



# Information Security Guideline for NSW Government – Part 1 Information Security Risk Management

Issue No: 3.2

First Published: Sept 1997

Current Version: Jun 2003

## Table of Contents

<b>1. INTRODUCTION</b>	<b>4</b>
1.1 Scope	6
1.2 Aim	6
1.3 Continuous process	6
1.4 Structure	7
1.5 Application	8
1.6 Definitions	8
<b>2. INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK</b>	<b>12</b>
2.1 Overview	12
2.2 Critical Success Factors	13
2.3 Information Security Risk Components	14
2.3.1 ASSETS	14
2.3.2 ASSET VALUES (AND POTENTIAL IMPACTS)	14
2.3.3 THREATS	14
2.3.4 VULNERABILITIES	15
2.3.5 SECURITY RISK	15
2.3.6 SECURITY REQUIREMENTS	15
2.3.7 SECURITY CONTROLS	15
2.3.8 RELATIONSHIP BETWEEN RISK COMPONENTS	16
<b>3. INFORMATION SECURITY MANAGEMENT SYSTEM POLICY</b>	<b>17</b>
3.1 Overview	17
3.2 Security Principles	17
3.3 Content and Format	19
3.4 Communications	19
3.5 Review	21
<b>4. PLANNING AND RESOURCING</b>	<b>22</b>
4.1 Management Commitment	22
4.2 Planning	22
4.3 Resourcing	24
<b>5. INFORMATION SECURITY RISK MANAGEMENT PROCESS</b>	<b>26</b>
5.1 Overview	26
5.2 Step 1 – Define the Information Security Policy	28
5.2 Step 1 – Define the Information Security Policy	28
5.3 Step 2 – Define the Approach to Risk Assessment	28
5.3.1 ESTABLISH THE STRATEGIC CONTEXT	29
5.3.2 ESTABLISH THE ORGANISATIONAL CONTEXT	30
5.3.3 ESTABLISH THE RISK MANAGEMENT CONTEXT	30
5.3.4 DEVELOP RISK EVALUATION CRITERIA	31
5.3.5 DEFINE THE RISK ACTIVITY STRUCTURE	33
5.3.6 DEFINE THE INFORMATION ASSETS	33

5.3.7	DOCUMENTATION.....	35
5.4	Step 3 – Undertake a Risk Assessment.....	35
5.4.1	RISK IDENTIFICATION.....	36
5.4.2	RISK ANALYSIS.....	36
	5.4.2.1 RECOMMENDED APPROACH.....	38
	5.4.2.2 HIGH LEVEL RISK ANALYSIS.....	38
	5.4.2.3 DETAILED RISK ANALYSIS.....	41
5.4.3	RISK EVALUATION.....	42
5.4.4	DOCUMENTATION.....	43
5.5	Step 4 – Manage the Risk.....	43
5.5.1	DOCUMENTATION.....	44
5.6	Step 5 – Select Controls.....	44
5.6.1	BASELINE APPROACH.....	45
5.6.2	OPERATIONAL AND TECHNICAL CONTROLS.....	45
	5.6.2.1 PHYSICAL SECURITY.....	45
	5.6.2.2 PERSONNEL SECURITY.....	45
	5.6.2.3 PROCEDURAL SECURITY.....	46
	5.6.2.4 TECHNICAL SECURITY.....	46
	5.6.2.5 EVALUATED PRODUCTS AND SYSTEMS.....	46
5.6.3	FACTORS INFLUENCING CONTROL SELECTION.....	46
5.6.4	SECURITY ARCHITECTURE.....	46
5.6.5	CONSTRAINTS THAT AFFECT THE SELECTION OF CONTROLS.....	47
	5.6.5.1 TIME CONSTRAINTS.....	47
	5.6.5.2 FINANCIAL CONSTRAINTS.....	48
	5.6.5.3 TECHNICAL CONSTRAINTS.....	48
	5.6.5.4 SOCIOLOGICAL CONSTRAINTS.....	48
	5.6.5.5 ENVIRONMENTAL CONSTRAINTS.....	48
	5.6.5.6 LEGAL CONSTRAINTS.....	48
	5.6.5.7 PEOPLE AND SKILL CONSTRAINTS.....	48
5.6.6	DOCUMENTATION - INFORMATION SECURITY PLAN.....	48
5.7	Step 6 – Prepare Statement of Applicability.....	50
5.8	Step 7 – Management Approval.....	50
5.9	Importance of Documentation.....	50
<b>6.</b>	<b>IMPLEMENTATION AND OPERATIONAL PROCEDURES.....</b>	<b>52</b>
6.1	Implementation of Risk Treatment Plan.....	52
6.2	Implementation of Controls.....	52
6.3	Information Security Training.....	52
<b>7.</b>	<b>FOLLOW UP PROCEDURES.....</b>	<b>55</b>
7.1	Follow-Up.....	55
7.2	Compliance Checking.....	55
7.3	Configuration Management.....	56
7.4	Monitoring.....	56
7.5	Incident Handling.....	57
<b>8.</b>	<b>LEGISLATION AND RELEVANT DOCUMENTS.....</b>	<b>59</b>
8.1	Legislation.....	59
	8.1.1 NSW.....	59
	8.1.2 COMMONWEALTH.....	59
8.2	Relevant Documents.....	60
	8.2.1 NSW.....	60
	8.2.2 COMMONWEALTH.....	60
	<b>APPENDIX 1– SAMPLE INFORMATION SECURITY POLICY.....</b>	<b>61</b>
	<b>APPENDIX 2 - INFORMATION SECURITY PLAN TEMPLATE.....</b>	<b>66</b>

**APPENDIX 3 – STANDARD CLASSIFICATION OF SECURITY INCIDENTS .....70**

**APPENDIX 4 – GLOSSARY OF USEFUL TERMS.....73**

**APPENDIX 5 – REFERENCES .....83**

**Table of Figures**

Figure 1: Information Security Continuous Process ..... 7

Figure 2: Information Security Risk Management Framework..... 12

Figure 3: Risk concept relationship..... 16

Figure 4: Sample Information Security organisational structure..... 25

Figure 5: Information Security Management Process..... 27

Figure 6: Security context – concepts and relationships ..... 29

Figure 7: Follow-up procedures ..... 55

# 1. Introduction

**Information** is an asset that has a value to an agency and must therefore be appropriately protected.

Information is the basis on which governments conduct their business activity. As the custodian of a great deal of information that is politically, commercially or personally sensitive, the NSW Government has a fundamental 'duty of care' responsibility to protect that information from unauthorised or accidental modification, loss or release.

Information can be in any form. ICT can be printed or written, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. ICT therefore includes:

- Documents and papers;
- Electronic data;
- The software or systems and networks on which the information is stored, processed or communicated;
- Intellectual information (knowledge) acquired by individuals;
- Physical items from which information regarding design, components or use could be derived.

The objective of **information security** is to preserve the agency's information assets and the business processes they support in the context of:

- **Confidentiality** – information is accessible only to those authorised to have access;
- **Integrity** – accuracy and completeness of information and processing methods are safeguarded;
- **Availability** – information and associated assets are accessible by authorised users when required.

The Organisation for Economic Cooperation and Development (OECD) has established 9 principles for the security of information systems and networks with the overall goal of promoting a culture of security among all participants. These are:

1. **Awareness**  
Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. **Responsibility**  
All participants are responsible for the security of information systems and networks.
3. **Response**  
Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. **Ethics**  
Participants should respect the legitimate interests of others.
5. **Democracy**

- The security of information systems and networks should be compatible with essential values of a democratic society.
6. **Risk assessment**  
Participants should conduct risk assessments.
  7. **Security design and implementation**  
Participants should incorporate security as an essential element of information systems and networks.
  8. **Security management**  
Participants should adopt a comprehensive approach to security management.
  9. **Reassessment**  
Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Within the context of overall government policy security is left to agencies to resolve individually - being the custodians of the information means they are best able to gauge its worth, the threats and risks, and the appropriate measures to protect it.

Agencies are constantly challenged with threats to their information and information systems, such as denial-of-service attacks, computer viruses and exploitation of vulnerabilities. There is also a proliferation of security products in the market that agencies are exposed to, which claim to combat security risks.

It is widely accepted that there is no such thing as perfect security. Information security risks need to be managed. Security products can provide some protection but the need and effectiveness of these products will depend on the information security management process in place. Just as important is prompt 'patching' of vulnerabilities.

Due to increased connectivity of information infrastructures (telecommunications, banking and finance, transport and distribution, energy and utilities, information services, and other critical government services or collectively known as the National Information Infrastructure) system boundaries are rapidly disappearing. Agencies need to review their existing security regimes to assess the implications of these connections and any changes to the threats or risks inherent in connecting to them.

So that agencies can directly compare and assess other networks' threats and risks, a 'whole-of-public-sector' approach was developed in 1997 to enable a common, best practice framework. This approach had been derived from national and international standards, other State Governments' policies and the direct input from the representatives of a number of central NSW Government agencies. To take into account the changes in national and international standards that have occurred since 1997, the previous guidelines have been replaced with this document.

This Guideline presents a consistent approach to information security management, regardless of the size, complexity or nature of the agency. Agencies within the New South Wales Government are able to adopt this approach as an integral part of their strategy for achieving compliance with the Information Management Policies and are strongly encouraged to be certified to AS/NZS 7799.2:2003, *Specification for Information Security Management Systems*.

This Guideline consists of three parts, as follows:

**Part 1** provides an overview of the information security risk management process.

**Part 2** provides examples of threats and vulnerabilities that an agency may face.

**Part 3** provides guidance for selecting controls and establishing a minimum set of controls to protect all or some of an agency's information.

## 1.1 Scope

This Guideline provides a generic framework to all NSW government agency personnel who are responsible for establishing, managing, implementing or maintaining information security in their respective agencies. The Guideline is based on and is consistent with the Australian/New Zealand Handbook on *Information Security Risk Management* (HB 231:2000).

The purpose of this document is to provide guidance, not solutions on the management of information security. ICT is not intended to provide a comprehensive guide to information security threats, vulnerabilities, and controls.

Not all steps and issues described in the Guideline are relevant in every situation nor can ICT take account of the technological and operational conditions unique to each agency. The Guideline may require augmentation from individual agency's existing policies and procedures.

Safety critical systems, in particular, will require additional guidance from relevant standards such as the IEC 61508 series on *Functional safety of electrical / electronic / programmable electronic safety-related systems* and the Standards Australia Handbook on *Safety Issues for Software* (HB 220:2000). Safety critical systems are systems whose failure could threaten human life.

## 1.2 Aim

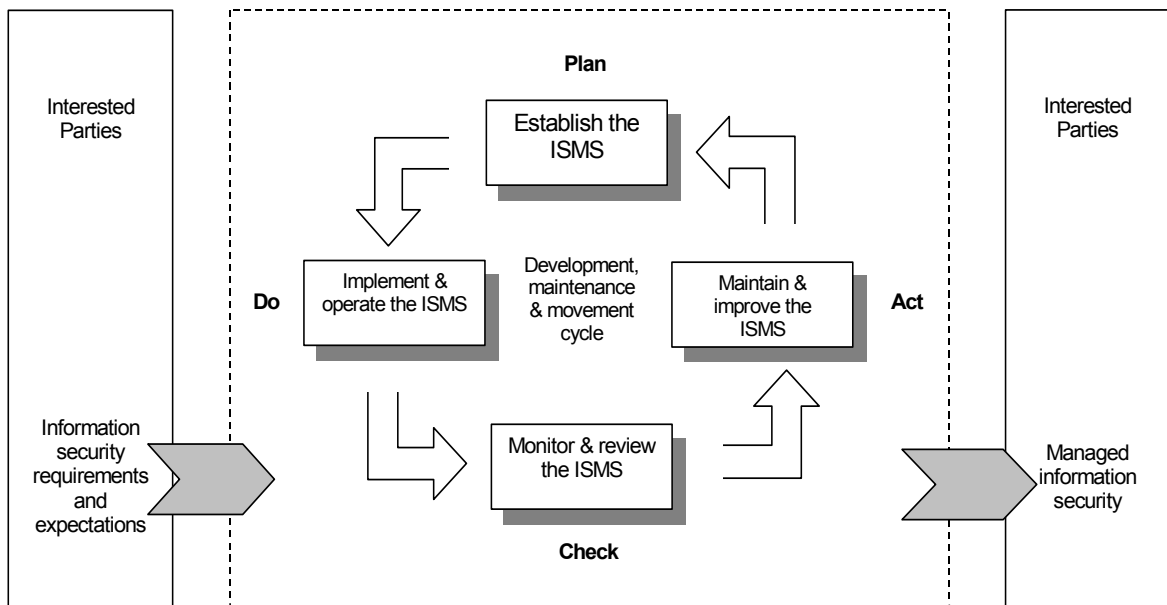
The aims of this Guideline are to:

- Create a framework to assist those responsible for the development and implementation of coherent measures, procedures and practices for the security of information and information systems;
- Raise awareness of the security risks with information and information systems;
- Identify measures that can be employed to help eliminate or reduce information security risks which agencies perceive as relevant to their environments;
- Serve as a starting point for developing agency-wide guidelines.

## 1.3 Continuous process

Information security management is a continuous cycle of 'Plan', 'Do', 'Check' and 'Act' (PDCA). ICT is illustrated below. ICT reflects the need to continuously adapt an information security management system to meet ever-changing threats

and vulnerabilities. ICT also has significant implications, not the least being the need for adequate resources.



**Figure 1: Information Security Continuous Process**

(Source: AS/NZS 7799.2:2003 Specification for information security management systems)

#### 1.4 Structure

This Guideline is structured as follows:

- Section 2:** “**Information Security Risk Management Framework**” provides a high level overview of an information management system and relationship of risk components.
- Section 3:** “**Information Security Policy**” describes the needs for and the elements of the information security policy.
- Section 4:** “**Planning and Resourcing**” discusses the management commitment, planning, responsibility and authority, and resourcing for the implementation of an information security risk program.
- Section 5:** “**Information Security Risk Management Process**” discusses the steps in the information security management process.
- Section 6:** “**Implementation and Operational Procedures**” describes the procedures for the implementation of the information security plan and the ongoing management and operation of the controls in the information security management plan.
- Section 7:** “**Statement of Applicability**” describes the requirements of documenting management decisions and justifications for selecting or rejecting particular controls.
- Section 8:** “**Legislation and Relevant Documents**” lists the relevant legislation and documents.

## [Sample information security policy](#)

## [Sample information security plan template](#)

### [Glossary of Useful Terms](#)

#### 1.5 Application

Risk management is recognised as an integral part of good management practice. ICT is an iterative process consisting of steps, which, when undertaken in sequence, enable continual improvement in decision making.

Information security risk management should be part of the agency's overall risk management.

Generally, information security risk management methods and techniques are applied to complete information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful. They should also be applied at an early stage in the life cycle of a new system.

This Guideline is applicable for three major audiences:

- 1) Managers accountable for the management of information security;
- 2) Personnel who are responsible for initiating, implementing and/or monitoring generic risk management systems within their agency;
- 3) Personnel who are responsible for initiating, implementing and/or maintaining information security within their agency.

This Guideline may be applied at all stages in the life of an activity, function, project, product or asset affected by information. Due consideration of the security issues at the planning stage of a project will produce significant benefits in terms of the development costs, functionality, integration, and user acceptance. Maximum benefit is usually obtained by applying the risk management process from the beginning.

ISO/IEC.AS/NZS 17799:2001 establishes a code of practice for selecting information security controls (or equivalently treating information security risks). AS/NZS 7799.2:2003 specifies an information security management system. Both parts require that a risk assessment process is used as the basis for selecting controls (treating risks).

This Guideline complements these Standards by providing additional guidance concerning management of information security risks.

