



Electronic Warfare Associates – Australia

## Information Security Standards: The Australian Business Perspective

*Standards can greatly assist organisations in the pursuit of effective Information Security policies and procedures. But which ones are right for you?*

By Jason Kempnich, BInfTech, CISSP  
Senior Information Security Consultant  
Electronic Warfare Associates Australia Pty Ltd

With the large number of national and international Information Security standards available, it can be somewhat of a challenge for Australian and New Zealand organisations and professionals alike to identify appropriate standards that meet their needs. Without an in-depth knowledge of each standard, there is no easy way to select which document best fits your organisation's requirements.

This paper explores Information Security standards relevant to the Australian and New Zealand contexts, with the goal of giving the reader a better understanding of the use and positioning of each standard. As this document is written as a guide with Australian and New Zealand organisations in mind, it will examine both international (ISO) and national (AS/NZS) documents.

### AS/NZS 7799.2:2003, Specification for Information Security Management Systems

Australian/New Zealand Standard 7799.2:2003 (henceforth 7799.2) was designed to act as a checklist of sorts for developing and auditing Information Security policies or management systems within organisations of any size. It achieves this by delivering a series of controls for various Information Security areas and activities. The content of the document is largely presented in a simple but effective format of:

1. *Section Title* – the topic the section examines.
2. *Objective* – what the section is supposed to achieve if it is implemented.
3. *The Controls* – a series of statements, outlining what must be adhered to in order for an organisation to achieve the objective.

For example, the standard defines the objective of "Information Security Policy" as

being "To provide management direction and support for information security". The document then proceeds to define that an Information Security Policy document "shall be approved by management, published and communicated, as appropriate, to all employees," amongst other statements. Thus it is fair to assume that if an organisation's Information Security Policy is not approved by management and published to employees, then it will not pass a 7799.2 audit.

The above example is typical for the content of the AS/NZS 7799.2:2003 standard, being a series of statements that if complied with will assure compliance with the stated objective. Accordingly, AS/NZS 7799.2:2003 makes for an excellent compliance tool for establishing and/or documenting Information Security Policies and processes within an organisation. 7799.2 refers to these as Information Security Management Systems (ISMSs). The controls listed within the document are generally optional, meaning they can be accepted and used, or discarded as appropriate for each organisation.

AS/NZS 7799.2:2003 is identical to the British Standard document of similar name, BS 7799.2:2002, Specification for Information Security Management Systems. In international circles, it is often the British Standard that is quoted and used.

7799.2 is occasionally confused with AS/NZS ISO/IEC 17799:2001, "Information Technology – Code of Practice for Information Security Management". Whilst the documents are complementary, they are different to each other, with 17799 being more related to providing guidance and support for some of the controls defined in 7799. 7799 and 17799 were originally developed as a pair of documents.

AS/NZS 7799.2:2003 can be sourced from Standards Australia at <http://www.standards.com.au/>

EWA AUSTRALIA



Electronic Warfare Associates – Australia

## **AS/NZS 17799:2001 (ISO/IEC 17799:2000), Information Technology – Code of Practice for Information Security Management**

The document AS/NZS 17799:2001 (henceforth 17799) is a duplicate of the international standard released a year before with Amendment Number 1, "ISO/IEC 17799:2000, Information Technology – Code of Practice for Information Security Management, incorporating Amendment Number 1". To confuse matters somewhat, this document was formerly known in Australia as "AS/NZS 7799.1" and "AS/NZS 4444.1", and "BS 7799.1" in the United Kingdom.

As can be seen, 17799's beginnings were as a document which was intended to be used in conjunction with another document, 7799.2 (detailed previously). 17799 was to originally provide guidance and support for some of the controls defined in 7799.2.

17799 is designed to provide a common basis for developing organisational security standards and effective security management practice and to provide a measure of confidence in inter-organisational dealings. It presents an objective for each chapter, then breaks the chapter down into a series of subsections. Each subsection provides an Information Security management related topic, in which best practice is presented. These topics may be audited with 17799 alone, or with considerable aid from 7799.2.

The standard is perhaps best known for its ten main chapter titles. Considerable work was placed into the chapters, to ensure they covered the majority of Information Security topic areas. These ten chapters were subsequently borrowed by the security industry at large and became known as the "Ten Domains of Information Security" and thus the basis for many training and certification programmes.

Subsequently, the reach of 17799's chapters is considerable and may contain information of benefit on a number of topics. The chapters are:

- Chapter 3: Security Policy
- Chapter 4: Organisational Security
- Chapter 5: Asset Classification and Control
- Chapter 6: Personnel Security
- Chapter 7: Physical and Environmental Security

- Chapter 8: Communications and Operations Management
- Chapter 9: Access Control
- Chapter 10: Systems Development and Maintenance
- Chapter 11: Business Continuity Management
- Chapter 12: Compliance

*AS/NZS 17799:2001 can be sourced from Standards Australia at <http://www.standards.com.au/>*

## **ISO/IEC TR 13335, Information technology guidelines for the management of IT Security**

ISO/IEC TR 13335 is a series of five documents published by the International Standards Organisation, meaning it is not an Australian Standard, but still represents best practice. The "TR" stands for Technical Report and has been designated as such because the information contained within the five documents is different to that which would normally be published as an international standard and may be an attractive alternative to the rigid Information Security Management Systems (ISMS) of the 7799/17799 standard combination. The five parts have been written over several years, with part one being published in 1996, whilst most recently part five was published in 2001. The parts are:

*Part 1: Concepts and models for IT Security.* The first document provides an overview of information security concepts and models that may be used by an organisation to define their IT Security. The document is pitched at Chief Security Officers (CSOs), general Information Security Managers and those who are generally responsible for or have an interest in the organisation's Information Security.

