ACSI 33
Changes in the June 2004 Release

Overview

Introduction

The *Australian Government Information Technology Security Manual*, also known as *ACSI 33*, was first released in its current form in March 2004. Updates to *ACSI 33* will be released quarterly. Documents covering the changes made in each update will also be published with each new release.

This document covers the changes made to the *Australian Government IT Security Manual* in the June 2004 release.

Not included

The following types of amendments have **not** been noted in this document:

- typographical corrections,
- changes to the Index, and
- additions to the Abbreviations section.

Versions

Two versions of this document have been produced, one at UNCLASSIFIED, the other at SECURITY-IN-CONFIDENCE, consistent with the two versions of ACSI 33.

Changes that apply only to the SECURITY-IN-CONFIDENCE version of *ACSI 33* will be included only in the SECURITY-IN-CONFIDENCE version of this document.

Continued on next page

Terminology

When referring to information within *ACSI 33*, the following definitions are used:

- **version** refers to the classification of the document, either UNCLASSIFIED or SECURITY-IN-CONFIDENCE,
- **release** refers to the month and year it was published,
- **part** refers to Part 1, 2 or 3 within *ACSI 33*, and is indicated by the part number followed by a dash, and
- **block** refers to the set of information delineated by horizontal lines within the document, and is denoted by a three digit number.

Within this document, blocks are referred to by their part number, followed by the block number.

Example: Block 430 within Part 3 is referred to as 3-430.

Note: Page numbers are not referenced, as they may not be consistent between versions or releases.

Feedback

Numerous comments and suggestions relating to the March 2004 release of *ACSI 33* have been received. Some of the changes noted in this document are a direct result of this feedback. Many other comments will require more time to resolve effectively, and the results will be seen in future releases.

Feedback on this latest release of *ACSI 33*, and on the format and/or content of this Changes document, is also encouraged.

Contact details are in *ACSI 33*, Part 2, Block 105.

Contents

This document contains the following topics:

Summary of Significant Changes

Introduction

The following blocks summarise the most significant changes included in the June 2004 release of *ACSI 33*. More detail on these changes is given in the last section, 'Listing of Changed Blocks'.

Security of hardware

The most significant change in this release is to *Part 3, Chapter 4 – Security of Hardware*. Many blocks have been added or amended within this chapter.

Noteworthy changes include:

- addition of definitions for:
  - **declassification** the removal of all classifications, and
  - **reclassification** changing the classification, up or down,
- improvement of the logic and readability of the table defining the Disposal Process,
- addition of a policy statement defining when sanitisation of media is required,
- addition of a section on media destruction,
- some updating of the types of media for which sanitisation and destruction procedures are given,
- some updating of the sanitisation and destruction procedures,
- addition of policy stating that agencies MUST use a DAP for the sanitisation of magnetic media classified HIGHLY PROTECTED, **if** the media is intended for public release or disposal, and
- removal of approval for the sanitisation of CONFIDENTIAL, SECRET and TOP SECRET magnetic media to the lowest classification level. Policy now states that TOP SECRET must not be reclassified below CONFIDENTIAL, and SECRET and CONFIDENTIAL must not be reclassified below RESTRICTED.

Deviating from "SHOULDs" and "SHOULD NOTs"

The documentation required to support a decision to deviate from a **SHOULD** or **SHOULD NOT** has been defined.

Continued on next page

Summary of Significant Changes, Continued

Documentation classification

The policy on classifying IT security documentation has been clarified with respect to documentation containing detailed security information.

Existing guidance covers this implicitly by stating that:

- Agencies **MUST** classify their IT security documentation in accordance with the PSM, and
- DSD **RECOMMENDS** that agencies, by default, classify system documentation at the same level as that of the system itself.

An explicit policy statement has now been added, which reads:

> Agencies **SHOULD** classify security documentation that contains specific security configuration details at the level of the system to which it refers.

Block reference: 2-219.

Template references

DSD originally intended to develop templates specifically for Australian Government use. However, a review of existing publicly available templates resulted in the decision to refer *ACSI 33* users to some of these templates instead.

Block reference: 2-220.1.

High Grade Equipment

The policy for the disposal of High Grade Equipment has been amended to cover all High Grade Equipment, not just High Grade Cryptographic Equipment.

Block reference: 3-320.

Requirements for transit encryption

The policy on transit encryption has been clarified. The minimum levels are now expressed as mandatory requirements.

Block reference: 3-840, 3-841.

