NSW Department of Commerce

Government Chief Information Office

GCIO Guidelines

Information Security Guidelines

Issue No: 6

First Published: Sept 2000

Current Version: Feb 2007

ISBN: 0734743904

Commerce Report NO: 07006

Information Security Guidelines

for NSW Government Agencies

Issue No: 6 First Published: Sept 2000 Current Version: Feb 2007

Table of Contents

Chapter 1 - Using this Guideline

1.1 Introduction

Every agency uses information, most are dependent on it. Various risks may affect the security - confidentiality, integrity and availability - of this information. Information security is founded on risk management because total security is unaffordable and probably unachievable. Information security is not an ‘IT problem’, it is a business issue. Risks are managed by reducing their likelihood and or mitigating their business consequences.

The purpose of this Guideline is to assist NSW Government agencies to establish and maintain their Information Security Management System (ISMS). An ISMS is appropriate to an agency’s ‘business’, information assets, the risks to them, any specific statutory or policy requirements and the agency’s risk appetite.

This Guideline is applicable to three main groups, not just ICT staff:

- executives and managers accountable for the security of information assets;
- staff who are responsible for initiating, implementing and or monitoring risk management within their agency; and
- staff who are responsible for initiating, implementing and or maintaining information security within their agency.

The aims of this Guideline are to:

- Raise awareness of the security risks to information assets and how to deal with them.
- Assist agencies to deploy and operate ISMS that comply with the ISMS standard by:
    - providing a coherent approach and method;
    - providing a starting point for policies and plans;
    - providing information about threats, vulnerabilities and safeguards.

This Guideline may be applied at any stage of an activity, function, project, product or asset involving information. Generally, information security management is applied to complete information systems and facilities. However, it can also be directed to individual system components or services where this is practicable and useful.

Information security risk management should start at the concept stage in the life-cycle of a new system to ensure that vulnerabilities are avoided and safeguards embedded in the design. This will produce significant benefits in terms of the development costs, functionality, integration, and user acceptance.

Security safeguards treat unacceptable risks by reducing their likelihood or mitigating their consequences. It is widely recognised that technology is only part of the solution for information security. Inappropriately or poorly managed technology and or neglect of human factors may increase vulnerability and hence security risks. Risks need to be continually managed because they change and new risks emerge. This means reviewing them periodically and when circumstances change. An ISMS deals with these matters.

1.2 Content Overview

This Guideline presents a consistent approach to information security management, regardless of the size, complexity or nature of the agency. However, it only provides a limited guide to information security threats, vulnerabilities and safeguards because these evolve continuously. Not all of the matters described in this Guideline are relevant in every situation nor does it take account of agency specific circumstances.

The approach taken by the Guideline is to present a harmonised process to establish an ISMS complying with AS/AZS ISO/IEC 27001:2005 *Information technology -Security techniques –Information security management systems – Requirements* (ISO 27001). It applies Risk Management processes and the principles of security architecture to facilitate and not hinder the agency's 'business'. This Guideline is cross-referenced to the requirements of ISO 27001. It complements AS/AZS ISO/IEC 27002:2007 *Information technology – Security techniques - Code of practice for information security management (*ISO 27002 – currently 17799:2005) by providing additional guidance on the processes for creating and operating an ISMS.

Establishing an ISMS to meet the requirements of ISO 27001 is a project and requires the application of project management methods and techniques. This detail is outside the scope of this Guideline. However, this Guideline is structured around a series of Stages and Steps to implement an ISMS.

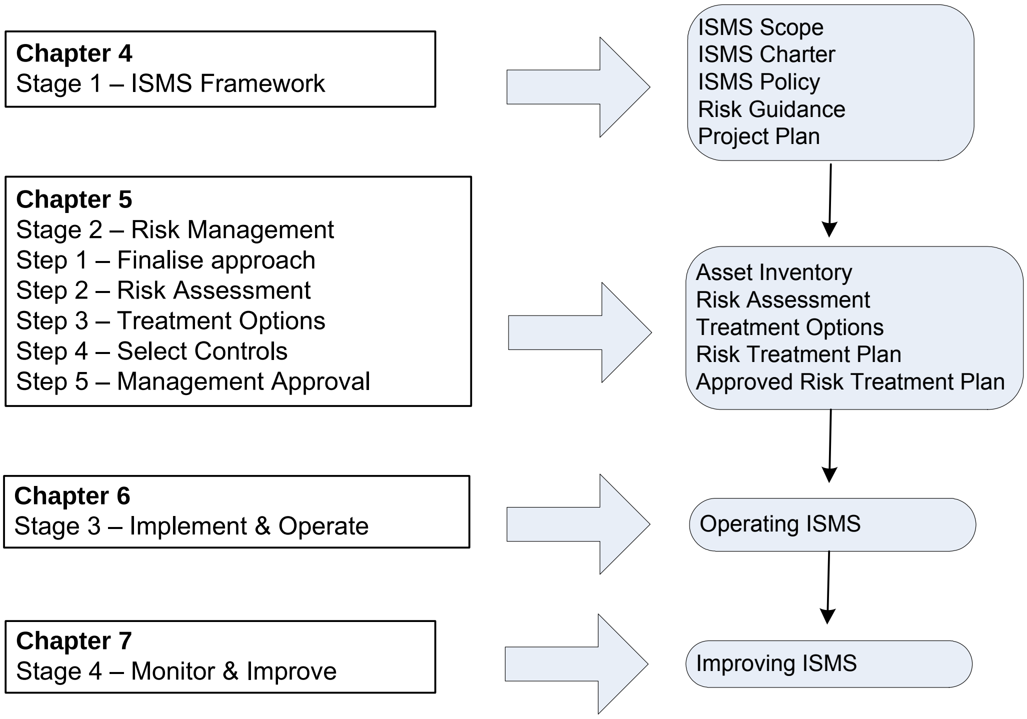


Figure 1 – This Guideline

Annex A illustrates how the various standards relate to one another. Annex B defines a set of 7 high level business consequences of security incidents, a method for assessing likelihood and the consequent risk levels. Supplement 1 provides additional information about threats and vulnerabilities. Supplement 2 provides additional information about security safeguards.

1.3 Government Direction

The Government's electronic information security objectives are:

- **Integrity**. To protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
- **Availability**. To provide authorised users with timely and reliable access to information and services.
- **Confidentiality**. To uphold authorised restrictions on access to and disclosure of information including safeguarding personal or proprietary information.
- **Compliance**. To comply with all statutes, regulations, Cabinet Conventions, policies and contractual obligations requiring information to be available, safeguarded or lawfully used.
- **Assurance**. To provide assurance to Parliament and the people of New South Wales that information held by the Government is appropriately secure.

Agencies are to act as follows in achieving these objectives:

- **Policy and Organisation**. Establish internal policies, an appropriate management structure and responsibilities up to executive level for information security management.
- **Risk**. Identify information assets and use a risk management process to reduce the likelihood and or consequences of security incidents to an acceptable level.
- **Appropriateness**. Ensure the totality of safeguards is commensurate with the significance, value of and risks to their information assets.
- **Compliance**. Establish and maintain an agency wide ISMS that complies with the national standard and covers all electronic information.
- **Certification**. Gain and maintain certified compliance of the most important part(s) of their ISMS by a duly accredited certifier.

The three principles for implementing electronic information security are:

- Managing risks to information assets is the basis for selecting and operating safeguards.
- Safeguards are implemented and operated as elements of an information security management system that is planned and controlled through effective management processes.
- The sum of safeguards must be proportionate to the risks to information assets.

In addition to these general principles and having regard to the Freedom of Information Act, access to information is to be on the basis of "need to know and least possible privilege".

Chapter 2: Introduction to Information Security

All forms of security are driven by 'business' needs. This means that security must reflect the 'business' perspective and contribute to and not hinder 'business' goals and objectives. All this makes information security a governance and management issue not an ICT problem. Only the board, or an executive management group where there is no board, has the necessary authority, accountability and perspective to:

- Decide the most important information assets and their safeguard level.
- Prioritise the investment in information security.
- Establish an organisation wide security management system.
- Ensure organisational compliance with information related legislation.

Managing risk is the basis for managing information security. Security management should be part of the agency's overall risk management. Information security is one aspect of security.

Information security is a cyclical management process called an Information Security Management System (ISMS). Within this process risks are continuously managed by applying appropriate safeguards to reduce the likelihood and or mitigate the consequences of unacceptable risks. This process applies the Plan – Do – Check - Act (PDCA) cycle.

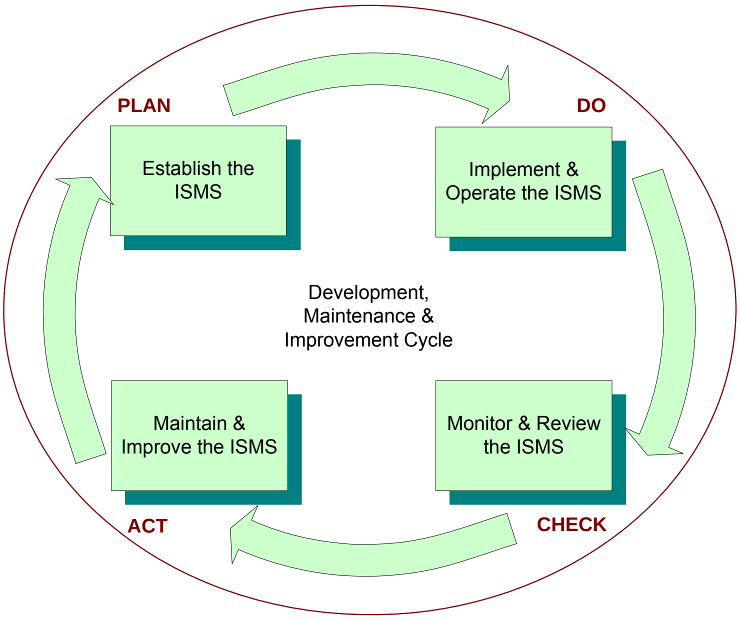

PLAN
DO
Establish the ISMS
Implement & Operate the ISMS
Development, Maintenance & Improvement Cycle
Maintain & Improve the ISMS
Monitor & Review the ISMS
ACT
CHECK

Figure 2 – The Plan – Do – Check – Act Cycle.

2.1 Security Principles

The 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. The principles 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.

ISO 27001 Annex B maps these principles to the Plan – Do – Check - Act cycle (Figure 2).

2.2 Information Assets

Information is an asset that has a value to an agency or to someone outside the custodial agency and must therefore be appropriately safeguarded.

Broadly defined Information is the basis on which governments conduct their business. Reliable information supports business capabilities, notably by enabling good decision making. The NSW Government holds information that is operationally, administratively, politically, commercially or personally significant. The government has a fundamental 'duty of care' and legal obligations to protect this information from unauthorised or accidental modification, loss or release. There are also moral and ethical considerations in the appropriate handling of information.

Implicit in the concept of information assets is the assumption that these assets are necessary if not essential to achieving 'business' goals and objectives. In some cases collecting and maintaining information may be 'business' objectives. Some information assets may not appear to have direct 'business' value, however, they may have illegal value to people not entitled to them. Objectives must, of course, include 'complying with legislation'.

Furthermore there are broader types of information that have safeguarding needs. These include less tangible values such as reputation and public perception of competence, effectiveness and efficiency that may be adversely affected by security failures. These intangible assets may be 'lost' as a consequence of a security failure affecting tangible information assets. Annex B identifies 7 broad types of business consequences that may result from a security failure that compromise the availability, integrity or confidentiality of information assets.

Information can be in any form. It may be printed or written, stored electronically, transmitted by post or electronically, shown on films, spoken in conversation or exist as perceptions. It therefore includes:

- documents and papers;
- electronic data;
- the systems (software, hardware and networks) on which the information is stored, processed or communicated;
- intellectual information (knowledge or perceptions) acquired by individuals; and
- physical items from which information regarding design, components or use could be derived.

Agencies are responsible and accountable for appropriately safeguarding the information assets in their custody. Agencies are best able to gauge the significance and worth of their information assets, the risks to them and the appropriate measures to safeguard them. The approach to be used by agencies is to establish and operate an ISMS that applies risk management.

In NSW Government agencies the security priority is on electronic information. However, it is neither secure nor credible to abandon security when information changes to a non-electronic medium. There are differences in the risks to electronic and non-electronic information.

2.3 Information Security Management System (ISMS)

An ISMS is a system for establishing, operating and continuously ensuring the appropriateness of safeguards against security threats to information assets. It cannot be overstressed that an ISMS it NOT merely a matter of technology and documentation. Both are necessary but the crucial elements of an ISMS are managed planning and operational processes in accordance with documented procedures, and properly recorded decisions and actions. An ISMS depends on people, with appropriate training and awareness. They are its greatest strength but without know-how they are its greatest vulnerability.

Existing information security has usually developed ‘bottom up’. It reflects tactical decisions, ‘point solutions’ and the availability of technology over many years. This means it tends to be an aggregation of security technology and other safeguards that lack cohesion and emergent properties; it is not a system. It is generally infeasible to convert these aggregations to an optimum ISMS quickly. However, it is possible to convert quickly to an effective ISMS by establishing systemic procedures aligned with business needs and against unacceptable risks. This ISMS can then be improved over time guided by an evolving goal architecture.

Having an ISMS is an aspect of ICT governance, and governance is a matter for Directors (board members, senior executives or similar). The national standard, AS 8015:2005 *Corporate Governance of Information & Communication Technology*, states that Directors may be held personally liable for security failures (Clause 1.4.2). Information security is particularly related to the governance principle “*Ensure ICT performs well, whenever required*”. Related to this is compliance with regulatory requirements and AS 3806:1998 *Compliance programs* gives guidance on this. Directors must create an environment that practices due care and due diligence.

Using the Plan – Do – Check – Act cycle reflects continuous evolution of an ISMS to meet ever-changing threats, vulnerabilities and business needs. It also has business implications, not the least being resources adequate to treat the unacceptable risks to an agency. If risks cannot be treated then they have to be formally accepted.

2.4 Risks and Safeguards

Information security is one aspect of ‘business security’, the other aspects being business continuity and physical/environmental security. Electronic information security requires consideration of all three aspects.

Risks to information assets are treated by safeguards. These typically involve procedures, peoples’ behaviour and technology. They operate synergistically in a coherent system. Both ISO 27002 and ISO 27001 require that a risk management process is used as the basis for selecting safeguards for treating risks. Neither this Guideline nor ISO 27001 require agencies to adopt particular technology for safeguards or to have safeguards of particular strength. These are matters for agencies' internal policy and decision-making for the unacceptable risks they face.

Risk management is the strategic approach to information security. Risk is the combination of the likelihood of a security event and its consequences. An event occurs when a threat exploits one or more vulnerabilities.

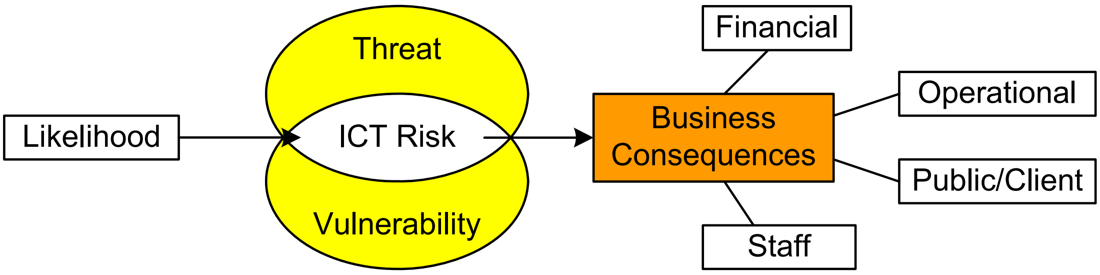


Figure 3 - Risk

The primary business benefit of information security is avoiding loss through security failures. These losses usually have an economic dimension, either directly or indirectly (eg the cost of making good reputational damage or damages awarded by a court). However, good security management presents opportunities for other benefits such as improved operational and administrative efficiency and effectiveness. Risk management is a process that uses appropriate tools and techniques at its various stages. It involves:

- Establishing the context for risk management.
- Identifying possible risks to information assets.
- Undertaking risk assessment comprising:
  - Risk analysis; and
  - Risk evaluation.
- Identifying and evaluating risk treatment options.
- Selecting, planning and implementing cost-effective treatments.

Safeguards treat risks by reducing their likelihood or mitigating their consequences. Safeguards need to demonstrate a return on investment (ROI); 'security' is not by itself a justification for expenditure. Security ROI is usually based on avoiding losses that might occur if safeguards were not in place. The possible losses reflect the likelihood of a risk eventuating and the expected cost if it did. However, improved processes arising from better security management may have an ROI of their own.

Risks need to be continually managed because they change and new risks emerge. This means reviewing them periodically and when circumstances change. It also means understanding the underlying threats and their possible consequences. Managing risks effectively means applying priorities. Both treated and untreated risks need to be reviewed.

2.5 Compliance and Certification

NSW Government agencies' ISMS are to comply with ISO 27001 and have this compliance certified by an accredited body in accordance with government policy. However, agencies vary greatly in there circumstances such as their size and budget, significance of their information assets, their risk exposure and the extent of their ICT operations including the extent of outsourcing. Responsibility for security compliance and certification rests with the Agency for their outsourced information assets and operations. An appropriate ISMS will reflect an agency's circumstances.

Compliance means operating the PDCA cycle and appropriately applying the control objectives and safeguards given in Annex A of ISO 27001 in accordance with business needs and priorities. Agencies with an ISO 9000 compliant quality management system will find that they have good foundations for their ISMS. Certification provides independent assurance to executive management, boards, parliament and the public that the State's information assets are being appropriately safeguarded through well-managed processes.

ISO 27001 identifies 134 possible security controls (safeguards). While all these safeguards must be considered they are only used if they are applicable and necessary. Additional safeguards may sometimes be needed.

However, the Code of Practice, ISO 27002, also recognises that safeguards to ensure legislative requirements such as privacy, records management and intellectual property rights are essential. The Code also judges that most organisations in most environments will need:

- information security policy;
- allocation of information security responsibilities;
- information security awareness, education and training;
- correct processing in applications;
- vulnerability management;
- business continuity management; and
- management of information security incidents and improvements.

Nevertheless there may be other applicable safeguards for unusual cases and other regimes use more, for example CobiT identifies 318 control objectives. ISO 27001 is technology neutral, it does not require that any specific technologies are used. It is also important that safeguards are implemented according to a security architecture and are not merely selected from a checklist. An ISMS evolves continuously as risks and agency capabilities change. The applicability of ISO 27001 is governed by:

- the agency's 'business' needs;
- the agency's security policies;
- the risks faced by an agency;
- the scope of an agency's ISMS; and
- the agency's appetite for risk.

While in principle an entire ISMS should be certified, pragmatism and value for money need to be considered. For example certifying every local office may be of marginal value and a legacy application that is unchanged and has operated for many years without incident may be an acceptable risk. The scope of the certifiable part of an ISMS is defined in a Statement of Applicability. The compliant ISMS may be substantially larger than the certified part and have its own supplementary Statement of Applicability. Uncertified elements, such as local offices should be audited under other arrangements using either internal or external auditors.

Agencies with their ICT provided by an external body do not 'outsource' their information security responsibilities. Generally, 'outsourcing' involves communications and operations management, information systems development and maintenance, and some access control. That leaves 9 information security categories to be considered. Particular points include:

- the agency owns the information and must agree security policies for safeguarding it, including its availability, in the Service Level Agreement with the outsource service provider;
- these security policies must be subject to the information security monitoring and review regime operated by the agency;
- the authorisation of users and the security rules that apply to them to ensure the appropriate confidentiality and integrity of information;
- human resource security including the secure behaviour of their staff and appropriate use of information assets;
- incident management;
- compliance with legislative, policy or related requirements; and
- physical security of information assets on their premises or under their direct control.

The purpose of certified compliance of an ISMS to the national standard is to provide independent assurance of the appropriate information security to executive management, boards, ministers, parliament and the public. Some very small agencies may decide that certified compliance does not provide value for money given the relatively insignificant value of their information assets and consequences of security failures. These circumstances should be discussed with the Government Chief Information Office.

However, executive management and boards of such agencies still need to satisfy themselves that information security measures are adequate. The suggested approach is to follow the guidance in Standards Australia's BEA 006 *Information Security for small to medium enterprises Part 1 How to achieve it* and *Part 2 A reference guide*. This outlines a simplified information security process that is consistent with ISO 27002. External and or internal auditors can report on compliance.

2.6 Information Security Architecture

A system's architecture is a set of rules and conventions that govern its design and maintenance. The architecture serves the purpose of the system including the needs of its stakeholders. It also reflects the constraints of the possible in terms of government environment and values, resources, skills and technology. It is a means for managing complexity and applying system engineering principles to meet 'business' goals.

A security architecture provides a framework of procedures, technology and processes. It ensures coherent, consistent, cost effective and secure implementation, use and maintenance of safeguards throughout an agency. It should:

- minimise the variety of technology;
- provide consistent security functionality across all information assets;
- integrate safeguards;
- segregate different domains and control the flow of information between them; and
- apply consistent security methods, techniques and naming conventions.

A security architecture should be layered where each layer represents a different perspective. A layer governs the layer below it. The architecture is developed top down and descending layers decrease in abstraction. A good approach to this is

SABSA®, which provides a mature approach to security architecture. SABSA® defines layers as:

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Facilities Manager's View	Operational Security Architecture

At each layer the SABSA® model requires answers to the questions What? Why? How? Who? Where? and When? This Guideline relates the Stages and Steps in establishing an ISMS to these layers.

2.7 Safety Critical Systems

Safety critical systems are a special class of secure system. A safety critical system is one in which a failure could directly result in death or injury to a person. Those with the authority to develop, approve or accept safety critical systems into use have a duty of care arising from their legal obligation to take reasonable precautions to avoid significant and reasonably foreseeable risks to people. A breach of this duty could make them liable in the case of an adverse event. A formal 'safety case' is usually required for systems where failure could put life at risk.

Safety critical systems are not specifically addressed in this Guideline. Guidance on this matter is provided by standards such as the IEC 61508 series on *Functional safety of electrical / electronic / programmable electronic safety-related systems,* Standards Australia Handbook on *Safety Issues for Software* (HB 220:2000) and *The Procurement of Computer-based Safety Critical Systems* (Def (Aust) 5679).

Chapter 3: Information Security Management

3.1 Overview

The loss of confidentiality, integrity and availability of information and related services can have a severe impact on agencies' objectives. It is essential to appropriately safeguard information assets within agencies. Appropriately safeguarding information assets, and hence business objectives, can be achieved by:

- recognising that information security management is a business issue;
- recognising that information security management is an integral part of managing risk; and
- establishing, implementing and operating an ISMS.

