Australian Government ICT Security Manual

Changes in the March 2005 Release

Overview

Introduction

The *Australian Government Information and Communications Technology Security Manual*, also known as *ACSI 33*, was first released in its current form in March 2004.

This document identifies the changes made to *ACSI 33* in the March 2005 release. Only changes made since the September 2004 release are included.

Documented changes

Over 300 changes have been made since the last release, making it impractical to do a full listing. This Changes document therefore lists only the most significant changes.

Types of changes that **have** been noted in this document include:

- addition of material covering new topics,
  Example: The addition of a section on Protective Marking Policy for email.
- addition of new standards to existing topics, and
  Example: The addition of a block stating that agencies SHOULD perform the given activities in support of patching and hardening products.
- amendments to existing standards.
  Example: Changed the requirement for an agency to appoint an ITSA from a "SHOULD" to a "MUST".

Not included

Types of changes that have **not** been noted in this document include:

- typographical corrections,
- clarifications,
- minor re-ordering of blocks or sections,
- changes to the Index, and
- additions to the Abbreviations section.

Continued on next page

Overview, Continued

Changes to PSM references

References in *ACSI 33* to specific sections of the *Commonwealth Protective Security Manual (PSM)* have been removed or replaced in anticipation of a new *PSM* to be published later this year.

Important: The standards defined in the March 2005 release of *ACSI 33* take precedence over ICT security standards included in the 2000 release of the *PSM*.

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* have been included only in the SECURITY-IN-CONFIDENCE version of this document.

Feedback

Numerous comments and suggestions relating to *ACSI 33* have been received. Many of the changes noted in this document are a direct result of this feedback. Some other comments require more time to resolve effectively; the results may 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*, Block 2.1.5.

Terminology

The list of changes below uses the following definitions to refer to information within ACSI 33:

- **Part** refers to Part 1, 2 or 3 within *ACSI 33*,
- **Ch.** refers to the chapter number within the given part,
- **Section Title** refers to the relevant sub-heading within the given chapter,
- **Block** refers to the set of information delineated by horizontal lines within the document, and is denoted by the block number and block title, and
- **Description** contains a brief description of the type of change made to the given block/s.

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

List of Changes

Part	Ch.	Section Title	Block	Description
1	N/A	Overview	1.0.2 Authority	Added a block defining ACSI 33's authority as deriving from the PSM.
1	N/A	Overview	1.0.7 Paragraph numbering	Amended to define the new paragraph numbering system.
1	N/A	Overview	1.0.18 Deviations from “SHOULDs” and “SHOULD NOTs”	Added a dot point stating that deviations from a "SHOULD" MUST include "the ITSA’s involvement in the decision". Added "DSD RECOMMENDS that ITSAs retain a copy of all deviations."
1	N/A	Overview	1.0.25 Further information	Added another column with the name of the organisation from which the document may be obtained.
2	1	Overview	2.1.5 Contacting DSD	Updated DSD's contact email address.
2	1	Overview	2.1.7 Requirement for ITSA	Increased the requirement for an agency to appoint an ITSA to a “MUST”.
2	4	Stage 3: Analysing the Risks	2.4.26 Consequence determination	Updated the examples of consequences.
2	7	Certifying and Accrediting ICT Systems	2.7.4 Definition: certification	Moved the requirement for certification to block 2.7.30.
2	7	About Certification and Accreditation	2.7.8 Accreditation documentation	Amended block to state "DSD RECOMMENDS that agencies document all system accreditations."
2	7	About Certification and Accreditation	2.7.9 Requirement for accreditation	Amended block to include "Agencies MUST accredit all agency systems."
2	7	Gateway Certification	2.7.19 Independent gateway certifications	Replaced some of the company-focussed information with "Agencies SHOULD ensure that any companies contracted by them to provide gateway services have received a gateway certification from DSD or an I-RAP assessor."
2	7	Gateway Certification	2.7.21 Gateway Certification Guide	Added a block recommending the use of DSD's Gateway Certification Guide
2	7	Accreditation Process	2.7.30 Prerequisites	Amended the block to define pre-accreditation activities as a "SHOULD".
2	8	Overview	2.8.4 Staffing and resources	Amended the block to define role and resource assignments as a "SHOULD".
2	8	Managing Change	2.8.7 Change management standards	Amended the block to update the requirements for change management.
2	8	Various	2.8.11 to 2.8.35	Made substantial amendments to the organisation of and policy for security incidents.
2	9	Process for Reviewing ICT Security	2.9.9 Gathering information for a review	Amended the block to clarify the intention of the recommendation.
2	9	Process for Reviewing ICT Security	2.9.11 Process	Amended the block to make the review method a RECOMMENDS.
3	3	DSD Approved Products	3.3.3 Definition: DSD Approved Product	Amended the block to remove products in evaluation from the definition of a DAP.