#### 1.6 Definitions

A Glossary is provided at the end of this document. For the purpose of this Guideline, the following definitions apply:

Consequence:	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, or disadvantage. There may be a range of possible outcomes associated with an event.
Cost:	Of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, goodwill, political and intangible losses.
Common Criteria:	An internationally agreed approach, replacing ITSEC, TCSC, etc, for evaluating the security qualities of products and systems. See ISO/IEC 15408.
Event:	An incident or situation, which occurs in a particular place during a particular interval of time.
Frequency:	A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.
Impact:	See consequence.
Information Security Management System:	A documented system that describes the information assets to be protected, an organisation's approach to risk management, the control objectives and controls, and the degree of assurance required.
Information Integrity:	The property that information has not been altered or destroyed in an unauthorised manner.
Likelihood:	Used as a qualitative description of probability or frequency.
Loss:	Any negative consequence, financial or otherwise.
Monitor:	To check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.
Organisation:	A company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.
Probability:	The likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes. Probability is expressed as a number between 0 and 1, with 0 indicated an impossible event or outcome and 1 indicating an event or outcome is certain.
Protection Profile:	An implementation independent set of security requirements for a category of Targets of Evaluation that meet specific user needs. See ISO/IEC 15408 – Common Criteria.
Residual risk:	The remaining risks after risk treatment measures have been taken.
Risk:	The chance of something happening that will have an impact upon objectives. ICT is measured in terms of

	consequences and likelihood.
Risk acceptance:	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk analysis:	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk assessment:	The overall process of risk analysis and risk evaluation.
Risk avoidance:	An informed decision not to become involved in a risk situation.
Risk control:	That part of risk management that involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks.
Risk evaluation:	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk identification:	The process of determining what can happen, why and how.
Risk management:	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
Risk management process:	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Risk reduction:	A selective application of appropriate techniques and management principles to reduce either likelihood of an occurrence or its consequences, or both.
Risk retention:	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organisation.
Risk transfer:	Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.
Risk treatment:	Selection and implementation of appropriate options for dealing with risk.
Safeguard:	See security control.
Security control:	A practice, procedure or mechanism that reduces risk.
Stakeholders:	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.
Target of	An ICT product or system and its associated administrator

- Evaluation: and user guidance documentation that is the subject of a formal security evaluation, eg, using Common Criteria.
- Vulnerability: A characteristic (including a weakness) of an information asset or group of information assets which can be exploited by a threat.

## 2. Information Security Risk Management Framework

### 2.1 Overview

The loss of confidentiality, integrity, availability, accountability, authenticity and reliability of information and related services can have a severe impact on agencies. There is a critical need to protect information and information systems within agencies.

Providing an effective regime for information security, in an affordable and unobtrusive manner, has always been a challenge. With the speed in changes in technology and the manner in which business is conducted, information security risk management can become increasingly dynamic and challenging. The provision of adequate security mechanisms is often treated as secondary to the provision of functionality. As a result, agencies with critical business processes could be at risk.

Protecting information assets is an important goal for any agency. This goal can be achieved by:

- Recognising that management of information security risk is an integral part of the risk management process;
- Establishing and implementing a logical and systematic program for information security risk management.

A systematic approach for establishing such a program is shown in Figure 1. This approach can be applied to the whole agency, parts of an agency, a specific project or system.

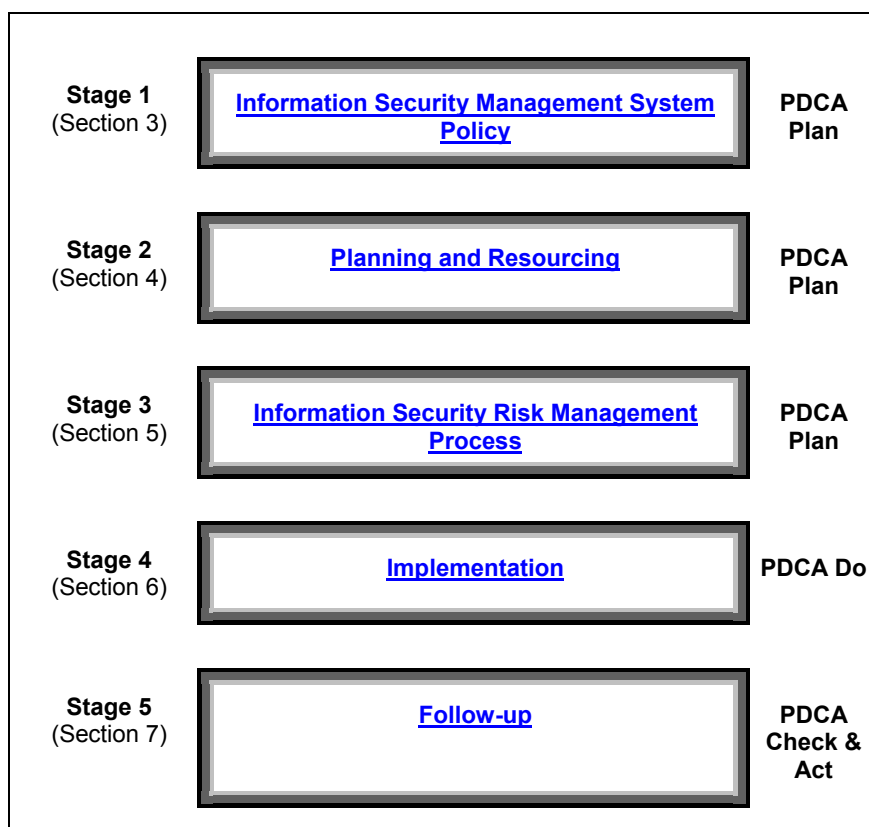


Figure 2: Information Security Risk Management Framework

This approach is discussed in the sections indicated above and is briefly described as follows:

- Stage 1** The starting point is to define the scope of the information security management system, once completed the process continues with the development of an information security policy, taking into account the agency's information security requirements. This is the essential first step and provides executive guidance for the following stages. However, its details may need subsequent modification, particularly after Stage 3.
- Stage 2** To effectively implement the policy, roles and responsibilities should be identified and adequate resources allocated.
- Stage 3** This step covers the assessment of information security risks and the selection of controls to reduce the likelihood and/or impact of these risks. The outcome of this step is an information security plan.
- Stage 4** The information security plan is implemented with an appropriate security awareness and training program. This step may also involve the approval of information systems before these are placed into production.
- Stage 5** To ensure that implemented controls work effectively, follow-up activities should be established and implemented. These activities include: maintenance, security compliance checking, change management, monitoring and incident handling.

Information security risk management is an iterative process that will require monitoring and review. Therefore any changes to the results of the above steps will require feedback into the process.

## 2.2 Critical Success Factors

The successful implementation of information security within the agency will depend on several factors, such as:

- Security policy, objectives and activities being based on business objectives;
- An approach to implementing security that is consistent with the organisational culture;
- Visible support and commitment from top management;
- A good understanding of the security requirements and risks;
- Effective marketing of security to all managers and employees;
- Distribution of comprehensive guidance on information security policy and standards to all employees and contractors;
- Appropriate training and education.

An effective information security risk management process also aids in the successful implementation of the program.

## 2.3 Information Security Risk Components

### 2.3.1 ASSETS

An asset is something that the agency values and therefore has to protect. Assets include all the information and supporting items that an agency requires to conduct its business. Examples of these assets include:

- 1) Information/data (eg, files containing payment details, voice records, image files, product information, manuals, and continuity plans);
- 2) Paper documents (eg, contracts, completed forms);
- 3) Software (eg, system software, application software, development tools and utilities);
- 4) Physical equipment (eg, computer and communications equipment, magnetic media, other technical equipment such as medical equipment and environmental equipment, furniture, accommodation);
- 5) Services (eg, computing and communications services, service providers, and utilities);
- 6) People and their knowledge (eg, technical, operational, marketing, legal, financial, contractors and consultants, outsourced providers);
- 7) Image and reputation of the agency.

### 2.3.2 ASSET VALUES (AND POTENTIAL IMPACTS)

Asset values are used to identify the appropriate protection for assets and to determine the importance of the assets to the business. These values can be expressed in terms of the potential business impacts of undesirable events affecting loss of confidentiality, integrity and/or availability. Potential impacts include financial losses, loss of revenue, market share or image (this topic is further discussed in [Section 5, Step 3 – Undertake a Risk Assessment](#)).

### 2.3.3 THREATS

A threat is the potential cause of an unwanted event that may result in harm to the agency and its assets. This can take many forms. Threats can be acts of nature (such as flood, fire and earthquake), intentional or accidental acts. In general, ICT could result in:

- 1) Destruction of an asset (facilities, data, equipment, communications, personnel);
- 2) Corruption or modification of an asset (data, applications);
- 3) Theft, removal or loss of an asset (equipment, data, applications);
- 4) Disclosure of an asset (data);
- 5) Use or acceptance of an illegal asset (equipment, unlicensed software, repudiated data, false data);
- 6) Interruption of services.

A threat would need to exploit the vulnerability of the asset in order to successfully cause harm.

Example of threats can be found in [Part 2 of this Guideline](#).

#### 2.3.4 VULNERABILITIES

Vulnerabilities are weaknesses associated with an agency's assets. A vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset, either with greater frequency, greater impact, or both. Therefore, a vulnerability that cannot be exploited by a threat, is not harmful to the asset.

Typically a vulnerability is a consequence of flawed procedures, under-skilled staff, incorrectly configured or defective technology. For a vulnerability to be exploitable it must be known to or discoverable by a threat. This makes it important to follow the 'need to know' principle with respect to security related information, and apply it to both people and technology. It also makes it important for an agency to react appropriately when learning of any vulnerabilities that affect it. Details of software vulnerabilities are widely available on the Internet.

Example of vulnerabilities can be found in [Part 2](#).

#### 2.3.5 SECURITY RISK

A security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and directly or indirectly affect the agency. The security risk level is determined from the combination of the asset values and assessed levels of related threats and associated vulnerabilities.

#### 2.3.6 SECURITY REQUIREMENTS

The three main sources of information security requirements are:

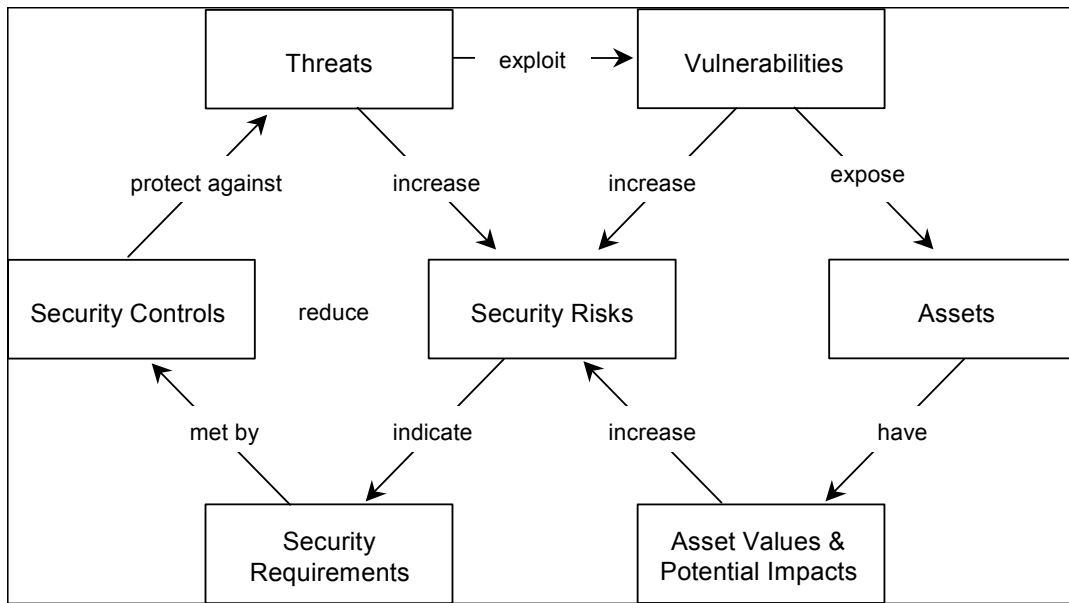
- 1) Unique security risks which could result in significant losses if they occur;
- 2) Legal, statutory and contractual requirements that the agency, its trading partners, contractors and service providers have to comply;
- 3) Agency-wide policies, principles, objectives and requirements to support its business operations.

Each of these requirements should be formulated in terms of the confidentiality, integrity and availability of the information

#### 2.3.7 SECURITY CONTROLS

Security controls are the practices, procedures or mechanisms that may protect assets against threats, reduce vulnerabilities or reduce the impact of an undesirable event.

### 2.3.8 RELATIONSHIP BETWEEN RISK COMPONENTS



**Figure 3: Risk concept relationship**

(Source: Australian Standard Handbook of Information Security Risk Management – HB231:2000)

### 3. Information Security Management System Policy

<i>AS/NZS 7799.2:2003 4.1.1.1 A.3.1.1 A policy document shall be approved by management, published, and communicated, as appropriate, to all employees.</i>
---

#### 3.1 Overview

As part of the agency's risk management process, the agency should have a risk management policy, as described in AS/NZS 4360:1999. This policy should include the objectives for and commitment to information security risk management. It should be consistent with the agency's strategic context, goals, objectives and the nature of its business.

Executive management should set a clear direction and demonstrate their support for and commitment to the Information Security Management System (ISMS) by issuing a formally agreed and documented ISMS policy across the agency. The policy should be endorsed and signed by the Chief Executive Officer.

However, before a policy can be prepared the scope of the ISMS has to be defined. It may be the entire organisation but could be a single site (physical or web) or a particular system or service. The goal is that the ISMS covers all parts of an organisation where information security is an issue, whatever the media of information. Nevertheless, where a large organisation is planning to achieve certification to AS/NZS 7799.2 It may be appropriate to adopt a phased approach.

The ISMS Policy serves as the foundation of the ISMS program and the basis for adopting specific procedures and technical controls. It is the first step in establishing a security culture that strives to make everyone in the agency aware of the need for security and the role they personally have to play.

The overall approach to information security in risk management. This means that the development of ISMS Policy is iterative with risk management activities. Preliminary risk management activities inform the development of policy, which then guides risk management and the development of information security plans. The ISMS Policy and the Statement of Applicability also have to be mutually consistent.

#### 3.2 Security Principles

There are nine generally accepted principles that provide guidance in the security of information. These are:

##### 1. Accountability

The responsibility and accountability of information / data custodians, information / data providers, users and other parties concerned with the security of information should be explicit.

## 2. Awareness

To foster confidence in information systems, custodians, providers and users shall have access to all documentation about information security policies and procedures.

## 3. Ethics

In the provision of information systems and the establishment of information security, the rights and legitimate interests of the organisation's personnel, its customers and business partners shall be respected.

## 4. Business Perspective

Security processes shall take account of and address the relevant business considerations and viewpoints; these include commercial, technical, administrative, organisational, operational, political and legal / statutory aspects.

## 5. Proportionality

The level and cost of security processes shall be appropriate and proportionate to the value and degree of reliance on information systems and to the severity, probability and extent of potential or actual harm to the organisation.

## 6. Integration

Security processes shall be coordinated and integrated with each other and with other measures, procedures and practices of the organisation to create a coherent system of information security.

## 7. Timeliness

Action to respond to a information security breach shall be timely and coordinated to prevent and overcome the breach of security.

## 8. Reassessment

The security of information systems shall be reassessed periodically recognising that information systems and the requirements for their security vary over time.

## 9. Freedom of Information

The security of information systems shall be compatible with the legitimate use and flow of data and information as permitted by "privacy" and required by "freedom of information" statutes.

### 3.3 Content and Format

A written policy is the primary means by which executive management gives direction to employees and informs its clients and business partners. It is part of good corporate governance.

The purpose of the ISMS Policy is to provide executive management direction and support. Policies establish the required outcomes and may vary widely in their specificity. Some may be expressed in terms of broad goals and objectives while others may detail a particular behaviour or actions. The Policy may comprise a single document or a set of documents depending on the size of the agency and its circumstances.