Some approaches to information security add other concerns to confidentiality, integrity and availability. For example authenticity, accountability and non-repudiation. This Guideline and ISO 27002 treats these as aspects of integrity.

Providing an effective system of information security, in an affordable and unobtrusive manner, is never easy. The speed of changes in technology and business make information security management dynamic and challenging. The provision of adequate security safeguards is often treated as secondary to the provision of business functionality. However, functionality that does not deliver business capability due to failures in confidentiality, integrity or availability is a failure and a wasted investment.

No NSW Government agency needs to approach an ISMS with a blank sheet of paper. The task is to provide structure and effective management to existing safeguards, and improving or adding new ones as necessary. It is likely that the most needed changes and enhancements are procedures to manage an ISMS and to staff behaviour.

The custodians (ie business owners) of information assets are responsible and accountable for the confidentiality, integrity and availability of information for their business operations. The ICT group may operate at least some ICT infrastructure and provide appropriately secure services to business units. If business units transfer part of their security responsibility to an ICT group then the transfer must include resources for the task and clear direction about their security needs.

However, a business unit can never transfer all its information security responsibilities. Business units are responsible for ensuring that their staff know and apply the relevant policies and behave securely. They usually have responsibility for at least some physical security measures and for elements of business continuity management. Furthermore while some information security services can be outsourced, responsibility for the security of information assets is always with the agency owning the assets.

3.2 Information Security Risk Components

Figure 4 below illustrates the security risk components and the relationships between them. The following paragraphs review the components.

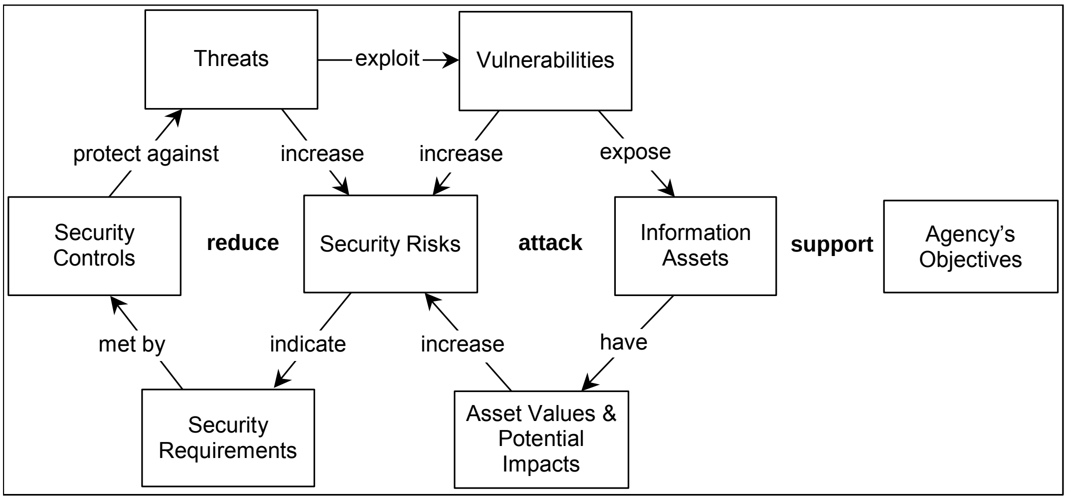


Figure 4 – Risk relationships
(Source: Based on Australian Standard Information technology – Guidelines for the management of IT Security – AS 13335.1:2003)

Information Assets

An asset is something that the agency values or has value (possibly illegal) to someone outside the agency. Therefore the agency has to protect it. Assets include all the information and supporting items that an agency requires to achieve its business objectives. Examples of these assets include:

- information and data (eg files and databases containing payment details, voice records, image files, product information, manuals, and continuity plans);
- paper documents (eg contracts, completed forms);
- software (eg system software, application software, development tools and utilities);
- physical equipment and facilities (eg computer and communications equipment, storage media, specialised sensors, effectors and devices);

- information services (eg computing and communications services);
- people and their knowledge (eg technical, operational, marketing, legal, financial, contractors and consultants, outsourced providers); and
- image, values, goals and reputation of the agency and government (however, it is usually more convenient to treat the loss of these as the negative consequences of a security incident).

Agencies also have legal obligations to safeguard personal information, agency records and intellectual property.

Information Asset Values (and potential impacts)

The most important and valuable information assets are those underpinning an agency's core or most critical duties, capabilities or goals. Recognising these and identifying their information dependencies reveals the highest business priorities for the ISMS. However, there are also non-negotiable statutory requirements such as the *Public Finance and Audit Act 1983*, *Privacy and Personal Information Protection Act 1998, State Records Act 1998, Workplace Surveillance Act 2005* and agency specific legislation.

The value of information assets is expressed in terms of the potential business consequences for events resulting in loss of confidentiality, integrity and or availability to them. Potential consequences include direct and indirect financial losses (immediate or subsequent), loss of revenue, failure to meet service obligations or reputational loss. Indirect consequences of a security failure also have to be considered. Annex B provides a list of seven broad classes of consequence with definitions and levels of severity.

Threats

A threat is the potential source of an event that may harm an agency's business through its information assets and information using capabilities. Threats can be acts of nature (such as flood, fire and earthquake), intentional or accidental acts originating inside or outside the agency. Most threats exploit vulnerabilities in information assets or their supporting infrastructure.

When a threat eventuates there are consequences for business objectives. An eventuating threat may impact several information assets and have several consequences of varying severity including creating new vulnerabilities. These effects undermine business objectives. In general, a threat could cause:

- destruction of an asset or capability (facilities, data, information, equipment, communications);
- corruption or modification of an asset (data, information, applications);
- theft, removal or loss of an asset or capability (equipment, data, information, applications);
- disclosure of an asset (data or information);
- use or acceptance of an illegal asset (equipment, unlicensed software, repudiated or false data or information); or
- interruption of services.

All risks are uncertainties, their likelihood, frequency and consequences are uncertain. Some threats may occur many times per hour, others once a decade or less. The frequency may be found from existing safeguards records. Others may be deduced from metrics and other sources but some will be a matter of judgement. It is advisable to look to several sources or seek several opinions before adopting a particular likelihood. It is useful to state likelihood as 'most likely', 'best case' and 'worse case'. This aids and clarifies thinking about risks and enables numerical methods.

Examples of threats can be found in Supplement 1 of this Guideline.

Vulnerabilities

Vulnerabilities are weaknesses associated with an agency's assets or capabilities. A vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset. Therefore, a vulnerability that cannot be exploited by a threat, or an asset with no known or suspected vulnerabilities cannot be a security risk. However, minor vulnerabilities in different systems may concatenate if the host systems are interconnected. This means it is important to analyse vulnerabilities for dependencies that reveal their full effect.

Typically a vulnerability results from 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 vulnerabilities or vulnerabilities that affect it. Details of software vulnerabilities are widely available via the Internet, for example the National Vulnerability Database, http://nvd.nist.gov. However, the most pervasive vulnerability is probably the susceptibility of staff to 'social engineering', which makes security awareness for all staff an important safeguard.

Security Risk

An information security risk is the potential that a given threat will exploit information vulnerabilities to cause loss or damage to information assets and dependent capabilities, duties and hence business objectives. The level of security risk is evaluated by considering the combination of the likelihood of identified threats eventuating and, if they did, the consequences for agency capabilities and values and their stakeholders. The relationship between threats and consequences is usually 'many to many', and some vulnerabilities enable others to be exploited.

The risk analysis initially considers threats without any existing treatment by the agency. This reveals the most significant threats, which facilitates prioritisation for implementing and maintaining safeguards. After this the efficacy of any existing safeguards is considered and the risk analysis adjusted to reflect them. This reveals where improvements may be needed, it is most likely that these will be in the operation of the existing safeguards not their theoretical capability. Recognising the most significant untreated ('inherent') risks also ensures that they and their treatments are monitored with appropriate priority.

Security Requirements

The three main origins of information security requirements are:

- security risks that could result in unacceptable business losses if they occur;
- legal, statutory and contractual requirements affecting the agency, its trading partners, contractors and service providers; and
- agency policies, principles, objectives and requirements to support its capabilities and values.

The primary sources of security requirements are the needs of the business units that collect and or use the information assets in their capabilities to meet business objectives. These must be mediated by the senior executive view of business risks. However, business unit needs are subject to the agency's information security charter and other policies. Furthermore, some of a business unit's capability will be derived from shared infrastructure provided by the agency ICT group and or outsourced service.

Security Safeguards

Safeguards are policies, procedures, behaviours or technology. These contribute to safeguarding assets against threats by reducing vulnerabilities, and hence likelihood, or mitigating the consequences of an undesirable event. Safeguards are selected, implemented and operated in the context of a security architecture.

Safeguards can have varying levels of strength. However, there is no generally accepted approach to defining or measuring this and individual safeguards will usually operate in series. Approaches include assumed levels of attacker competence or reducing the likelihood of a successful attack to a particular probability.

3.3 Security Policies

ISO/IEC 27001:2005	***A.5.1.1 An information security policy document shall be approved by management, and published, and communicated to all employees and relevant external parties.***
ISO/IEC 27001:2005	***4.2.1 b) Define an ISMS policy.***

A policy is an expression of intent. A written policy is the primary means by which a board or executive team gives direction to management and staff, and informs other stakeholders. Effective security policies provide clear direction and commitment, and establish clear roles and responsibilities. Policy is part of effective corporate governance.

Information security policies provide executive direction and support, and establish operating plans and processes. Information security policy is a control category in ISO 27001 that will exist for every ISMS. Policies establish the required behaviours and outcomes, and may vary widely in their specificity. There are no hard and fast rules to define the format or content of information security policies.

The term 'Security Policy' is broad and includes matters that may not be considered 'policy' in the conventional government sense. In an ISMS Policy there are three main classes of information security policy:

- Executive Policy (or ISMS Charter) signed by the Chief Executive. It states the commitment, business goals, objectives and key responsibilities for the ISMS.
- ISMS Policy, management plans that provide the cohesive and holistic framework to establish and manage the ISMS, and select and implement its security safeguards. It establishes the ISMS organisation, responsibilities and accountabilities that flow through to more detailed policies
- ISMS operating policies, typically comprising management, implementation and operating procedures guidelines and plans. They require actions by management, all staff, specific staff and others. These policies are risk treatments expressing security safeguards. They include technical 'policies' such as firewall settings. It is vital that they are actionable, practicable, reflect what actually happens and are not aspirational.

Operating policies must also be appropriate to the organization, smaller organisations usually operate with less formality than larger ones and policies may reflect this. In addition operating policies:

- have various audiences, including users, IT staff and managers;
- are clearly related to 'business' needs and objectives;
- have different purposes, levels of detail and explicitness of direction; and
- require operation of the Plan – Do – Check - Act cycle over time.

When preparing and maintaining policies it is vital to ensure they are consistent. This is helped by not having too many policies and by having some overall structure to them. For example the ISMS Management Plan should provide the policy architecture. However, large policy documents are seldom 'user friendly'. The key is documents designed for their users that clearly tell them what they have to do, when they have to do it and what they must not do. Policies that are incompatible with an organisation's culture are likely to fail.

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, legal and regulatory aspects of the agency's functions and activities. The information security policy may involve both internal and external stakeholders, and must be part of the contract if IT is outsourced.

Within its scope effective ISMS Policy must be:

- achievable by agency members with clearly defined responsibilities and actions for at least users, IT staff and management;
- enforceable both procedurally and technically, and with sanctions when breaches occur; and
- implementable through procedures, technical controls or other methods, via clearly documented directives, guidelines, instructions and the like.

There are no definitive ISMS policies that can be readily adopted by all organisations. Ideally each agency should develop its policies in its own style to reflect its own culture and circumstances. The best approach is to document existing practices then rationalise, integrate and improve them to meet security needs. This approach minimises the subsequent training and awareness raising effort. However, adapting another organisation's ISMS policies, particularly lower level ones, may sometimes be the most cost effective solution. Detailed operating policies, particularly for security technology, developed by third parties may prove useful.

ISO/IEC 27001:2005 ***A.5.1.2 The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure it remains appropriate.***

The ISMS policies may become inadequate as changes occur in technology, laws and regulations, threats or operations. As a minimum, policies should be assessed annually, as part of the PDCA cycle, to ensure their currency and adequacy.

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

3.4 Configuration Management

An operating ISMS must have effective configuration management. Configuration management is also explicitly referenced in some safeguards. Ideally a configuration management system already exists in an agency, and will do so in agencies that comply with AS/NZS ISO 9001 *Quality management systems – Requirements* or the Information Technology Infrastructure Library (ITIL). The standard for configuration management is AS ISO 10007:2003 *Quality management systems – Guidelines for configuration management*.

The main elements of configuration management are:

- formal plan and procedures;
- a system of configuration item (CI) identification;
- change control arrangements;
- configuration status accounting; and
- configuration audit.

CIs may include hardware, software, networks and documents of all types. Change control necessitates change management including organisation and processes. ITIL is widely recognised as providing authoritative guidance on this change management.

The mechanics of a change control process require that:

- The need for a change is identified and a formal Change Request is raised.
- The Change Request is evaluated to understand its implications.
- A change control authority formally decides to accept or reject the change.
- If accepted the change is implemented.

3.5 Management Commitment

A key factor for successful information security in any organisation is the:

visible support and commitment from all levels of management

This will not guarantee success but lack of it will guarantee failure.

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:

- Effective and functioning governance arrangements originating at the highest level of the organisation.
- The ISMS Charter reflects executive commitment.
- The ISMS management plan establishes detailed organisation, management responsibilities and accountabilities and has executive level endorsement.
- An ISMS is established, implemented and maintained.
- Adequate resources are allocated to information security.
- The performance of the ISMS is reported to executive management for review and as a basis for improvement, taking into account any regulatory reporting requirements.

Management commitment can be developed and sustained by providing regular reports and status information. ‘Dashboard’ style is recommended for this.

3.6 Critical Success Factors

In addition to management commitment the successful implementation of information security within an agency will depend on several factors, notably:

- Information security policy, objectives and activities reflect business objectives.
- Recognition that information security is a business issue not an IT problem.
- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organisational culture and involves stakeholders.
- A realistic assessment of the security risks.
- Provision of resources for information security management.
- The existence and use of an agency security architecture.
- Effective promotion of information security to all managers, staff and other parties to achieve awareness.
- Appropriate awareness training and education to all staff.
- Establishing an effective information security incident management process.
- Processes to measure the ISMS, evaluate its performance and feed into the improvement process.

Indicators of an effective ISMS include:

- The Board or equivalent requires and receives regular reports about information security performance and events.
- Information security is a standing item on the agendas of risk management committees up to executive level.
- Information security risk levels are set by the executive level and reflect the agency’s risk appetite.
- Business unit managers are responsible for the security of the information underpinning their operations.
- The inherent information risks in critical business processes are understood and documented.
- Individuals are held accountable for any security breaches in which they participate, whether intentional or accidental.
- Regular review of information security products and services to ensure they are cost effective.
- Regular review of information security arrangements to ensure continued relevance and continuous improvement.

An effective information security risk management process is essential for the successful implementation of the program. The basic ISMS framework is shown in the following figure.

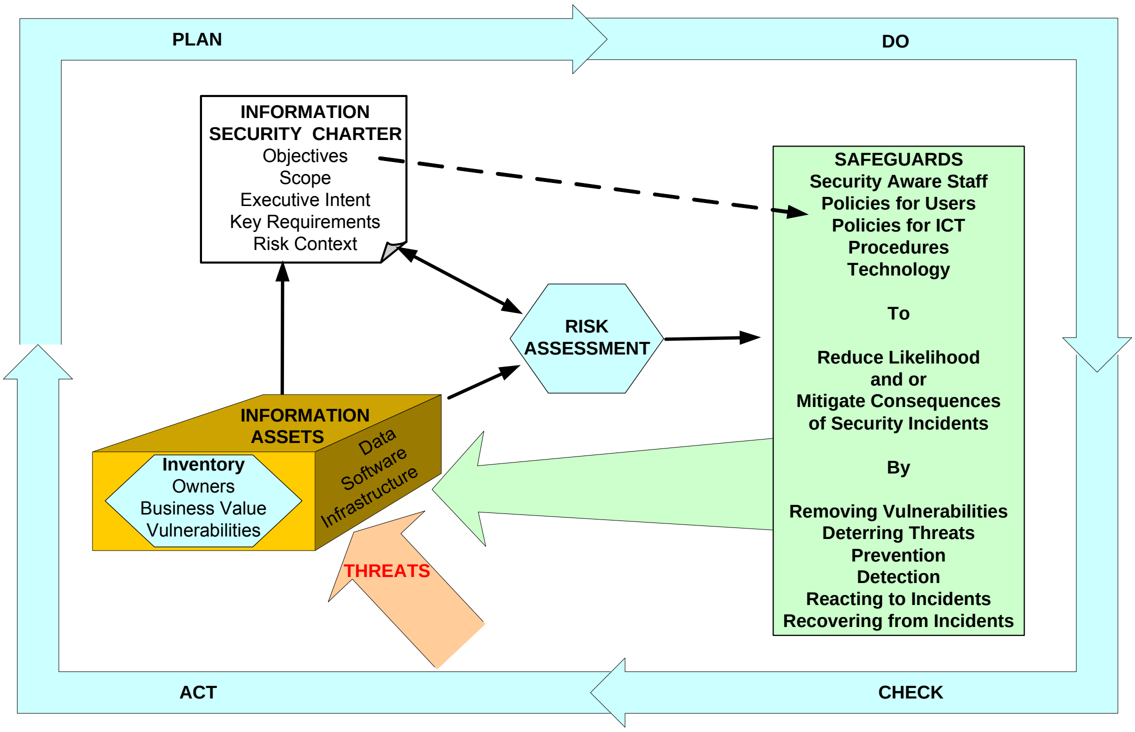


Figure 5 – ISMS Framework

Chapter 4: Stage 1 - ISMS Framework

ISO/IEC 27001:2005	***4.2.1 Establish the ISMS a) Define the scope of the ISMS. b) Define the ISMS policy. c) Define the risk assessment approach.*** ***4.3 Documentation requirements.*** ***5.1 Management commitment a) Establishing an ISMS policy, b) Ensuring that ISMS objectives and plans are established, d) Communicating the importance of meeting security objectives, f) Deciding the acceptable level of risk.*** ***5.2.1 Provision of resources.*** ***5.2.2 Training, awareness and competence.***

4.1 Overview

Plan (establish the ISMS) - Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall polices and objectives.

The assumed inputs of this stage are:

- Management commitment to an ISMS.
- Staff and or other resources to undertake the stage.

The outputs of this Stage are:

- The agreed scope of the ISMS including identification of core information assets and values, and the business rationale for their identification.
- An ISMS Charter.
- The contextual layer of an information security architecture and some parts of the conceptual layer.

- An initial ISMS Management Plan including the information security organisation.
- Guidance for risk management in the next stage.
- An approved project plan and resources for the next stage.

It is important to establish documentation standards as early as possible. This is particularly important when the ISMS is to be certified because it starts the 'evidence' for the certification auditors.

4.2 Consultation, Communication and Support

This Stage necessitates extensive consultation and communication with stakeholders. This will inevitably lead to iteration during development of the outputs because these influence each other. Furthermore, developing ISMS Policy is to some extent iterative with risk management activities in the next stage.

As part of its governance processes, an agency should have an overall risk management policy, as described in AS/NZS 4360:2004 *Risk Management*. This policy should include the objectives for and commitment to information security management. It should be consistent with the agency's business imperatives, strategic context, goals and objectives. Where an overall risk management policy does not exist then the outputs of the stage will have to be developed from scratch. This will involve extensive consultation.

Executive management must give clear direction and demonstrate their support for and commitment to the ISMS by formally agreeing an ISMS Charter for all parts of the agency. This Charter should be endorsed and signed by the Chief Executive Officer. Once the Charter has been developed and approved, it should be communicated, understood, implemented and maintained at all levels of the agency. The Charter should be covered in awareness and training programs.

A stakeholder communication plan must be developed and implemented when stakeholders have been identified, and organisation and responsibilities established. Communications must reflect stakeholders' particular interests and concerns. It must facilitate a two-way exchange of information.

4.3 ISMS Scope

Before risk management can start and policy prepared the scope of the ISMS must be clearly defined. Scope sets the framework for the rest of the process within which risks must be managed and provides guidance for making decisions. It also enables better informed organisational and resourcing plans. A clear definition of the ISMS boundary avoids unnecessary work and improves the quality of the risk assessment.

The ISMS may cover 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 agency where information security failure may unacceptably affect business objectives, whatever the media of information.

Identifying the scope of an ISMS requires a broad understanding of:

- the agency's information assets,
- the business capabilities that use them,
- the values they affect and the significance of these to business objectives, and
- the agency's Results & Services Plan.

It will usually involve workshops with a wide mix of stakeholders.

Scoping aims to clarify the following:

- What agency capabilities and values rely on the confidentiality, accuracy, integrity or availability of information for decisions and operations?
- What are the issues that need to be considered in assessing information security risks?
- What information needs to be protected?
- What criteria are to be used in assessing risk?
- What are the information security requirements of the agency?

The key components in scoping the ISMS are:

- establish the external context;
- establish the internal context;
- develop overall risk evaluation criteria;
- define the risk management structure; and
- define the key information assets.

Scoping should include developing the Contextual and parts of the Conceptual layers of a security architecture.

4.4 Risk Context and Criteria

The risk context is an essential element in scoping the ISMS and developing the top level ISMS Policies. Broad direction for risk assessment must also be developed at this Stage. Additional context and detailed criteria are developed at the start of the risk management activities, the next Stage.

Establish the External Context

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

The agency should understand the following:

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

There should be a close alignment between information security risk management and the agency's mission statement, strategic objectives and Results & Services Plan.

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.

Establish the Internal 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 safeguards 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. A key element is to identify all the internal stakeholders.

Establishing the internal context will influence and be influenced by the ISMS Charter.

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 safeguards their privacy.

Develop Risk Evaluation Criteria

In order to assess the risks, impacts, consequences and the selection of safeguards, 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 tolerate. The extent of this tolerance will be reflected in the definitions used with risk criteria.

