record the classification of the system within your comments for this requirement.

R111 Organisations **SHOULD** reduce potential vulnerabilities on systems by (ACSI 33 3.5.8):

R111.1 removing unneeded software;

R111.2 removing unused accounts;

R111.3 removing unnecessary file shares;

R111.4 renaming required default accounts;

R111.5 replacing default passwords;

R111.6 ensuring patching is up-to-date;

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R111.7 disabling unused features on installed software and operating systems; and	<input type="checkbox"/>
R111.8 disabling access to all unnecessary input/output devices, 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.	<input type="checkbox"/>
R112 DSD RECOMMENDS that organisations consider seeking and applying additional information on hardening techniques relevant to their specific equipment (ACSI 33 3.5.8).	<input type="checkbox"/>
R113 DSD RECOMMENDS that organisations (ACSI 33 3.5.10):	
R113.1 limit information that could be disclosed about what software is installed; and	<input type="checkbox"/>
R113.2 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.	<input type="checkbox"/>
For further information for HIGHLY PROTECTED systems, please see ACSI 33 3.5.11.	
R114 DSD RECOMMENDS that organisations develop a hardened Standard Operating Environment (SOE) for workstations, covering the (ACSI 33 3.5.12):	
R114.1 requirements for hardening during installation;	<input type="checkbox"/>
R114.2 implementation of access controls on relevant objects to limit users and programs to the minimum access required to perform their duties;	<input type="checkbox"/>
R114.3 installation of workstation firewalls; and	<input type="checkbox"/>
R114.4 configuration of either remote logging or the transfer of local event logs to a central server.	<input type="checkbox"/>
For further information for HIGHLY PROTECTED systems, please see ACSI 33 3.5.13.	
R115 Where known vulnerabilities cannot be patched, organisations SHOULD use other protective measures as determined from a risk assessment (ACSI 33 3.5.15).	<input type="checkbox"/> <input type="checkbox"/> N/A
R116 DSD RECOMMENDS that protective measures include:	<input type="checkbox"/> <input type="checkbox"/> N/A
R116.1 email filters that strip potentially harmful content before forwarding messages to email clients;	<input type="checkbox"/>
R116.2 web proxy filters that strip harmful content to web browsers;	<input type="checkbox"/>
R116.3 additional access controls on file and configuration settings; and	<input type="checkbox"/>
R116.4 firewalls configured to block high risk traffic.	<input type="checkbox"/>
R117 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):	<input type="checkbox"/> <input type="checkbox"/> N/A
R117.1 maintain effective functional separation between servers allowing them to operate independently;	<input type="checkbox"/>

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R117.2 minimise communications between servers at both the network and file system level, as appropriate; and	<input type="checkbox"/>	
R117.3 limit users and programs to the minimum access required to perform their duties.	<input type="checkbox"/>	
R118 DSD RECOMMENDS that organisations, for all servers and workstations (ACSI 33 3.5.70):		
R118.1 install anti-virus scanners;	<input type="checkbox"/>	
R118.2 ensure that users do not have the ability to disable the scanner;	<input type="checkbox"/>	
R118.3 check vendor virus pattern signatures for updates daily;	<input type="checkbox"/>	
R118.4 apply virus pattern signature updates as soon as possible after vendors make them available; and	<input type="checkbox"/>	
R118.5 regularly scan all disks.	<input type="checkbox"/>	
R119 Organisations SHOULD review all commercial software applications to determine whether they are configured to connect back to the vendor (ACSI 33 3.5.23).	<input type="checkbox"/>	
R120 If connection back to the vendor functionality is included, then organisations SHOULD make a business decision to determine whether to permit or deny these connections, including an assessment of the risks involved in doing so (ACSI 33 3.5.23).	<input type="checkbox"/>	<input type="checkbox"/> N/A