There may be a corporate security policy, which comprises the security principles and directives for all aspects of security throughout the agency, as part of the broader corporate policies. Often this is prepared in a strategic context taking into account the financial, operational, customer and legal / regulatory aspects of the agency's functions and activities. The policy may involve both internal and external stakeholders, and must be part of the contract if ICT is outsourced.

The ISMS Policy establishes the framework for risk management. This necessitates preliminary risk management activities:

- Establishing the risk context for the ISMS (when scoping the ISMS);
- Consideration of business, legal, regulatory and contractual requirements;
- Establishing the approach to risk management and the criteria for evaluating risks.

Within its scope an effective ISMS policy must be:

- Achievable by agency members with clearly defined responsibilities for at least users, ICT staff and management;
- Enforceable both procedurally and technically, and with sanctions when breaches occur;
- Implementable through processes, procedures, technical controls or other methods, via clearly documented directives, guidelines, instructions and the like.

The aim of the ISMS Policy is to address the issues of awareness, behaviour and deterrence. ICT is usually not specific about the control measures and procedures that implement the Policy but will establish requirements for these measures. There are no hard and fast rules to define the format or content of an ISMS Policy. However, agencies may find it appropriate to structure their Policies in four main parts:

A short statement of executive intent including:

- 1) An introduction that emphasises the dependence of the agency on information for its operational and administrative activities, and the importance of protecting it;
- 2) A definition of information security, its overall objectives and scope in the agency;
- 3) A statement of the goals and principles of information security in the agency;
- 4) An outline of the assets that require protection and guidance on how they are to be valued.

A possible outline of this is provided at Appendix 1. This forms part of the context for and is an input to risk management. (4) may be sensitive and documented separately.

- Direction on the responsibilities and accountabilities of individual staff of all types including contractors. It is essential that this is explicit and enforceable and should focus on the proper use and protection of the ICT resources provided for their use. It should be no more than one page and issued to all staff. It may reference subject specific policies required for various users, these are best published in a staff manual on the Intranet.
- General direction to all managers (including ICT security) and business units including specific security requirements for the whole agency, including:
  - 1) The method of risk assessment, security requirements including legal and regulatory, and criteria for the acceptability of risks;
  - 2) Security education and training;
  - 3) Sensitive information handling;
  - 4) Business Continuity Planning
  - 5) Procedures for handling suspected security incidents and the consequent actions to be taken;
  - 6) Requirements for internal auditing;
  - 7) Reviews of information security policies and plans.

Implementation may require 'plans' and other documented procedures.

- Direction to the ICT organisation (operators, maintainers, developers, etc), which provides additional and specific information for their planning of security controls for general and specific purposes. These controls will be procedural and technical, covering system administration and the capabilities required in systems, and will be documented in 'plans'. The detail should provide the context and significant risk scenarios for use in the risk management process.

There is no definitive ISMS Policy that can be readily adopted by all organisations. In practice ICT is preferable for each agency to compose its policy in its own style to reflect its own culture. This should not, however, discourage an agency from adapting another organisation's ISMS Policy where ICT is applicable.

### 3.4 Communication

Once the ISMS Policy has been developed and approved, ICT should be communicated, understood, implemented and maintained at all levels of the agency.

Procedures should be established to ensure that the Policy and any revisions are issued to all existing and new employees and contractors, perhaps even requiring them to sign to acknowledge receipt. Furthermore, it ensures that ignorance cannot be used in defence of a breach.

The ISMS Policy should be covered in [awareness and training programs](#).

### 3.5 Review

<b>AS/NZS 7799.2:2003</b>	<b><i>A.3.1.2 The policy shall be reviewed regularly, in case of influencing changes, to ensure ICT remains appropriate.</i></b>
---------------------------	--

The Policy may become inadequate as changes occur in technology, laws and regulations, threats or operations. As a minimum, the Policy should be assessed annually to ensure currency and adequacy.

## 4. Planning and Resourcing

### 4.1 Management Commitment

One of the key factors for successful information security in any organisation is the:

**visible support and commitment from management**

Executive management direction on, and commitment to, information security can influence the culture of the agency. Executive management interest helps ensure that information security is taken seriously at lower organisational levels.

Management's commitment to information security can be demonstrated by ensuring that:

- This is reflected in the [ISMS policy](#);
- Adequate resources are allocated to information security;
- An [information security management system](#) is established, implemented and maintained in accordance with AS/NZS 4360:1999 and AS/NZS 7799.2:2003;
- The performance of the ISMS is reported to top management for review and as a basis for improvement, taking into account any regulatory reporting requirements.

### 4.2 Planning

Information security planning is the product of the agency's ISMS policy and information security risk management processes. However, some of its outputs may lead to modification (or completion) of the ISMS Policy, particularly detailed aspects of staff conduct. There is also likely to be iteration between planning and policy as organisational and resourcing issues are resolved, and further policy review when the Statement of Applicability is developed and its implications considered.

Information security needs should be addressed at all planning and decision making activities. This includes enhancements to existing systems and new business and their supporting ICT systems.

The establishment of an ISMS program is part of the planning process.

At this stage the preparations for the next step have to be made. These include establishing and staffing a management structure and defining the approach to be taken by the security risk management process. A key organisational issue is to plan the relationship between ISMS responsibilities and those for information management, information systems, risk management and physical security.

### 4.3 Responsibility and Authority

The responsibility, authority and the interrelationship of personnel who perform and verify work affecting information security management should be defined and

documented, particularly for people who need the organisational freedom to do one or more of the following:

- Identify those areas where information security risks need management;
- Initiate action to prevent or reduce the adverse effects of risk;
- Control further treatment of risks until the level of risk becomes acceptable;
- Identify and record any problems relating to the management of risk;
- Initiate, recommend or provide solutions through designated channels;
- Verify the implementation of solutions;
- Communicate and consult internally and externally as appropriate.

<b>AS/NZS 7799.2:2003</b>	<b><i>A.4.1.1 A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place.</i></b>
---------------------------	---

Information security is an interdisciplinary activity and can be achieved through various organisational schemes, depending on the size and structure of an organisation.

Typically the responsibility for the security of information will rest with the agency's personnel (and ultimately the Chief Executive Officer). To effectively initiate and control the implementation of information security within the agency, all members of the management team share this responsibility.

The Information Security management team undertakes the following:

- Review and approve information security policy and overall responsibilities;
- Monitor significant changes in the exposure of information assets to major threats;
- Review and monitor security incidents;
- Approve major initiatives to enhance information security.

In small to medium size agencies, this team may be the executive management.

<b>AS/NZS 7799.2:2003</b>	<b><i>A.4.1.2 Where appropriate to the size of the organisation, a cross-functional forum of management representatives from relevant parts of the organisation shall be used to co-ordinate the implementation of information security controls.</i></b>
---------------------------	---

For large agencies, it may be necessary to co-ordinate the implementation of information security through a cross-functional forum of management representatives from relevant parts of the organisation. This forum will:

- Agree specific roles and responsibilities for information security across the organisation;
- Agree specific methodologies and processes for information security, eg, risk assessment, security classification system;
- Agree and support organisation-wide information security initiatives, eg, security awareness programs;
- Ensure that security is part of the information planning process;
- Assess the adequacy and co-ordinate the implementation of specific information security controls for new systems or services;

- Review information security incidents;
- Promote the visibility of business support for information security throughout the agency.

<b>AS/NZS 7799.2:2003</b>	<b><i>A.4.1.3 Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined.</i></b>
---------------------------	---

Effective security requires accountability and the explicit assignment of responsibility to asset custodians, providers and users of information.

The ISMS Policy should provide general guidance on the allocation of security roles and responsibilities in the agency. Where necessary, this is supplemented by more detailed guidance for specific sites, systems or services. Local responsibilities for individual physical and information assets and security processes, such as business continuity planning, should be clearly defined.

An agency must appoint an officer to be responsible for all information security matters in the agency. The Information Security Officer should have sufficient authority and have access to agency executive when issues require escalation. This officer has overall responsibility for the development and implementation of security to support the identification of controls. However, responsibility for resourcing and implementing the controls will often remain with the individual managers.

A custodian should be assigned to each information asset. This custodian will be responsible for the day-to-day security of the information asset. This responsibility may be delegated to individual managers or service providers. However, the custodian remains ultimately responsible for the security of the asset and should be able to determine that any delegated responsibility has been discharged correctly.

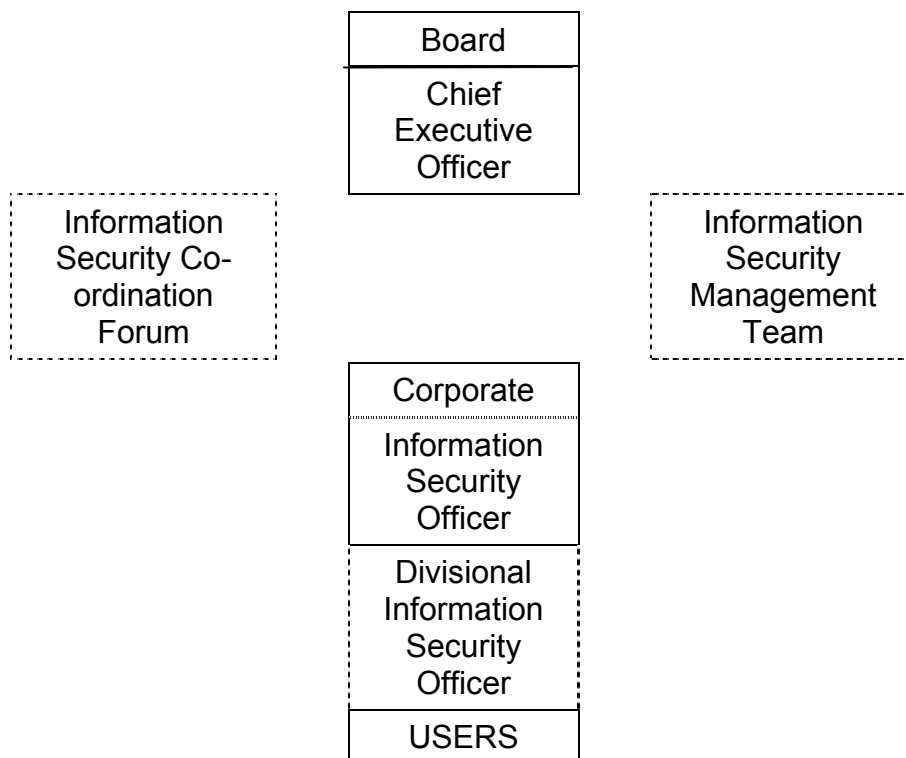
Obligations and responsibilities under the State Records Act 1998 should be clearly understood by all relevant personnel.

#### 4.4 Resourcing

Tasks do not necessarily have to be carried out by several persons. Staffing requirements for information security will depend on the size of the agency and its security requirements.

Management should provide adequate resources to implement the ISMS program. Management should also ensure that personnel involved in various aspects of the program have the skills and knowledge they need to effectively carry out their tasks.

Figure 4 is an illustration of a simple ISMS organisational structure. Optional roles are depicted in dotted lines.



**Figure 4: Sample Information Security organisational structure**

*AS/NZS 7799.2:2003 A.4.1.5 Advice on information security provided by in-house or specialist advisors shall be sought and communicated throughout the organization.*

In-house specialists (usually the Information Security Officer and/or the Information Security section, if any) provide advice on information security issues to agency personnel.

With the rapid changes in technology, it is challenging for in-house specialists to keep up-to-date with ongoing developments in the area of information security. Where necessary, their skills should be supplemented with external expertise and knowledge. External sources for advice include peer contacts within the Federal and State governments, contacts from professional organisations, and external security consultants.

## 5. Information Security Risk Management Process

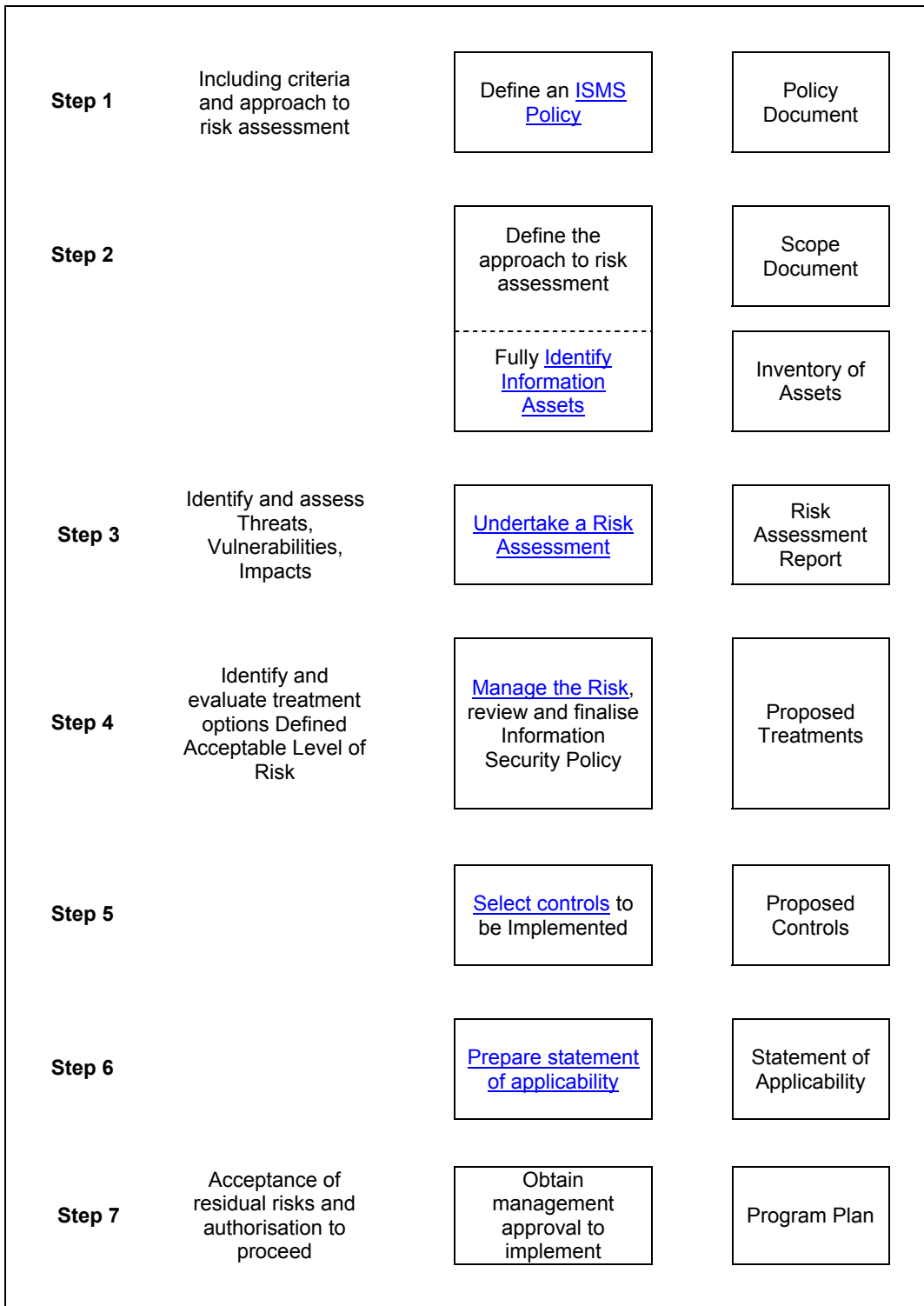
### 5.1 Overview

**Information Security Risk Management** is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating information security risks.

Information security management can be successfully implemented with an effective information security risk management process. AS/NZS 4360:1999 specifies a generic risk management process and HB 231:2000 specifies an information security risk management system to implement this process for information security risks. The agency's overall risk management philosophy, culture and structure will determine whether steps could be combined or omitted. However, all underlying concepts should be taken into consideration.