Criteria must be developed, but once established should become part of policy and subject to periodic review. It is important that appropriate criteria be determined at the outset of the risk assessment and continually reviewed throughout the risk assessment process. Risk criteria may be further developed and refined to ensure that they correspond to the types of risks and the way in which the levels are expressed. Criteria include:

- Types of consequence (eg operational, financial, service delivery, client & staff well-being, reputational).
- Likelihood definitions and levels (qualitative and or quantitative).
- Consequence definitions and levels (qualitative and or quantitative).
- Evaluation grading (product of likelihood and consequence).
- Risk acceptability, treatments and priorities.

Examples of Likelihood, Consequence and Evaluation levels are at Annex B.

Several factors will influence development of high level criteria including:

- government policy;
- the agency's internal policy, goals and objectives;
- expectations of stakeholders and customers;
- legal requirements and 'reasonableness'; and
- the agency's risk appetite and any 'zero tolerance' areas.

Decisions concerning risk acceptability and the subsequent risk treatment may be based on the operational, technical, financial, legal, social, humanitarian or other criteria. Many risks have several different types of consequence. Most risks have financial and reputational consequences as well as more specific ones.

The legal consequences of a failure to meet statutory requirements also need consideration. For the purposes of planning cost effective safeguards it is useful to assign a financial value to these and to reputational consequences.

The NSW Government has 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 common law confidentiality and the Crimes Act 1914)*;
- the availability of official information to the public *(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 assets from fraud and corruption; and
- expectations of providing appropriate protection to security classified information.

ISO/IEC 27001:2005	***A.15.1.1***	***All relevant statutory, regulatory and contractual requirements and the organisation's approach to meet requirements shall be explicitly defined, documented, and kept up to date for each information system and organisation.***

4.5 ISMS Charter

The Charter signed by the Chief Executive, states the business goals, objectives, ISMS scope, executive intent, key requirements and key responsibilities for information security management. It demonstrates executive commitment to all staff and other stakeholders. It may also provide:

- risk context and guidance on the core business values, assets and capabilities;
- policy on assigning ownership of information assets;
- business oriented guidance on risk assessment including costing;
- guidance on security priorities and levels (strengths) of protection; and
- a basis for justifying security expenditure in business terms.

Physically, the Charter may be or become part of the ISMS Policy document.

4.6 ISMS Policy

The overall ISMS Policy is a management plan and with the contextual architecture layer is the foundation of the ISMS. It is the basis for the lower layers of the security architecture including the framework for adopting specific operating policies and technical controls. It is the second key step (after the Charter) 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.

Preliminary risk management activities inform the development of architectural and operating policies, which then guide more detailed risk management and the development of information security plans. Executive management must decide the level of acceptable business risk, which may affect the resources required to establish and operate the ISMS.

The ISMS Policy establishes the high level framework for risk management. Producing this plan necessitates preliminary risk management activities:

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

The ISMS Policy should also outline the information assets to be protected, the approach to risk management, the control objectives and safeguards, and the degree of assurance required.

ISMS Policy will grow into a document set providing a set of policies governing all aspects of the ISMS. This document set should have a coherent structure. The hierarchy ‘Manual’ – ‘Procedure’ – ‘Work Instruction’ used in AS ISO 10013:2003 *Guidelines for quality management system documentation* provides a suitable framework.

4.7 Security Management Structure

Organisation

ISO/IEC 27001:2005	***A.6.1.1 Management shall actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.***

A security management organisation has to be established, staffed and responsibilities assigned. A key issue is to plan the relationship between ISMS responsibilities and those for information management, information systems, risk management and physical security. The security organisation must be defined in the ISMS Policy.

Responsibility and Authority

The responsibility, authority and the interrelationship of staff (or contractors) 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 areas where information security risks need managing;
- initiate action to prevent or reduce adverse risks;
- control further treatment of risks until the level of risk becomes acceptable;
- identify and record any problems related to managing risks;
- initiate, recommend or provide security measures through designated channels;
- verify the implementation of security measures; and
- communicate and consult internally and externally as appropriate.

ISO/IEC 27001:2005	***A.6.1.2 Information security activities shall be co-ordinated by representatives from different parts of the organisation with relevant roles and functions.***
ISO/IEC 27001:2005	***A.6.1.3 All information security responsibilities shall be clearly defined.***

Information security is an interdisciplinary activity and can be achieved through various organisational schemes, depending on the size and structure of the agency. Effective security requires accountability and the explicit assignment of responsibility to asset custodians, service providers and information users.

Typically the responsibility for the security of information will rest with the agency’s staff (and ultimately the Chief Executive Officer). All members of the management team share the responsibility for initiating and controlling the implementation of effective information security within the agency.

The ISMS Policy must assign the security roles, responsibilities and accountabilities 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, must be clearly defined.

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.

The tasks of the Information Security management team (ie up to executive level) typically includes :

- managing the agency's ISMS, its Plan – Do – Check – Act cycle and security calendar;
- monitoring for changes in information security risks;
- advising on information security risks and control measures;
- reviewing and revising of information security policies and plans;
- monitoring and reviewing information security measures;
- assisting with information security incident management;
- compiling information security status reports; and
- assisting and supporting staff security awareness training.

The size of the team will depend on the size of the agency and its likely risks. A key role in the team is an officer appointed to be responsible for all information security matters in the agency. The Information Security Officer should have sufficient authority and have access to agency executives when issues require escalation. However, responsibility for resourcing and implementing the safeguards will often remain with the individual managers.

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 safeguards for new systems or services;
- review information security incidents; and
- promote the visibility of business support for information security throughout the agency.

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:

- agency functions and or activities;
- different types of information assets as described below;
- organisational structure;
- physical locations; or
- projects.

The risk activity structure should be submitted to senior management to ensure that it reflects the agency's service functions, business objectives, activities, priorities and that senior management endorses subsequent activities.

4.8 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. Establishing an ISMS will usually require a project. However, once established the ISMS has to be operated and this is not a project. In a large agency operation may require one or more full time staff. It will always require some scheduled time by managers and executives as part of the 'Plan', 'Check' and 'Act' activities.

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

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.

Chapter 5: Stage 2 - Risk Management

ISO/IEC 27001:2005	***4.2.1 Establish the ISMS d) Identify the risks, e) Analyse and evaluate the risks, f) Identify and evaluate options for the treatment of risks, g) Select control objectives and controls for the treatment of risks.***
	4.2.2 a) Formulate a risk treatment plan
	4.3 Documentation requirements.
	5.2.1 Provision of resources.

5.1 Overview of Stage 2

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.

Plan (establish the ISMS) - Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall polices and objectives.

An effective information security risk management process underpins information security management. AS 4360 describes a generic risk management process that is amplified in HB 436:2004, and HB 231:2004 provides further information. 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 considered. Risks are uncertainties with consequences, the critical part of risk assessment is estimating the nature and extent of uncertainty and its consequences.

The first risk management steps were taken in the previous stage when the risk management context was established and stakeholder consultation and communications started. At this stage risks are identified, assessed and treatments planned.

The initial inputs are the outputs from Stage 1.

The outputs from Stage 2 are:

- An approved Risk Treatment Plan.
- The conceptual and logical layers of the Security Architecture.

Information security risk treatment planning is the product of the agency's ISMS Management Plan and associated guidance and, and information security risk management processes. There is likely to be iteration between planning and policy as organisational and resourcing issues are resolved.

As the stage progresses it will usually be possible to start risk treatments before the Risk Treatment Plan is approved. These treatments will typically involve the development and implementation of operating policies.

5.2 Consultation, Communication and Support

Consultation and communications continue throughout the stage to:

- ensure the ISMS is aligned with business needs;
- harvest expertise and knowledge from all stakeholders;
- understand priorities;
- develop security awareness throughout the agency; and
- ensure 'no surprises' for management.

5.3 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, actions and processes;
- to provide an accountability mechanism;
- to facilitate continuing monitoring and review;
- to provide an audit trail; and
- 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. ISMS certification to ISO 27001 makes good documentation vital. Because of the need for auditability, including for certification, documentation must be planned, designed and initiated at the start of the process. The ISMS Management Plan could provide the documentation architecture if the agency lacks documentation standards.

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 with current documents clearly identified;
- it is periodically reviewed and updated as necessary to ensure that it is current;
- obsolete documentation is promptly withdrawn, identified and retained if necessary for legal or knowledge preservation purposes; and
- configuration management is applied.

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 safeguards should be distributed on a “need-to-know” basis.

Step 1 – Finalise the Approach to Risk Assessment

The outputs from this Step are:

- A plan with appropriately detailed guidance for the Stage.
- An inventory of assets.

Finalise the Risk Management Context

Stage 1 established external and internal risk management contexts, identified the ISMS scope and key criteria for risk management. This Step starts by finalising the risk management context. However, as the work progresses refinements may be necessary to Stage 1’s outputs. The general security context is illustrated in Figure 6.

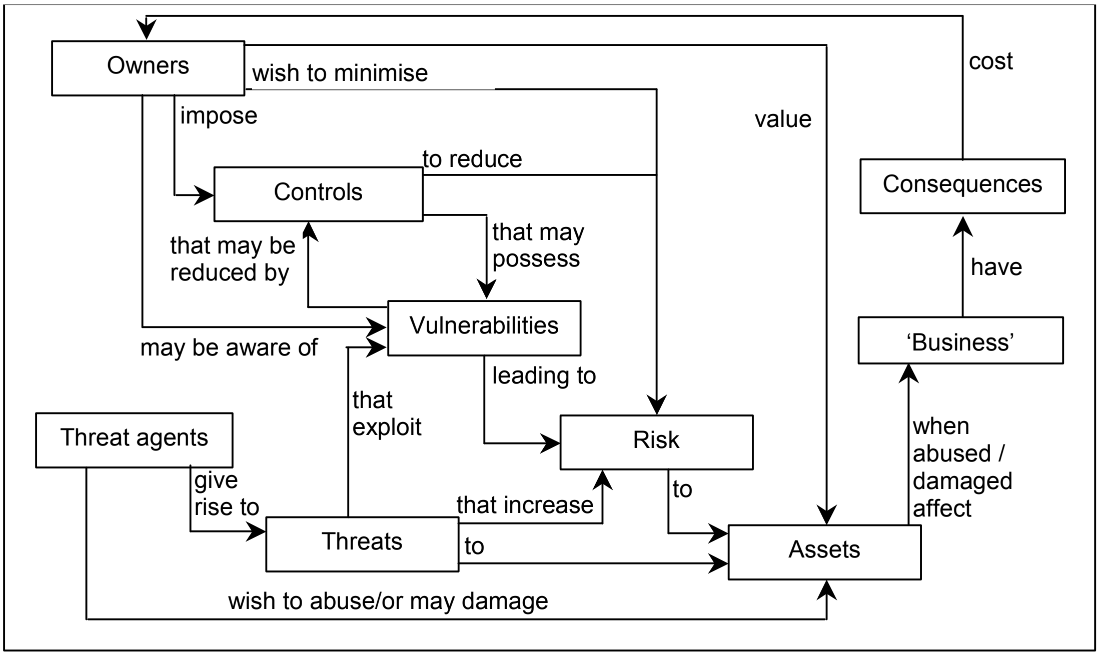


Figure 6 - Security context – concepts and relationships
(Source:derived from ISO/IEC 15408-1 Common Criteria)

Refinement and amplification of the risk management context is guided by the outputs of Stage 1 and involves the following to the extent that they were not completed in Stage 1:

- Defining the review 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?
- Defining the timeframe and locations to be reviewed. What is the time allotted to complete the assessment? Where will the review take place - just Head Office, Divisions, or a particular business unit, site or a group of sites?
- Identifying guides, aids and the resources required to conduct the review. Guides may identify the generic sources of risk, examples of common vulnerabilities, exposures 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?
- Defining the granularity of risk identification and the approach to deciding which risks should be subject to detailed analysis.
- Defining the extent and comprehensiveness of the risk management activities to be carried out. Specific issues that may be considered include:
  - The roles and responsibilities of various parts of the agency that manage risk;
  - The relationship between information security risk assessment and other parts or projects in the agency.

Define the Information Assets

ISO/IEC 27001:2005	***A.7.1.1***	***All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.***

The most important information assets are those the an agency's most valued activities rely upon. An asset is part of a system or capability used by an agency to meet its ‘business’ objectives. It therefore requires protection. Information assets may be identified in existing asset registers, enterprise architecture and ICT strategic plans.

In identifying assets, information should be considered in the wider context than just an ICT system and its associated hardware and software. It may be appropriate to structure the risk assessment based on the type of assets.

All assets in the risk management context must be identified to an appropriate level of granularity and detail. This will involve recognising their security significance, priority and scope, and judging the best use of effort and resources. Conversely, any assets excluded from the context, for whatever reason, may need to be assigned to another review to ensure that they are not ignored and that all major assets are considered.

ISO/IEC 27001:2005	***A.7.1.2***	***All information and assets associated with information processing facilities shall be owned by a designated part of the organisation.***

The Inventory of Assets should include the following information:

- asset identification;
- asset description;
- asset type;
- custodian; and
- location.

Information Classification and Labelling

ISO/IEC 27001:2005	***A.7.2.1 Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation.***
ISO/IEC 27001:2005	***A.7.2.2 An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.***

Information is labelled in accordance with security classification based on the criteria established by the agency. This provides a consistent basis for deciding the level of protection required,

The Commonwealth security classification system and labelling guidelines described in the Protective Security Manual (PSM) provide a means of grading information confidentiality. The classifications are grouped into National and Non-national Security Information. National security information is any official information that “affects the security of the nation (for example, its defence or its international relations)”. Non-national security information refers to any official information 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.”

For Non-national Security Information agencies are to use the Commonwealth’s sensitivity labels, slightly modified, as directed in Premier’s Circular 2002-69 - *Labelling Sensitive Information*, which includes the *Guide to Labelling Sensitive Information*.

NSW government agencies handling National Security Information must do so in accordance with the PSM using the labels Restricted, Confidential, Secret and Top Secret. Using any of these terms for non National Security Information is strongly deprecated because it may result in handling errors.

It is essential that agencies respect the rule that the 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. This ensures that the costs of protection do not outweigh the consequences of a breach.

Step 2 – Undertake a Risk Assessment

The output of this Step is a completed Risk Assessment.

The step combines the risk identification, analysis and evaluation elements of the risk management process outlined in AS/NZS 4360. Steps 2 and 3 together provide the conceptual and logical security architecture layers and SABSA® questions What? Why? How? Who? Where? and When? focus on key issues.

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 knowledgeable on the various aspects of the information asset being assessed. Whatever method is used, it must fit the agency's culture and practices.

Risk Identification

The aim of this component is to identify, classify and list all the risk events, vulnerabilities, exposures or threats that may affect information assets identified in Step 1. It examines the sources of risk from the perspective of all stakeholders, whether internal or external. Possible causes or scenarios are also considered. It is important to identify risks in their untreated condition.

Generic risks can provide a useful starting point, these typically reflect a historical perspective and must be filtered for relevance. The current situation should also be analysed for possible vulnerabilities and threats. Finally, there may be scope for creative thinking about future threats. Relevance and significance must be related to the agency's business circumstances and information assets. Supplement 1 provides a historical view of the main types of threat and the vulnerabilities they exploit. The main types of threat are Environmental, Deliberate and Accidental.

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, vulnerabilities or threats may affect more than one of integrity, confidentiality and availability.

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 directly or indirectly?

It is best practice to identify risks with a three part statement. This could be a table with columns for ‘Source’, ‘Event’ and ‘Consequences’. Alternatively a structured statement: ‘There is a Risk that [*threat(s) to* | *vulnerability(s)* | *exposure(s)*] results in [*security event(s)*] that impacts [*business objective(s)* | *values* | *capabilities*].’

A significant issue in risk identification is the granularity of the risks defined. Risks can be decomposed into ever greater detail, with a tendency to ‘paralysis by analysis’. It requires careful judgement to deal with risks at an appropriate granularity. In general it is best to keep identification at a fairly high level. However, it is usually useful to explore back through the causes of an event because this may reveal causes common to several events and may reveal an optimum point for preventative treatment. Drilling down into a major risk will give better understanding of it and help select cost effective safeguards.

Risk Analysis

Risk analysis involves determining the likelihood of a risk and its consequences and then combining these to estimate the overall level of risk. It will separate the minor acceptable risks from the major risks, and provide data for the evaluation and treatment of risks.

During this initial analysis the level of risk is determined without considering any existing safeguards. Ignoring existing safeguards ensures that the most significant risks are recognised and subsequently monitored as such, even when they are treated. This ensures that the effects of changes in treatment are readily identifiable.

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 should be used. 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.

Whatever method is used it is essential to use agreed definitions. When estimating likelihood or consequences these should be at the level of ‘most likely’, not the best or worst cases. 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. The Guide *Return on Security Investment* includes terms, definitions and values for likelihood, and consequences in sections 4.1 and 5.4.2.

Likelihood and consequences are combined to give a overall ‘Level of Risk’. Annex B provides a purely qualitative approach. The levels shown are not absolute, they will vary between agencies that have different acceptability of risk. Other examples are given and issues discussed in HB 436. Establishing preliminary risk levels is part of establishing agency context.

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.
- Delphi method.

Particular care must be taken when considering likelihood because of a possible tendency to pessimism. There are several reasons for this including liability considerations and an inclination to 'play safe'. Conversely there may also be a tendency to optimism, particularly with internal threats in smaller organisations. Where possible, the confidence placed on the assessments should be included. Using 'three-point' estimates - 'most likely', 'best case' and 'worst case' - aids understanding, reduces confusion and ambiguity, and enables quantitative methods.

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). Unusual and potentially serious risks may be included. For the latter type of risks, a detailed analysis of risks is conducted. This approach has the advantage of focussing attention and resources on those risks that are not well understood or serious.

High Level Risk Analysis

This component considers the business value 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 achieved via the information asset;
- The degree to which the agency capabilities depend on the information asset, ie whether critical functions are dependent on the confidentiality, integrity and availability of this asset; and
- The level of investment in an information asset, in terms of developing, maintaining or replacing the asset and its infrastructure.

If the business objectives supported by the asset are important to the conduct of the agency's business, recovery costs are high, or 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 capabilities or its assets, then a detailed risk analysis is necessary to identify suitable treatment options. Otherwise, a baseline approach to risk treatment usually provides appropriate protection. However, the baseline must be appropriate – applying a baseline designed for a high risk situation to a low risk one is not value for money and 'best practice' may also involve unnecessary safeguards.

Valuation of information assets (and possible consequences)

To assist in the identification of risks, the value and importance of the asset need to be understood. The key is understanding which information assets are depended on by an agency's most valued activities or those with the greatest public impact.

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 with the value and importance of the assets and the consequences of a security failure.

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.

Consideration of the possible consequences of asset security failures should be structured in a consistent manner. Annex B gives reasonably comprehensive approach to consequences. A simple approach uses the following dimensions for each of Confidentiality, Integrity, Availability:

Financial Impact	**Operational Impact**	**Public or Client Impact**	**Staff Impact**
Loss of revenue Loss of assets Legal liabilities Unbudgeted costs	Loss of capability Regulatory breach Failed activity Loss of control	Delayed service Adverse publicity Loss of reputation Injury or death Material damage	Loss of morale Lost productivity Injury or death

Depending on the nature of an agency's business other categories may be appropriate.

Clearly items in the columns other that Financial Impact may have financial implications. Avoiding these losses is a business benefit. 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.

All this highlights the existence of several types of value:

- Monetary value, typically associated with tangible assets, and reflecting replacement cost or depreciated value.
- Hidden value, may reflect the effort to create information or its market price, includes:
  - Sensitive information that needs to be kept confidential because its loss is damaging to the organisation, its clients or other stakeholders, including the fact of a loss damaging reputation.
  - Loss of information integrity undermines the reliability of information based services, it may result in lost revenue, higher than necessary operating costs, client dissatisfaction and legal action.
  - Loss of availability of information and processing facilities may curtail business activity, lose staff productivity, service delivery and revenue.
  - Rectification of security failures can have a pervasive nuisance value as staff and resources are diverted to myriad activities to make good the failure. It is particularly pernicious if the failure affects clients and they have to make good the consequences of the organisation's failure on them.
- Adversary or competitor value, 'common knowledge' or other intellectual property in one organisation may be valuable to another, particularly if they do not have a legitimate right to it or can use it to the detriment of owning organisation.

The assigned monetary value must be carefully determined because it may be the basis for determining the cost/benefit of protecting the asset.

When qualitative ratings are used they must be defined and their qualitative scale explained. Annex B provides examples.

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; or
- 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 identification of assets in terms of:

- their value relative to confidentiality, integrity, availability and recovery costs;
- for which baseline controls or protection is sufficient; and
- for which further analysis is required.

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. Supplement 1 of this Guideline provides examples of threats and vulnerabilities that may be used as a starting point. The list is by not exhaustive and threats are continually changing. A threat may originate internally or externally. The impact of a security incident may be temporary or permanent. Vulnerabilities may be in the physical environment, procedures, personnel, management, administration, hardware, software or communications.

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.

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

- source;
- value of unauthorised access;
- motivation, perceived capabilities and resources available;
- geographical factors for environmental threats; and

- frequency of occurrence.

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

Examples of typical vulnerabilities include:

- unprotected connections (for example to the Internet, wireless devices);
- processes for authenticating remote users;
- untrained users;
- inadequately trained ICT staff;
- wrong selection and use of passwords;
- ineffective access control (logical and or physical);
- incorrectly configured security safeguards;
- known software security defects not patched;
- ICT security information too widely available;
- no back-up copies of information or software; and
- location in areas susceptible to flooding.

Some threats and vulnerabilities may affect more than one information asset. They may cause different consequences depending on which assets are affected. For important assets in may be useful to develop risk trees to fully understand their risk exposure.

The result of this is a list of threats and vulnerabilities mapped to information assets, the likelihood and the consequences of the threat eventuating.

Risk Evaluation

This component involves comparing the analysed risks with the risk evaluation criteria developed in Step 1.

Evaluation must consider the effectiveness of existing safeguards in treating the likelihood and or consequences of the risks to information assets. In evaluating existing safeguards, various methods (including inspections and control self-assessment techniques) may be used to determine operational effectiveness. Weaknesses in existing safeguards may be due to out of date technology, inadequate management or procedures. A control may be treating several risks.

Once the risks have been evaluated a prioritised list of the risks for further action should be produced using the revised level of risk that reflects existing treatments. The purpose is to identify the risks that are acceptable and those that are not in accordance with the risk evaluation criteria.

A prioritised list:

- Gives an overview of the general level and pattern of risk with and without the existing information security safeguards.
- Focuses attention on the current higher risk items.
- Helps decide where action is most immediately needed and where the agency should develop plans for longer-term treatment.
- Identifies treated risks that require careful monitoring.
- Facilitates the allocation of resources to support any treatment decisions.