Part	Ch.	Section Title	Block	Description
3	3	DSD Approved Products	3.3.5 to 3.3.6	Added blocks relating to protection profiles.
3	3	Product Selection	3.3.10 Policy	Moved the policy statement relating to the use of cryptographic products to block 3.9.4.
3	3	Product Selection	3.3.11 to 3.3.12	Split the existing block into two blocks: the first block relating to DAPs, and the second relating to other options. Moved "In Evaluation" products out of the definition of a DAP. Added a preference for DAPs evaluated against a Protection Profile.
3	3	Installing and Using Products	3.3.23 Patches and hardening products	Added a block on requirements to patch and harden products.
3	4	Classifying, Labelling and Registering Hardware	3.4.13 Classifying volatile media	Amended the block to apply to a wider range of classifications.
3	4	Disposing of Hardware	3.4.24 Standards	Amended the block on hardware disposal to require sanitisation/destruction/authorisation prior to disposal.
3	4	Disposing of Hardware	3.4.25 Occupational Health and Safety	Added a block on the requirement to meet OH&S standards.
3	4	Disposing of Hardware	3.4.28 Disposal process	Removed the reference to "classified" information only, to make the disposal process relevant to UNCLASSIFIED hardware also.
3	4	Media Sanitisation	3.4.39 Degaussers	Added a block on degaussers.
3	4	Media Destruction	3.4.43 to 3.4.50	Made substantial additions and amendments to blocks relating to media destruction requirements.
3	4	Portable Computers and Personal Electronic Devices	3.4.55 to 3.4.59	Made additions and amendments to blocks relating to portable computers and PEDs.
3	4	Portable Computers and Personal Electronic Devices	3.4.60 Labelling portable computers and PEDs	Amended the labelling requirement to make it SHOULD rather than MUST.
3	5	[Old] Software Applications	N/A	Deleted this section, and moved relevant blocks into other sections.
3	5	Electronic Mail – Protective Marking Policy	3.5.41 to 3.5.53	Added a section on requirements for protectively marking emails.
3	6	User Identification and Authentication	3.6.6 Policy	Amended to include a recommendation to identify and authenticate users of UNCLASSIFIED systems.
3	7	Vulnerability Analysis	3.7.21 to 3.7.24	Made substantial additions and amendments to blocks relating to vulnerability analysis.
3	8	Wireless Communications	3.8.41 to 3.8.47	Made substantial additions and amendments to blocks relating to wireless communications, and moved them from the Network Security chapter into the Communications Security chapter. Also incorporated RF transmitter policy from Telephones and Pagers.
3	8	Telephone Systems	3.8.48 to 3.8.50	Added blocks on policy for using telephones for classified information.
3	8	IP Telephony	3.8.52 to 3.8.59	Added blocks on policy for using IP telephony.

Part	Ch.	Section Title	Block	Description
3	8	Telephones and Pagers	3.8.63 to 3.8.72	Made additions and amendments to blocks on push-to-talk handsets, speaker phones, cordless and mobile phones.
3	8	Facsimile Machines	3.8.73 to 3.8.74	Added blocks on the use of facsimile machines.
3	9	N/A	N/A	Moved policy on cryptography out of the Communications Security chapter and into a separate chapter.
3	9	Cryptographic Requirements	3.9.5 Requirements for storage encryption	Amended the block to define reductions to handling requirements for encrypted information.
3	9	DSD Approved Cryptographic Algorithms	3.9.11 Asymmetric/public key algorithms	Amended block to add Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) to the list of DSD Approved Cryptographic Algorithms. Removed the recommendation for DSA.
3	9	DSD Approved Cryptographic Algorithms	3.9.12 Hashing algorithms	Amended the block to include the SHA family of algorithms.
3	9	DSD Approved Cryptographic Protocols	3.9.17 Implementing DACPs	Added block requiring the use of only approved cryptographic algorithms, and removed similar statements from the individual protocol sections.
3	9	Secure Sockets Layer and Transport Layer Security	3.9.21 Standards	Amended the SSL/TLS configuration requirements.
3	9	Secure Shell	3.9.24 Standards	Amended the SSH configuration requirements.
3	9	Secure Multipurpose Internet Mail Extension	3.9.27 to 3.9.29	Added policy on the use of S/MIME.
3	10	Internetwork Connections	3.10.11 to 3.10.12	Made additions and amendments to blocks on cascaded connections.
3	10	Gateways	3.10.15 to 3.10.18	Made additions and amendments to blocks on gateway standards for various classifications and caveats.
3	10	Gateways	3.10.19 Cascaded connections	Added a block on the requirement to meet the overall assurance requirements for cascaded connections.
3	10	Firewalls	3.10.21 to 3.10 27	Made additions and amendments to blocks on firewalls to clarify the requirements. In particular, made all firewall assurance levels a MUST, and increased the assurance requirement for a firewall between IN-CONFIDENCE and UNCLASSIFIED to EAL2.
3	10	Firewalls	3.10.28 Interconnecting networks within an agency	Added a block to reduce the requirements for firewalls when separating networks within an agency.
3	10	Multifunction Devices	3.10.58 Usage	Amended block to include PROTECTED under the SHOULD statement, and deleted the following block.