An Information Security Management System (ISMS) is a documented system that describes the information assets to be protected, the agency's approach to risk management, the control objectives and controls, and the degree of assurance required. The ISMS can be applied to a specific system, components of a system or to the agency as a whole.

A systematic approach is outlined in Figure 5 which shows the major steps and the documentation as a result of each step. Each of these steps is dealt with in the subsequent sections of this Guideline.



**Figure 5: Information Security Management Process  
(Adapted from AS/NZS 7799.2:2003)**

## 5.2 Step 1 – Define the Information Security Policy

This activity has been discussed in [Section 3](#). It sets out the management direction for information security. Specific security policies may have been defined to reflect particular security requirements in the context of the business needs of the organisation. It is unlikely that the Policy will have been completed at this stage, but key policy aspects must be established to provide the framework for the subsequent Steps. When risk management activities are completed then additional detail may be added to some parts of the Policy.

## 5.3 Step 2 – Define the Approach to Risk Assessment

The scope and the parameters of the ISMS must be clearly defined at the beginning of the process, building on the work in the previous step. This sets the framework for the rest of the process within which risks must be managed and provides guidance for making decisions. A definition of the boundaries avoids unnecessary work and improves the quality of the risk analysis.

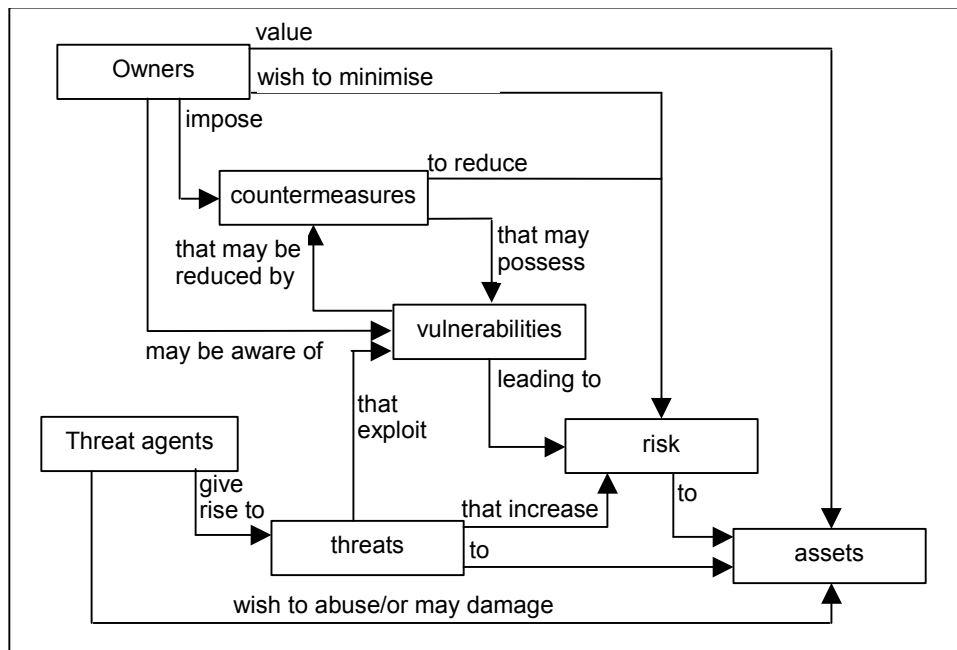
This step aims to clarify the following:

- What are the parts of the business / agency that rely on the accuracy, integrity or availability of information for essential decisions?
- What are the issues that need to be considered in assessing information security risks?
- What information needs to be protected?
- What are the information security requirements of the agency?

The key components in the scoping of the ISMS are:

- Establish the strategic context;
- Establish the organisational context;
- Establish the risk management context;
- Develop risk evaluation criteria;
- Define the risk activity structure;
- Define the information assets.

The general security context is illustrated in [Figure 6](#).



**Figure 6: Security context – concepts and relationships**  
(Source: ISO/IEC 15408-1 Common Criteria)

### 5.3.1 ESTABLISH THE STRATEGIC CONTEXT

Any decisions regarding the management of information security risk need to be consistent with the public sector environment and the agency’s own environment.

This component is focused on the environment in which the agency operates. The agency should determine the crucial elements that might support or impair its ability to manage its information security risks. The Information Security Policy created at Step 1 is one of the inputs at this stage.

The agency should understand the following:

- Its strengths, weaknesses, opportunities and threats;
- Its internal and external stakeholders, taking into account their objectives and perceptions;
- The financial, operational, competitive, political (public perceptions/image), social, client, cultural and legal aspects of the agency’s functions.

There should be a close relationship between information security risk management and the agency’s mission statement or strategic objectives.

Where risks may be shared between the agency and another organisation, cross-organisational issues should be identified. In addition, attacks on any one of the organisations in the National Information Infrastructure could have an impact on the agency.

### 5.3.2 ESTABLISH THE ORGANISATIONAL CONTEXT

This component requires an understanding of the agency, how it is organised, its capabilities, goals, objectives and the strategies that are in place to achieve them. This will help to define the criteria to determine whether a risk is acceptable or not, and form the basis of controls and risk treatment options. The general nature of the agency's information assets in broad terms of their tangible and intangible value is part of the organisational context.

The Information Security Policy created at Step 1 is one of the inputs at this stage.

Failure to achieve the objectives of the agency or specific business activity or project being considered may, in part, be due to poorly managed information security risks.

An example could be the reluctance of customers to undertake electronic commerce transactions if they do not have the confidence that the agency understands the importance of privacy of information, the potential impact of breaches of privacy or has put in place appropriate policies and procedures to protect their privacy.

### 5.3.3 ESTABLISH THE RISK MANAGEMENT CONTEXT

The scope and depth of the review of information security risks are determined in this component. This involves:

- 1) Defining the review project or activity and establishing its goals and objectives. Will the review cover agency-wide issues or will it be limited to a specific project, activity, consolidated groups of information assets or to individual assets?
- 2) Defining the timeframe and locations to be covered by the review. What is the time allotted to complete the assessment? Where will the review take place - just Head Office, Divisions, or a particular business unit or site or a group of sites?
- 3) Identifying guides, aids and the resources required to conduct the review. Guides may identify the generic sources of risk, examples of common vulnerabilities and threat types and the areas of impact. Is the assessment to be undertaken internally or by an external source? How many people will be involved? If undertaken internally, who is the best person(s) to undertake the task? What tools are to be used in the risk assessment – computer software or manual records?
- 4) Defining the extent and comprehensiveness of the risk management activities to be carried out. Specific issues that may be considered include the following:
  - The roles and responsibilities of various parts of the agency participating in managing risk;

- The relationship between the information security risk assessment project and other parts of the agency or other projects undertaken or planned within the agency.

#### 5.3.4 DEVELOP RISK EVALUATION CRITERIA

In order to assess the risks, impacts, consequences and the selection of controls, the quantitative and/or qualitative criteria to be used should be defined. Consideration is given to the level of risk that the agency is willing to accept. The Information Security Policy created at Step 1 is one of the inputs at this stage.

The development of the detailed risk criteria will be influenced by a number of factors such as:

- The agency's internal policy, goals and objectives;
- Expectations of stakeholders and customers;
- Legal requirements.

It is important that appropriate criteria be determined at the outset of the risk assessment and be continually reviewed throughout the risk assessment process. Risk criteria may be further developed and refined to ensure that risk criteria correspond to the types of risks and the way in which the levels are expressed.

Decisions concerning risk acceptability and the subsequent risk treatment may be based on the operational, technical, financial, legal, social, humanitarian or other criteria.

Criteria for evaluating information security risks are typically (and not limited to) financial consequences associated with:

- 1) Customer perceptions and regulatory impacts of breaches of privacy;
- 2) Operational and business impacts of unavailable information;
- 3) Business impacts of loss of confidentiality;
- 4) Operational and business impacts of loss of integrity.

The NSW Government also has a series of policies that must form part of every agency's criteria. These include:

- Expectations regarding the care and confidentiality to be given to official information (*eg, Public Service Regulations and the Crimes Act 1914*);
- The availability of official information to the public (*the Freedom of Information Act 1989*);
- Expectations about the collection, use and care of personal information (*Privacy and Personal Information Protection Act 1998*);
- Measures and procedures agencies must adopt to protect official resources from fraud and corruption;

- Expectations of providing appropriate protection to security classified information.

Each agency has to define its own descriptions and measurements as what may be disastrous for a small agency might be low or even rare for a very large agency.

An example of the criteria in determining the protection requirements is shown below. It makes reference to the classification of information as recommended in the topic [“Information Classification and Labelling”](#) under “Define the information assets” in this section.

<p><b>Very High</b></p>	<ul style="list-style-type: none"> <li>• Confidentiality of information must be guaranteed and comply with strict secrecy requirements. Information is classified as national security information, or “Highly Protected” for non-national security information.</li> <li>• Information must be correct at all times.</li> <li>• Critical decisions require constant presence of up-to-date information. Downtime is not acceptable.</li> </ul> <p>General rule is that the failure of information systems could lead to total collapse of the agency or has severe consequences to the Government, the agency, its customers, its business partners and/or members of the public. Baseline controls may not be sufficient. Additional controls will be required based on the risk analysis.</p>
<p><b>High</b></p>	<ul style="list-style-type: none"> <li>• Information is classified “Protected”.</li> <li>• Information must be correct and any errors must be detectable and avoidable.</li> <li>• Processes in critical areas must be carried out within a strict timeframe. Short periods of downtime is acceptable.</li> </ul> <p>General rule is that in the event of damage, critical areas can no longer function, resulting in a considerable harm to the Government, the agency, its customers, its business partners and/or members of the public. Baseline controls may not be sufficient. Additional controls may need to be selected based on the risk analysis.</p>
<p><b>Moderate</b></p>	<ul style="list-style-type: none"> <li>• Confidentiality of information must be guaranteed for internal use only. Information is classified “X-In-Confidence”.</li> <li>• Errors that considerably disrupt the completion of tasks must be detectable and avoidable. Minor errors can be tolerated.</li> <li>• Business activities can tolerate moderate periods of downtime.</li> </ul> <p>General rule is that the consequence of damage to the Government, the agency, its customers, its business partners and/or members of the public is limited. Baseline</p>

	controls may be sufficient.
<b>Low</b>	<ul style="list-style-type: none"> <li>• Confidentiality of information is not required.</li> <li>• Errors can be tolerated and will not disrupt the completion of tasks.</li> <li>• Downtime will have minor impact to the agency.</li> </ul> <p>General rule is that the consequence of damage is only a minor disruption to the Government, the agency, its customers, its business partners and/or members of the public. Baseline controls may be sufficient.</p>

### 5.3.5 DEFINE THE RISK ACTIVITY STRUCTURE

Depending on the nature of the risks and the scope of assessment, the structure of the risk assessment can be broken down into a set of elements. These elements should provide a logical framework for risk identification and analysis to ensure that significant risks have not been overlooked. For instance, the structure could be based on the:

- Different types of information assets as described below;
- Business processes (or organisational structure);
- Physical locations;
- Projects.

The risk activity structure should be submitted to senior management to ensure that ICT reflects the agency's priorities and that senior management endorses subsequent activities.

### 5.3.6 DEFINE THE INFORMATION ASSETS

<b>AS/NZS 7799.2:2003</b>	<b><i>A.5.1.1 An inventory of all important assets shall be drawn up and maintained.</i></b>
---------------------------	--

An asset is a component or part of a total system to which the agency directly assigns a value and therefore, requires protection. In the identification of assets, information should be considered in the wider context than just an ICT system and its associated hardware and software. Hence, it may be appropriate to structure the risk activity based on the type of assets. For example, asset types (in no particular order) can be any of the following:

- 1) Information/data (eg, files containing payment details, voice records, image files, product information, web sites);
- 2) Hardware (eg, computer, printer, scanner);
- 3) Software, including applications (eg, text processing programs, programs developed for special purposes);
- 4) Communications equipment (eg, telephones, cable, fibre);
- 5) Firmware (eg, floppy discs, CD Read Only Memories, Programmable ROMs);
- 6) Documents (eg, contracts, completed forms, manuals);

- 7) Services (eg, information services, computing resources, service providers, utilities);
- 8) Confidence and trust in services (eg, payment services);
- 9) Other equipment (eg, environmental equipment, building management systems, medical equipment);
- 10) Personnel (eg, technical, operational, marketing, legal, financial, contractors and consultants, outsourced providers);
- 11) Image and reputation of the agency.

All assets within the risk management context must be identified to an appropriate level of detail. Conversely, any assets to be excluded from the context, for whatever reason, may need to be assigned to another review to ensure that they are not forgotten or overlooked and that all major assets are accounted for.

The Inventory of Assets should include the following information:

- Asset identification;
- Asset description;
- Asset type;
- Custodian;
- Location.

#### Information Classification and Labelling

<b>AS/NZS 7799.2:2003</b>	<b><i>A.5.2.1 Classifications and associated protective controls for information shall be suited to business needs for sharing or restricting information and the business impacts associated with such needs.</i></b>
-------------------------------	--

<b>AS/NZS 7799.2:2003</b>	<b><i>A.5.2.2 A set of procedures shall be defined for information labelling and handling in accordance with the classification scheme adopted by the organization.</i></b>
-------------------------------	---

To provide a consistent basis for determining the level of protection required, information is labelled in accordance with security classification based on the criteria established by the agency.

The Commonwealth security classification system and labelling guidelines described in the Commonwealth Protective Security Manual (Part C) provides a means of categorising the confidentiality of information. NSW government agencies should adopt the same classification system and labelling guidelines.

The classifications are grouped into National and Non-national Security Information. National security information is any official resource (including equipment) that records information that “affects the security of the nation (for example, its defence or its international relations)”. Non-national security information refers to any official resource (including equipment) that “do not threaten the security of the nation but rather the security or interests of

individuals, groups, commercial entities, government business and interests, or the safety of the community.”

The recommended classifications for NSW Government Non-national Security Information are:

- [X-IN-CONFIDENCE](#) - where “X” is “Budget”, “Personnel”, “Commercial” etc. as the case may be;
- [PROTECTED](#);
- [HIGHLY PROTECTED](#).

National Security Information classifications from the Protective Security Manual are Restricted, Confidential, Secret and Top Secret. The use of these terms for non National Security Information is strongly deprecated.

It is essential that agencies respect the rule that its originator classifies information. Information received from another agency cannot have the classification changed without the permission of the originating agency.

Agencies are cautioned not to over-classify information to ensure that the costs of protection do not outweigh the consequences of not providing for its protection.

#### 5.3.7 DOCUMENTATION

This step should document the following:

- The strategic and organisational context of the agency (or parts thereof, project or system), including significant factors affecting the internal and external environment of the agency and requirements of relevant stakeholders;
- The scope and structure of the risk review;
- Information assets;
- Information and resources required for the review;
- Risk evaluation criteria.

All the above information could be included in a project plan, which should be endorsed by senior management.

#### 5.4 Step 3 – Undertake a Risk Assessment

The step combines the risk identification and risk analysis elements of the risk management process outlined in AS/NZS 4360:1999.

A variety of methods exist for the performance of a risk assessment. These range from a checklist based approach to system engineering techniques. Experience has shown that a structured workshop approach is the most efficient way of risk assessment. This requires the participation of three to eight people who are knowledgeable on the various aspects of the information asset being assessed. Whatever method is used, it must fit the agency’s culture and philosophies.

#### 5.4.1 RISK IDENTIFICATION

The component is to identify, classify and list all the risks or vulnerabilities or threats that may affect information assets identified in [Step 2](#).

It is essential that a well-structured systematic process is used to ensure a comprehensive identification of risks. This identification should include all risks whether or not they can be controlled by the agency. Potential risks not identified at this stage will be excluded from further analysis.