Reasons for accepting a risk include:

- The level of risk is so low that specific treatment is inappropriate within available resources.
- No treatment is available for the risk, for example, the risk is beyond the control of the agency.
- The cost of treating the risk including insurance costs, (particularly for lower ranked risks), outweighs the benefit.

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 consequences;
- a list of threats, vulnerabilities and exposures mapped to the information assets, together with the likelihood and the consequences of the threat occurring in a stated timeframe; and
- a prioritised list of risks for determining risk acceptability.

Step 3 – Identify Treatment Options

The outputs of this Step are documented options for treating risks and associated security architecture down to the logical layer.

Organisations must manage risks and safeguard their operations to protect their information assets effectively. Assessing whether the security of information is appropriate includes acknowledging that most risks cannot be avoided completely and there will always be some residual risk.

Risks that have been assessed as unacceptable should be treated in order to make them acceptable. In some cases it may only be possible or practical to mitigate the consequences of a risk. Constraints that may influence how to manage a risk include:

- Organisational.
- Financial.
- Personnel.
- Time.
- Legal and jurisdictional.
- Technical.

Risk treatment may include any or a combination of the following options:

- Risk avoidance – by deciding not to become involved with or to withdraw from a situation or activity that places information assets at risk.
- Reduce the likelihood – by implementing safeguards that deter or prevent the threats and or reduce vulnerabilities affecting information assets.
- Reduce the consequences – by implementing safeguards to mitigate the threat’s impact by reducing the information assets exposed to the threat or by treating the aftermath if the threat eventuates.
- Risk sharing – by arranging another party to bear part of the risk, eg insurers.
- Risk retention – the agency will accept all or part of a particular risk.

At the logical layer a security architecture normally comprises one or more security domains. A security domain refers to an area of the same or similar security requirements and safeguards, 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.

Documentation

The output from this step is a list of possible treatment options for the unacceptable risks identified in Step 2. The Policy created in Stage 1 should also be reviewed and modified or enhanced as necessary to guide the selection of safeguards and add any matters that are best handled as Policy. Residual (acceptable) risks must also be documented, some may become controlled because many safeguards are broad spectrum, but residual risks must be approved, Step 6.

Step 4 – Assess and Select Safeguards

The output of this Step is a proposed Risk Treatment Plan and physical layer of the security architecture.

Safeguards must be selected taking into account the agency's business objectives, security architecture, and priorities with the resources available. It is unlikely that any one of the above mentioned risk treatment options by itself would provide the complete solution for a particular risk.

Appropriate safeguards to reduce the assessed risks to an acceptable level should be identified and selected with life-cycle cost/benefit justification. The general principle is that the cost of implementing and operating a safeguard should be no greater that the cost of the consequences. The *Return on Security Investment model* provides a method for assessing the cost/benefit of safeguards. The output of this step is a draft Risk Treatment Plan and the physical layer of the security architecture, possibly extending into the component layer.

Safeguards should be selected with reference to the control objectives provided in ISO 27002. This divides safeguards into the 11 categories shown in Figure 7. Note that the first 4 categories in red will always be applicable and the numbers in brackets refer to the number of control objectives and safeguards in each category.

Safeguards are implemented via operating policies that establish operational safeguards, and by technology. When authentication is involved then selection should be informed by the Australian Government Authentication Framework (AGAF).

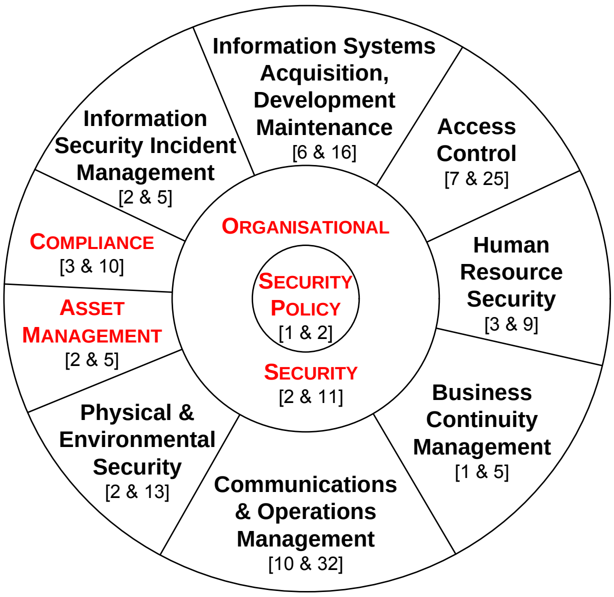

Information Systems Acquisition, Development Maintenance [6 & 16]
Access Control [7 & 25]
Human Resource Security [3 & 9]
Business Continuity Management [1 & 5]
Communications & Operations Management [10 & 32]
Physical & Environmental Security [2 & 13]
Asset Management [2 & 5]
Compliance [3 & 10]
Information Security Incident Management [2 & 5]
Organisational Security [2 & 11]
Security Policy [1 & 2]

Figure 7 – Security Control Categories

Existing and planned safeguards must be taken into account. Existing safeguards should be checked to ensure that are working effectively if this was not done during evaluation. The vulnerabilities or exposures to the threat indicate where additional safeguards may be required and the form it should take. Key questions in treating risks are:

- Can existing safeguards be improved to reduce risk to an acceptable level?
- Are new or replacement safeguards needed to reduce risk to an acceptable level?
- Can new safeguards replace existing safeguards for lower costs?
- Are the safeguards cost effective – are their life cycle costs less than the product of the probability of the risk and the cost of its untreated consequences?
- What resources are needed (people, funds, equipment)?
- Who has responsibility and accountability for treating and managing the risk?

It is useful to identify the function of the safeguard. Many safeguards can serve several functions and contribute to two or more control objectives. Often it is more cost effective to select safeguards that can serve multiple functions. A well designed security architecture provides diversity and defence in depth by using safeguards providing a mixture of functions:

Deter: Prevent or reduce the likelihood of an undesirable security event being attempted.

Avoid: Eliminate known vulnerabilities and prevent new ones being created.

Protect: Safeguard information assets with vulnerabilities or exposures from adverse security events.

Detect: Identify the occurrence of a security event and initiate protective, reactive or recovery safeguards.

React: Respond to or counter a security event to minimize its impact and ensure business continuity.

Recover: Restore the integrity, availability and confidentiality of information assets to their expected state.

The first three deal with the likelihood of an event and the last two deal with its consequences. Annex A to Supplement 2 of this Guideline tabulates types of safeguard to these functions.

Baseline Approach

A baseline approach to risk treatment requires the establishment of a minimum set of safeguards to safeguard all or some of the agency's information against the most common threats. The baseline used must reflect agency security policy. It should normally be part of the logical layer of the security architecture but sometimes a physical layer baseline may be applicable. These baseline safeguards are compared with existing ones. 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 safeguards against an appropriate and justifiable baseline. This may be the applicable safeguards from ISO 27001.

The benefit of the baseline approach is a simplified risk assessment. The risks in using a baseline are that:

- there may be unidentified assets, 'non-standard' threats or vulnerabilities that are missed by gap analysis and or baseline safeguards;
- the baseline is used unthinkingly as a checklist and or substitute for all risk management;
- 'standard' baselines may be excessive for the security risk exposure, they may be unnecessarily costly to acquire and operate; and or
- where there is a choice of baseline 'level' lack of risk assessment leads to using an unnecessarily 'strong' and costly baseline.

Lack of an Information Security Policy exacerbates these risks. A baseline must not be adopted by an agency without ensuring that it is appropriate to the agency's risk profile and circumstances. When there are doubts about the relevance of a baseline control then a simple risk assessment should be made.

The level of baseline security must be adjusted to suit the needs of the agency. Supplement 2 of this Guideline provides a sample of baseline safeguards. ACSI 33 also provides useful guidance.

Some agencies may be contractually obliged to adopt the baseline required by the Payment Card Industry Data Security Standard (PCI DSS). This standard applies to on-line services incorporating payment card transactions and supporting infrastructure. The standard is set by Visa and Mastercard and can be mapped to ISO 27001.

Operational and Technical Safeguards

Control selection should always include a balance of operational (non-technical) and technical safeguards. Operational safeguards include physical, personnel, and administrative, procedural or behavioural security safeguards, typically they are polices requiring adherence. These safeguards include:

Physical Security

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

Personnel Security

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

Procedural Security

Procedural security includes operating procedures, application development and acceptance procedures as well as procedures for incident handling. It may include change management. It also encompasses procedures for business continuity, including contingency planning and or disaster recovery plans as well as crisis management.

Technical Security

Technical security encompasses hardware, software and communications safeguards. It may include: identification and authentication, logical access control, audit trail/security logging, dial-back security, message authentication, encryption and digital signatures, network firewalls, network monitoring and analysis, anti-virus software and intruder prevention and detection.

Evaluated Products and Systems

An organisation may acquire products or systems that have been independently examined or evaluated. The evaluation should be against an appropriate protection profile for the system or product and the threats to it. Evaluated products or systems provide confidence that implemented functionality meets requirements and the implementation is correct and complete. The Common Criteria are the preferred basis for evaluation, however, the protection profile and evaluation assurance level must be appropriate to the agency's risks.

Factors Influencing Safeguard Selection

Factors for consideration when selecting safeguards for implementation, in addition to cost and benefit, include:

- ease of use of safeguards;
- transparency to the user,
- proximity of the control to the asset being protected;
- the help provided to the users to perform their activities;
- compatibility and complementarity with existing safeguards;
- integration with overall security management tools;
- the relative strength of the safeguards;
- protection profile and evaluation assurance level;
- the types of functions performed – deterrence, protection, detection, response, recovery; and
- return on investment.

Constraints that Affect the Selection of Safeguards

Constraints must be taken into account when making recommendations and during the implementation.

Time Constraints

Time constraints include:

- Implementing safeguards in a time period that is acceptable to management.

- Whether safeguards can be implemented within the lifetime of the system.
- The length of time that management decides is acceptable to have information exposed to a particular risk.

Financial Constraints

Agencies have many conflicting demands on their financial resources. 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 additional funds become available. If management is not prepared to accept risks then they must change financial priorities.

Technical Constraints

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

Sociological Constraints

Sociological or organisation culture constraints to the selection of safeguards may be department or branch specific within an agency. They cannot be ignored because many technical and operational safeguards rely on the active support of the staff. If the staff do not find a control culturally acceptable, it is likely that it will become ineffective. It is almost certain that if staff find that a control unacceptably hinders their work then they will develop short-cuts and or work-arounds. This situation will be exacerbated if they do not understand the need for the safeguard and may be encouraged by low-level management.

Environmental Constraints

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

Legal Constraints

At least four legal factors influence information security for NSW Government agencies in terms of risk exposure and selecting safeguards:

- *Privacy and Personal Information Protection Act*
- *State Records Act*
- *Workplace Surveillance Act*
- Commonwealth legislation concerning intellectual property rights.

Other laws and regulations covering fire, workplace relations, codes of conduct, and occupational health and safety could also affect control selection. If the sources of threats are likely to be in the local jurisdiction then safeguards that facilitate prosecution may have worthwhile deterrent effects.

Contractual obligations may also exist. Agencies handling national security information are likely to be bound by MoU. Those handling credit card payments by PCI-DSS.

People and Skill Constraints

Some safeguards may require specialist skills to implement or operate them. Safeguards may not be operated correctly if people with the necessary skills and competencies are not available.

Documentation

The result of this Step and the end of the Planning phase of the PDCA cycle is a security Risk Treatment Plan. When approved it is the plan for how the agency will manage its information security, it is a program plan. The plan may be used to derive business case(s) for enhanced or new safeguards and will also provide inputs to any project plans for specific security implementation projects.

The Risk Treatment Plan is based on the information security policy, the results of the risk assessment and reflects management's acceptance of risk. It should ensure that any new or changed safeguards are implemented, in accordance with the priorities established within short, medium and long timeframes. The plan may be in parts to reflect the sensitivity of its details. It should include:

- the security objectives in terms of confidentiality, integrity and availability of information;
- summarised results of risk assessment including the designated owners of each risk;
- a security architecture;
- a list of required safeguards, including existing and planned safeguards with an estimate of their effectiveness, this list should include priorities;
- a mapping of the contribution of safeguards to managing risks;
- a protection profile to enable selection of evaluated products and any system security evaluations;
- an appraisal of the residual risks accepted after implementing the safeguards;
- a schedule or annual calendar for actions to maintain the ISMS;
- the estimation of the life-cycle costs (from acquisition to disposal, and reflecting the Plan – Do – Check - Act cycle) for new safeguards and operating costs for existing safeguards;
- implementation details, including:
  - priorities,
  - a schedule reflecting the priorities,
  - the budget needed,
  - responsibilities and accountability for treating risks; and
- the security awareness and training arrangements for staff and end users which are needed to ensure the effectiveness of the safeguards.

In addition procedures will be required for ISMS performance monitoring and reporting, including against the risk treatment plan.

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.

Step 5 – Management Approval

The output of this Step is an approved Risk Treatment Plan.

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

5.4 Prepare Statement of Applicability

When the ISMS is going to be certified to ISO 27001 then a Statement of Applicability (SoA) is essential. However, it is also extremely useful for any ISMS. The usual approach to a SoA is a tabular structure to reflect Annex A of ISO 27001, it also needs to cover Chapters 4 – 7 of the standard. Typically, the SoA tabulates the control objectives and safeguards and:

- cross references safeguards to identified risks;
- briefly explains why safeguards are applicable or not,
  - with greater explanation where the choice is complex or has a significant impact on risks,
  - record reasons why any of the safeguards specified in ISO 27001 are not been implemented; and
- summarises the treatments being used for each applicable control.

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. It is important to note that certification of compliance does not require that the Risk Treatment Plan is fully implemented.

Chapter 6: Stage 3 - Implementing and Operating

ISO/IEC 27001:2005	***4.2.2 Implement & operate the ISMS, b) Implement the risk treatment plan, c) Implement controls to meet control objectives, d) Define how to measure control effectiveness, e) Implement training and awareness programmes, f) Manage operations, g) Manage resources, h) Implement procedures & other controls.*** ***4.3 Documentation requirements.*** ***5.2.1 Provision of resources.*** ***5.2.2 Training, awareness & competence.*** ***6 Internal ISMS audits.***

6.1 Overview

Do (implement and operate the ISMS) – Implement and operate the security policy, safeguards, processes and procedures.

During this Stage the initial task is to implement selected safeguards in accordance with the Risk Treatment Plan and the higher layers of the security architecture. It also defines and applies the component layer of a security architecture. It will include:

- Training staff to implement safeguards.
- Designing processes, developing and deploying operating policies, procedures and instructions.
- Providing training and inculcating awareness to ensure the required security behaviour (including compliance with procedures and instructions) by information users and system operators.
- Acquiring (if necessary) and configuring technology in accordance with operating policies and procedures.

Implementing an ISMS is a boot-strapping change management task. Depending on the extent of the tasks it will be managed as a project or as a program of several projects.

Operation of the ISMS will occur with the progressive deployment of safeguards. During this activity issues will emerge and be handled and documented in accordance with the ISMS procedures. As implementation progresses operation will become increasingly routine as the safeguards and operational management of the ISMS become established and institutionalised.

An important aspect of operating the ISMS is incident handling, which implies that incidents are detected. Monitoring is covered in the next Stage. Operating the ISMS also includes routine activities such as access management, training and awareness development activities, and any other routine procedures for operating specific safeguards.

6.2 Implementation of the Risk Treatment Plan

The Risk Treatment Plan was produced from the information and documents created during the planning phase (previous sections). The correct implementation of safeguards relies on a well-structured and documented Risk Treatment Plan approved by executive management.

Implementing the risk treatment plan must include arrangements to measure the effectiveness, the extent to which objectives are achieved, of the ISMS. This is covered in more detail in Section 7.2 Monitoring and review.

In addition to the Risk Treatment Plan day-to-day management of the ISMS is also required. Particular attention must be given adherence to operating policies and other safeguards, and to handling security incidents or issues.

A senior manager should be given responsibility for the implementation of the Risk Treatment 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.

The design and implementation of safeguards for a new information system should be undertaken concurrently with the implementation of that system. Retroactive implementation of security, once a new system is operational, may be difficult, expensive and less effective.

6.3 Operating the ISMS

Operating the ISMS means handling day-to-day issues. Most of these will be in accordance with operating policies. It applies the operational layer of a security architecture. Operating the ISMS includes properly documenting events, decisions and actions.

ISO/IEC 27001:2005	***A.8.2.1***	***Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation.***

However, two significant matters are information security training and incident handling. The latter may lead to urgent corrective changes to the ISMS.

Information Security Training

ISO/IEC 27001:2005	***A.8.2.2***	***All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant to their job function.***

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 safeguards are necessary and are able to use them correctly. New staff will require induction training and all staff will need periodic refresher training.

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 and availability;
- 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, operating policies, 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 actual and attempted breaches of security;
- procedures, responsibilities and job descriptions;
- the consequences if staff are responsible for security breaches; and
- procedures related to security compliance checking.

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;
- staff that are remote or mobile users,
- contractors, temporary staff and vendors who access agency information and information systems
- the responsibilities of all staff as information users; and
- personnel with information security administration responsibilities, eg, for access control, directory management or manual records management.

The information security training program should emphasise the need for balance between non-technical and technical safeguards. Most importantly it must cover appropriate behaviours by all staff including identifying and dealing with social engineering attempts, security incidents and their role in business continuity management. Training should include both induction training and periodic refresher training.

Incident Management

No information security system works perfectly all the time. Sometimes there are positive and negative events. Some events will be security incidents - they have a significant probability of compromising business operations and threatening information security. These events must be documented and analysed to determine their effects and what changes or corrective actions may be necessary. Security events and incidents should be documented in accordance with Annexes A and B to ISO/IEC TR 18044:2004 *Information technology – Security techniques – Information security incident management*.

ISO/IEC 27001:2005	***A.13.2.1***	***Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.***
ISO/IEC 27001:2005	***A.13.1.2***	***All employees contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.***

Administrative procedures must be established to ensure that when possible security events are detected they are promptly reported and investigated. These procedures must reflect government and agency policies. Organisationally they may include having staff designated and trained as an Information Security Incident Response Team and external experts available ‘at call’. However, it is also important to ensure that evidence is preserved so all staff need to know to leave investigation to the experts. Staff being able to recognise the symptoms of a security event and knowing what to do (and not do) are key matters for security awareness and training.

ISO/IEC 27001:2005	***A.13.1.1***	***Information security events shall be reported through appropriate management channels as quickly as possible.***

Investigation requires forensic procedures for collecting evidence and maintaining the chain of evidence in case there is a subsequent prosecution. HB 171 provides guidance on forensic procedures and ISO TR 18044 provides comprehensive advice and guidance, and applies the PDCA cycle to security incident management. In addition:

- conditions leading to the breach will be rectified;
- recovery action will be taken promptly; and
- disciplinary action may be taken.

ISO/IEC 27001:2005	***A.8.2.3***	***There shall be a formal disciplinary process for employees who have committed a security breach.***
ISO/IEC 27001:2005	***A.13.2.3***	***Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).***

Some incidents may lead to a review and reassessment of the security safeguards leading to improvements.

ISO/IEC 27001:2005	***A.13.2.2***	***There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.***

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 groups such as computer emergency response teams.

Other key aspects that should be addressed include:

- using a standard system for classifying security incidents, ISO TR 18044 Annex A;
- establishing incident management plans; and
- training nominated staff as an Information Security Incident Response Team.

Incident management plans should include:

- preparation - incident handling guidelines and procedures, forensic arrangements, 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-establishing normal service; and
- review - the procedures and responsibilities for post-incident actions, including investigation of legal implications and trend analysis.

6.4 Consultation and Communication

While training is pre-eminently a communication activity other consultation and communication continues throughout the implementation stage. It is particularly important because issues will emerge that have to be resolved promptly. Furthermore the design of policies and processes and the development of procedures and instructions will require consultation with stakeholders.

Chapter 7: Stage 4 - Monitoring and Improving the ISMS

ISO/IEC 27001:2005	***4.2.3 Monitor & review the ISMS.*** ***4.2.4 Maintain & improve the ISMS.*** ***4.3 Documentation requirements.*** ***5.2.1 Provision of resources.*** ***5.2.2 Training, awareness & competence.*** ***6 Internal ISMS audits.*** ***7 Management review of the ISMS.***

7.1 Overview

Check (monitor and review the ISMS) - Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the result to management for review.
Act (maintain and improve the ISMS) – Take corrective and preventative actions, based on the results of the management review, to achieve continual improvement of the ISMS.

An ISMS requires continuous modification and improvement. Threats, business activities, ICT systems and infrastructure, vulnerabilities and exposures all change. In particular attackers thwarted by safeguards will look for different vulnerabilities. Lessons will be learned from security incidents. Policies and treatments must be kept under review. The ISMS, its documentation and performance against policies and plans must be measured and audited. This Stage reflects the operational layer of a security architecture.

Implemented safeguards 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 tendency for the performance of the ISMS to deteriorate if there is no follow-up.

Executive management and boards have a responsibility to monitor conformance to policies and performance against plans as part of their Direct → Monitor → Evaluate cycle for ICT governance. This assesses the ISMS' effectiveness.

7.2 Monitoring and Review

The purpose of monitoring and review is to assess the extent to which ISMS objectives are being achieved, its effectiveness. Monitoring captures data and information for analysis. There are two types of monitoring and review:

- periodic verification and validation against objectives and the Risk Treatment Plan; and
- continuous operational monitoring and review.

The purpose of verification and validation is to ensure that safeguards are:

- appropriate for the actual risks to the information assets (Validation against and of objectives); and
- are operating properly and being complied with (Verification against the Risk Treatment Plan and ISMS policies).

Operational monitoring and review focuses on what is happening in and to the ISMS and requires application of the intelligence cycle. It includes external monitoring of emerging threats and security trends. This informs validation and may lead to adjustments in verification activities.

Continuous monitoring is also part of the feedback control loop for managing the day-to-day operation of the ISMS. This may lead to routine maintenance action. Two key components in security monitoring are:

- analysis of information security incidents; and
- measuring the effectiveness of security controls for verification purposes.

Effective and efficient monitoring requires appropriate metrics to monitor ISMS performance trends over time. Some metrics will be used to monitor technical functioning but meaningful business oriented reports are required for executive reporting. Metrics should provide comparisons to performance targets.