6.3.2 Database Security

R121 Organisations SHOULD ensure that all information stored within a database is associated with an appropriate protective marking if the information (ACSI 33 3.5.30):	<input type="checkbox"/>	<input type="checkbox"/> N/A
• may be exported to a different system; or		
• contains differing classifications and/or different handling requirements.		
R122 Organisations SHOULD ensure that these protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any information retrieved or exported from a database (ACSI 33 3.5.30).	<input type="checkbox"/>	<input type="checkbox"/> N/A
R123 Organisations SHOULD protect database files from access that bypasses the database's normal access controls (ACSI 33 3.5.32).	<input type="checkbox"/>	<input type="checkbox"/> N/A
Example: Performing input validation on database queries to prevent SQL injection attacks.		
R124 Organisations SHOULD ensure that databases provide accountability of users' actions (ACSI 33 3.5.34).	<input type="checkbox"/>	<input type="checkbox"/> N/A

6.3.3 Network Management

R125 Organisations SHOULD keep the network configuration under the control of a central network management authority (ACSI 33 3.10.5).	<input type="checkbox"/>	
--	--------------------------	--

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R126 Organisations **SHOULD** commit to regularly reviewing the configuration to ensure it conforms to the documented configuration (ACSI 33 3.10.5).

R127 Organisations **MUST** have (ACSI 33 3.10.6):

R127.1 a high level diagram showing all connections into the system; and

R127.2 a logical network diagram showing all network devices.

R128 These diagrams **SHOULD** (ACSI 33 3.10.6):

R128.1 be updated as network changes are made; and

R128.2 include a “Current as at <date>” on each page.

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

R129 Organisations **SHOULD** configure networks to limit opportunities for unauthorised access to information transiting the network infrastructure (ACSI 33 3.10.8).

Options to achieve this include the use of:

- switches rather than hubs,
- routers and firewalls isolating parts of the network on a need-to-know basis,
- encryption on the LAN, and
- application-level encryption.

R130 DSD **RECOMMENDS** organisations implement protection measures to minimise the risk of unauthorized access to management traffic travelling across a network (ACSI 33 3.10.9).

R131 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/or
- implement port security on network switches to limit access based on MAC address and disable all unused ports.

6.3.4 External Connections (Gateways)

R132 Organisations **SHOULD** ensure that gateways (ACSI 33 3.10.23):

R132.1 are the only communications routes into and out of internal networks;

R132.2 by default, deny all connections into and out of the network;

R132.3 allow only explicitly authorised connections;

R132.4 are managed via a secure path;

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- R132.5** provide sufficient audit capability to detect gateway security breaches and attempted network intrusions; and
- R132.6** provide real-time alarms.
- R133** Cascaded connections **MUST** meet overall assurance requirements as described in ACSI 33 3.10.27. N/A
- R134** Organisations **SHOULD** use Demilitarised Zones (DMZs) to separate externally accessible systems, such as web servers, from both the public and from the organisation's internal networks. (ACSI 33 3.10.29) N/A

6.3.5 Security Devices

- R135** 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).
- R136** 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).
- R137** Firewalls **MUST** meet the minimum levels of assurance outlined in ACSI 33 3.10.34 – 3.10.35.
- R138** 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).
- R139** When choosing a product, organisations **MUST** document (ACSI 33 3.3.9):
- R139.1** the desired degree of assurance in the product's key functions;
 - R139.2** the actual degree of assurance provided by the chosen product, based on the level of evaluation it has received for its key functions;
 - R139.3** 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
 - R139.4** 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.
- R140** Organisations **SHOULD** (ACSI 33 3.5.14):
- R140.1** monitor relevant sources for information about new vulnerabilities, patches and hardening methods in software and hardware used by the organisation;
 - R140.2** take corrective action when vulnerabilities that could affect gateway systems are discovered;

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- R140.3** 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
- R140.4** replace obsolete software and hardware with products for which ongoing support is available.
- R141** Organisations **SHOULD** ensure that any leasing agreements for ICT equipment take into consideration the (ACSI 33 3.3.16): N/A
- R141.1** difficulties that may be encountered when the equipment requires maintenance; and
- R141.2** sanitisation of the equipment prior to its return.