It is not uncommon that certain risks or vulnerabilities or threats may affect more than one of the information security concerns (integrity, confidentiality, availability, accountability, authenticity and reliability). An organisation should be aware that risks, vulnerabilities or threats are continually changing.

The focus is on the nature and source of the risk, such as:

- What could happen or go wrong?
- How could it happen?
- Why can it happen?
- Who or what can be harmed?

The aim of this component is to identify a comprehensive list of events that might affect each element of the risk structure. It examines the sources of risk from the perspective of all stakeholders, whether internal or external. Possible causes or scenarios are also considered.

#### 5.4.2 RISK ANALYSIS

Risk analysis will separate the minor acceptable risks from the major risks, and provide data for the evaluation and treatment of risks. It involves the determination of the consequences arising from an undesirable event and the likelihood of the risk occurring. The level of risk is determined by the combination of likelihood and consequence assessments in the context of existing controls.

In determining existing controls, various methods (including inspections and control self-assessment techniques) may be used to identify the effectiveness of existing management, technical mechanisms and procedures to protect the assets.

The risk analysis may be qualitative, quantitative or semi-quantitative. In most cases, a qualitative analysis is used, where explicit scales for likelihood, consequences and level of risk are determined. A semi-quantitative method can also be used by assigning numbers (usually between 0 to 1) to the qualitative scales. Where risks can be quantified, the quantitative method may be suitable. The general rule is that the method should be consistent and practical for the agency's needs. Quantitative methods lend themselves to use in probability based appraisals of return on security investment.

Examples of qualitative measures for consequence or impact, likelihood and level of risk are shown below. When assessing likelihood it is important to determine the timeframe for a possible event, for example the likelihood of an event in a 5 year period. However, different events may have different timeframes, for example if an organisation is moving premises in the next 12 months then considering many types of risk over a 5 year period is inappropriate.

### Consequence

<b>Qualitative Measure</b>	<b>Description</b>
Catastrophic	The consequences would threaten the provision of key services, causing major problems for customers, the Government and the agency. Possible loss of greater than \$10 million.
Major	The consequences would threaten the continued effective provision of services and require top level management or Ministerial intervention. Possible loss of between \$5 million and \$10 million.
Moderate	The consequences would not threaten the provision of services, but would mean the agency would be subject to review or changed ways of functioning. Possible loss of between \$1 million and \$5 million.
Minor	The consequences would threaten the efficiency or effectiveness of some services, but could be dealt with internally. Possible loss of between \$100,000 and \$1 million.
Insignificant	The consequences are dealt with by routine operations. Possible loss of less than \$100,000.

### Likelihood

<b>Qualitative Measure</b>	<b>Description</b>
Almost Certain	The event is expected to occur in most circumstances (one or more times per year).
Likely	The event will probably occur in most circumstances (once in two years).
Moderate	The event should occur at some time (once in five years).
Unlikely	The event could occur at some time (once in ten years).

Rare	The event may occur only in exceptional circumstances (once in fifty years).
------	--

Level of Risk

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	H	H	E	E	E
Likely	M	H	H	E	E
Moderate	L	M	H	E	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

E = Extreme Risk – Immediate Action Required

H = High Risk – Senior Management Attention Required

M = Moderate Risk – Management Responsibility must be Specified

L = Low Risk – Manage by Routine Procedures

There are a large variety of sources of information and data that can assist in the assessment of consequences and likelihood of risks. This may include:

- Historical records;
- Past actual experience (such as a flooding or an earthquake);
- Industry practice and experience;
- Research and studies;
- Expert and specialist judgements;
- Reference benchmarks and statistics.

Where possible, the confidence placed on the assessments should be included.

5.4.2.1 RECOMMENDED APPROACH

An analysis of information security risks could be time-consuming. One of the most effective approaches for analysing risks is the combined approach for risk identification, assessment and treatment. This involves conducting an initial [high level risk analysis](#) of the assets to identify risks that are common and for which there is an established treatment code of practice (or baseline controls) and risks that are unusual and potentially serious. For the latter type of risks, a [detailed analysis of risks](#) is conducted. This approach has the advantage of focussing attention and resources to those risks that are unusual or serious.

5.4.2.2 HIGH LEVEL RISK ANALYSIS

This component considers the business values of the information systems and the information handled, and the risks from a business point of view. The following should be considered in determining which risks require further analysis:

- The business objectives to be achieved by using an information system;
- The degree to which the agency depends on the information system, ie, whether functions that the agency considers critical to the survival or the effective conduct of business are dependent on this system, or on the confidentiality, integrity, availability, accountability, authenticity and reliability of the information processed on this system;
- The level of investment in an information system, in terms of developing, maintaining or replacing the system; and
- The assets of the information, for which the agency directly assigns value.

If the business objectives of the system are important to the conduct of the agency's business, if system replacement costs are high, or if the values of the assets are at high risk, then a detailed risk analysis is required. Any one of these conditions may be enough to justify conducting a detailed risk analysis.

The general rule is that if the lack of information security can result in significant harm or damage to an agency, its business processes or its assets, then a detailed risk analysis is necessary to identify suitable treatment options. Otherwise, a baseline approach to risk treatment provides appropriate protection.

#### Valuation of assets (and possible impacts)

To assist in the identification of risks, the value and importance of the asset need to be understood.

Each information asset or group of assets will have different requirements for protection of integrity, confidentiality and availability. The agency has to provide levels of protection commensurate to the value and importance of the assets.

The custodians and users of the assets should provide the input for the valuation of assets. Assistance could be sought from business planning, finance, information systems and other relevant activities.

Where applicable, the monetary value assigned to the asset or group of assets may be the maximum value or the total of some or all of the possible values based on, for example:

- The original, replacement and/or re-creation cost;
- Penalties and/or damages arising from violation of legislation and/or regulation;
- Potential revenue loss; and/or

- Potential loss from damage arising from disclosure, modification, destruction and/or misuse of information.

The assigned monetary value must be carefully determined as this can be used as the basis for determining the cost/benefit of protecting the asset.

For all assets, a qualitative assessment must be assigned. This could be in the scale of low → moderate → high → very high. Issues to be considered could be damages resulting from:

- Violation of legislation, regulations and/or contracts;
- Impairment of agency performance;
- Loss of goodwill or negative effect on image and reputation;
- Breach of confidentiality;
- Endangerment of personal safety;
- Adverse effects on law enforcement;
- Breach of public order;
- Financial loss;
- Disruption to services;
- Endangerment of environmental safety.

Explanation for the qualitative scale must be provided.

The dependencies of assets on other assets and the cumulative effects should also be considered. This could influence the values of the assets. For example, a seemingly less important information system may require more protection if another information system depends on its results.

The values of assets with interdependencies may be modified in the following way:

- If the values of the dependent assets (eg, data) are lower or equal to the value of the asset considered (eg, software), its value remains the same;
- If the values of the dependent assets (eg, data) are greater, then the value of the asset considered (eg, software) should be increased according to the degree of dependency or the values of the other assets.

Consideration should also be given to the existence of assets in more than one location (eg, multiple copies of software programs or the same type of PC used in most of the offices). This could reduce availability problems.

The outputs from this component are:

- A list of assets and their values relative to confidentiality, integrity, availability and replacement costs;
- A list of assets for which baseline controls or protection is sufficient;
- A list of assets for which further analysis is required.

#### 5.4.2.3 DETAILED RISK ANALYSIS

For assets that require more detailed analysis, the analysis involves a threat and vulnerability assessment.

##### Threat and vulnerability assessment

Information assets are subject to many kinds of threats. Threats can occur from a direct or indirect source. Threats can be from natural (environmental) or human causes (either accidental or deliberate). A threat may arise from within an organisation or from outside. The impact caused by the unwanted incident may be of a temporary nature or it may be permanent. Vulnerabilities of the asset may be exploited and may lead to undesirable consequences affecting the confidentiality, integrity, availability, accountability, authenticity and/or reliability of information.

Weaknesses in the physical environment, agency, procedures, personnel, management, administration, hardware, software or communications equipment, that may be exploited by a threat should be identified.

Asset custodians, users, ICT specialists, and security personnel should contribute to the threat and vulnerability assessment. Other organisations such as legal bodies and national organisations may assist, for example, by providing threat statistics. An example of threats and vulnerabilities that may be used as a starting point is contained in [Part 2 of this Guideline](#). The list is by no means comprehensive and exhaustive as threats are continually changing.

Some of the most common threats are:

- Errors and omissions;
- Fraud and theft;
- Employee sabotage;
- Loss of physical and infrastructure support;
- Malicious hacking, eg, through masquerading;
- Malicious code;
- Industrial espionage.

The likelihood of the threat occurring should be assessed for an agreed timeframe. In assessing the threat, the following should be considered:

- Source;
- Motivation, perceived capabilities and resources available;
- Geographical factors for environmental threats;
- Frequency of occurrence;
- Threat severity.

Where possible, threat statistics from reliable sources such as insurance organisations should be considered in determining the likelihood.

Examples of vulnerabilities include:

- Unprotected connections (for example to the Internet);
- Processes for identifying remote users;
- Untrained users;
- Inadequately trained ICT staff;
- Wrong selection and use of passwords;
- Ineffective access control (logical and/or physical);
- Incorrectly configured security controls;
- Known software security defects not patched;
- IT security information too widely available;
- No back-up copies of information or software;
- Location in an areas susceptible to flooding.

Some threats or vulnerabilities may affect more than one information asset. They may cause different impacts depending on which assets are affected.

The result of this component is a list of threats and vulnerabilities mapped to the information asset, the likelihood and the consequences of the threat occurring.

#### 5.4.3 RISK EVALUATION

This component involves the review of the [risk evaluation criteria](#) in [Step 1](#) with the level of risk to ensure that criteria have been identified for all significant risks and that the level of risk is consistent with the criteria.

Once the likelihood and consequences have been identified and assessed, a priority of list of the risks for further action should be produced based on the level of risk. The purpose is to identify the risks that are acceptable and those that are not.

A prioritised listing:

- Gives an overview of the general level and pattern of risk with information security;
- Focuses attention on the higher risk items;
- Helps decide where management needs to take action immediately and where the agency should develop action plans for future activities;
- Facilitates the allocation of resources to support any management action decisions.

Reasons for accepting a risk include:

- The level of risk is so low that specific treatment is not appropriate within available resources.
- No treatment is available for the risk, for example, the risk is not within the control of the agency.
- The cost of the treatment of the risk including insurance costs, (particularly for lower ranked risks), outweighs the benefit.

#### 5.4.4 DOCUMENTATION

The documentation expected from this step includes:

- A list of risks identified, including the source and cause of each risk.
- An asset profile, including the valuation and possible impacts.
- A list of threats and vulnerabilities mapped to the information assets, together with the likelihood and the consequences of the threat occurring in a stated timeframe.
- A prioritised list of risks for determining risk acceptability.

#### 5.5 Step 4 – Manage the Risk

Organisations must manage risks and safeguard their operations to protect effectively information. Part of the process of judging whether the security of information is appropriate is by acknowledging that risks cannot be avoided completely and there will always be some residual risk.

Management would need to treat the risks that have been identified as unacceptable in order that those risks become acceptable. Constraints that may influence how to manage a risk include:

- Organisational;
- Financial;
- Personnel;
- Time;
- Legal;
- Technical.

Risk treatment may include a combination of the following:

- Risk avoidance – by deciding by not going ahead with an activity likely to generate risk;
- Reduce the likelihood – by implementing controls to reduce the threats and vulnerabilities;
- Reduce the consequences – by implementing controls to reduce the threats and vulnerabilities or by modifying the assets at risk in some way;
- Risk transference – by arranging another party to bear the whole or part of the risk, eg, insurers;
- Risk acceptance – the agency bears all the risk.

Key questions in treating risks are:

- What processes, protection controls and safeguards exist, or are needed to reduce risk to an acceptable level?
- Are the processes, protection controls and safeguards the most cost effective – do they match the value of the asset or the adverse consequences that will follow if the risk occurs?
- What resources are needed (people, funds, equipment)?
- Who has responsibility and accountability for treating and managing the risk?

Before undertaking the treatment there should be the selection of the appropriate controls taking into account the agency's overall strategic and operational objectives and priorities with the resources and funds available. It is unlikely that any one of the above mentioned risk treatment options by itself will provide the complete solution for a particular risk issue.

#### 5.5.1 DOCUMENTATION

The output from this step is a list of treatment options for the unacceptable risks identified in [Step 3](#). The Policy created in [Step 1](#) should also be reviewed and modified or enhanced as necessary to guide the selection of controls and add any matters that are best handled as Policy.

Residual (acceptable) risks must also be documented, some may become controlled because many controls can be broad spectrum, but residual risks must be approved, [Step 7](#).

#### 5.6 Step 5 – Select Controls

Appropriate controls to either reduce the assessed risks to an acceptable level should be identified and selected with cost/benefit justification.

Already existing and planned controls should be taken into account in the selection to avoid unnecessary duplication of controls. A check should be made to ensure that existing controls are working effectively. It is also possible that an existing or planned control may no longer be justified and may need to be removed, replaced by a more suitable control, or remain due to cost reasons. The vulnerabilities to the associated threat indicate where additional controls may be required and the form it should take.

In considering controls to be selected, it is beneficial to identify the function of the control in terms of protection, deterrence, detection, response and recovery. Many protective controls can serve multiple functions. Often it is more cost effective to select protective controls that can serve multiple functions. A well designed security regime provides 'defence in depth' by using controls that provide a mixture of these functions. These functions are briefly described below:

- Deter:**        **Avoid or prevent the occurrence of an undesirable event**
- Protect:**    **Safeguard the information assets from adverse events**
- Detect:**     **Identify the occurrence of an undesirable event**
- Respond:**   **React to or counter the adverse event**
- Recover:**    **Restore the integrity, availability and confidentiality of information assets to their expected state**

Areas where controls can be used include:

- Security policy;

- Security organisation;
- Personnel;
- Physical and environment;
- Communication and operations management;
- Access control;
- Systems development and maintenance;
- Business continuity management;
- Compliance.

Controls are selected in the context of the risks to provide security functionality and assurance.

#### 5.6.1 BASELINE APPROACH

A baseline (code of practice) approach to risk treatment requires the establishment of a minimum set of controls to safeguard all or some of the agency's information against the most common threats. These baseline controls are compared with existing or planned safeguards for the context being considered. Those that are not in place, and are applicable, should be implemented. An early step in the baseline approach may be a gap analysis of existing controls against a baseline.

The risk in the baseline approach is that there may be unidentified assets, 'non-standard' threats or vulnerabilities that is missed by gap analysis and/or baseline controls. Lack of an Information Security Policy exacerbates this risk.

The level of baseline security can be adjusted to suit the needs of the agency. A set of baseline controls can be found in [Part 3 of this Guideline](#).

This approach reduces the investment that an agency has to make in the performance of risk reviews.

#### 5.6.2 OPERATIONAL AND TECHNICAL CONTROLS

Control selection should always include a balance of operational (non-technical) and technical controls. Operational controls include physical, personnel, and administrative or procedural security controls. Examples of these controls include:

##### 5.6.2.1 PHYSICAL SECURITY

Physical security controls include building access and design, key coded door locks, fire suppression systems, and guards.

##### 5.6.2.2 PERSONNEL SECURITY

Personnel security covers personnel recruitment checks, (especially people in 'positions of trust'), staff monitoring, and information security awareness programs.

#### 5.6.2.3 PROCEDURAL SECURITY

Procedural security may include operating procedures documentation, application development and acceptance procedures as well as procedures for incident handling. It may include change management procedures. It also encompasses procedures for the continuity of business, including contingency planning / disaster recovery strategies and plan(s) as well as crisis management.

#### 5.6.2.4 TECHNICAL SECURITY

Technical security encompasses hardware and software security as well as communications controls. This may include: identification and authentication, logical access control requirements, audit trail/security logging needs, dial-back security, message authentication, encryption and digital signatures, network firewalls, network monitoring and analysis, anti virus software.