ISO/IEC 27001:2005	***A.15.3.1***	***Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruption to business processes.***
ISO/IEC 27001:2005	***A.10.10.1***	***Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.***
ISO/IEC 27001:2005	***A.10.10.2***	***Procedures for monitoring the use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.***
ISO/IEC 27001:2005	***A.10.10.4***	***System administrator and system operator activities shall be logged.***
ISO/IEC 27001:2005	***A.10.10.5***	***Faults shall be logged, analysed, and appropriate action taken.***
ISO/IEC 27001:2005	***A.15.3.2***	***Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.***
ISO/IEC 27001:2005	***A.10.10.3***	***Logging facilities and log information shall be protected against tampering and unauthorised access.***

ISMS Validation

Validation considers new or changed threats, vulnerabilities and consequences. It answers the question '*Is the ISMS using the appropriate safeguards?*' It means reviewing risk identification, analysis and evaluation, including residual and accepted risks.

Changes to risks may have internal or external sources. Sources include changes to:

- information assets and their supporting technology;
- business objectives, processes, organisation and structure;
- the legal, regulatory, operational, social or physical environment; and
- threat capabilities.

Metrics and lessons from ISMS verification may provide indicators of changing risks.

Formal validation takes place annually, it should be timed to feed in to the budgetary cycle. The schedule should be established in the annual security management calendar.

ISMS Verification

Verification focuses on the operation of the ISMS and its implemented safeguards safeguarding information assets. It involves examination of safeguards of all types and analysis of the results. It answers the question '*Is the ISMS operating as it should?*', an implicit objective, and has three aspects:

- measuring compliance with operating policies (ie processes, procedures, instructions, etc);
- providing functional and physical configuration audits of safeguards; and
- appraising the efficacy of the operating policies and other types of control in achieving the overall security objectives.

ISO/IEC 27001:2005	***A.15.2.1***	***Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security implementation standards..***
ISO/IEC 27001:2005	***A.15.2.2***	***Information systems shall be regularly checked for compliance with security implementation standards.***

Verification includes measures that are periodic or continuous, routine or exceptional, and active or passive. In all cases they should capture metrics. Some verification measures must be implemented when the ISMS is initially implemented, for others it is better to gain experience of the ISMS operation before establishing verification needs:

- Periodic measures are usually active and routine, and should be established by the annual security management calendar.
- Continuous measures are usually routine and passive, when possible they should be automated and provide exception reporting and metrics.
- Active checking takes the form of tests and inspections, and practicing procedures that would react to events.
- Exceptional measures will usually be active and in response to a security incident or change in circumstances.

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); and
- 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 safeguards protecting the information system may be checked by:

- practising contingency plans;
- examining log files;
- auditing actual against documented configuration of individual hardware and software items;
- monitoring operational performance against actual incidents occurring; and
- conducting spot checks or tests for weaknesses in particular areas of sensitivity or concern.

Compliance checking should be based on the agreed safeguards lists from the risk treatment plan and security operating policies created in accordance with the plan. One approach to grading the effectiveness of controls in treating risks, which can also be used for existing controls when establishing an ISMS, is shown below.

Effective	• Controls are effectively reducing risk(s), and • are operating as required in all material respects.
Improvement Required	• Controls are reducing some risk(s), and • are operating as required in most material respects.
Ineffective	• Controls are not in place for the risk(s), or • are not operating as required.
Not applicable | Not required	• There are no appropriate controls that can be used, or • the inherent risk(s) are low and controls cannot be cost justified, or • compensating controls exist.

Compliance with policies will also be the subject of audits. These may include internal audit, performance audit by external authorities and surveillance audits if the ISMS is certified to ISO 27001.

Operational Monitoring - Intelligence Cycle

Aimless monitoring is ineffective and inefficient; monitoring must focus on identifying matters that are relevant to the business and its ISMS. When relevant issues are identified they can be reviewed and decisions taken about any changes that are needed to the ISMS. Application of the intelligence cycle ensures focussed monitoring and effective review. The cycle, Figure 8, operates continuously and all four stages may occur simultaneously.

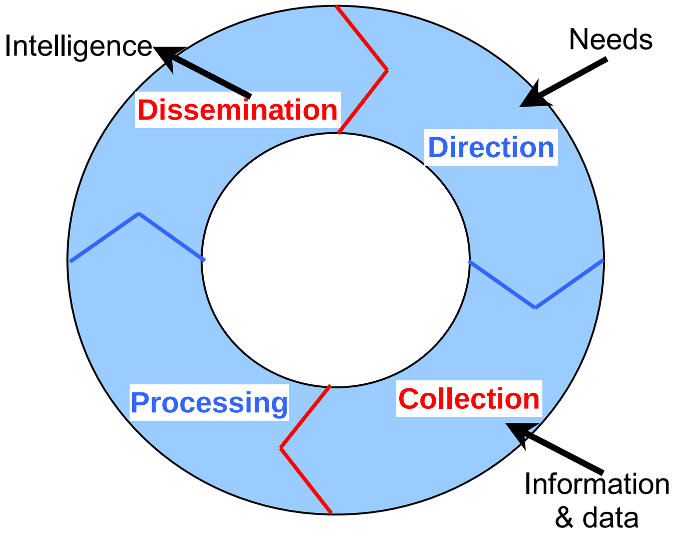


Figure 8 – The Intelligence Cycle

- Direction is a management responsibility that determines what intelligence is needed to operate and maintain the ISMS to safeguard information assets. It implies committing resources to collecting and processing information and metrics. Direction will reflect the identified risk exposure, possible emerging threats and the key indicators needed to verify the ISMS. It will identify the possible sources of information and metrics needed to produce the required intelligence.
- Collection is the activity of gathering information from external and internal sources. The former includes security advisories and newsletters, the latter log files and incident reports. Both include metrics.
- Processing is analytical activity that converts information and metrics into intelligence. It comprises three main steps:
  - Collation – filtering and sorting information including deciding what is potentially relevant to needs.
  - Evaluation – determining the quality, relevance and potential significance of the information and identifying links with other information.
  - Interpretation – in essence any changes to existing risk identification and assessment and the potential impact on the business and the ISMS.
- Dissemination delivers the intelligence to the decision makers, who decide whether or not to act on it and change the ISMS. The pre-cursor of effective dissemination is to render the intelligence into a form that is appropriate to and usable by its intended audience. This may include an updated risk register.

New, unforeseen or changed threats, vulnerabilities, and consequences that adversely affect the agency could appear at any time. These may reveal themselves in major security incidents that demonstrate that the ISMS is not providing appropriate safeguards. The ISMS will need contingency arrangements to cope with this situation.

7.3 Maintenance and Improvement

Most safeguards will require maintenance to ensure that they continue to function correctly and meet evolving risks. Maintenance is continuous improvement to the ISMS. The need for maintenance and improvement will be driven by:

- lessons learned from security incidents;
- operational monitoring identifying changing risks that necessitate immediate action;
- validation and verification of the ISMS; and
- upgrades and patches to and supportability of the technology used by ISMS safeguards.

Maintenance will involve corrective, preventative, adaptive and perfective changes to the ISMS.

- Corrective changes arise from non-conformities found during verification and from flaws identified after security incidents.
- Preventative changes arise from formal validation and identification of changing risks. The latter may come from continuous monitoring.
- Adaptive changes are needed when there are removed, new or enhanced information assets. For major changes that involve the purchase of new hardware, software or service, an analysis may be necessary to determine the new security requirements.
- Perfective changes reflect continuous improvements to the efficiency of the ISMS.

It is important to determine the impact of ISMS changes. On the other hand, many changes are minor in nature and may not require extensive analysis. The whole-life costs and benefits of any change must be considered and a business case prepared. This should include an analysis of the security return on investment that considers the cost of safeguards against avoidable loss expectancy.

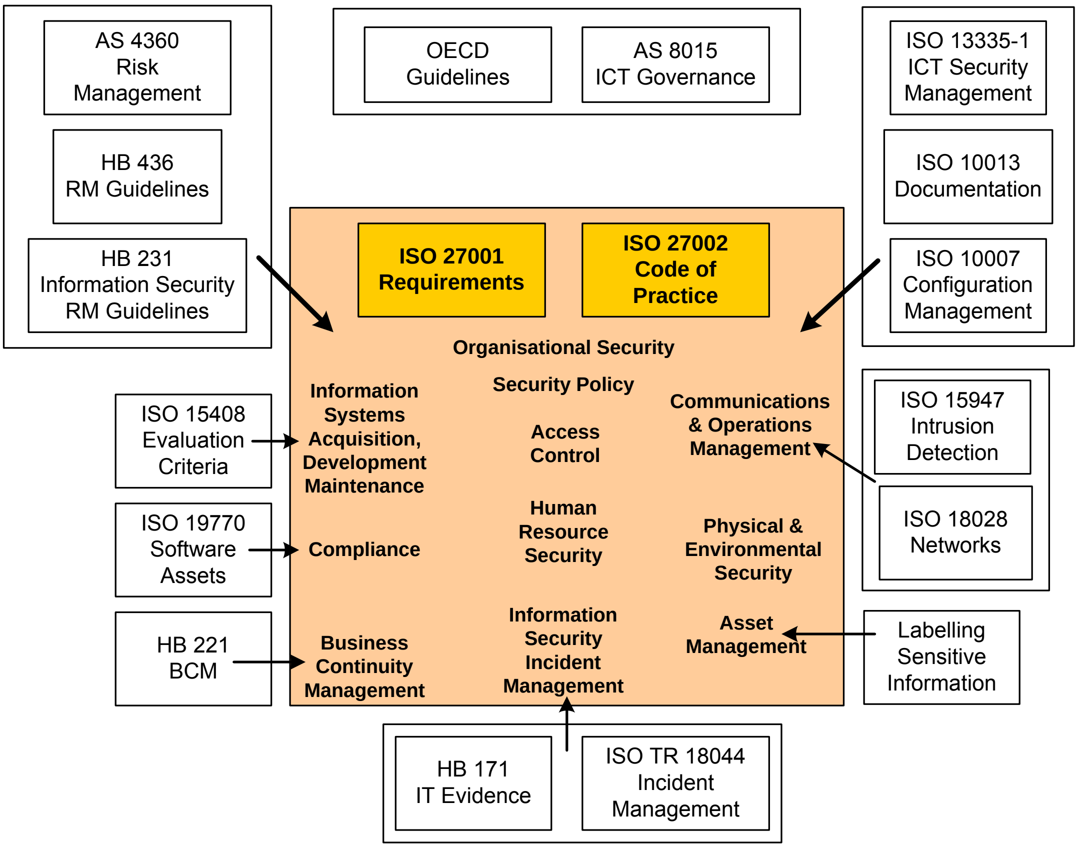
All modifications will require changes to documentation, which must be under formal configuration management. Furthermore some changes will necessitate changes to security training.

7.4 Consultation and Communication

Validation and verification will require consultation and communication with stakeholders.

Annex A - Standards

The following figure shows the main standards that apply to an ISMS and support the 11 control categories.


AS 4360 Risk Management
HB 436 RM Guidelines
HB 231 Information Security RM Guidelines
OECD Guidelines
AS 8015 ICT Governance
ISO 13335-1 ICT Security Management
ISO 10013 Documentation
ISO 10007 Configuration Management
ISO 27001 Requirements
ISO 27002 Code of Practice
Organisational Security
Security Policy
Information Systems Acquisition, Development Maintenance
Access Control
Communications & Operations Management
Human Resource Security
Compliance
Physical & Environmental Security
Business Continuity Management
Information Security Incident Management
Asset Management
ISO 15408 Evaluation Criteria
ISO 19770 Software Assets
HB 221 BCM
ISO 15947 Intrusion Detection
ISO 18028 Networks
Labelling Sensitive Information
HB 171 IT Evidence
ISO TR 18044 Incident Management

Standards and Guides in Figure

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

AS 8015:2005 - Corporate governance of information and communication technology

AS/NZS ISO/IEC 27001:2006 - Information technology – Security techniques – Information security management systems - Requirements. (Identical to ISO/IEC 27001:2005)

AS/NZS ISO/IEC 27002:2007 - Information technology – Security techniques - Code of practice for information security management. (Identical to ISO/IEC 17799:2005)

AS/NZS 4360:2004 - Risk management.

HB 436:2004 - Risk management guidelines.

HB 231:2004 - Information security risk management guidelines.

ISO/IEC 13335-1:2004 - Information technology.- Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

AS ISO 10007:2003 - Quality management systems – Guidelines for configuration management.

AS ISO 10013:2003 - Guidelines for quality management system documentation.

ISO/IEC 15947:2004 - Information technology – Security techniques – IT intrusion detection framework.

ISO/IEC 18028 - Information technology – Security techniques – IT network security. Part 3 – Securing communications between networks using security gateways: 2005. - Part 4 Securing remote access: 2005.

Premier's Circular 2002-69 '*Guide to Labelling Sensitive Information*'.

ISO/IEC TR 18044:2004 - Information technology – Security techniques – Information security incident management.

HB 171:2003 - Guidelines for the Management of IT Evidence.

HB 221:2003 - Business continuity management.

ISO/IEC 15408-1:2005 - Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model; – Part 2: Security functional requirements; – Part 3: Security assurance requirements.

ISO/IEC 19770-1:2006 - Information technology – Software asset management – Part 1: Processes.

NSW Government Publications

22 minute video '*I wish [it wasn't] me*' provides a training resource for user awareness training. It is supported by material for facilitators.

'*Executive Guide to Electronic Information Security*' provides guidance on executive management responsibilities and is written for that audience.

'*Return on Security Investment*' provides a model for calculating ROI.

Other Relevant Standards and Guides

AS 13335-3:2003 - Information technology—Guidelines for the management of IT Security, Part 3: Techniques for the management of IT Security.

AS 13335-4:2003 - Information technology—Guidelines for the management of IT Security, Part 4: Selection of safeguards.

AS 13335-5:2003 - Information technology-Guidelines for the management of IT Security, Part 5: Management guidance on network security.

AS 3806:1998 - Compliance programs.

BS 25999-1:2006 – Code of Practice for Business Continuity Management.

ACSI 33 - Security Guidelines for Australian Government IT Systems, Defence Signals Directorate, March 2004.

Commonwealth Protective Security Manual - Attorney General's Department, Commonwealth of Australia, 2005.

Australian Government e-Authentication Framework (AGAF) - Department of Finance and Administration, Commonwealth of Australia, 2005.

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.

Information Security Forum - http://www.securityforum.org - The Standard of Good Practice for Information Security, 2005.

Annex B – Risk Assessment

This Annex provides a standard method of categorising security risks, risks being the likelihood of a security incident and its consequences. The key to managing information security risks in an agency is to understand the agency's information assets and their 'business' significance.

- An information asset has a business owner, business purpose and business value.
- Asset significance includes its legitimate and illegitimate 'value' as well as its importance to the business and the business and wider consequences of a security incident.

The criteria and definitions used with likelihood and consequences are derived from several sources and are provided as reasonably balanced examples. Actual definitions used by agencies will reflect their appetite for risk, which in turn will affect the cost of security controls.

Identifying risks

Identifying risks means recognising scenarios where threats may affect assets. This involves considering threats in terms of the impact on assets, assets in terms of their vulnerabilities and threats to them, and security objectives relevant to assets.

- Risks should be initially identified as if there were no security measures in place, this is the 'inherent risk'. Understanding these untreated risks facilitates risk management throughout the life of the system.
- Risks should be explored to understand their causes, the extent of affected information assets and possible consequences.
- Identified risks should be expressed in the form of a triplet: Cause → Event → Consequences, merely assigning a name to a risk is totally insufficient. Consequences should be expressed in a manner that reveals the affected security objectives.
- Risks should be classified according to their business consequences, the consequences table below gives a comprehensive approach to consequence categories.

Determining expected likelihood

Once inherent risks have been properly identified then their likelihood of eventuating can be analysed. Once the inherent likelihood is understood, then likelihood can be re-assessed taking into account any existing security measures that may provide risk treatment. The criteria below are derived from US NIST's model and reflect timescales that are relevant to the life of ICT systems.

The following table identifies 5 levels for the likelihood for any security event that may affect any information asset. To use the table, start at the left (Improbable) column and ask if the envisaged security event is likely to occur in the indicative frequency period. If the answer is 'Yes' then ask the same question for the next column to the right, when the answer is 'No' the likelihood is that in the previous column. In making this judgement the perspective of 'most likely' level should be used, not 'worst case' or 'best case'. Changing the definitions and frequencies provides a way to reflect the risk appetite of an agency.

	LIKELIHOOD				
	Improbable	**Remote**	**Occasional**	**Probable**	**Frequent**
Definition	Practically impossible	Not expected to occur	May occur	Isolated incidents	Repeated incidents
Indicative frequency	In any time frame	In a 10 year period	In a 5 year period	In a 3 year period	In a year

Determining possible unacceptable consequences

Once inherent risks have been properly identified then their consequences can be analysed. Once the inherent consequences are understood, then consequences can be re-assessed taking into account any existing security measures that may provide risk treatment.

The following table identifies 7 possible types (left hand column) for the consequences of a security event that may affect an information asset. For each type it then identifies and defines 5 levels of severity for the consequences. A security event affecting a single information asset may result in more than one type of consequence. Changing definitions provides a means for an agency to tailor the table to reflect to reflect their own risk appetite.

The table is used to determine the severity of a risk. In making this judgement the perspective of 'most likely' level should be used, not 'worst case' or 'best case'. Critical means: decisive, vital, essential, life-threatening, ruinous. Significant means: important, major, notable.

TYPE OF CONSEQUENCE	EXPLANATION	SEVERITY				
		Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Loss of financial or material assets by agency or public	May include losses through theft or fraud, rectification costs, legal liabilities, other unbudgeted costs or lost entitlements. Losses will usually be a consequence of a failure in information integrity but failures in confidentiality or availability may create opportunities for loss.	Minimal financial loss to any party.	Insignificant financial loss to any party.	Significant financial loss to any party or loss of lesser irreplaceable assets.	Very significant financial loss to any party or loss of important irreplaceable assets.	Critical financial loss to any party or loss of highly valued irreplaceable assets.
Injury or death of public or staff	Could be the result of confidentiality, integrity or availability failures. If the consequences are a direct result of an ICT failure (eg in a real-time control system) then that system is 'safety critical' and appropriate methods must be applied to it.	No injury to any person.	Injuries requiring first aid to a few people.	Injuries requiring treatment at a medical facility.	Injuries necessitating hospitalisation.	Live threatening injuries or death.
Inconvenience or distress to public or staff	May be a direct or secondary consequence of an event, eg even temporary financial loss may cause inconvenience and distress. Could be the	Minimal discernable inconvenience or distress to any	Insignificant inconvenience or distress to a few people.	Inconvenience or distress to many people.	Significant and extensive inconvenience or distress.	Very significant and pervasive inconvenience or distress.

	result of confidentiality, integrity or availability failures.	person.				
Damage to standing or reputation of the Government, an agency or person	Includes the confidence or morale of stakeholders in a service or agency. It may be lost by confidentiality, integrity or availability failures. Treatments may include publicity campaigns to rebuild reputation or confidence and these have financial costs.	Minimal damage to any party's standing or reputation, or loss of stakeholder confidence.	Insignificant damage to any party's standing or reputation, or limited loss of stakeholder confidence.	Damage to any party's standing or reputation, or loss of stakeholder confidence.	Significant damage to any party's standing or reputation, or extensive loss of stakeholder confidence.	Very significant damage to any party's standing or reputation, or pervasive loss of stakeholder confidence.
Assist an offence or regulatory breech, hinder investigation or enforcement	May directly impact law enforcement or regulatory operations. Crime or regulatory avoidance may threaten confidentiality, integrity and availability elsewhere and have any other types of consequence. Stolen, modified or unavailable information may be used to enable other crime.	No assistance to an offence or minimally hinder investigation or regulation.	Assist a minor offence or hinder its detection, investigation or regulation.	Facilitate an offence or hinder detection, investigation, regulation or offender prosecution.	Enable an offence or obstruct detection, investigation, regulation or offender prosecution.	Enable a major offence or prevent detection, investigation, regulation or offender prosecution.
Degrade the capability to operate critical infrastructure or deliver major services internally or externally	A loss of operating capability is most likely from loss of information integrity or availability. The period required for a failure to become significant will depend on the nature of the information affected and the extent of operating dependency on it. Loss of capability may also cause regulatory non-compliance, adverse effects on stakeholders and loss of control over activities.	No degradation to the operating capability of any party.	Minimal degradation to the operating or delivery capability of any party.	Noticeable degradation to the operating capability or delivery of any party over a limited area.	Significant degradation to the operating or delivery capability of any party over an extended area.	Very significant and extensive degradation to the operating or delivery capability of any party.
Degrade the capability deliver minor or administrative services internally or externally	Similar to the previous consequence type but affect less significant assets. A loss of operating capability is most likely from loss of information integrity or availability.	Minimal degradation to the operating or delivery capability of any party.	Insignificant degradation to the operating capability or delivery of any party.	Significant degradation to the operating or delivery capability of any party.	Very significant and extensive degradation to the operating or delivery capability of any party.	Critical and widespread degradation to the operating or delivery capability of any party.

Notes:

Loss of privacy (usually a confidentiality failure, but integrity could be affected) may have several types of consequence including:

- Financial – legal liabilities or rectification costs including by an individual recovering from identity theft.

- Staff or Public Safety – when a person is at risk from another person.
- Distress or Inconvenience – particularly if sensitive personal information is involved or the person has to ‘recover’ their stolen identity. If sensitive personal information is involved the consequences may be at a higher level.
- Standing or Reputation – compromising personal information is not good for organisational reputation or stakeholder confidence, it may also lead to additional negative perceptions from action under the Privacy and Personal Information Protection Act.
- Enforcement or Regulatory – identity theft facilitates crime, which may be the purpose of the theft.

Loss of commercially sensitive information or compromise of intellectual property may result in legal liabilities and may involve criminal activities.

Risk level

The levels of likelihood and consequence severity are combined to give an overall level for each risk. Where a risk has several types of consequence then the most severe should be used. The following table is derived from Standards Australia HB 436:2004 *Risk Management Guidelines* Table 6.6. Changing the position of Low, Medium, High and Very High levels in the table provides a way to reflect the risk appetite of an agency. This may also affect the cost of security measures.

LIKELIHOOD	**SEVERITY**				
	Negligible	**Minor**	**Moderate**	**Major**	**Extreme**
Frequent	Medium	High	High	Very High	Very High
Probable	Medium	Medium	High	High	Very High
Occasional	Low	Medium	High	High	High
Remote	Low	Low	Medium	Medium	High
Improbable	Low	Low	Medium	Medium	High

Once risk levels are understood then treatment priorities and plans can be established, including deciding the balance between reducing the likelihood of security events and mitigating their consequences. Low risks will usually be accepted although this is a decision for the information asset owner but may have to be referred to the program or project board if the owner requires treatment at disproportionate cost.