6.3.6 Cryptographic Devices

- R142** Organisations **MUST** use encryption products that meet the minimum level of assurance, as shown in ACSI 33 3.9.7, if using encryption to reduce the requirements for transiting classified information over networks of a lower classification than that of the information (ACSI 33 3.9.7). N/A
- R143** Before using an unevaluated product that implements a DSD Approved Cryptographic Protocol (DACP), organisations **MUST** (ACSI 33 3.9.15): N/A
- R143.1** ensure that the minimum requirements as stated in ACSI 33 3.9.7 will be met; and
- R143.2** consider and accept the risks.
- R144** 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). N/A
- R145** 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). N/A
- Please see ACSI 33 3.9.72 for requirements relating to HIGHLY PROTECTED systems.
- R146** 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). N/A
- ACSI 33 3.9.73 describes the minimum contents which **SHOULD** be documented in the KMP.
- R147** 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). N/A
- R148** Audits of cryptographic system material **SHOULD** be conducted (ACSI 33 3.9.67): N/A
- R148.1** on handover/takeover of administrative responsibility for the system;

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- | | | |
|--|--------------------------|------------------------------|
| R148.2 on change of individuals with access to the cryptographic system; and | <input type="checkbox"/> | |
| R148.3 at least annually. | <input type="checkbox"/> | |
| R149 The Secure Hashing Algorithms (SHA) family of hashing algorithms SHOULD be used wherever hashing is required (ACSI 33 3.9.12). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R150 Symmetric encryption using AES or 3DES SHOULD NOT use Electronic Codebook (ECB) Mode (ACSI 33 3.9.13). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R151 If IPsec is used, it SHOULD be used in tunnel mode (ACSI 33 3.9.39). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R152 If Internet Security Association Key Management Protocol (ISAKMP) is used, Aggressive Mode SHOULD be disabled (ACSI 33 3.9.46). | <input type="checkbox"/> | <input type="checkbox"/> N/A |

6.3.7 Wireless communications

- | | | |
|--|--------------------------|------------------------------|
| R153 Organisations MUST , where they have a requirement to use wireless communications for the transmission of classified information, ensure that the information is protected by DSD Approved Cryptography that meets the assurance level required for the transmission of the information over public or unprotected infrastructure (ACSI 33 3.8.42). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R154 Key generation, distribution, and re-keying procedures SHOULD be documented in the wireless system security plan (ACSI 33 3.8.45). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R155 Organisations SHOULD address the following vulnerabilities if they choose to use wireless communications for the transmission of classified information (ACSI 33 3.8.42): | | <input type="checkbox"/> N/A |
| R155.1 man-in-the-middle attacks; | <input type="checkbox"/> | |
| R155.2 weak cryptography; | <input type="checkbox"/> | |
| R155.3 unauthenticated users brute forcing authentication; and | <input type="checkbox"/> | |
| R155.4 availability. | <input type="checkbox"/> | |
| R156 In order to prevent a range of man-in-the-middle attacks, organisations SHOULD use an authentication protocol that authenticates each end of the link (ACSI 33 3.8.44). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R157 DSD RECOMMENDS that pre-shared keys not be used for wireless authentication, as dictionary attacks can be performed on captured key exchanges (ACSI 33 3.8.45). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R158 DSD RECOMMENDS using WPA2 with EAP-TLS and/or an evaluated VPN in 802.11 wireless deployments (ACSI 33 3.8.45). | <input type="checkbox"/> | <input type="checkbox"/> N/A |
| R159 DSD RECOMMENDS organisations take steps to ensure the confidentiality, integrity, and authenticity of 802.11 management frames (ACSI 33 3.8.45). | <input type="checkbox"/> | <input type="checkbox"/> N/A |

Example: Install additional software or hardware as needed.