#### 5.6.2.5 EVALUATED PRODUCTS AND SYSTEMS

An organisation may acquire products or systems that have been examined or evaluated, by an independent specialist, as part of their solution. The evaluation should be against an appropriate protection profile for the system or product and the threats to it. Evaluated products or systems provide the agency the confidence that an implemented set of functionality meets requirements and the implementation of that functionality is correct and complete. Focused pragmatic security testing could also be performed to confirm the level of assurance of security provided. The Common Criteria are the preferred basis for evaluation, however, the protection profile and hence evaluation assurance level must be appropriate to the agency's risks.

#### 5.6.3 FACTORS INFLUENCING CONTROL SELECTION

Factors for consideration when selecting controls for implementation include:

- Ease of use of the protective controls and safeguards;
- Transparency to the user;
- Proximity of the control to the asset being protected;
- The help provided to the users to perform their activities;
- Cost of the control;
- Compatibility with existing controls;
- The relative strength of the controls,;
- Protection profile and evaluation assurance level;
- The types of functions performed – protection, deterrence, detection, response, recovery.

#### 5.6.4 SECURITY ARCHITECTURE

Another consideration for control selection is the security architecture that describes how the security requirements are to be achieved.

A security architecture can be used when new systems are being developed and when major changes are made to existing systems. Based on the results of the risk analysis or baseline approach, the requirements for security are refined into a set of technical security services for the system. Some of the requirements, particularly when changes are being made to existing systems, may be in the form of specific controls to be used.

A security architecture normally consist of one or more security domains. A security domain refers to an area of the same or similar security requirements and controls, for example, payroll, finance, e-mail services, etc. A security problem in a unique security domain must not be permitted to adversely impact the security of another security domain. Security domains may have their own protection profiles.

Issues to be considered when constructing a security architecture include:

- Interrelationships and interdependencies between unique security domains;
- Impacts or implications of interrelationships and interdependencies weakening security services;
- Extra services or precautions required to correct, control or counter any weakness.

A security architecture should aim to adversely impact users as little as possible while ensuring that the environment has the optimum protection in place.

A number of other documents that are related to the security architecture or are dependent on it, include the:

- Security design;
- Security operational concept;
- Security plan;
- Security policy;
- Certification and accreditation documentation, if required.

#### 5.6.5 CONSTRAINTS THAT AFFECT THE SELECTION OF CONTROLS

There are many constraints that can affect the selection of controls. These constraints must be taken into account when making recommendations and during the implementation.

##### 5.6.5.1 TIME CONSTRAINTS

Many types of time constraints may exist. For example:

- Controls should be implemented within a time period that is acceptable to management.
- Whether controls can be implemented within the lifetime of the system.

- The period of time management decides is an acceptable period to leave information exposed to a particular risk.

#### 5.6.5.2 FINANCIAL CONSTRAINTS

Organisations have many conflicting demands on the limited financial resources available. For example, funds may not be available to fully implement a proposed control and management is prepared to accept a partial implementation and carry the residual risk until such time as additional funds become available.

#### 5.6.5.3 TECHNICAL CONSTRAINTS

Technical problems, like the compatibility of programs or hardware, can easily be avoided if such issues are taken into account during the selection of controls. Also, the retrospective implementation of controls to an existing information system is often hindered by technical constraints.

#### 5.6.5.4 SOCIOLOGICAL CONSTRAINTS

Sociological constraints to the selection of controls may be specific department or branch within an agency. They cannot be ignored because many technical and operational controls rely on the active support of the staff. If the staff do not understand the need for the control or do not find it culturally acceptable, It is likely that the control will become ineffective over time.

#### 5.6.5.5 ENVIRONMENTAL CONSTRAINTS

Environmental factors may influence the selection of controls, like space availability, extreme climate conditions, etc.

#### 5.6.5.6 LEGAL CONSTRAINTS

Legal factors such as the Privacy and Personal Information Protection Act provisions for information processing could affect the selection of controls. Non-ICT specific laws and regulations like fire regulations, work relations laws, codes of conduct, occupational health and safety regulations etc. could also affect control selection.

#### 5.6.5.7 PEOPLE AND SKILL CONSTRAINTS

Some controls may require availability of specialist skills to implement or operate them. Controls may not be performed correctly if people with the necessary skills and competencies are not available.

#### 5.6.6 DOCUMENTATION - INFORMATION SECURITY PLAN

The result of this step is an information security plan, based on the information security policy and the results of the risk review. It should ensure that the controls are implemented in time in accordance with the priorities established, and in line with the description of how to implement the controls

and how to reach the appropriate security level. It should also include a schedule for follow-up procedures to maintain the security level. The base plan would normally apply to an entire agency or there may be separate but consistent plans for major discrete elements of an agency.

The information security plan is a document setting out the actions to be undertaken to implement the required controls. This plan should contain the results of the risk analysis, the actions to be undertaken within short, medium and long timeframes to achieve and maintain the appropriate security level, the costs, and an implementation schedule. It should include:

- The security objectives in terms of confidentiality, integrity, availability, accountability, authenticity and reliability of information;
- The risk analysis approach;
- A protection profile to enable selection of evaluated products and any system security evaluations;
- An assessment of the residual risks accepted after implementing the controls identified;
- A list of the selected controls to be implemented, and a list of existing and planned controls including a determination of their effectiveness and the safeguard upgrades needed; this list should include priorities for the implementation of the selected controls and the upgrading of existing controls, and how these controls should work in practice;
- The estimation of the installation and running costs for these controls;
- The estimation of personnel resources for the implementation of these controls, and for follow-up actions;
- A detailed workplace for the implementation, containing:
  - priorities;
  - an implementation schedule in relation to priorities;
  - the budget needed;
  - responsibilities;
- The security awareness and training procedures for staff and end users which is needed to ensure the effectiveness of the controls;
- A schedule for approval process to take place where needed;
- A schedule for follow-up procedures.

Moreover, the information security plan should describe the facilities to control the process of correct implementation of controls, like:

- The definition of progress reporting procedures;
- Procedures to identify possible difficulties, an;
- Procedures to validate each of the points listed above, including procedures related to the possible modification of single parts or the plan itself, when needed.

Projects for significant new systems will usually require their own Security Plan. Such plans will need to address system specific matters as well as security aspects of integrating the new system with existing systems and security measures.

[Attachment 2](#) provides a template for an Information Security Plan.

#### 5.7 Step 6 – Prepare Statement of Applicability

The Statement of Applicability (SoA) documents the control objectives and controls for each risk where treatment is considered necessary. The decision to select (or reject) particular controls should be recorded and explained. In some cases this explanation can be very brief, but in other cases where the choice is complex or has a significant impact on risks more detail will be necessary. The SoA may refer to other documents such as security reviews and internal or external audit reports where specific recommendations for action have been made. Most importantly the SoA must record reasons why any of the controls specified in AS/NZS 7799.2 have not been implemented.

The SoA should be signed off by the person(s) accountable for the security domain(s) covered by it.

#### 5.8 Step 7 – Management Approval

The final step in the planning phase is to obtain management approval for the residual risks and for a program to develop and implement a risk treatment plan. Budgetary cycles may require that an initial risk treatment plan is developed and costed at this Step.

#### 5.9 Importance of Documentation

Documenting each step of the information risk management process is imperative for the following reasons:

- To demonstrate that the process has been carried out correctly;
- To provide evidence of decisions and processes made;
- To provide an accountability mechanism;
- To facilitate continuing monitoring and review;
- To provide an audit trail;
- To share and communicate information.

The level of documentation required will depend on legislative requirements, costs and benefits, taking into account the above factors. The agency should take the best practical approach that is appropriate to its circumstances.

As in any documented system, the agency should establish and maintain procedures for controlling all documentation and assign responsibilities to ensure that:

- Documentation is readily available;
- It is periodically reviewed and updated as necessary to ensure that it is current;
- Version control is applied to documentation and all documents include the date of effect and the name of the accountable person;

- Obsolete documentation is promptly withdrawn, identified and retained if necessary for legal or knowledge preservation purposes, or both.

The agency should also establish and maintain procedures for the identification, maintenance, retention and disposal of records showing evidence of compliance with the requirements of the ISMS.

All documentation and records should be legible, identifiable, dated and traceable to the activity involved. They should be stored and maintained in such a manner that they are readily retrievable and protected against damage, deterioration and loss. Documentation relating to the operation of security controls should be distributed on a “need-to-know” basis.

## 6. Implementation and Operational Procedures

### 6.1 Implementation of Risk Treatment Plan

A Risk Treatment Plan is produced from the information and documents created during the planning phase (previous sections). The correct implementation of controls relies heavily upon a well-structured and documented risk treatment plan. When the risk treatment plan is completed, approval by senior management of all controls may be required before the plan can be implemented.

The main elements of the Risk Treatment Plan are:

- Organisational and resource matters including priorities;
- Measures to achieve identified control objectives;
- Security training.

Day to day management of the ISMS operations and resources are also required, with particular attention to security incidents.

### 6.2 Implementation of Controls

A senior manager should be given responsibility for the implementation of the plan. This manager must ensure that the priorities and the schedule(s) outlined in the plan are followed.

Much of the plan documentation, particularly on threats, vulnerabilities and risks, can be very sensitive and must be protected against unauthorised disclosure.

### 6.3 Information Security Training

<b>AS/NZS 7799.2:2003</b>	<b>A.6.2.1 All employees of the organization and, where relevant, third party users, shall receive appropriate training and regular updates in organizational policies and procedures.</b>
---------------------------	--

The objective of the information security training program is to increase the level of awareness and skills within the agency. The program should ensure that all people in the agency have appropriate knowledge of the information systems, and that they understand why controls are necessary and are able to use them correctly.

The input to the information security awareness program should come from all levels and areas of an agency. Management support from all departments is necessary for the training and awareness team.

In detail, the following topics should be covered in the security awareness program:

- The explanation of the importance of security to both the agency and the individual;
- The security needs and objectives for the information systems in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability;

- The implication of security incidents to both the agency and the individual;
- The correct use of the agency's information;
- The objectives behind, and an explanation of, the corporate information security policy, any security guidelines and directives, and the risk management strategy, leading into an understanding of risks and safeguards;
- The necessary protection for and the risks to information systems;
- Restricted access to areas (authorised personnel, door locks, badges, entrance log) and to information (logical access control, read/update rights), and why these restrictions are necessary;
- The need to report breaches of security or attempts;
- Procedures, responsibilities and job descriptions;
- The consequences if staff are responsible for security breaches;
- Procedures related to security compliance checking;
- Change and configuration management.

The development of the security training and awareness program starts with the agency's information security strategies, objectives and policies.

In addition to the information security awareness program, which should apply to everybody within an agency, specific security training is required for those personnel with direct tasks and responsibilities related to information security.

When determining personnel for whom specific information security training and awareness is necessary, the following groups should be considered:

- Personnel with key responsibilities for information, including management and operations;
- Personnel with information security administration responsibilities, eg, for access control or directory management or manual records management.

The information security training program should emphasise the need for balance between non-technical and technical controls. Examples of control-related topics that could be covered include:

- Information security infrastructure,
  - roles and responsibilities;
  - information security policy;
  - regular security compliance checking;
  - security incident handling,
- Physical security;
  - Buildings;
  - office areas, equipment rooms;
  - equipment;
- Personnel security;
- Media security;
- Hardware/software security;
  - identification and authentication;
  - logical access control;
  - accounting and security audit;

- actual storage clearance;
- Communications security;
  - network infrastructure;
  - bridges, routers, gateways, firewalls,
  - Internet and other external connections;
- Business continuity, including contingency planning/disaster recovery, strategy and plan(s).

## 7. Follow up Procedures

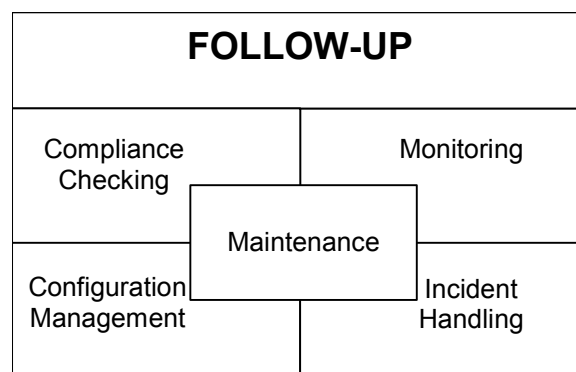
### 7.1 Follow-Up

Implemented controls can only work effectively if they are checked, used correctly and any changes or breaches are detected and dealt with promptly.

Over time there is a danger or tendency for the performance of the information security plan to deteriorate if there is no follow up or monitoring.

The management of information security is an ongoing process that continues after the implementation of the information security plan. All aspects of it should be audited.

Figure 7 shows the activities involved in this step.



**Figure 7: Follow-up procedures**

#### Maintenance

Most controls will require maintenance and administrative support to ensure that they continue to function correctly and meet evolving business needs. The cost of maintenance and administration of the controls should have been considered when selecting the relevant controls. This is because costs can vary greatly from one control to another.

Maintenance activities include:

- The checking of log files;
- Modifying configuration and parameters to reflect changes and additions;
- Re-initiation of seed values or counters;
- Updating with new versions.

All modifications will require changes to documentation, which must be under formal configuration management.

### 7.2 Compliance Checking

Compliance checking is the review and analysis of the implemented controls. It is used to check whether information systems or services conform to the security

requirements documented in the information security policy and information security plan including the documented configuration of individual hardware and software items. Compliance checks may be used to check the conformance of:

- New information systems and services after they have been implemented;
- Existing information systems or services after elapsed periods of time have occurred (eg, annually);
- Existing information systems and services when changes to the information system security policy have been made, to see which adjustments are necessary to maintain the required security level.

The controls protecting the information system may be checked by:

- Conducting periodic inspections and tests;
- Monitoring operational performance against actual incidents occurring;
- Conducting spot checks to check the status of security levels and objectives in particular areas of sensitivity or concern.

Compliance checking should be based on the agreed controls lists from the risk analysis results on the information system security policy, as well as security operating procedures which the senior management have approved, including incident reporting. The objectives are to ascertain whether controls are implemented and used correctly.

### 7.3 Configuration Management

Information systems and the environment in which they operate are constantly changing. Changes can result in new threats and vulnerabilities.

Changes to information systems may include:

- New procedures;
- New features;
- Updates;
- Equipment changes;
- New users to include external groups or anonymous groups;
- Additional networking and interconnection.

When a change to an information system occurs or is planned it should be managed within the configuration management process. It is important to determine what impact the change will have on the security of the system. For major changes that involve the purchase of new hardware, software or service, an analysis may be necessary to determine the new security requirements. On the other hand, many changes made to systems are minor in nature and may not require extensive analysis. The costs and benefits of any change should be considered.

### 7.4 Monitoring

An essential element in meeting the security objective is to measure, on a routine basis, adherence to the security policy. Monitoring is an important part of the maintenance of information security.

The management technique for controlling day to day monitoring is to establish and document security operating procedures for the necessary activities. This document should describe all the actions required to ensure that the level of security for all systems and services is maintained. For example, administrative procedures should be established to ensure that attempted and real breaches are investigated on a timely basis, and, where appropriate, that:

- Disciplinary or corrective action is taken promptly;
- Conditions leading to the breach are rectified.

Some of these breaches may lead to a reassessment of the security measures and procedures. If necessary, this may result in a change or refinement to the level of security.

For example, the agency's security violation reports may indicate shortcomings in the existing security measures, practices and procedures. Or, for example, the periodic test of a Business Recovery Plan, taking into account the security architecture, may reveal inadequacies or excessive delays in the recovery and resumption of processing.

In any event, the effectiveness of the security of information systems must be reviewed on a periodic basis to ensure that the security objective and agency specific policies are being met. Should an agency's responsibilities, for example, be expanded or modified, the relative importance of the information held would require reassessment. Further, if an agency is restructured, the responsibility for information security may require reassessment.