*Part 2: Managing and planning IT Security.* This document is concerned with planning and management aspects of Information Security and is pitched at managers who are responsible for design, implementation, testing, procurement or the operation of IT systems. It may also be of interest to managers who's staff make use of IT systems impacted by security issues.

*Part 3: Techniques for the management of IT Security.* Pitched at a development market, this document is concerned with management activities that are directly related



Electronic Warfare Associates – Australia

to project life cycles: planning, design, implementation, testing, etc.

*Part 4: Selection of safeguards.* Somewhat complementary to part 3, part 4 describes the selection of safeguards for projects (including operations), as well as the importance and use of baseline models and controls.

*Part 5: Management guidance on network security.* This document provides CSOs and others charged with the management of Information Security some guidance on communications and networks, particularly the analysis of communications related factors which must be considered in order to establish correct and true network security requirements and safeguards. It also provides a risk assessment style approach to the establishment of trust levels.

The technical report highlights to the reader that it is not a standard and consequently the report is only there to provide guidance. Individuals who are responsible for Information Security within an organisation may need to adapt the presented material to something more appropriate for their organisation and individual implementations. It should be noted that unlike 7799.2 and 17799, ISO/IEC 13335 does not specifically help an organisation establish an organisational baseline or related audit.

*The ISO/IEC TR 13335 documents, parts 1 through 5 can be sourced as a set or individually from Standards Australia at <http://www.standards.com.au/>*

### **ISO/IEC 21827:2002, Systems Security Engineering Capability Maturity Model (SSE-CMM) Description Document, version 3.0**

ISO/IEC 21827 (henceforth The SSE-CMM) is a freely available publication designed to aid an organisation in identifying the maturity of their information security processes. Like AS/NZS 7799.2, the SSE-CMM is focused at auditing. However unlike 7799.2, the audit has three aims:

- Identify the organisation's current information security maturity
- Identify what the organisation's information security maturity should be
- Display the results, identifying gaps between current and desired

The model describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. However, it is up to the organisation and assessor to decide how many of the SSE-CMM's 22 process areas are appropriate for the application at hand.

The SSE-CMM addresses security engineering activities that span the entire trusted product or secure system life cycle, including concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning. It is this "lifecycle spanning" that makes the SSE-CMM a useful tool for Information Security audits.

*The SSE-CMM Description Document can be downloaded in PDF format for free from <http://www.sse-cmm.org/> under the "Model" section. A hardcopy can be sourced from Standards Australia at <http://www.standards.com.au/>*

### **HB 231:2004, Information Security Risk Management Guidelines**

Risk management is an integral part of good management technique and has become well entrenched into the Information Security psyche. HB 231:2004 is an Australian/New Zealand document that aims to introduce guidelines for risk management within the Information Security context.

Effectively, HB 231 is a complement to the more commonly known AS/NZS 7799.2 and ISO/IEC 17799 standards. Both of those documents require that a formal risk assessment process be undertaken as a basis for selecting controls. HB 231 was written to fill that requirement.

The handbook provides a generic guide for an individual or organisation to establish and implement a formal risk management process specifically targeted on information security risks. The defined process involves establishing the context within the organisation, then identifying, analysing, evaluating, treating, communicating and monitoring of the risks.

*HB 231:2004 can be sourced from Standards Australia at <http://www.standards.com.au/>*



Electronic Warfare Associates - Australia

**Other documents of interest****AS/NZS 4360:2004, Risk Management**

Not specifically Information Security related, this standard may be of use for those requiring a better understanding of the risk management process in general. Within Australia and New Zealand, AS/NZS 4360:2004 is considered the premiere risk management standard.

The standard is meant to be used in conjunction with a handbook, HB 436.

*AS/NZS 4360 is available from Standards Australia at <http://www.standards.com.au/>*

**HB 436:2004, Guidelines to AS/NZS 4360:2004**

This document is a companion for AS/NZS 4360. The handbook reproduces the full text of 4360 section-by-section, following each section with notes that are relevant to the subject matter.

*HB 436:2004 is available from Standards Australia at <http://www.standards.com.au/>*

**HB 171-2003, Guidelines for the management of IT evidence**

In order to bring successful convictions in a court of law, all IT evidence must be carefully managed, from initial design of process

and procedure, to the collection and storage of the evidence. HB 171 was written to bring an Australian law perspective to requirements for judicial or administrative proceedings within Australia. Whilst the document is aimed at maximising the potential for evidence to be accepted by a court, it also presents processes that are international best practice in many other jurisdictions.

In the words of the handbook itself the content does not cover protective security, incident handling, administrative procedures, operational procedures and electronic evidence processing systems (e.g. DNA, fingerprints, etc.).

*HB 171-2003 is available from Standards Australia at <http://www.standards.com.au/>*

**About the author:**

Jason Kempnich is a Senior Information Security Consultant with Electronic Warfare Associates Australia Pty Ltd (EWA-Australia), with ten years of specialised experience in secure network architecture, risk assessments, and information security policies and standards.

Jason is a Certified Information Systems Security Professional (CISSP)

**For more information contact: [infosec@ewa-australia.com](mailto:infosec@ewa-australia.com)**

**Canberra:**

Level 1  
214 Northbourne Ave  
Braddon  
ACT 2612

Tel: +61 2 62 30 6833  
Fax: +61 2 6230 5833

**Brisbane**

MarketShare House  
2a / 96 Lytton Rd  
East Brisbane  
QLD 4169

Tel: +61 7 3891 6536  
Fax: +61 7 3891 6538

**Adelaide:**

Innovation House  
Mawson Lakes Boulevard  
Technology Park, Mawson Lakes  
South Australia 5095

Tel: +61 8 8260 8261  
Fax: +61 8 8260 8260