Note: WPA2 provides no protection for management frames, and therefore does not prevent spoofing or denial of service attacks.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R160 Organisations **MUST** consider the risks before allowing non-agency accredited devices to connect to agency controlled wireless infrastructure; or allowing agency accredited devices to connect to non-agency controlled wireless infrastructure (ACSI 33 3.8.47).

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

R161 DSD **RECOMMENDS** organisations limit the effective range of wireless communications by (ACSI 33 3.8.48):

<input type="checkbox"/>
N/A

R161.1 minimising the output power level of wireless devices; and/or

<input type="checkbox"/>

R161.2 RF shielding.

<input type="checkbox"/>

6.3.8 Peripheral switches

Peripheral switches, such as Keyboard/Video/Mouse (KVM) switches, are devices used to share a set of peripherals between a number of computers.

R162 KVM switches **SHOULD** conform with the requirements stipulated in ACSI 33 3.10.56.

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

6.3.9 Multifunction Devices (MFDs)

MFDs can be sophisticated devices with significant capabilities that make them similar to servers. Which server and other device requirements will apply to MFDs used in a system will need to be decided by the reviewer.

R163 Organisations deploying MFDs **MUST** develop a set of policies, plans and procedures governing the use of the equipment (ACSI 33 3.10.71).

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

R164 Organisations **MUST NOT** permit network-connected MFDs to be used to copy documents classified above the level of the connected network (ACSI 33 3.10.66).

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

6.3.10 Remote access

Remote access is any access to an organisation's system from a location not within the physical control of the organisation. Part H of the PSM concerning 'Working From Home' may help organisations identify and develop responsibilities, policies and procedures for home remote access use.

R165 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).

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

R166 Organisations **SHOULD** disable split tunnelling when using VPN technology to connect remotely to the system (ACSI 33 3.10.50).

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

R167 Organisations **SHOULD** authenticate each user and device prior to allowing remote connection to services that are not intentionally anonymous (ACSI 33 3.10.51).

<input type="checkbox"/>	<input type="checkbox"/>
	N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R168 Organisations **SHOULD** implement additional security controls for devices used to connect remotely (ACSI 33 3.10.52).

N/A

R169 Organisations **SHOULD** consider the following additional controls when implementing remote access systems (ACSI 33 3.10.52):

N/A

R169.1 Appropriate Use policies and procedures;

R169.2 user training and education;

R169.3 storage and transit encryption;

R169.4 application white listing;

R169.5 host intrusion detection systems;

R169.6 network access control;

R169.7 host based personal firewalls;

R169.8 device-level authentication;

R169.9 enhanced user-level authentication e.g. two factor authentication; and

R169.10 a hardened standard operating environment.

R170 DSD **RECOMMENDS** that organisations do not allow the use of privileged access remotely (ACSI 33 3.10.53).

N/A

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

R171 Organisations **MUST** ensure that the standards for the use of DSD Approved Cryptographic Protocols (DACPs) are met if using Secure Shell (SSH) (ACSI 33 3.9.25).

N/A

R172 ACSI 33 3.9.25 – 3.9.27 contain further information that **SHOULD** be followed when using SSH.

N/A

6.4 Media Handling and Security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

6.4.1 Management of computer media

R173 Removable media containing classified information **MUST** be stored in accordance with the PSM requirements for information of that classification (ACSI 33 3.1.46).

N/A

R174 Devices holding removable media, such as CD and DVD towers, backup devices and RAID arrays, **MUST** be secured in containers in accordance with the standards for servers and communications equipment (ACSI 33 3.1.48).

N/A

R175 Hardware containing media **MUST** be classified at or above the classification of the media (ACSI 33 3.4.10).

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R176 Non-volatile media **MUST** be classified to the highest classification stored on the media, unless it has been sanitized in accordance with the standards in ACSI 33 Part 3 Chapter 4 (ACSI 33 3.4.11).