It is important that the design and implementation of measures, practices and procedures for the security of information systems, should be undertaken, to the extent possible, concurrently with the implementation of new information systems. Retroactive implementation of security, once the system is operational, is not only difficult and expensive but may not be as effective.

## 7.5 Incident Handling

No information security system works perfectly all the time. Sometimes there are positive and negative events. It is necessary to document those events and undertake any analysis to determine the impact and what changes or corrective actions may be necessary.

The purpose of the incident analysis is to:

- Improve risk analysis and management reviews;
- Assist in the prevention of incidents;
- Raise the level of awareness of information security related issues; and
- Provide 'alert' information for use by such as computer emergency response teams.

Related to these, other key aspects that should be considered, include:

- Use of a standard system for classifying security incidents, see [Attachment C](#)
- The establishment of pre-determined plans for the handling of Unwanted incidents when they occur, whether caused by external or internal factors;
- The training of nominated personnel in incident investigation, for instance to form computer emergency response teams.

The pre-determined plans may encompass:

- Preparation - pre-documented preventive measures, incident handling guidelines and procedures, documentation required, and business continuity plans;
- Notification - the procedures, means and responsibilities for reporting incidents, and to whom;
- Assessment - the procedures and responsibilities for investigating incidents and determining their seriousness;
- Management - the procedures and responsibilities for dealing with, limiting the damage from, and eradicating incidents, and notifying higher management;
- Recovery - the procedures and responsibilities for re-establishment of normal service;
- Review - the procedures and responsibilities for post-incident actions, including investigation of legal implications and trend analysis.

## 8. Legislation and Relevant Documents

This list is not complete and refers to only the more important legislation. Agencies should refer to the particular legislation and supporting procedural documents that may relate directly to their operations.

### 8.1 Legislation

#### 8.1.1 NSW

Crimes Act 1900 and Regulations  
Electronic Transactions Act 2000  
Evidence Act 1995 and Regulations  
Freedom of Information Act 1989 and Regulations  
Occupational Health and Safety Act 1983 and Regulations  
Public Sector Management Act 1988 and Regulations  
Public Finance and Audit Act 1983 and Regulations  
Privacy and Personal Information Protection Act 1998  
State Records Act 1998 and Regulations  
Codes of Conduct / Ethics

#### 8.1.2 COMMONWEALTH

Crimes Act 1989 and Regulations  
The Evidence Act 1985 and Regulations  
Income Tax Assessment Act and Regulations  
Social Security Act 1991 and Regulations

Laws prohibiting attacks against aspects of the National Information Infrastructure (NII) include:

- *Crimes Act 1901 Part VIA* dealing with attacks against Commonwealth computers and attacks against any computer by using the Australian telecommunications system (or, more accurately, attacks by the use of 'a facility operated or provided by the Commonwealth or a carrier...');
- *Telecommunications (Interception) Act 1979* prohibiting the interception of telecommunications (including data transmissions) within Australia except under warrant;
- *Crimes Act 1901 s. 70* dealing with disclosure of official information;
- *Crimes Act 1901 Parts II and VII* dealing with national security offences such as treason and espionage;
- State legislation dealing with particular aspects of the information infrastructure or of more general application;
- Common law of civil liability for damage to property.

## 8.2 Relevant Documents

### 8.2.1 NSW

Fraud Control Plans Policy Statement for NSW Government Procurement

Code of Practice for NSW Government Procurement

Code of Tendering for NSW Government Procurement

ICAC Reference Materials

Office of Information Technology Information Management Guidelines on:

- Information Management Framework;
- Information Audit;
- Information Classification;
- Information Inventory.

### 8.2.2 COMMONWEALTH

Commonwealth Protective Security Manual

Australian Communications-Electronic Security Instruction 33 (ACSI-33)-  
Security Guideline for Australian Government ICT Systems, Defence Signals  
Directorate, December 2000.

# APPENDIX 1– Sample Information Security Policy

This sample Information Security Policy statement is provided to guide agencies in developing or reviewing their own policies. It is general in nature and by no means definitive. Each agency must assess whether the content and style is relevant to its own environment and unique business requirements. The sample policy statement follows.

(AGENCY NAME)

## INFORMATION SECURITY POLICY

### Introduction

Information is the basis on which *(Agency Name)* conduct its business. As the custodian of a large volume of information that is either commercially, personally or politically sensitive, *(Agency Name)* have a fundamental responsibility to protect that information from unauthorised or accidental modification, loss, release or impact on the safety and well-being of individuals. Furthermore trustworthy information must be available to undertake *(Agency Name)* day to day business.

Specifically, information plays a vital role in supporting business processes and customer services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. Accordingly, information must be protected to a level commensurate with their value to the organisation.

### Goal

The goal of information security is to protect *(Agency Name)* from adverse impact on its reputation and operations that could result from failures of:

- **Confidentiality** - in the context of access or disclosure of the information without authority;
- **Integrity** - in the context of completeness, accuracy and resistance to unauthorised modification or destruction;
- **Availability** - in the context of continuity and the business processes and for recoverability in the event of a disruption.

### Objectives

The objectives of this policy are to:

- Ensure the continuity of *(Agency Name)* and its services to its customers and business partners;

- Minimise the possibility of a threat to information security causing loss or damage to *(Agency Name)*, the Government, its customers and business partners;
- Minimise the extent of loss or damage from a security breach or exposure;
- Ensure that adequate resources are applied to implement an effective information security program;
- Identify the essential measures of the information security program;
- Inform all *(Agency Name)* personnel, other government agencies, customers and business partners who have access to *(Agency Name)* information of their responsibilities and obligations with respect to security;
- Ensure that the principles of information security are consistently and effectively applied during the planning and development of the *(Agency Name)* activities.

## Scope

This policy applies to:

- All users of *(Agency Name)* information, including service providers of *(Agency Name)*;
- All information assets encompassing facilities, data, software, paper documents and personnel.

**Facilities** includes all equipment, as well as the physical and environmental infrastructure:

- Computer processors of all sizes, whether general or special purpose, and including personal computers;
- Peripheral, workstation and terminal equipment;
- Telecommunications and data communications cabling and equipment;
- Local and wide area network equipment;
- Environmental control systems, including air-conditioning and other cooling equipment;
- Alarms, and safety equipment;
- Required utility services, including electricity, gas and water;
- Buildings and building improvements accommodating personnel and equipment.

**Data** includes both raw and processed data:

- Electronic data files, regardless of their storage media and including hard copies and data otherwise in transit;
- Information derived from processed data, regardless of the storage or presentation media.

**Software** includes locally developed programs and those acquired from external sources:

- Operating system software and associated utility and support programs;

- Application enabling software, including data base management, telecommunications and networking software;
- Application software.

**Paper documents** includes systems documentation, user manuals, continuity plans, contracts, guidelines and procedures.

**Personnel** includes employees, contractors, consultants, service providers, representatives of customers and other bodies that access the agency's information and data.

## **Approach**

(*Agency Name*) adopts a proactive approach to information security management and uses the standards on information security management (AS/NZS 17799 and 7799) and risk management (AS/NZS 4360) as the framework.

Applying risk management techniques, information assets shall be evaluated for the purpose of determining their individual value to (*Agency Name*) and for the selection of appropriate protection measures. The evaluation shall take into consideration the relevant legal and statutory compliance requirements.

## **Obligations**

The guiding principle is that controls in place shall be effective as measured against security standards and compliance requirements that are of particular relevance to (*Agency Name*). These controls shall focus on the requirements outlined herein.

### **Authenticity**

Users of information assets shall be uniquely identified to the information being accessed.

### **Integrity**

There shall be adequate protective controls / safeguards to ensure completeness and accuracy during the capture, storage, processing and presentation of information.

### **Confidentiality**

There shall be adequate protective controls / safeguards to ensure that information is disclosed only to authorised users.

### **Availability**

There shall be adequate protective controls / safeguards to ensure that information can be delivered to the (*Agency Name*) activities when required.

### **Reliability**

There shall be adequate protective controls / safeguards to ensure that information available is complete and accurate.

### **Accountability**

There shall be adequate protective controls / safeguards to ensure that responsibility for information undertaken by providers and users of information.

### **Conduct**

Information assets owned, leased or rented by (*Agency Name*) shall be solely for the conduct of (*Agency Name*) business; no private use, or use for any other purpose shall be permitted.

### **Education and Training**

(*Agency Name*) recognise the importance of security education and the need for training and continuing education programs for all (*Agency Name*) personnel, customers and business partners.

## **Responsibilities**

The ***Manager responsible for Information Security*** (nominally the CIO,) will co-ordinate the development of guidelines and procedures for the implementation of this policy, and will be responsible for an on-going review of their effectiveness. The Manager must ensure that all personnel are fully informed of their obligations and responsibilities with respect to these guidelines and procedures.

***All personnel***, whether employees, contractors, consultants or visitors, are required to comply with the information security guidelines, procedures and mechanisms and to play an active role in protecting the information assets of the organisation. They must not access or operate these assets without authority and must report security breaches or exposures coming to their attention to the Manager responsible for Information Security.

***Managers*** have a responsibility as custodians of the data and other Information assets that support the business activities performed under their supervision to ensure that those assets are adequately secured. They must also ensure that the appropriate information security guidelines, procedures and mechanisms are observed in the performance of these activities.

The ***Information Security Administrator*** is responsible for the day-to-day administration of the information security procedures and practices. This person reports directly to the ***Manager responsible for Information Security*** on the performance of the information security procedures and practices.

## **Monitoring and Review**

Compliance with the Policy will be monitored on a regular basis. Security logs and audit trails will be produced to monitor the activities of users in their usage of information assets.

This policy, with its supporting guidelines and procedures, will be reviewed on at least an annual basis to ensure completeness, effectiveness and useability.

## **Sanctions**

Deliberate breach of circumvention of the principles of this policy, or of the guidelines and procedures that implement it, will lead to the appropriate disciplinary action.

*(Signed)*

**Chief Executive Officer**

*(Dated)*

# APPENDIX 2 - Information Security Plan Template

The sample template is intended as a guide only. As a general rule, the level of detail in the plan should be consistent with the value and importance of the information to the agency's corporate goals. The security plan should fully identify and describe the controls currently in place or planned.

**(AGENCY NAME)**

## INFORMATION SECURITY PLAN

### INFORMATION ASSET IDENTIFICATION

Date:

#### Information Asset Name/Title

- Unique Identifier and Name Given to the Information Asset.

#### Responsible Organisation

- List organisation responsible for the Information Asset.

#### Information Contact(s)

- Name of person(s) knowledgeable about, or the custodian of, the Information Asset.

Name  
Title  
Address  
Phone

#### Assignment of Security Responsibility

- Name of person responsible for security of the Information Asset.

Name  
Title  
Address

## OVERVIEW OF THE INFORMATION ASSET

### General Description / Purpose

- Describe the function or purpose of the information asset;
- Describe the processing flow of the information from input to output;
- List user organisations (internal and external) and type of data and processing provided;
- If applicable, describe the hardware / software configuration required for the information asset;
- If applicable, describe the interrelationship of this information asset to other information assets.

### Information Security Requirements

- Describe, in general terms, the information security requirements in terms of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **Very High, High, Moderate, or Low**;
- List any laws or regulations that specifically affect the confidentiality, integrity, availability, accountability, authenticity, and reliability of the information asset.

## RISK ASSESSMENT OVERVIEW

### Risk Assessment Methodology

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

### Review of Security Controls

- List any independent security reviews conducted on the information asset in the last three years.

### Threats and Vulnerabilities

- Summarise the threats and vulnerabilities identified and the consequences arising from these.

## Value of Assets

- Briefly summarise the value of the asset or the component of the asset, if applicable, and the basis for the valuation.

## Level of Protection Required

- Briefly state the level of protection required including a Protection Profile if security products or system evaluation is required;
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorised access to or modification of information in the system.

## Acceptable Level of Risk

- Briefly state the assessment of the residual risks accepted after implementing the controls identified.

## RISK TREATMENT

- Provide a high level matrix of the controls mapped to the threats identified;
- Describe the controls implemented or planned for the information asset, covering the following areas (refer [Part 3 of this Guideline](#)):

### ORGANISATIONAL AND MANAGEMENT CONTROLS

Information Security Policy  
Information Security Infrastructure  
Authorisation Process for Information Processing Facilities  
Security of Third Party Access  
Outsourcing  
Mobile Computing  
Teleworking  
Asset Classification and Control  
Personnel Practices  
Security Awareness and Training  
Compliance with Legal and Regulatory Requirements  
Compliance with Security Policies and Standards  
Incident Handling  
Disciplinary Process  
Business Continuity Management  
System Audits

### PHYSICAL AND ENVIRONMENTAL CONTROLS

Secure Areas  
Equipment Security  
Clear Desk and Screen Policy

Securing Unattended User Hardware  
Authorised Removal of Property

### **OPERATIONAL CONTROLS**

Documented Operating Procedures  
Network Management  
Configuration and Change Management  
Incident Management  
Segregation of Development and Operational Environments  
Capacity Planning  
System Acceptance  
Protection Against Malicious Code  
Back-up of Information  
Logging Events and Faults  
Software and Information Exchange  
Electronic Commerce Security  
Security of Electronic Mail  
Security of Electronic Office Systems  
Security of Electronically Published Information  
Media Handling and Security

### **TECHNICAL CONTROLS**

User Identification and Authentication  
Access Control Policy  
User Access Management  
Review of Access Rights  
Network Access Controls  
Operating System Access Control  
Application Access Control  
Monitoring System Access and Use

### **SYSTEMS DEVELOPMENT AND MAINTENANCE CONTROLS**

Specification of Security Requirements  
Application Controls  
Cryptography  
Restrictions to Software Package Modifications

## APPENDIX 3 – Standard Classification of Security Incidents

Security incidents are to be classified according to:

- The type of incident, there are 8 of these;
- The status of the incident when it is reported
- The causes of the incident

### TYPES OF SECURITY INCIDENT

#### 1) Access to data or a system without authorisation

Such attempts may include:

- unauthorised use of an account (privileged or otherwise);
- unauthorised access to directories, files or media;
- placement of 'sniffing' hardware or software on network segment to capture data travelling across it;
- abuse of trust relationships (eg, inter-domain trust) to access data.

#### 2) Modification of data without authorisation

Such attempts may include:

- placement of files:
  - new data;
  - trojan horse or virus code.
- deletion of data
- modification of data:
  - change of file permissions;
  - web page defacement;
  - alteration of file content.

#### 3) Denial of service or disruption to system activity

Such incidents include:

- distributed denial of service attack (DDoS) causing loss of external network connections through packet flooding;
- exploitation of vulnerabilities causing network outage;
- causing system to crash;
- causing system to lose connectivity;
- causing system to partially or completely fail;
- physical loss or damage to systems.

#### 4) Changes to system software/firmware, hardware or environment without approval

Such incidents include:

- installation of back door code without authorisation (including violations by system developers);
- modification of system code without authorisation;

- modification to cabling (patching, rack connections etc.);
- addition of software/hardware with malicious intent (eg, keystroke logging or backdoor);
- unauthorised removal, addition or replacement of equipment.

## **5) Use of systems for processing or storage of data without authorisation**

Such incidents include:

- use of systems to perform unauthorised work;
- use of systems to perpetrate attacks on third parties (eg, Denial of Service);
- use of systems to store unauthorised data (eg, private files, sound or movie files, illegal copies of software).

## **6) Probe**

Attempts to gain information that may be used to perpetrate an attack, including:

- automated scans;
- ping/portscan;
- traceroute;
- targeted scans across whole, or large part of, IP range;
- social engineering;
- unexpected inquiries into network capabilities/vulnerabilities;
- unauthorised password resets.