Supplement 1 - Vulnerabilities and Threats

1 - Introduction

This Supplement catalogues various types of information security risks, it is not meant to be exhaustive. Appendix A tabulates possible threats against confidentiality, integrity and availability and Appendix B tabulates vulnerabilities.

Threats exploit vulnerabilities in the information assets. A vulnerability is a weakness in the physical environment, organisation and management, procedures, personnel, operations, hardware or communications equipment, and software. Most significantly vulnerabilities are created when safeguards, in the broadest sense, are either incorrectly configured or not updated when flaws are found by users or vendors.

Identifying threats will require input of asset owners or users, facility planning and IT specialists, and possibly other organisations such as insurance companies and other government agencies.

It is not possible to provide a complete list of threats and vulnerabilities. The agency's information security officer will have to keep abreast with possible security threats and vulnerabilities by sharing information with their peers or other information security specialists and by reference to security information sources such as Australian Computer Emergency Response Team (AUSCERT), CERT Co-ordination Center (operated by the Carnegie Mellon Software Engineering Institute), Forum of Incident Response and Security Teams (FIRST) and the SANS Institute.

2 Environmental Threats

Environmental threats include natural disasters and other environmental conditions. These threats result in the loss of ***availability*** of information which could lead to:

- Incorrect decisions being made.
- Inability to perform critical tasks.
- Loss of public confidence or image.
- Financial loss.
- Legal liabilities and breakdown of "duty of care".
- Additional costs being incurred.

In addition, these threats can affect the health and safety of staff.

If these threats are coupled with inadequate physical security, they could also result in loss of ***confidentiality*** of information.

2.1 Natural Disasters

According to information from Emergency Management Australia, "New South Wales is regularly affected by a large range of natural hazards. Every year numerous communities are threatened and damaged by severe storms and floods, while most summer seasons bring the risk of serious bushfires to many regions. Also, parts of the state are still geologically unstable and therefore prone to damaging earthquakes."

The likelihood of a natural disaster affecting the agency will depend on its location of its information processing facilities and stored data. For example, a computer facility near bushland will be more likely to be affected by bushfire than one that is located in the city area.

Natural disasters in NSW are briefly described below.

Earthquake

NSW earthquakes are not rated as 'severe' on a world scale. However, the earthquakes in Newcastle in December 1989 and in Cessnock in August 1994 have made this State the worst affected by this hazard in Australia. Other areas, including Sydney, have experienced earth tremors.

Examples of Vulnerabilities:

- Location is in an area susceptible to earthquakes.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Fire

The threat of serious bushfires usually occurs from October to April in the more forested eastern area of NSW. The most widespread serious bushfire in recent years was in January 1994 along the eastern seaboard of NSW including Sydney, Hunter and Blue Mountains regions.

Fire may be local, emanating from within the agency's premises or from adjoining offices and properties, or regional (e.g. bushfire).

Building fire and associated smoke damage (see Environment below) is one of the most common cause of damage to information processing facilities in Sydney. It may arise from a natural event or it may be deliberately or accidentally started. Fire may be caused by short circuit, ground fault or other electrical fault, carelessly discarded cigarettes, improper storage or negligent handling of materials subject to spontaneous combustion, or improper operation of heating devices.

Examples of Vulnerabilities:

- Location is in an area susceptible to bushfires or adjacent flammable premises.
- Lack of fire detection devices.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Flood

Based on information from Emergency Management Australia, "on average, NSW experiences a really serious flood about every 5 years, with many more-frequent smaller events. Some major ones since the mid-1970s include: April, 1974, Sydney region ($415m); March, 1975, Sydney region ($295m); November, 1984, South Eastern region including western Sydney ($550m). Damage costs shown are 1997 values."

Flood can be caused by a natural source, such as a river overflowing its banks or as a result of storm water, or as a result of another event. In Sydney, flood damage to an information processing facility is more likely to come from:

- Burst pipes.
- Failure of a water tank or an air-conditioning cooling tank located on a building roof.
- Water used to put out a fire in the immediate area.

Examples of Vulnerabilities:

- Location is in an area susceptible to floods.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Storm

The east coast of NSW, particularly the Sydney region, has the most frequent and costly severe storms in Australia. Most are severe thunderstorms involving damaging winds, intense rain, lightning, large hail and even tornadoes. Severe storms have occurred in Sydney's south western suburbs in March 1990, Sydney's north shore area in January 1991, and Armidale in September 1996.

Storm, wind and lightning strikes can all cause power outages, resulting in damage to hardware, potential loss of data and denial of service. These events can also cause physical damage to buildings through fallen trees and damage to glass windows.

Examples of Vulnerabilities:

- Location is in an area susceptible to storms.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Tidal Surge or Wave

There have been no specific reports of tidal surges or waves in the Sydney area causing financial damage since 1967. However, geological evidence does exist to suggest that there was a major tidal wave in the area prior to European settlement.

Examples of Vulnerabilities:

- Location is in an area susceptible to tidal surges or waves.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

2.2 Environmental Conditions

Environmental conditions affect the performance and reliability of the information assets as well as the handling, storage, packaging, preservation and delivery of information. Examples of environmental conditions are described below.

Contamination

Contamination can take many forms, including:

- Smoke from bushfires can cause contamination in computer equipment when drawn in through the air-conditioning system.
- Smoke from building fires containing chemicals which combine on circuit boards to form corrosives can cause permanent damage to equipment.
- Dust accumulation in computers can cause its cooling system to fail, and thus resulting in damage the equipment and possible loss of data.
- Cleaning chemicals can cause damage to equipment if they get into disk drive enclosures.

- Biological, chemical or nuclear agents can affect human health and cause permanent or temporary staff loss. Access to affected equipment or areas may be prevented for an extended period of time.

Examples of Vulnerabilities:

- Location is in an area susceptible to contamination.
- Lack of maintenance of equipment and facilities.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Electronic Interference

Signals from radars and other sources of radio frequency interference can cause computers to fail. They could also introduce glitches and errors into executable programs and data files.

Examples of Vulnerabilities:

- Location is in an area susceptible to electronic interference.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Extremes of Temperature and Humidity

Extreme heat can cause damage to magnetic media and computer equipment. Humidity beyond the level required to maintain equipment is a contributing factor to corrosion and can therefore cause equipment to fail. One of the sources of this threat is air conditioning failure which could be caused by power or equipment failure.

Examples of Vulnerabilities:

- Location is in an area susceptible to extreme temperature and humidity.
- Inadequate monitoring of environmental conditions.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Failure of Power Supply

Failure of essential utilities such as power can threaten the ***availability*** of information. It can lead to hardware failures, technical failures or problems with storage media.

The likelihood of this failure is increasing as demands for power increase due to the number of old electricity generating plants and distribution systems still operating, heatwave periods, and increased use of equipment using power. One notable example is Auckland's power crisis in February 1998.

Examples of Vulnerabilities:

- No Uninterruptible Power Supply equipment
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Power Fluctuations

Electricity supply can be affected by a number of factors, e.g. faults in the transmission grid, nearby construction and maintenance works, and usage by other consumers in the same grid or by own equipment. Fluctuations in power could cause equipment to fail.

Examples of Vulnerabilities:

- Location is in an area susceptible to power fluctuations.
- No power conditioning equipment.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Vermin

Vermin are any creatures that are unwanted in the work environment. These may be rodents, insects, or other animals. Vermin are more likely to be present in older, poorly maintained or shared premises, and in some areas of NSW more than others. They can cause damage to:

- cables resulting in loss of electrical power and damage to equipment.
- paper documents or magnetic media resulting in loss of data.

Examples of Vulnerabilities:

- Location is in an area susceptible to vermin.
- Lack of maintenance of equipment and facilities.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

3 Deliberate Threats

Deliberate threats are those threats involving the wilful destruction or manipulation of data, information, software or hardware.

Potential sources of these threats include disgruntled employees or contractors, consultants, hackers, maintenance people, activists, customers, suppliers, extortionists, criminals, terrorists or foreign agents.

Deliberate threats can result in loss of availability, confidentiality, integrity, accountability, authenticity and reliability with consequences including:

- Financial loss.
- Loss of public confidence, image, credibility and or reputation.
- Incorrect or poor decisions being made and or taking a long time.
- Legal liabilities and breakdown of “duty of care”.
- Injury or loss of life.
- Inconvenience to the public.
- Breach of Service Level Agreements to Public and other Government departments.
- Breach of Statutory Duty re confidentiality or other obligations.
- Inability to perform critical or statutory tasks.

Denial of Service

A Denial of Service attack disrupts or completely denies service to legitimate users, networks, systems and resources. Such attacks often target Web Sites, however, ‘carriers’ such as instant messaging can enable DoS attacks on servers deep within an organisation. DoS attacks can cause loss of business and credibility.

The intention of such an attack is malicious. It requires little skill as the requisite tools are readily available. These attacks can be carried out by:

- Starting a number of programs simultaneously
- Deliberately overloading a network by consumption of all the available bandwidth on a network
- Resource starvation attack which consumes system resources such as CPU utilisation, disk space, memory
- Router or Domain Name server attacks manipulate table entries to deny legitimate users access.

Denial of Service attacks will continue to have a greater impact as e-commerce continues to grow. Not only are these attacks perpetrated by malicious individuals, many governments use such attacks as offensive weapons to disable opponents during times of war.

Examples of Vulnerabilities:

- Lack of a Firewall.
- Inadequate network management (resilience of routing).
- Not using the latest version of the operating system can lead to exploitation of a security weakness.
- Not keeping up to date with various online Security organisations such as CERT will lead to a known weakness not being corrected in a timely manner.

Eavesdropping

Intercept, Eavesdropping or Sniffing is where an attacker uses software to “listen” to all traffic passing across an internal or external network. Wireless networks are especially vulnerable. This software essentially captures, interprets and stores data packets for later analysis. Data such as username password combinations, confidential emails, reports etc can all be viewed. This type of software poses significant risk to the network as it can be used to capture the most sensitive network passwords and allow an attacker to do anything on the network. Devices with a wireless or other broadcast communications channel may be accessed by a similarly equipped device in their vicinity. ‘Wireless’ includes any part of the electromagnetic spectrum used to carry data through the atmosphere.

Examples of Vulnerabilities:

- Unencrypted communications.
- Lack of physical security over data communications closets or hubs.
- Use of Shared Ethernet means that all traffic is broadcast to any machine on a local segment.

Fire

Fire can be the result of deliberate as well as natural causes. Disgruntled employees, or members of the public with a grudge against the organisation are a source of fires. Even forest or bush fires can be deliberately started and if IT resources are located in these areas then proper precautions may need to be undertaken.

Examples of Vulnerabilities:

- Lack of Physical Security.
- Lack of fire detection devices.
- Lack of automatic fire suppression system.
- Availability of flammable materials such as paper or boxes.
- Where IT facilities are located in bush surroundings, a lack of clearing or backburning can be exploited by someone intent on starting a fire.

Industrial Action

Labour disputes with IT staff or other staff can cause disruption to IT services. If staff required to maintain data communications facilities decide to take industrial action and a problem in the communications occurs then this will effect the delivery of IT services. This type of threat could lead to severe disruption outside of the agency's control.

Examples of Vulnerabilities:

- Lack of an industrial agreement.
- Lack of Business Continuity Plan.

Malicious Code

Malicious code refers to viruses, worms, Trojan horses and other undesirable software. The purpose of such software is to cause disruption either by deleting files, sending emails, including with harvested sensitive information, rendering the host system inoperable or converting machines into Zombie servers for spam, Denial of Service attacks or illegal material such as pornography. It includes the following:

Virus Code that replicates by attaching itself to existing executables. The virus may include an additional payload that triggers when specific conditions are met.

Trojan horse A program that performs a desired task, but also includes unexpected functionality.

Worm A self replicating program that is self-contained and does not require a host program. The program creates a copy of itself and causes it to execute; no user intervention is required.

Spyware A program that records a users activities and sends details to another party. Such software may be covertly loaded onto a machine through a network or a small device may be attached to a machine.

Malicious code is most usually carried by email. However, it can also arrive by physical media or instant messaging.

Computer viruses can occur on any operating system, however the largest threat is from IBM compatible personal computers and their most common operating system. Viruses can have various types as well. Malicious code may also be inserted into wireless devices and later transfer itself to a wired network and these are continuously evolving.

Examples of Vulnerabilities:

- No Anti Virus software.
- Lack of regular update of Anti virus software.
- Inadequate education of staff on Software viruses.

- Uncontrolled downloading and use of software off the Internet.
- Lack of policy for opening email attachments.
- Lack of control of instant messaging.
- Lack of checks for unauthorised software.
- Lack of policy on using portable storage devices and media before scanning by Anti virus software.

Malicious destruction of data, information or facilities

The destruction of databases, master files and IT hardware can easily disrupt the operation of most IT facilities. Anybody with sufficient knowledge can render a system unusable if they know what they are doing and have sufficient access. This can also extend to damage to hardware and communication lines.

In a 1999 study on computer security the actions of disgruntled employees were found to be the most likely source of an attack. While most organisations protect their computer facilities behind locked rooms, data communications facilities, including public ones or those across physically accessible areas, may not be as well protected.

Examples of Vulnerabilities:

- Lack of Physical Security.
- Lack of Logical Access security (User Id & Password) leading to deletion of data.
- Lack of communication between Human Resources and Information Technology group in respect of terminated employees leading to terminated employees still having access to system.

Masquerade

Masquerading is used to falsify the identity of the perpetrator. A user or computer which has been deceived as to the identity of the person they are communicating with can be induced to disclose sensitive information.

Examples of Vulnerabilities:

- Lack of identification and authentication mechanisms.
- Unprotected password tables.
- Lack of identification of sender and receiver.

Repudiation

When conducting business over the Web both parties must agree that a particular transaction took place. If one party to a transaction denies that it took place then this is repudiation of the transaction. Proper safeguards are needed to ensure integrity and validity of all web based transactions. These safeguards need to ensure that both parties are protected and that transactions can not be repudiated.

Examples of Vulnerabilities:

- Lack of proof of sending or receiving a message.
- Lack of use of Digital signatures.

Sabotage

Insiders (employees or contractors) are most familiar with their organisations ICT. systems. This knowledge provides them with the capability to cause maximum disruption to the organisation by sabotaging the computer systems. The number of incidents of employee sabotage is believed to be less than for Theft and Fraud but the individual losses can be high. Examples of sabotage include:

- Destroying hardware and infrastructure
- Changing data
- Entering erroneous data
- Deleting software
- Planting logic bombs
- Deleting data
- Planting a virus

Examples of Vulnerabilities:

- Lack of Physical Security.
- Lack of Logical Access controls.
- Lack of Change Management controls.
- Incorrect Access rights.
- Revealing too much information about systems to people without a “need to know”.

Social Engineering

Social Engineering is similar to Masquerading except the deceit is perpetrated on another human being. It is the practice of misleading and misdirecting a person in such a way as to attain information through social interaction. The hallmark of a successful social engineer is that they receive the information they request without raising any suspicion. Employees should be educated not to give information over the phone or email without knowing who the requestor is. All requests for information should be funnelled through designated staff who can verify the authenticity of the caller.

Examples of Vulnerabilities:

- Lack of awareness of the social engineering threat.
- Lack of policy restricting the provision of information by staff over the phone.
- Lack of policy requiring all enquires for information to be withheld until the identity of the requestor can be verified.

Theft and Fraud

Theft can include loss of data, information, equipment or software. Theft can be undertaken by internal staff or external parties. Fraud involves the stealing by deception and includes Credit Card Fraud, overpayment of salary, payment for non existent employees, payment for goods and services never provided.

Peer to peer file sharing applications can enable discovery and transfer of any type of file by any other user of such an application, wherever they are. This could result in the theft of significant information. Instant messaging provides similar capabilities. These types of application may transmit files that bypass firewalls and other standard safeguards.

Examples of Vulnerabilities:

- Lack of physical security.
- Lack of application safeguards leading to fraudulent payments being made.
- Lack of procedural safeguards leading to fraudulent payments being made.

- Lack of authentication leading to acceptence of false information and or provision of information to an unentitled entity.
- Lack of logical access controls leading to compromise of confidential data which could be used to perpetrate a fraud.
- Lack of effective Software Change management leading to unauthorised software modifications which could be used to perpetrate a fraud
- Lack of checks for unauthorised software.
- Lack of appropriate control of outbound traffic.
- Uncontrolled copying of data and software.

Unauthorised Data Access

Confidentiality of data and information may be important principle, and is especially so in the Government sector where sensitive information is obtained from the public. Privacy legislation requires that sensitive information collected from the public is not divulged to unauthorised persons and only used for the purposes agreed by the subject. This places a duty of care on the public agency collecting such data to ensure that adequate safeguards are in place to prevent its unauthorised disclosure.

The use of the Internet as a means of communication and doing business increases the risk of unauthorised disclosure and the incidence of breaches of confidentiality via the Internet has risen with its use. Examination results, medical data, credit card information, tax file numbers are all protected by law from unauthorised disclosure and in some cases financial penalties apply. Agencies must consider carefully how such data is to be protected.

Portable devices with wireless access are especially vulnerable to being accessed by similar devices in their vicinity. 'Wireless' includes any part of the electromagnetic spectrum used to carry data through the atmosphere. Any portable device is at increased risk of being lost or stolen.

Examples of Vulnerabilities:

- Lack of logical access controls.
- Inability to authenticate requests for information.
- Unsecured wireless ports.
- Inadequate operating policies for handling, processing or storing sensitive information.
- Transmission of unencrypted sensitive data or information.
- Lack of physical security over data communications cabinets.
- Portable devices storing unencrypted data and information.

Unauthorised Dial-in Access

Linked with the rise of mobile computing is the use of dial in access. Authentication of the user dialling into an agency's computer site is a basic requirement of such access. In a 1999 Computer Crime & Security Survey, 33% of respondents reported at least one attempted break in to their computer system in the previous 12 months. Of these 83% were attacked by an internal source and 58% were attacked by an external source.

Examples of Vulnerabilities:

- Unrestricted use of modems to dial into the network.
- Lack of an inventory of dial-up lines leading to inability to monitor dial up access.

- Lack of audit logs to detect unauthorised access.
- Lack of user authentication.
- Lack of intrusion detection software.
- Lack of firewall.
- Lack of policies in respect of dial up access, modem use, and software use.
- Lack of time restrictions on user access.
- Lack of physical security over telecommunications equipment cabinets (located in public areas leading to taping of communication lines and unauthorised dial in access).
- Dial in banner leading to information which can expose the organisation to unauthorised dial in access
- Lack of dial back authentication.

Unauthorised Software Changes

Unauthorised changes to program code can be used to commit fraud, destroy data or compromise the integrity of a computer system.

All software changes must be authorised before being implemented and adequate segregation of functions imposed between software programming staff and operational information technology staff who implement all authorised changes.

Examples of Vulnerabilities:

- Lack of Software Configuration Management policies and procedures.
- Lack of Configuration Management Software to enforce Configuration Management.
- Inadequate Segregation of Duties between software developers and operations staff.
- Inadequate engineering and quality processes for design and code review.
- Inadequate supervision of programming staff.
- Inadequate reporting and handling of software malfunctions.
- Easily accessible SCADA devices.
- Lack of backups.

Use of Pirated Software

The use of pirated or unauthorised software is illegal. Use of such software on a network places the agency in danger of legal action by the software supplier. All software used on the agency's network must be authorised and legal in keeping with NSW Government policy. Penalties for breach of licenses can be severe and entail a fine for each offence.

Examples of Vulnerabilities:

- Lack of policy restricting staff to use of licensed software.
- Inadequate control of software distribution.
- Lack of software auditing.
- Unrestricted copying of software.

Web Site Intrusion

Penetration and hacking of web sites is a daily occurrence. With the development of Virtual private networks and the growth of E-Business the risk both in terms of likelihood and consequence of Web Site Intrusion is rising.

Many web sites are hacked just for the publicity. In the US, the FBI, Department of Justice and the CIA have all had their home pages vandalised. If nothing else these have been highly embarrassing incidents for the organisations involved. Even worse is the situation where confidential data is obtained.

Examples of Vulnerabilities:

- Lack of Intrusion detection software.
- Lack of Firewall.
- Inadequate Firewall Policies.
- Lack of update of Operating System security patches.
- Inadequate Software Development standards.

4 Accidental Threats

Accidental threats relate to errors and omissions. Errors and omissions by employees or insiders are the main causes of information security problems. Errors may sometimes be a threat (for example, programming error causing system to crash) or may create a vulnerability (for example, a computer screen left unattended may be exploited by an unauthorised user).

A particularly common threat, usually accidental, is enhanced vulnerability through incorrectly configured or out of date security safeguards or exploitable software such as operating systems and databases. Such threats may be the result of sabotage but are most likely to be accidental errors or omissions.

These threats can result in:

- Incorrect decisions being made.
- Disruption of business functions.
- Loss of public confidence or image.
- Financial loss.
- Legal liabilities and breakdown of “duty of care”.
- Additional costs being incurred.

Examples of accidental threats are described below.

Building Fire

As discussed in the earlier sections, a building fire may be due to natural causes, or deliberate or accidental actions. Such an event may affect the ***availability*** of information.

Examples of Vulnerabilities:

- Location is in an area susceptible to bushfires.
- Inadequate or careless use of physical access control to buildings or rooms.
- Lack of fire detection devices.
- Lack of automatic fire suppression system.

- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Failure of communications services

Failure of communications services could result in a loss of ***availability*** of information through these services. If communications services are not available, the agency may not be able to communicate between various sites, send messages to external parties via e-mail, access information stored on network storage media or process information using application software located on the network.

A communications failure could be caused by accidental damage to network cabling, loss of network equipment such as routers or servers, software failure, loss of the computer environment through fire or water damage to building, or loss of essential services such as telecommunications or power.

Examples of Vulnerabilities:

- Lack of redundancy and back-ups.
- Inadequate network management.
- Lack of planning and implementation of communications cabling.
- Inadequate incident handling.

Failure of outsourced operations

Outsourcing of operations presents another threat to the agency. Outsourcing contracts must include security requirements and responsibilities. The failure of outsourced operations because of environmental events, deliberate or accidental actions, could result in a loss of ***availability, confidentiality*** and ***integrity*** of information.

Examples of Vulnerabilities:

- Unclear obligations in outsourcing agreements.
- No business continuity plans or procedures for recovery of information and information assets.
- Back-up files and systems not available.

Loss or Absence of Key Personnel

Certain personnel may be critical to the effective provision of services. The absence or loss of such personnel could result in a loss of ***availability, confidentiality*** and ***integrity*** of information.