6.5 Exchanges of Information and Software

Objective: To prevent loss, modification or misuse of information exchanged between organisations.

6.5.1 Security of electronic mail

R177 Organisations that allow staff to email externally **MUST** have a policy governing the use of email (ACSI 33 3.5.41).

N/A

R178 Organisations that allow staff to email externally **SHOULD** ensure that users are informed of the associated dangers (ACSI 33 3.5.41).

N/A

R179 Organisations **SHOULD** perform regular email server auditing to detect threats such as denial of service attacks and use of the server as an email relay (ACSI 33 3.5.43).

R180 Organisations **SHOULD NOT** allow staff to send and receive email using web-based public email services (ACSI 33 3.5.44).

R181 Organisations **MUST** ensure that the standards for blocking unmarked and outbound emails are also applied to automatically forwarded emails (ACSI 33 3.5.45).

N/A

R182 Organisations **SHOULD** warn staff that the automatic forwarding of email to another staff member may result in the new recipient seeing material that (ACSI 33 3.5.45):

R182.1 they do not have a need-to-know; or

R182.2 the intended recipient and/or sender considered private.

R183 DSD **RECOMMENDS** that organisations route email through a centralised email gateway (ACSI 33 3.5.47).

R184 Organisations **MUST** (ACSI 33 3.5.48):

R184.1 develop and maintain a set of email policies, plans and procedures, derived from a risk assessment, covering topics such as:

- integrity of the email's content,
- authentication of the source,
- non-repudiation of the message,
- verification of delivery,
- confidentiality of the email's content,
- retention of logs and/or the email's content, and

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- R184.2** make their users aware of the organisation's email policies, plans and procedures.
- R185** Organisations **SHOULD** (ACSI 33 3.5.49):
- R185.1** restrict access to email servers to administrative users;
- R185.2** ensure that email servers available to the public are separated from the agency's internal systems;
- R185.3** disable open email relaying so that email servers will only relay messages destined for the agency's domain(s) and those originating from within the domain; and
- R185.4** ensure that account names cannot be determined from external email servers.
- R186** DSD **RECOMMENDS** that organisations (ACSI 33 3.5.50):
- R186.1** enable Transport Layer Security (TLS) encryption on incoming and outgoing email connections on email servers;
- R186.2** configure TLS to negotiate a DACA in preference to an unapproved algorithm, finally reverting to unencrypted email transmission if no algorithm can be negotiated; and
- R186.3** implement TLS authentication between email servers where significant volumes of official information are passed via email.
- R187** Organisations **SHOULD** block (ACSI 33 3.5.51):
- R187.1** inbound and outbound email, including any attachments, that contain:
- R187.1.1** malicious code;
- R187.1.2** content in conflict with the system's email policy;
- R187.1.3** content that cannot be identified by the system;
- R187.2** emails addressed to internal email aliases with source addresses located from outside the domain; and
- R187.3** all emails arriving via an external connection where the source address uses an internal agency domain name.

6.5.2 Publicly available systems and web security

- R188** Organisations that allow staff to browse the Internet **MUST** have a policy governing web use (ACSI 33 3.5.36). N/A
- R189** Organisations that allow staff to browse the Internet **SHOULD** ensure that users are informed of the associated dangers (ACSI 33 3.5.36). N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

R190 Organisations **SHOULD** block the automatic launching of files downloaded from external websites (ACSI 33 3.5.38).

R191 DSD **RECOMMENDS** that organisations consider implementing whitelists for all HTTP Internet traffic (ACSI 33 3.5.37).

R192 DSD **RECOMMENDS** considering blocking client-side active content, noting that such a decision may restrict the legitimate activity of users (ACSI 33 3.5.39).

6.5.3 IP Telephony (IPT)

R193 If the voice network is connected to another IPT network, a secure voice-aware firewall **MUST** be installed (ACSI 33 3.8.87).