## **7) Physical damage or loss**

Rendering systems or data unavailable due to:

- theft;
- vandalism;
- fire;
- flood;
- damage.

## **8) Violation of an implicit or explicit security policy**

As identified by the agency relative to its own security policies or procedures.

## **STATUS OF THE INCIDENT**

Incidents should be classified as:

- ongoing/continuing in real time;
- suspected;
- unsuccessful;
- successful;

They should then be identified as:

- accidental;
- deliberate.

## **CAUSES OF THE INCIDENT**

Incidents may be caused by:

- employees;
  - permanent;
  - casual/contractor;
- outside entity;
- natural disaster.

## APPENDIX 4 – Glossary of Useful Terms

In addition to definitions at page 8.

<b>Access Control</b>	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
<b>Access Control List</b>	A list of entities, together with their access rights, which are authorised to have access to a resource.
<b>Accountability</b>	The property that ensures that the actions of an entity may be traced uniquely to the entity.
<b>Assurance</b>	Confidence that an entity meets its security objectives.
<b>Asymmetric Authentication Method</b>	A method of authentication, in which not all authentication information is shared by both entities.
<b>Asymmetric Cryptographic Technique</b>	A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.
<b>Asymmetric Key Pair</b>	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.
<b>Asynchronous</b>	A form of electronic information transmission in which consecutive characters can be separated by variable time intervals
<b>Attacker</b>	A person who attempts to penetrate a computer system's security controls.
<b>Audit</b>	Audit is defined as an independent review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
<b>Audit Event</b>	An action, detected internally by the system which may generate an audit record. If an event causes an audit record to be generated [for recording in the audit trail], It is a "recorded event" otherwise, it is an "unrecorded event". The system decides, as each event is detected, whether to generate an audit record by the audit pre-selection algorithm. The set of audit events is based upon a

system's security policy.

<b>Audit Trail</b>	Audit trail is defined as a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event.
<b>Authenticated Identity</b>	A distinguishing identifier of a principal that has been assured through authentication.
<b>Authentication</b>	Measures designed to provide against fraudulent transmission and imitative communications deception by establishing the validity of transmission, message, station or individual.
<b>Authentication Certificate</b>	A security certificate that is issued by a certification authority and that is used to bind the identity (ie, unique name or role) of an entity to a public authentication key and a set of attributes (eg, purpose for which the key is intended to be used)."
<b>Authentication Data</b>	Information used to verify the claimed identity of a subject.
<b>Authenticity</b>	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
<b>Authorisation</b>	The granting of rights, which includes the granting of access based on access rights.
<b>Availability</b>	The property of information being accessible and useable upon demand by an authorised entity or process.
<b>Baseline Controls</b>	A minimum set of safeguards established for a system or organisation.
<b>Business Transaction</b>	Any event, condition, action or commitment, the result of which is the acquisition, disposition or use of assets or resources; the increase or reduction in a liability; the receipt or payment of funds; or the provision of services for which a client is charged. Business transactions occur commonly in, but are not limited to, such diverse areas as finance, administration, personnel, contracts, and program management. Business transactions may also include formal approvals or authorisations such as correspondence.
<b>Certification Authority</b>	An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the user's keys.
<b>Compliance Audit</b>	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and

operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

<b>Confidentiality</b>	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
<b>Contingency</b>	An event that is possible but of uncertain probability.
<b>Copyright</b>	Legal protection against copying the intellectual property of another party in the form in which it is made available for use.
<b>Cryptographic Key</b>	A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment.
<b>Cryptography</b>	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.
<b>Data Encryption Standard (DES)</b>	An encryption algorithm used for the cryptographic protection of electronic information. It was published by the U.S. National Bureau of Standards in January 1977.
<b>Data Integrity</b>	The quality or condition of being accurate, complete and valid, and not altered or destroyed in an unauthorised manner.
<b>Database</b>	A collection of related electronic information items and files stored in a structured manner that supports different representations for different purposes.
<b>Database Management System (DBMS)</b>	A software system that facilitates the creation, retrieval and manipulation of data in a database by computer programs written for the purpose.
<b>DBMS</b>	Refer to "database management system".
<b>Decryption</b>	In cryptography the transformation of electronic information or data from an unintelligible to a clear form.
<b>Denial of Service</b>	The prevention of authorised access to resources or the delaying of time-critical operations.
<b>DES</b>	Refer to "data encryption standard".
<b>Dial-In (Also Dial-Up, Dial-Out)</b>	A means of connecting to a computer system over the telephone network.
<b>Digital Signature</b>	Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the

cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery eg, by the recipient.

<b>Domain</b>	A group of entities subject to the same security policy and under the jurisdiction of a domain authority that is responsible for enforcing that policy.
<b>Electronic Authentication</b>	The process by which an electronic authorisation is verified to ensure, before further processing, that the authoriser can be positively identified, that the integrity of the authorised data was preserved and that the data are original.
<b>Electronic Authorisation</b>	The process by which an electronic signature is linked to a financial or other transaction to signify that an entity having the authority to authorise such a transaction has done so.
<b>Electronic Commerce</b>	Electronic Commerce encompasses computer-to-computer interchanges of business documents in a standardised format, the exchange of freely formatted data, such as facsimile or electronic mail, and such applications as electronic transmission of letters of credit or electronic funds transfers.
<b>Electronic Data Interchange (EDI)</b>	The transmission of documents and other correspondence between the computer systems of different organisations via a communications network, normally for the exchange of business transactions.
<b>Electronic Funds Transfer (EFT)</b>	The servicing of financial transactions using computer systems and data communications facilities.
<b>Electronic Key</b>	Key in digital electronic format regardless of transport and/or storage medium.
<b>Electronic Key Management (EKM)</b>	Cryptographic mechanisms are used in information technology to protect data from unauthorised disclosure or manipulation. Their security and reliability are directly dependent on the protection afforded to a security parameter named the key. The purpose of key management is to provide procedures for handling cryptographic keying material. Electronic key management is the provision of this capability through electronic means.
<b>Encryption</b>	The process by which plain text data are transformed to conceal their meaning. Encryption is a reversible process effected by using a cryptographic algorithm and key.
<b>End-To-End</b>	Having the property of persisting along the entire communications path between two entities engaged in some transaction (for example, end to end security in a messaging environment would imply messaging security

measures which are not broken in the network, but which persist between sender and receiver).

<b>Evaluation</b>	Assessment of an ICT system or product against defined criteria in order to give a measure of confidence that the system or product meets the security requirements.
<b>Evaluation Authority</b>	A body that implements the criteria for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
<b>Evaluation Scheme</b>	The administrative and regulatory framework under which the criteria are applied by an evaluation authority within a specific community.
<b>Evidence</b>	<p>Information that either by itself or when used in conjunction with other information is used to establish proof about an event or action.</p> <p>NOTE - Evidence does not necessarily prove truth or existence of something (see proof) but contributes to establish proof.</p>
<b>File Server</b>	In a computer network, a node that maintains and manages a collection of files that are accessed from other components of the network.
<b>Hacker</b>	Refer to "attacker".
<b>Hand Held Authentication Device (HHAD)</b>	A uniquely configured physical token in the possession of a person requesting connection to a computer system that can be used in the authentication process to help confirm the user's identity.
<b>Identity</b>	A method for identifying the user, which can either be the real name of that user or a pseudonym.
<b>Identity-Based Security Policy</b>	A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.
<b>Impact</b>	The result of an unwanted incident.
<b>Information and Communications Technology (ICT)</b>	The application to information processing of current technologies from computing, telecommunications and microelectronics.
<b>Information Technology Security (ITS)</b>	The protection resulting from an integrated set of safeguards designed to ensure the confidentiality, accountability, authenticity, and reliability of information electronically stored, processed or transmitted; the integrity of the related information and related processes;

and the availability of systems and services.

<b>Integrity</b>	Integrity refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.
<b>Interoperability</b>	Interoperability implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.
<b>ISDN (Integrated Services Digital Network)</b>	A telecommunications technology that allows a single communications channel to simultaneously carry different services, including but not limited to voice, data, video and facsimile.
<b>ITSEC (Information Technology Security Evaluation Criteria)</b>	Criteria developed by a consortium of European countries for rating the security of computer components and systems.
<b>Key</b>	A sequence of symbols that controls the operation of a cryptographic transformation (eg, encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).
<b>Key Generation</b>	Key generation is the process by which key is created. It is the function of generating variables required to meet particular key attributes.
<b>Key Management</b>	The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.
<b>Key Management Facility</b>	A protected enclosure (eg, room or cryptographic equipment) and its contents where cryptographic elements reside.
<b>Key Pair</b>	The keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.
<b>Logical View</b>	In a DBMS, the representation of a database structure that is made available to a processing program to simplify electronic information access and to provide a measure of security.
<b>Masquerading</b>	An attempt to gain access to a computer system by posing as another user.
<b>Message Authentication Code</b>	A data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of the message by any entity

holding the secret key.

<b>Messaging</b>	The process of sending information between two parties by electronic means and in a store and forward manner ie, the sender and receiver are not engaged in an interactive, real time communication. Messaging therefore encompasses simple e-mail systems to formal military messaging systems.
<b>Non-Repudiation</b>	The generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes.
<b>Notarization</b>	In cryptography, an additional assurance as to the identity of communicating parties, via an independent and trusted third party.
<b>One Way Encryption</b>	An encryption technique in which encrypted electronic information cannot be decrypted back to clear text. This technique allows detection of changes to electronic information, as well as comparison of a supplied and stored value. It is often used for storage of passwords.
<b>Operating System</b>	A set of computer software that interfaces to the computer hardware and provides services to the users of the system.
<b>Password</b>	A secret logical possession of a person requesting connection to a computer system or access to a protected resource that can be used to confirm the authenticity of the request.
<b>Personal Identification Number (PIN)</b>	A form of password used in conjunction with a physical possession or device to confirm the identity of a person accessing a computer system.
<b>Physical Security</b>	The measures used to provide physical protection of resources against deliberate and accidental threats.
<b>Point-To-Point Key Establishment</b>	The direct establishment of keys between entities, without involving a third party.
<b>Privacy</b>	The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed.  NOTE - Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.
<b>Private Key Cryptography</b>	A form of cryptography that relies upon the secrecy of cryptographic keys at the point of both encryption and decryption.

decryption.

<b>Public Key Cryptography</b>	An asymmetric form of cryptography that utilises a public cryptographic key at the point of encryption and a secret cryptographic key at the point of decryption.
<b>Recovery</b>	Recovery is the process of responding to a failure or compromise.
<b>Repudiation</b>	Denial by one of the entities involved in a communication of having participated in all or part of the communication.
<b>Residual Data</b>	The data images left on a storage device after it has been logically deleted. (A 'common' method of 'deleting' a file or data image is to simply remove access to it by removing its location from the disk or volume index. This does not actually 'delete' the information, it simply frees that space for re-use by the system. Utilities do exist to recover information without an index.)
<b>RSA (Rivest-Shamir-Adleman)</b>	An important public key cryptographic algorithm named after its designers.
<b>Security Objective</b>	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.
<b>Sensitivity</b>	The characteristic of a resource which implies its value or importance, and may include its vulnerability.
<b>Smart Card</b>	A form of physical token capable of performing some degree of processing, such as calculating and presenting a variable password for use during an authentication process.
<b>Symmetric Authentication Method</b>	A method of authentication in which both entities share common authentication information.
<b>Symmetric Cryptographic Technique</b>	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.
<b>Synchronous</b>	A form of electronic information transmission in which each bit is transmitted according to a defined time sequence. The sender and receiver must maintain exact time synchronisation over the period of the transmission.
<b>System Integrity</b>	The property that a system performs its intended function in an unimpaired manner, free from deliberate or

accidental unauthorised manipulation of the system.

<b>Tamper-Resistant</b>	The property of a device that ensures the destruction of any secret information stored within it if the device is physically attacked.
<b>TCSEC (Trusted Computer System Evaluation Criteria)</b>	Criteria developed by the National Computer Security Center of the US Department of Defence for rating the security of computer components and systems.
<b>Tempest Proof</b>	The property of a device that prevents the emission of undesirable electromagnetic radiation whose interception might constitute a breach of confidentiality.
<b>Terminal</b>	A device, typically incorporating a keyboard and a VDU, which a person can use to interact with a computer system for the purpose of establishing a connection or session with it. The device may have significant local processing capabilities of its own, such as with a personal computer or workstation, or may have little or no local intelligence.
<b>Time Stamp</b>	To append or attach to a message, as a minimum, a digitally signed notation indicating the date and time. The identity of the person appending or attaching the notation may also be included.
<b>Token</b>	A possession that can be used to help authenticate the identity of a computer user. It may be a physical item used at the point of connection to the computer system, or a logical item used to identify the user to processes and other systems within the computing environment.
<b>Topology</b>	The physical relationship between network components.
<b>TQM (Total Quality Management)</b>	The application of principles and procedures to assure continuous improvement to the quality of all aspects of an enterprise, according to international quality standards.
<b>Transparency</b>	Transparency implies that a feature or service is provided without noticeable impact to the user.
<b>Trusted</b>	The property of a computer system or component whose security controls, particularly the authentication controls, have been verified as being of a sufficiently high standard to satisfy the requirements of the assessor.
<b>Trusted Third Party</b>	A security authority, or its agent, trusted by other entities with respect to security related activities.
<b>Unilateral Authentication</b>	Entity authentication which provides one entity with assurance of the other's identity but not vice versa.
<b>User</b>	A person who employs a computer system and its facilities to assist in the performance of a task.

to assist in the performance of a task.

**Validation**

The process of checking the integrity of a message, or selected parts of a message.

**Virus**

A piece of computer software introduced into another program for malicious purposes.

## APPENDIX 5 – References

The following are relevant to either risk management or security planning:

AS/NZS 4360:1999

Risk management (Standards Australia, 1999)

AS/NZS 17799:2001

Information security management - Code of practice for information security management (Standards Australia, 2001)

ISO/IEC.AS/NZS 7799.2:2003

Information security management Part 2: Specification for information security management systems (Standards Australia, 2003)

HB 231:2000

Information security risk management guidelines (Standards Australia, 2000)

HB 143:1999

Guidelines for managing risk in the Australian and New Zealand public sector (Standards Australia, 1999)

OECD Guidelines for the Security of Information Systems and Networks, 25 July 2002.

ISO/IEC TR 13335-1:1996

Information technology—Guidelines for the management of IT Security, Part 1: Concepts and models for IT Security

ISO/IEC TR 13335-2:1997

Information technology—Guidelines for the management of IT Security, Part 2: Managing and planning for IT Security

ISO/IEC TR 13335-3:1998

Information technology—Guidelines for the management of IT Security, Part 3: Techniques for the management of IT Security

ISO/IEC TR 13335-4:2000

Information technology—Guidelines for the management of IT Security, Part 4: Selection of safeguards

ISO/IEC TR 13335-5:2001

Information technology-Guidelines for the management of IT Security, Part 5: Management guidance on network security

[Note the TR 13335 series is being adopted in Australia as AS 13335 series, parts are being updated and some parts may change from TRs to standards]

IEC 61508 (Series)

Functional safety of electrical/electronic/programmable electronic safety-related Systems

ISO/IEC 15408-1:1999

Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

ISO/IEC 15408-2:1999

Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.

ISO/IEC 15408-3:1999

Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.

Australian Communications-Electronic Security Instruction 33 (ACSI-33)-Security Guideline for Australian Government IT Systems, Defence Signals Directorate, December 2000.

Commonwealth Protective Security Manual

Attorney General's Department, Commonwealth of Australia, 2000

IT Threat Identification and Risk Assessment – A Framework for Agencies in the New South Wales Government, 1997

Standing Document 6, SC 27 N1954

Draft Glossary of IT Security Terminology, National Committee for Information Technology Standards

Special Publication 800-18

Guide For Developing Security Plans for Information Technology Systems (National Institute of Standards and Technology, December 1998)