Loss or absence of key personnel could be caused by a number of factors, for example, natural events; the failure of the national infrastructure such as power supply, water, gas, transport; stress; sickness; and others.

Examples of Vulnerabilities:

- No backup of key personnel.
- Undocumented procedures.
- Lack of succession planning.

Misrouting or re-routing of messages

Accidental directing or re-routing of messages to the wrong person can lead to a loss of ***confidentiality*** if these messages are not protected, and loss of ***availability*** to the intended person. Both misrouting and re-routing of messages can lead to the loss of ***integrity*** of those messages by allowing unauthorised changes to be made prior to delivery to the original addressee. Accidental misrouting is usually caused by user error.

Examples of Vulnerabilities:

- Inadequate user training.
- Sensitive data not encrypted.
- Lack of proof of receiving a message.

Operational Staff or User Errors

Erroneous actions by operators or users can threaten the ***integrity, availability*** and ***confidentiality*** of data. Examples include:

- Incorrect set-up of security features could result in loss of confidentiality, integrity and availability of data.
- Switching off computers when an error is displayed instead of correctly closing all current applications.
- Inadvertent over-writing or deletion of files.
- Inadequate back-ups.
- Processing of incorrect versions of data.

The following are some examples of actual incidents that are breaches of privacy:

- In August 2000, BBC reported that a UK bank clerk incorrectly keyed in account details which resulted in two customers with the same street address and postcode having access to each other's account details.
- In December 1999, a retail music chain in Sydney accidentally revealed the e-mail addresses of more than 140 users of its service to all these users. This was caused by including each e-mail address in the "To:" field instead of the "Bcc:" (blind carbon copy) field. In addition to a breach of privacy, this error could cause e-mail accounts of these users to be spammed (that is, users get unsolicited mail which can then cause the accounts to be unusable).

Examples of Vulnerabilities:

- Lack of user awareness.
- Insufficient security training.
- Lack of documentation.
- Lack of efficient configuration change control.
- Complicated user interface.

Software or Programming Errors

If errors are made during the software development, maintenance or installation process, the ***integrity***, ***confidentiality*** and ***availability*** of the information processed could be threatened.

Commercial off-the-shelf software does not guarantee error-free software. Microsoft has released software which made systems vulnerable to security breaches. For example, Hotmail had a bug that allowed anyone to read the accounts of their subscribers with or without a password. Microsoft Outlook and Outlook Express software had a bug that could allow malicious code to run on a computer without the knowledge of the user and cause Outlook and Outlook Express to fail, or allow the hacker to use the user's access rights to reformat the disk drive, change data or communicate with other external sites.

Examples of Vulnerabilities:

- Inadequate system development life cycle procedures.
- Unclear or incomplete specifications.
- Lack of efficient and effective configuration change control.
- Unskilled staff.

Technical failures

Failures can occur in hardware devices or network. These may be caused by:

- faults in the manufacture of the equipment,
- changes in temperature or humidity,
- mishandling of equipment during relocation,
- accidental spillage or impact eg to desktop equipment or notebook computers,
- loss of computer environment through fire or water damage to a building,
- airconditioning failure,
- loss of essential services such as telecommunications or power.

Examples of Vulnerabilities:

- Lack of environmental protection.
- Lack of user awareness.
- Improper or inappropriate maintenance of technical facilities.
- Lack of back-up facilities or processes.
- Lack of network capacity through improper planning or maintenance.
- Failures in the change management process.
- No business continuity plans or procedures.

Transmission errors

Transmission errors can destroy the ***integrity*** of data, and can lead to a loss of ***availability***. This may occur due to the failure of any one of the network components that are used for the transmission of such data.

Examples of Vulnerabilities:

- Improper or inappropriate cabling.
- Inadequate incident handling.
- Lack of backup facilities or processes.
- No business continuity plans or procedures.

Appendix A - Threats and Security Concerns

This list relates the threats identified in this Supplement to the security concern(s).

Threat	Security Concern		
	Confidentiality	Integrity	Availability
Environmental Threats			
Contamination			✓
Earthquake			✓
Electronic Interference			✓
Extremes of Temperature and Humidity			✓
Failure of Power Supply			✓
Fire			✓
Flood			✓
Power Fluctuations			✓
Storm			✓
Tidal Surge/Wave			✓
Vermin			✓
Deliberate Threats			
Denial of Service			✓
Eavesdropping	✓		
Fire			✓
Identity Crime	✓	✓	
Industrial Action			✓
Malicious Code	✓	✓	✓
Malicious destruction of data and facilities		✓	✓
Masquerade	✓	✓	
Repudiation			
Sabotage		✓	✓
Social Engineering	✓	✓	✓
Theft and Fraud	✓	✓	✓
Unauthorised Data Access	✓	✓	
Unauthorised Dial-in Access	✓	✓	
Unauthorised Software Changes	✓	✓	✓
Use of Pirated Software			✓
Web Site Intrusion	✓	✓	✓
Accidental Threats			
Building Fire			✓
Failure of communications services			✓
Failure of outsourced operations	✓	✓	✓
Loss or absence of key personnel	✓	✓	✓
Misrouting or re-routing messages	✓	✓	✓
Operational Staff Errors		✓	✓
Software or Programming Errors	✓	✓	✓
Technical failures		✓	✓
Transmission errors		✓	✓

Appendix B - Vulnerabilities

This Appendix lists examples of vulnerabilities, the threats that may exploit them and the type of asset that could be affected. This list is not intended to be exhaustive. In particular only generic ICT assets are considered. It does not state the business consequences.

Vulnerability	Threat	Asset Type
Availability of flammable materials such as paper or boxes	Fire	Facilities Hardware Data or Information
Back-up files and systems not available	Earthquake Fire Flood Storm Tidal Surge/Wave Contamination Electronic Interference Extremes of Temperature and Humidity Power Fluctuations Vermin Failure of outsourced operations Transmission errors Unauthorised Software Changes	Facilities Data or Information Hardware Software
Complicated user interface	Operational Staff or User Errors	Data or Information
Dial-in banner leading to information which can expose the organisation to unauthorised dial in access	Unauthorised Dial-in Access	Data or Information
Easily accessible SCADA devices.	Unauthorised Software Changes	Data or Information
Failures in the change management process	Technical failures	Hardware
Improper or inappropriate cabling	Transmission errors	Data or Information
Improper or inappropriate maintenance of technical facilities	Technical failures	Hardware
Inadequate control of software distribution	Use of Pirated Software	Software
Inadequate education of staff on software viruses	Malicious Code	Data or Information
Inadequate engineering and quality processes for design and code review	Unauthorised Software Changes	Data or Information
Inadequate Firewall Policies	Web Site Intrusion Unauthorised Data Access Unauthorised Software Changes Malicious destruction of data Theft and Fraud	Data or Information
Inadequate incident handling	Failure of communications services Transmission errors	
Inadequate information security policy	Malicious Code	Software Data or Information
Inadequate monitoring of environmental conditions	Extremes of Temperature and Humidity	Facilities Hardware
Inadequate network management	Failure of communications services	Facilities
Inadequate network management (resilience of routing)	Denial of Service	Facilities Data or Information
Inadequate operating policies for handling, processing or storing sensitive information.	Unauthorised Data Access Malicious destruction of data Theft and Fraud	Data or Information
Inadequate reporting and handling of software malfunctions	Unauthorised Software Changes	Software Data or Information
Inadequate Segregation of Duties	Unauthorised Software Changes	Software

Vulnerability	Threat	Asset Type
between software developers and operations staff		Data or Information
Inadequate Software Development standards	Web Site Intrusion	Software Data or Information
Inadequate supervision of programming staff	Unauthorised Software Changes	Software Data or Information
Inadequate system development life cycle procedures	Software or Programming Errors	Software Data or Information
Inadequate user training	Misrouting or re-routing messages	Data or Information
Incorrect Access rights	Sabotage	Software Data or Information
Incorrectly configured or maintained application security features	Unauthorised Data Access Malicious destruction of data Theft and Fraud	Data or Information
Incorrectly configured or maintained operating system	Unauthorised Data Access Unauthorised Software Changes Malicious destruction of data Web Site Intrusion Theft and Fraud	Software Data or Information
Incorrectly configured or maintained security safeguards	Denial of Service Unauthorised Data Access Unauthorised Software Changes Malicious destruction of data Web Site Intrusion Theft and Fraud	Software Data or Information Facilities
Insufficient security training	Operational Staff or User Errors	Data or Information
Lack of a Firewall	Denial of Service Unauthorised Dial-in Access Unauthorised Data Access Unauthorised Software Changes Malicious destruction of data Web Site Intrusion Theft and Fraud	Data or Information Software Facilities
Lack of an industrial agreement	Industrial Action	Facilities Hardware Data or Information
Lack of an inventory of dial-up lines leading to inability to monitor dial up access	Unauthorised Dial-in Access	Data or Information
Lack of application safeguards leading to fraudulent payments being made	Theft and Fraud	Data or Information
Lack of appropriate control of outbound traffic	Theft and Fraud	Data or Information
Lack of audit logs to detect unauthorised access	Unauthorised Dial-in Access	Data or Information
Lack of automatic fire suppression system	Fire	Facilities Hardware
Lack of awareness of the social engineering threat	Social Engineering	Software Data or Information
Lack of back-up facilities or processes	Technical failures	Facilities
Lack of backups	Unauthorised Software Changes	Software Data or Information
Lack of checks for unauthorised software	Malicious destruction of data and facilities Malicious Code Theft and Fraud	Software Data or Information
Lack of communication between HR and IT groups in respect of terminated employees leading to such employees still having access to system	Malicious destruction of data and facilities	Facilities Software Data or Information
Lack of Configuration Management controls	Sabotage	Software Data or Information

Vulnerability	Threat	Asset Type
Lack of Configuration Management Software to enforce Configuration Management	Unauthorised Software Changes	Software
Lack of control of instant messaging	Malicious Code	Data or Information
Lack of safeguards leading to false credentials being created or accepted	Theft and Fraud Identity Crime	Data or Information
Lack of dial-back authentication	Unauthorised Dial-in Access	Data or Information
Lack of documentation	Operational Staff or User Errors	Data
Lack of effective Software Change management leading to unauthorised software modifications that could be used to perpetrate a fraud	Theft and Fraud	Software Data or Information
Lack of efficient and effective configuration change control	Operational Staff or User Errors Software / Programming Errors	Software Data or Information
Lack of environmental protection	Technical failures	Facilities Hardware
Lack of fire detection devices	Fire	Facilities Hardware
Lack of identification and authentication mechanisms	Masquerade	Data or Information
Lack of identification of sender and receiver	Masquerade	Data or Information
Lack of intrusion detection software	Unauthorised Dial-in Access Web Site Intrusion Unauthorised Data Access Unauthorised Software Changes Malicious destruction of data	Data or Information Software
Lack of Logical Access security	Malicious destruction of data and facilities Sabotage Theft and Fraud	Data or Information
Lack of maintenance of equipment and facilities	Contamination	Facilities Hardware
Lack of network capacity through improper planning or maintenance	Technical failures	Hardware
Lack of Physical Security	Fire Malicious destruction of data and facilities Sabotage Theft and Fraud Unauthorised Data Access	Facilities Hardware Data or Information
Lack of physical security over data communications closets or hubs	Eavesdropping	Data or Information
Lack of physical security over telecommunications equipment cabinets	Unauthorised Dial-in Access	Data or Information
Lack of planning and implementation of communications cabling	Failure of communications services	Data or Information
Lack of policies in respect of dial up access, modem use, and software use	Unauthorised Dial-in Access	Data or Information
Lack of policy requiring enquires for information to be withheld until the identity of the requestor can be verified	Social Engineering	Software Data or Information
Lack of policy restricting staff to use of licensed software	Use of Pirated Software	Software
Lack of policy restricting the provision of information by staff over the phone	Social Engineering	Software Data or Information
Lack of procedural safeguards leading to fraudulent payments being made.	Theft and Fraud	Data or Information
Lack of proof of receiving a message	Misrouting/re-routing of messages	Data or Information
Lack of proof of sending or receiving a message	Repudiation	Data or Information
Lack of redundancy and back-ups	Failure of communications services	Data or Information

Vulnerability	Threat	Asset Type
Lack of regular update of Anti virus software	Malicious Code	Software Data or Information
Lack of software auditing	Use of Pirated Software	Software
Lack of Software Configuration Management policies and procedures	Unauthorised Software Changes	Software Data or Information
Lack of time restrictions on user access	Unauthorised Dial-in Access	Data or Information
Lack of update of Operating System security patches	Web Site Intrusion	Software Data or Information
Lack of use of Digital signatures	Repudiation	Data or Information
Lack of user authentication	Unauthorised Dial-in Access	Software Data or Information
Lack of user awareness	Operational Staff or User Errors Technical failures	Software Data or Information Hardware
Location is in an area susceptible to environmental conditions such as contamination, electronic interference, extreme temperature and humidity, vermin	Contamination Electronic Interference Extremes of Temperature and Humidity Vermin	Facilities
Location is in an area susceptible to natural disasters	Earthquake Fire Flood Storm Tidal Surge/Wave	Facilities
Location is in an area susceptible to power fluctuations	Power Fluctuations	Facilities
No Anti-Virus software	Denial of Service Malicious Code	Software Data or Information
No business continuity plans or procedures for recovery of information and information assets	Earthquake Fire Flood Storm Tidal Surge/Wave Contamination Electronic Interference Extremes of Temperature and Humidity Power Fluctuations Vermin Failure of outsourced operations Industrial Action Technical failures Transmission errors	Facilities
No power conditioning equipment	Power Fluctuations	Hardware
No Uninterruptible Power Supply equipment	Failure of Power Supply	Facilities Hardware
Not keeping up to date with Security advisories will lead to a known weakness not being corrected in a timely manner	Denial of Service	Data or Information
Portable devices storing unencrypted data and information	Hardware theft	Data or Information
Revealing too much information about systems to people without a “need to know”	Malicious destruction of data and facilities Sabotage Theft and Fraud	Data or Information
Transmission of unencrypted confidential data	Misrouting or re-routing messages Unauthorised Data Access	Data or Information
Unclear obligations in outsourcing agreements	Failure of outsourced operations	Software Data or Information
Unclear or incomplete specifications	Software or Programming Errors	Software Data or Information
Uncontrolled copying of data and or	Theft and Fraud	Data or Information

Vulnerability	Threat	Asset Type
software		Documents Software
Uncontrolled downloading and use of software off the Internet	Malicious Code	Software
Unencrypted communications	Eavesdropping	Data or Information
Unprotected password tables	Masquerade	Data or Information
Unrestricted copying of software	Use of Pirated Software	Software Data or Information
Unrestricted use of modems	Unauthorised Dial-in Access	Data or Information
Unsecured wireless ports	Unauthorised Data Access Malicious destruction of data Theft and Fraud	Data or Information
Unskilled staff	Software or Programming Errors	Software Data or Information
Use of Shared Ethernet means that all traffic is broadcast to any machine on a local segment	Eavesdropping	Data or Information

Supplement 2: Information Security Safeguards

1 Introduction

This Supplement provides guidance that supplements that provided in ISO 27002. For convenience it groups the standard control categories into four ‘super-categories. Annex A relates the safeguards to the six security functions that provide defence in depth: Deter, Avoid, Protect, Detect, React and Recover.

2 Organisational and Management Safeguards

This section describes the safeguards dealing with the management of information security, planning, assignment of responsibilities for these processes, and all other relevant activities. The objective of these safeguards is to achieve an appropriate and consistent level of security throughout the agency.

Strong management practices provide a vital role in the implementation of effective safeguards. It is human nature for personnel to readily resort to shortcuts or circumventions when it suits them. Failure by management to respond to such situations will legitimise these actions and increases the risk of damage to the agency. For example password sharing is unacceptable if there is any need for individual accountability, management condonation of password sharing makes management culpable for any security failures arising from password sharing.

2.1 Information Security Policy

ISO/IEC 27002:2007	***5.1***	***To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.***

The importance of security policy cannot be over-emphasised. A policy issued and approved by executive management should clearly define the agency’s direction on Information Security, including the use of assets, the performance standards expected and the conduct of all users within the agency.

Procedures, guidelines and standards for the performance of business and administrative functions, in support of the information security policy, should be developed. These procedures should be kept current and clearly communicated to all personnel.

A discussion on Information Security Policy can be found in Chapter 3, section 3.3 and Chapter 4, section 4.6.

2.2 Information Security Infrastructure

ISO/IEC 27002:2007	***6.1***	***To manage information security within the organisation.***

Information security should be managed within the agency in a structure that is appropriate to its size. The organization and responsibilities must be detailed in security policy.

The agency should allocate resources and assign the roles and responsibilities to ensure the effective management of information security. This may involve use of specialist resources (internal and or external) if appropriate.

Security responsibilities for the following roles include:

- Executive management – has ultimate accountability for information security.
- Information security officer – has responsibility for the development and implementation of security such as assisting asset owners in assessing risks and defining security measures, advising on security issues, investigating suspected security incidents, and co-ordinating with other security organisations.
- Information Asset Owner – is accountable for the security of their information assets.
- ICT Management – has responsibility for development, implementation, management and maintenance of information system security as agreed with information asset owners and in accordance with agency policies.
- Users – must be aware of their responsibilities relating to information security, and be accountable for their actions.
- Auditor – must be an independent person (either within or outside the agency) who conducts reviews to provide assurance that information security policies and processes are complied with.

Contact with external Information Security specialists and advisory services should be established to ensure that the agency keeps up with industry standards (best practice) and known security vulnerabilities.

Information security officers should be encouraged to join security and industry forums to maintain and update their knowledge in a changing environment.

2.3 Security of Third Party Access

ISO/IEC 27002:2007	***6.2***	***To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.***

The agency must control access to information processing facilities by third party organisations and access should be assigned based on the assessment of the risk of granting such access. It is usually appropriate to establish policies for this.

Third parties include:

- Hardware and software staff of service providers located off-site
- Trading partners or joint ventures
- On-site contractors for hardware and software maintenance and support
- Cleaning, catering, security guards and other outsourced support services
- Student placements
- Casual short-term appointments
- Consultants

If confidentiality of information is an issue, third parties should be required to sign a non-disclosure agreement. Policy should be established for this.

Outsourcing

An agency with any outsourcing arrangement must ensure that it has appropriate control over the service provider and its staff and contractors to enable management of the agency's security risks.

The agency should address the risk, safeguards and procedures required for all aspects of information security through contractual arrangements in the outsourcing agreement. Some of the issues that need to be considered are:

- Responsibilities for the management and security of information.
- Ownership of data, software, policies and procedures.
- The protection of the agency's information from other clients using shared resources.
- Access to agency data by staff of the service provider.
- Service provider's change control procedures.
- Business continuity plans consistent with agency's availability requirements
- Service provider's compliance with relevant NSW government regulations.
- Independent security compliance audits.

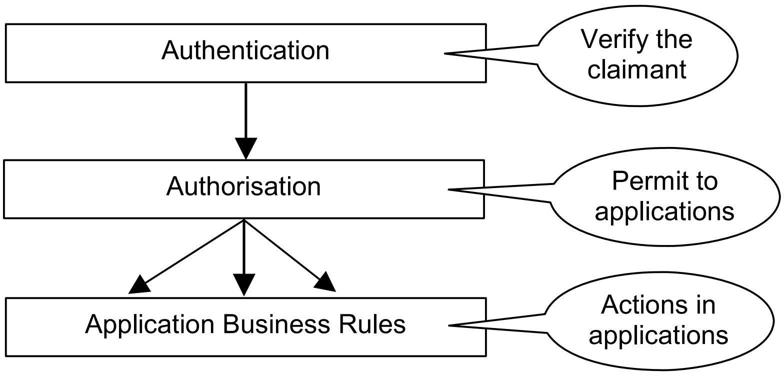
2.4 Access Control

Access control requires mainly technology solutions to meet business needs.

Business requirement for access control

ISO/IEC 27002:2007 11.1 To control access to information.

Access control involves a three layer model, the appropriate use of this model by individual users is a business management decision based on agency policy.



The strength of authentication to verify that a user id claimant is who they claim to be depends on the risks arising from unauthorised access to the information. The Australian Government Authentication Framework (AGAF) provides further guidance.

Mobile Computing

ISO/IEC 27002:2007 11.7 To ensure information security when using mobile computing and teleworking facilities.

Policies and procedures should be established for the use of mobile computing facilities such as laptops, notebooks, palmtops and mobile phones. These should cover:

- Physical security.
- Transit security.
- Security labelling.
- Access controls including remote access.
- Virus protection, including when mobile users re-connect to agency networks.
- Encryption of data.

- Backups.
- Sanitisation, declassification and destruction of equipment.

As a minimum, security features should include user identification and authentication before access is given to data and applications, and a screen lock facility. Mobile devices joining an internal network as a normal ‘desktop’ pose particular risks because they may have acquired malicious software by direct connect to public networks, including wireless connections.

Safeguards should be commensurate with the risks associated with working with mobile computing facilities.

Teleworking

Policies and procedures should be established to control teleworking activities. Teleworking activities must be authorised by management. Policies concerning personal firewalls and other defensive software or hardware will be required.

Appropriate safeguards should be implemented to achieve the same level of security as that in an office environment. Safeguards for mobile computing also apply to teleworking activities.

2.5 Information Assets

Responsibility for assets

ISO/IEC 27002:2007	***7.1***	***To achieve and maintain appropriate protection of organisational assets.***

In order to assess information security risks effectively, the agency needs to identify all major assets that require protection and assign an Owner who has primary responsibility for the protection of this asset. The Owner of the asset will usually be the person responsible for the business process using it. TAM and ICT Strategic Plans should help in identifying key assets. Equipment asset registers and the question ‘what is this equipment for’ provide a useful cross-check. However, non-technology based information assets such as ‘reputation’ should also be considered.

The Owner should be able to establish the relative importance and value of the asset to the agency. This should be in terms of its confidentiality, integrity and availability and the consequences of a failure affecting these.

Information classification

ISO/IEC 27002:2007	***7.2***	***To ensure that information receives an appropriate level of protection.***

Appropriate information labelling and handling procedures in accordance with the classification scheme should be established.

Premier’s Circular 2002-69 and *Guide to Labelling Sensitive Information* provide details of the standard information labelling system to be used in NSW. National security information uses different labels and handling rules, details of these are given in the Commonwealth’s Protective Security Manual. It is particularly important that other labels are not used and that these ‘reserved’ labels are not used incorrectly. A common failing is to use the term ‘Confidential’ for items that are not related to national security.