R194 Organisations **MUST NOT** run an IPT network over the same physical medium as a data network of a different classification (ACSI 33 3.8.88).

R195 Organisations **SHOULD** separate IPT traffic from other data traffic (ACSI 33 3.8.89).

R196 Organisations that do not run the IPT traffic on a separate network infrastructure **SHOULD** use VLANs or similar mechanisms to logically separate the IPT traffic from the rest of the data network (ACSI 33 3.8.89).

R197 Organisations **SHOULD** (ACSI 33 3.8.92):

R197.1 configure IP phones to authenticate themselves to the call controller upon registration;

R197.2 block unauthorised devices by default;

R197.3 disable phone auto-registration and only allow a whitelist of authorised devices to access the network; and

R197.4 disable any unused functionality such as speakerphones, USB ports, management interfaces etc.

Please see ACSI 33 3.8.93 for additional information for HIGHLY PROTECTED IPT systems.

R198 Organisations **SHOULD NOT** connect workstations to IP phones unless the computer and/or the phone, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between IPT and other data traffic (ACSI 33 3.8.95).

Please see ACSI 33 3.8.96 for additional information for HIGHLY PROTECTED IPT systems.

R199 Organisations **SHOULD NOT** use software phones (ACSI 33 3.8.100).

Please see ACSI 33 3.8.101 for additional information for HIGHLY PROTECTED IPT systems.

N/A
N/A
N/A
N/A
N/A
N/A
N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

7.0 Access Control

7.1 Business Requirement for Access

Objective: To control access to information.

7.1.1 Regulation of access

R200 Organisations **MUST** (ACSI 33 3.6.2):

R200.1 develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering user:

R200.1.1 identification;

R200.1.2 authentication;

R200.1.3 authorisation; and

R200.2 make users aware of these policies, plans and procedures.

R201 All system users **MUST** be (ACSI 33 3.6.6):

R201.1 uniquely identifiable; and

R201.2 authenticated on each occasion that access is granted to the system.

R202 DSD **RECOMMENDS** that multiple methods are combined for authenticating users (ACSI 33 3.6.7).

7.2 User Access Management

7.2.1 User registration

R203 Organisations **SHOULD** (ACSI 33 3.7.19):

R203.1 maintain a secure log of all authorised users, their user identification and who provided the authorisation and when; and

R203.2 maintain the log for the life of the system.

7.2.2 Privilege management

R204 As a minimum, all privileged users **MUST** (ACSI 33 2.1.25):

R204.1 comply with the relevant policies, plans and procedures for the system they are using;

R204.2 possess a security clearance at least equal to the highest classification of information processed on the system;

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- R204.3** protect the authenticators for privileged accounts at the highest level of information it secures;
- Example: Passwords for root and administrator accounts.
- R204.4** not share authenticators for privileged accounts without approval;
- R204.5** be responsible for all actions under their privileged accounts;
- R204.6** use privileged access only to perform authorised tasks and functions; and
- R204.7** report all potentially security-related information system problems to the ITSA.
- R205** Organisations **MUST** (ACSI 33 2.1.26):
- R205.1** restrict privileged access to the minimum required to fulfil designated roles; and
- R205.2** closely audit privileged access.
- R206** Access Policy **SHOULD** ensure that (ACSI 33 3.6.21):
- R206.1** administrators are assigned an individual account for the performance of their administration tasks;
- R206.2** privileged accounts are kept to a minimum; and
- R206.3** privileged accounts are used for administrative work only.
- R207** DSD **RECOMMENDS** clearing privileged users to a level one classification above the classification of the system (ACSI 33 3.2.15).