Listing of Minor Changes

Introduction	This section lists those changes considered to have only minor impact on users of *ACSI 33*.
Cabinet Handbook reference added	References to the *Cabinet Handbook* have been added to blocks relevant to CABINET-IN-CONFIDENCE information. **Blocks affected:** 1-112, 1-124.
"SHOULD" and "SHOULD NOT" interpretations	The "**Note:**" paragraphs have been replaced with references to a new block, number 116.1. **Block affected:** 1-115.
HB 231 references updated	All references to *HB 231:2000 Information Security Risk Management guidelines* have been updated to refer to *HB 231:2004*. **Blocks affected:** 1-124, 2-403, 2-408, 2-410, 2-414, 2-418, 2-423, 2-436, 2-443.
Templates references amended	All references to template documents have been amended to refer to the added block 2-220.1. (See next section.) **Blocks affected:** 2-406, 2-503.
Risk matrix amendment	The entry within the risk matrix that mapped "Almost certain" to "Insignificant" was not consistent with AS/NZS 4360. This has now been corrected. **Block affected:** 2-432.
Glossary changes	The following terms have been added or amended in the Glossary: • Certification Report, • Declassification, • Reclassification, and • Sanitisation

Continued on next page

Listing of Minor Changes, Continued

Other minor changes	Various other minor changes have been made to some blocks to improve the readability, accuracy or consistency of the document. These changes have no impact on policy. **Blocks affected:** 2-202, 2-303, 2-414, 2-418, 2-423, 2-436, 2-443, 2-705, 3-125, 3-135, 3-402, 3-403, 3-404.

Listing of Changed Blocks

Introduction

This section lists all the blocks that have been added, deleted, or significantly amended.

Deleted blocks

Deleted blocks are indicated within the June 2004 release by a block label. The block text has been replaced with "<deleted>", and the block number is retained.

Blocks affected: 3-406.

Added blocks

All added blocks have been copied in their entirety (not including unchanged tables) into this section. Added blocks are indicated by a block number that includes a period followed by another number.

Example: 2-220.1 indicates a new block inserted after block 2-220.

Hardware Security chapter

Part 3, Chapter 4 – Security of Hardware has had substantial changes made to it. The volume of changes makes it inappropriate to list all the changed blocks in this document. Readers are therefore advised to refer to the new release of *ACSI 33* to familiarise themselves with the new policy.

A summary of the most significant changes is included in this document on page 3.

Format

From this point onward, all blocks are presented as they appear in the June 2004 release, with following exceptions:

- any text within an existing block which has been added or amended has been highlighted,
- any unchanged tables within a block have not been shown,
- where information has been deleted, this is indicated by strike-through text, and
- the block number has been prefixed with the part number.

Deviations from "SHOULDs" and "SHOULD NOTs"

1-116.1. Agencies deviating from a "**SHOULD"** or **"SHOULD NOT", MUST** document:

- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- a date by which to review the decision, and
- management's approval.

Continued on next page

Document classification

2-219. Agencies **SHOULD** apply the following classifications, as a minimum, to IT security documentation.

Exception: Agencies **SHOULD** classify security documentation that contains specific security configuration details at the level of the system to which it refers.

Continued on next page

References

2-220.1. The table below provides references for templates that may assist agencies with the development of their security documentation.

Note: A reference for a template for SOPs has not been provided.

Type	Publication Title	Available from …	Notes
IT Security Policy (ITSP)	*AS/NZS 7799.2:2003 Information Security Management - Part 2*	Standards Australia **URL:** www.standards.com.au	Section 3 of Annex A contains the basis of an Information Security Policy which is slightly broader than an Information Technology Security Policy.
Risk Management Plan (RMP)	*HB 231:2004 Information Security Risk Management Guidelines*	Standards Australia **URL:** www.standards.com.au	Section 5 discusses documentation. **Note:** This document is based on *AS/NZS 4360:1999 Risk Management* which is also available from Standards Australia.
System Security Plan (SSP)	*NIST 800-18 Guide for Developing Security Plans for Information Technology Systems*	National Institute of Standards and Technology (US) **URL:** http://csrc.nist.gov/publications/nistpubs/index.html#sp800-18	This document is around 80 pages, however, Appendix C contains a template that could be used in isolation from the rest of the document. **Note:** This is a US document and it contains references to US agencies, legislation and policies.

Continued on next page

Listing of Changed Blocks, Continued

Template	2-301.1 **See:** 'Templates' on page 2-18.
Definition: Server	3-116.1 A server is a computer used to run programs that provide services to multiple users. **Examples:** • file server, • mail server, and • database server.
High Grade Equipment	3-311.1 Agencies intending to use High Grade Equipment **SHOULD** contact DSD.
High Grade Equipment ~~HGCE~~	3-320. Agencies **MUST** contact DSD for advice on the disposal of High Grade Equipment ~~HGCE~~.
Introduction	3-514. This section explains security requirements for software applications. Software applications include: • database applications, • web servers and client browsers, and • email servers and clients. • ~~data fusion servers and clients~~.
Requirements for transit encryption [IC, R, P]	3-840. The table below provides the **minimum** levels of assurance that ~~are acceptable~~ **MUST** be used for the encryption of IN-CONFIDENCE, RESTRICTED and PROTECTED information whilst in transit over a network.
High Grade Cryptographic Equipment standards	3-866. Agencies **MUST** comply with *ACSI 53* and *ACSI 105(B)* when using High Grade Cryptographic Equipment (HGCE). Agencies operating both HGCE and commercial grade cryptographic products may wish to use ACSI 53 for their commercial grade products also.