7.3 User Responsibilities

7.3.1 Unattended user equipment

- R208** Organisations **SHOULD** (ACSI 33 3.6.15):
- R208.1** configure systems with a screen and/or session lock;
- R208.2** configure the lock to activate after a maximum of 15 minutes of user inactivity;
- R208.3** configure the lock to completely conceal all information on the screen;
- R208.4** ensure the screen does not appear to be turned off while in the locked state;
- R208.5** require the user to re-authenticate to unlock the system; and
- R208.6** deny users the ability to disable the locking mechanism.

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

7.4 Proactive Security Audit

R209 Organisations **MUST** develop and document audit requirements reflecting the overall audit objectives, derived from the ICTSP and SRMP, covering (ACSI 33 3.7.26):

R209.1 the scope of audits;

R209.2 the audit schedule;

R209.3 actions to be taken when violations are detected;

R209.4 reporting requirements; and

R209.5 specific responsibilities.

R210 Organisations **SHOULD** (ACSI 33 3.5.19):

R210.1 characterise all devices whose functions are critical, and those identified as being at high risk of compromise;

R210.2 store the characterisation information securely;

R210.3 update the characterisation information after every legitimate change to the system;

R210.4 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;

R210.5 perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and

R210.6 resolve any detected changes in accordance with the documented incident management procedures.

R211 DSD **RECOMMENDS** that organisations meet the requirement for characterisation using a SHA DACA to perform cryptographic checksums (ACSI 33 3.5.19).

R212 Organisations **MUST** develop and document logging requirements reflecting the overall audit objectives derived from the ICTSP and SRMP, covering (ACSI 33 3.7.12):

R212.1 the logging facility, including:

R212.1.1 log server availability requirements;

R212.1.2 the reliable delivery of log information to the log server;

R212.2 the list of events associated with a system or software component to be logged; and

R212.3 event log protection and archival requirements.

R213 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):

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

- R213.1 date and time of the event;
 - R213.2 relevant user(s) or process;
 - R213.3 event description;
 - R213.4 success or failure of the event;
 - R213.5 event source (e.g. application name); and
 - R213.6 terminal location/identification.
 - R214 Event logs **MUST** be (ACSI 33 3.7.17):
 - R214.1 protected from modification and unauthorised access;
 - R214.2 archived and retained for future access; and
 - R214.3 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** systems.
- R215 The ITSA **SHOULD** be responsible for managing and auditing the event logs (ACSI 33 3.7.25).
 - R216 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).
 - R217 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).

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

8.0 Portable Computers, Portable Electronic Devices (PEDs) & Teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

For the purposes of this checklist, PEDs are defined as portable devices that can process, store and/or transmit data electronically.

Other considerations should include DSD's policy on BLACKBERRY computing.

8.1 Portable Computers and Portable Electronic Devices (PEDs)

R218 Organisations **SHOULD** encrypt the data on all PEDs (ACSI 33 3.4.62).

N/A

R219 DSD **RECOMMENDS** that organisations deploying PEDs for business purposes (ACSI 33 3.4.53):

N/A

R219.1 have a policy and associated procedures for the use of the device and associated services;

R219.2 ensure that staff acknowledge the policy and associated procedures before they are allowed to use the device and associated services; and

R219.3 have a policy and procedure governing PED connections to their corporate system.

R220 DSD **RECOMMENDS** that personally owned devices are not approved for use with organisation systems (ACSI 33 3.4.55).

N/A

R221 DSD **RECOMMENDS** that organisations train staff in the use of devices and associated services, including the security requirements, before they are permitted to use them (ACSI 33 3.4.57).

N/A

R222 Organisations **SHOULD** put a label warning against unauthorised use on all PEDs (ACSI 33 3.4.68).

N/A

R223 DSD **RECOMMENDS** an additional label be affixed to PEDs asking finders of lost devices to hand the equipment in to any Australian police station or, if overseas, an Australian Embassy, Consulate or High Commission (ACSI 33 3.4.68).

N/A

UNCLASSIFIED (RECLASSIFY after first entry)

Information System Review Checklist V4.0.0

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	