2.6 Personnel Practices

Personnel practices cover permanent and casual employees of the agency. They and extend to contractors, consultants and other individuals working on the agency's premises or using the agency's information and information processing assets. It includes individuals working for vendors and other service providers.

There is a personnel life cycle: personnel are engaged, preparations are made for them to start work, they work, they may change roles during their employment and they finally separate from the organisation. These stages each have security implications.

Prior to employment

ISO/IEC 27002:2007	***8.1***	***To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of fraud or misuse of facilities.***

The recruitment process is summarised in the Personnel Handbook http://www.premiers.nsw.gov.au/our_library/employment_conditions/personnel_handbook/index.htm. References and previous employment details of applicants should be validated and criminal record checks may be performed on applicants for sensitive positions. Where the position involves access to information of significant use or value to criminals then consideration should be given to more rigorous checks, to retraining existing staff of established honesty or to redesign the position to ensure effective segregation of duties.

In developing job descriptions, it is important to ensure that no individual has the ability to both perpetrate and conceal an accidental or intentional breach of information security. This is best achieved by the segregation of incompatible duties or knowledge so that collusion between two or more personnel is required to conceal a security breach. Where segregation of duties is not practical, there must be appropriate supervision and review of activities.

Extending the segregation of duties to the 'two person' rule, is good practice; this means that two people, of similar knowledge and expertise, must work together to perform certain tasks. This helps protect against mistakes as well as deliberate weaknesses and is particularly important when setting up and maintaining security safeguards.

ISO/IEC 27002:2007	***10.1.3***	***Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.***

Mobile use policies with additional rules about downloading agency information should be applied to consultants and temporary staff that are to use their own ICT equipment on the agency's network. However, such use is strongly deprecated.

During employment

ISO/IEC 27002:2007	***8.2***	***To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.***

Information security policies and procedures are of little use unless they are understood and observed by all who are affected by them. The agency must be proactive in communicating its expectations and requirements to its personnel, as well as in prescribing disciplinary action for non-compliance. It is not sufficient to publish policies and assume that personnel are aware of them, will read them and will adhere to them.

A video '*I wish [it wasn't] me*' designed for NSW government uses has been distributed to agencies. It may be used as part of awareness training. Other material is commercially available. Inculcating a culture of security awareness is a significant undertaking and will take considerable time to become entrenched. This must be personalised so that all personnel are aware of their responsibilities.

Personnel should be appropriately trained to perform their tasks, prior to access to systems and information being granted. Different levels of training may be required to match the requirements of their jobs. Security officers may require specialised security training or education.

Activities of personnel should be supervised and peer reviews of their work may be established. Close supervision is especially important for junior personnel with privileged access authorisation.

Periodic rotation of tasks between personnel should be implemented to limit the opportunity for fraud and to increase the chance of exposure. Where shift work is involved, rotate personnel through all shifts and mix the composition of shift rosters.

Management should be aware of changes to a person's morale, attitude to work and external pressures and take appropriate action to ensure that information security is not threatened. Suspicions should be aroused when staff do not take holidays, work unduly long hours or live beyond their means.

When personnel are disciplined or otherwise feel disaffected, a program of closer supervision and audit of their activities should be implemented.

Termination or change of employment

ISO/IEC 27002:2007	***8.3***	***To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.***

Adequate training of all personnel is critical to the effective implementation of information security. Security awareness and training activities should be ongoing to further demonstrate management's commitment to information security.

There are endless anecdotes about people leaving an organisation and some of their access authorisations remaining active. Formal communication between the human resources function and the information security function should be in place for notification of any terminations or changes in employment. Security managing systems should provide a view giving details of all of a person's access rights, not merely their roles.

A formal exit procedure for personnel leaving the agency must be established to ensure that:

- All assets of the agency are returned, including policy and procedure manuals and technical documentation,
- Keys, passes and other access devices are returned,
- Deactivation or deletion of the person's access identifiers and the removal of the access authorities granted to them revokes access to information systems.

Management should ensure that personnel leaving the agency under duress or with ill-feeling do not have access to information assets during any period of notice. Escalating the provisions of the exit procedures, especially immediately revoking system access, is a recommended first step. For additional protection the person, particularly if he or she is in a position of trust, should not be required to serve the period of notice and should be escorted from the premises.

Similar procedures should be applied to personnel who have temporarily or permanently changed jobs within the agency, particularly for those moving from a sensitive position to a less sensitive one.

2.7 Information Systems Acquisition, Development and Maintenance

Security requirements must be considered from the earliest stages of the acquisition of new or upgraded information systems.

ISO/IEC 27002:2007	***12.1 To ensure that security is an integral part of information systems.***

Web applications are especially important as sources of significant vulnerabilities. Therefore it is essential to ensure that these applications are implemented applying good security practices. This is a contractual issue.

The recommended approach is to apply the OWASP Secure Software Contract Annex, http://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex. The details of this will need to be negotiated with suppliers. The matters it raises should also be addressed in project documents used by internal development teams.

2.8 Compliance

The scope of compliance includes both external and internal obligations and policies. Compliance with legislation is a legal baseline and is not treated as a risk management matter.

Compliance with legal requirements

ISO/IEC 27002:2007	***15.1 To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirement.***

This Guideline does not provide a complete list of legislation that an agency must comply with. This should be sought from the agency's legal advisors and arrangements instituted for changes to be notified to the information security officer. To this must be added the agency's internal policies and other policies established by the government.

In particular attention should be given to:

- Ensuring that restrictions relating to intellectual property rights such as copyright, design rights or trademarks are complied with.
- Preventing unauthorised copying and piracy of software for in-house use. This also applies to unauthorised copying and distribution of internally developed software to external organizations or individuals.
- Compliance with the *State Records Act*.
- Compliance with the *Privacy and Personal Information Protection Act.*

Compliance with security policies and standards

ISO/IEC 27002:2007 15.2 Managers shall ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the organisation shall be subject to regular review to ensure compliance with security policies and standards.

Compliance reviews provide an opportunity to assess the appropriateness of policies.

Information system audit considerations

ISO/IEC 27002:2007 15.3 Audits of operational systems shall be planned and agreed such as to minimise the risk of disruptions to business.

The importance of independent audit as a control cannot be underestimated. It can take many forms, from reviewing other safeguards and identifying their strengths and weaknesses, to monitoring user behaviour and system activity. Audits are a key element in managing vulnerabilities.

When system audit tools are used, these should be separated from the development and operational systems environments to prevent any misuse or compromise. Both software and data files should be restricted from access by IT personnel (e.g. in tape libraries) or users (e.g. in user areas).

2.9 Incident Management

Information security incidents may occur at any time. This means that robust processes must be establish to deal with them. Mistakes in incident management may prevent a subsequent successful prosecution. Loss of information may hinder subsequent corrective action.

Reporting information security events and weaknesses

ISO/IEC 27002:2007 13.1 To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Whatever factors contribute to an incident, it is important that the cause be analysed and corrected, to prevent a recurrence.

Policies should incorporate Premier's Circular 2004-21 *Procedures for Reporting Security Incidents* as appropriate. Agencies should use the incident report format in ISO/IEC TR 18044:2004 *Information technology – Security techniques – Information security incident management, Annex A*.

Management of information security incidents and improvements

ISO/IEC 27002:2007 13.2 To ensure a consistent and effective approach is applied to the management of information security incidents.

Incident management helps to contain and repair damage from incidents, prevent recurrences and damage, provide input to threat and vulnerability assessments, and improve internal communications, training and awareness programs.

When planning incident management procedures agencies should accommodate the practices in Standards Australia's HB 171:2003 *Guidelines for the Management of IT Evidence*. Policies should require contracts to ensure that service providers such as ISPs retain transitory records for sufficient time for them to be forensically collected.

2.10 Business Continuity Management

ISO/IEC 27002:2007 14.1 To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Standards Australia’s HB 221:2003 *Business continuity management* provides additional guidance.

Several business continuity plans may be developed, eg for different information processing platforms. A single framework must be maintained to ensure consistency and to identify priorities for testing and maintenance. Each plan must have an owner and should clearly specify the conditions for its activation, emergency procedures, fall back procedures, resumption procedures, maintenance procedures, awareness and education activities, and individuals responsible for the execution of the plan.

The common types of backup facility are categorised below, in increasing order of protection and likely cost:

- *Reciprocal arrangements* may be made with another organisation using similar ICT hardware and software for each party to make a portion of its facilities available should the other party suffer a disaster. The major concern with this approach is in the commitment of the partner organisation and its ability to deliver the promised ICT resources when they are needed. The partner organisation will still have to satisfy the processing needs of its own business functions. In addition, its spare resources may not be easily realisable and may be insufficient to provide the backup service required. This type of facility is best suited to an organisation that has a low level of dependence on ICT for its critical business functions, and only limited or no requirement for on-line services. Even then it is advisable to make reciprocal arrangements with more than one partner.
- *Cold sites* are premises fitted out with the necessary utility supplies and ready to receive replacement equipment. The premises may belong to the organisation or to a service provider who contracts to make them available when required. It may take some days, perhaps a week or two, to make the site fully operational.
- *Warm sites* are premises already housing ICT equipment suitable for sustaining the critical business functions. The data backups must firstly be loaded and other vital records used to resume business processing. Communications lines may also have to be rerouted to the site. It should typically take several hours, perhaps up to a day or two, to make the site operational. Again the site may be owned by the organisation or the service may be contracted from an external supplier.
- *Hot sites* are premises housing ICT equipment and duplicate communications facilities that are continuously available and that process critical business functions in parallel with the primary site. It is possible to activate the site instantaneously, or with a delay of several minutes at most. One effective implementation is referred to as site mirroring, in which two identical sites share the workload and continuously update each other. They can each provide instantaneous backup of the other. Hot sites may be owned by the organisation.

Once the type of facility has been selected, there are several important issues to consider in selecting a suitable partner or service provider. In particular, the likelihood of the other party also being affected by the same disaster.

Separate power grids and communications exchanges might be prudent, for example. Accommodation and telephone access for personnel is also important. When contracting with service providers additional considerations might include the compatibility of the hardware and software available, the location and numbers of other subscribers, and the capability to support joint emergency use. Formal contracts or written agreements must be used with external parties to guarantee access to the backup facilities when required, including for testing. They should be required to periodically reconfirm their ability to supply the service.

3 Physical and Environmental Safeguards

This part describes the safeguards associated with physical protection of data, systems, buildings and related supporting infrastructure to prevent:

- Unauthorised access, damage and interference to business premises and information;
- Loss, damage or compromise of assets;
- Compromise or theft of information and information processing facilities.

3.1 Physical and Environmental Security

Physical security is concerned with controlling physical access to facilities and preventing the loss of equipment or compromise of information through physical activity.

Secure Areas

ISO/IEC 27002:2007	***9.1***	***To prevent unauthorised access, damage, and interference to the organisation's premises and information.***

Information processing facilities should be maintained within secure areas to protect them from unauthorised access destruction or manipulation. Such protective measures may include physical security, fire protection, water and liquid protection, power and air-conditioning protection, infrastructure planning (building design or cabling), and visitor control systems.

Equipment security

ISO/IEC 27002:2007	***9.2***	***To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.***

All information processing equipment should be safeguarded from the environment and only accessible to authorised personnel. Equipment should be protected from the elements, power surges, power failures, electromagnetic interference and unauthorised access.

Consideration could be given to anchoring all desktop computers to prevent their theft and passwords being implemented before access to laptops is allowed.

4 Operational Safeguards

This section describes the safeguards relating to the secure, correct and reliable functioning of the ICT Facilities. Operational safeguards can be implemented by instituting organisational procedures. Most operational control will be the result of policy decisions arising from information security polices.

4.1 Communications and Operations Management

Responsibilities will be established in information security policies.

Operational procedures and responsibilities

ISO/IEC 27002:2007	***10.1 To ensure the correct and secure operation of information processing facilities.***

Documentation includes all types of security 'policy', including operating procedures and contingency plans.

Configuration management includes change management organisation and the processes and procedures that control changes to configurations. This ensures that changes to ICT systems do not introduce security vulnerabilities by reducing the effectiveness of existing safeguards.

AS ISO 10007:2003 *Quality management systems – Guidelines for configuration management* provides authoritative information. The key to configuration management is identification of configuration items (CIs). They may be synonymous with some individual information assets but also include documents, and the rules and settings of ICT security devices. The standard provides a format for a configuration management plan that addresses the major elements of configuration management: configuration identification, change control, configuration status accounting and configuration audit. *ISO/IEC 20000-2:2005 Information technology – Service management – Part 2 – Code of practice* (ITIL) is recognised as providing good guidance on change management.

Change management should ensure that the movement of code from development to testing and production (operations) is done in a controlled and authorised manner. Segregation of duties is desirable so as to reduce the risk of accidental or deliberate change or unauthorised access to operational software and data.

Operational libraries should only be updated by authorised operational staff. Audit logs should be maintained for all access to Operational program source and object libraries.

Third party service delivery management

ISO/IEC 27002:2007	***10.2 To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.***

Concerns the security aspects of operational or development services delivered by third parties.

Outsourced IT facilities can introduce security exposures, such as unauthorised access, damage or loss of data at the outsourced facility. Risks should be identified and addressed in the outsourcing agreement.

Specific security issues that need to be addressed are:

- Determining whether sensitive data and or applications can be outsourced.
- Defining the security standards to be applied and how compliance is to be measured.
- Obtaining authorisation from information owners.
- Defining security roles and responsibilities for monitoring, reporting and handling incidents.
- Business continuity requirements and responsibilities

Outsourced software development requires consideration of the following issues:

- Quality assurance procedures to be applied, including the rights and obligations of the Agency and Outsourcer.
- Licensing arrangements and ownership of code.
- Rights to software in the event of financial failure of the outsourcer.

Monitoring and review of third party services should be integrated with similar internal activities.

Typically, change management, including configuration management, will be a joint activity between the parties.

Systems planning and acceptance

ISO/IEC 27002:2007 10.3 To minimise the risk of system failures.

Capacity planning should be used to avoid failures due to inadequate capacity. In planning future capacity requirements for a system, current trends should be taken into account. Potential bottlenecks should be avoided that could cause a threat to system security or user access.

System Testing, which tests that the system meets its System Requirement, must be completed, before the system is handed over to the business users for Acceptance Testing. System Testing must be planned and comprehensive in scope. Live data should not be used for System Testing. During System Testing, safeguards over test data need to be implemented. These safeguards may include:

- All actual data should be changed prior to use
- Authorisation should be obtained every time copies of actual data are made
- Where live data is used it should be deleted after use
- Logs should be updated when copying of operational data is made.

System Testing must ensure that security functional and non-functional requirements are met, including fail-soft modes. Acceptance Testing should include the useability of the security safeguards.

Protection against malicious code

ISO/IEC 27002:2007 10.4 To protect the integrity of software and information.

Viruses, trojans, worms and spyware are all examples of malicious code. Malicious code may also compromise confidentiality, integrity or availability. Safeguards involve both technology and user awareness, including social engineering aspects.

Safeguards need to be in place to avoid, protect, detect and correct the effects of malicious code. The malicious software threat is very varied, dynamic and pervasive, single point solutions are unlikely to sufficiently reduce the risk. While external email is the most pervasive threat channel, there are other routes for malicious software to enter an organisation.

The threat of targeted attack is increasing, and attacking a ‘low risk’ agency as path to others is a possibility.

Back-up

ISO/IEC 27002:2007 10.5 To maintain the integrity and availability of information and information processing facilities.

Information back-up is an essential element of any information security management system. It would be exceptional if off-site backup was not justifiable.

Network security management

ISO/IEC 27002:2007 10.6 To ensure the protection of information in networks and the protection of the supporting infrastructure.

While there is a threat to information transiting networks, this should not be over-estimated.

Media handling

ISO/IEC 27002:2007 10.7 To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

Accountability for media should be clearly defined, particularly in respect of easily removed media such as disks, back-up tapes, memory sticks and paper. Media that contains sensitive or classified data must be distinguished from other media.

Media brought into an installation should be added to the inventory. In maintaining an inventory it is essential that removable media are labelled. Media stocktakes should be regularly scheduled so that any lost items are quickly identified and action taken to recover them if possible.

Disposal of sensitive media should be logged to maintain an audit trail. Where the media containing sensitive data can be reused, it must have the data erased before being reused.

Exchange of Information

ISO/IEC 27002:2007 10.8 To maintain the security of information and software exchanged within an organisation and with any external entity.

Information exchange may be by physical media or electronic. Electronic exchange can use a variety of protocols. E-mail is only one of channels available via public networks. Others include FTP, HTTP, Instant Messaging and Peer-to-Peer.

Anybody in an organisation may be in a position to exchange information both wittingly and unwittingly. Awareness training is a key element in managing the risks.

Exchanges of data between organisations should be controlled and comply with relevant legislation and the sending organisation's privacy policies.

For sensitive information see Premier's Circular 2002-69 and *Guide to Labelling Sensitive Information*. Commonwealth rules apply to national security classified information.

Only reputable couriers or postal services should be used. Protective packaging should be utilised to protect the contents from physical damage.

Agencies should develop an e-mail and instant messaging (IM) policy that addresses the following:

- When it is appropriate to use e-mail and IM.

- What can be said in e-mails and IM on the agency's behalf.
- How to protect e-mail and IM from viruses.
- Caution to be applied when opening e-mail and IM attachments.
- Responsibilities in respect of e-mail and IM usage (not to defame others, not to use profanities, not to send private e-mails or IM, not to send spam mail or harassment).
- Retention policies.
- Use of cryptography to protect confidentiality, integrity and authenticity.
- Use of digital signatures to authenticate originators and provide evidence against repudiation.

In some circumstances it may be important to ensure that email recipients cannot deny receipt of an email or sending an email.

Electronic office systems include computers, laptops, mail, voicemail, fax, multimedia and postal services. These systems provide for speedier distribution of information. Policies need to be implemented to control what is distributed and how it is distributed.

Electronic commerce services

ISO/IEC 27002:2007 10.9 To ensure the security of electronic commerce services, and their secure use.

In the NSW government context electronic commerce services include any form of service delivery using electronic channels.

Authentication should comply with the Australian Government Authentication Framework (AGAF) and should use 'common use' credentials.

Electronic commerce between trading partners should be supported by a written agreement that clearly states the terms upon which they are to transact business.

Transactions involving personal information must comply with the *Privacy and Personal Information Protection Act*. Transactions involving payment cards must comply with the *Payment Card Industry – Data Security Standards* (PCI-DSS).

The risks of web site defacement should be considered.

Agencies must not publish data which has been provided by the public and which is confidential in nature and protected by law.

At least one firewall should be installed between the web server and the external network and also between the internal network and the web server. In effect the web server is maintained in what is termed a "demilitarised zone". Different firewalls should be used to complicate an attackers task.

Monitoring

ISO/IEC 27002:2007 10.10 To detect unauthorised information processing activities.

Without appropriate audit records it is difficult to hold users and operators accountable for their actions.

Monitoring the performance of security safeguards is an essential element in the Plan – Do – Check - Act cycle.

The length of retention of audit logs is a policy matter, at the absolute minimum it should be sufficient to support the investigation of security incidents. Two archive copies of all logs should be kept one locally and one at the designated offsite backup.

The files containing audit trails should be protected by the operating system against alteration or deletion. It should be recognised that in some situations the System Supervisor can alter log files (Unix Root access). Audit trails should be implemented such that there can be no loss of records. If disk space is unavailable then the system should stop processing.

Fault logs must be reviewed to ensure there are no outstanding issues and that corrective action is appropriate and does not compromise security.

To ensure accuracy of audit log data, the computer system clocks should be synchronised. This is important especially when daylight saving changes occur, normally in late October and March.

4.2 Access Control

User responsibilities

ISO/IEC 27002:2007 11.3 To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

Good security practices by users are essential. These are an important safeguard against internal threats.

4.3 Incident Management

ISO/IEC 27002:2007 13.2.3 Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules of evidence laid down in the relevant jurisdictions(s).

Policies for legal or disciplinary action should be established as part of organisational and management planning activities.

5 Technical Safeguards

Technical safeguards must be implemented to maintain data integrity and confidentiality, and authorised access to systems. Safeguards will restrict access to information, computers, networks, applications, system resources, files and programs.

5.1 Access Control

User access management

ISO/IEC 27002:2007 11.2 To ensure authorised user access and prevent unauthorised access to information systems.

Identification is the means by which a user provides a claimed identity to a system. Authentication is the means by which this claim is verified. Once authenticated then a user can be given system access in accordance with their authorisation and the business rules for their authorised application.

Authorisation and business rules control the resources users can access and the types of access permitted. An access control policy should be created which clearly defines, for each user or group of users, their access rights. This policy should be determined by the organisational or business needs of the Agency. Access should be granted on the basis of "as many rights as are necessary, and as few rights as are possible". The access management system should provide a view listing all access rights for any named individual.

The Access Control policy should:

- Identify the resources that require confidentiality or integrity protection.
- Define how user access will be managed, how new users are added and old users deleted.
- Define how users' access will be managed in a distributed environment.
- Define any legislative obligations or contractual requirements with regard to access.
- Define how access to data, services and applications will be controlled including number of grace logins when incorrect password is entered.
- Define Access review policies.

All access rights given to users should be reviewed regularly and updated if the security or business needs for access have changed. Privileged access rights should be reviewed more frequently to ensure that they are not misused. Access rights should be withdrawn immediately they are no longer required.

There are three types of "authentication" that are available to the user and known to the verifier:

- What a **User knows**. Eg passwords or phrases, PIN.
- What a **User has**. Eg tokens such as magnetic cards, fobs and smartcards.
- What a **User is**. Biometric methods such as finger prints, iris scans or voice recognition.

Passwords are easy to implement, change and are inexpensive. Most user access systems employ them. Unfortunately they are also the easiest to compromise and require security aware users to be effective. Bad password management practices contribute to weak password controls. Examples of this include:

- Using short or simple passwords,
- Writing down passwords,
- Sharing passwords, and
- Not changing passwords regularly.

An effective password management policy has to balance password useability with password strength. Passwords that are difficult to remember are likely to be written down. Effective policy should include:

- Choosing passwords which are not found in the dictionary.
- Choosing passwords that are a combination of alphabetic characters, numbers and special characters that are meaningful to users.
- Using a combination of upper and lower case characters.
- Choosing passwords with a minimum length of 8 characters.
- Changing passwords every 30 days.
- Preventing a password that has been used in the last 10 cycles.
- Disabling all default userid's such as Guest.
- All userid's must require a password.
- Not retaining written records of passwords.

- Password confidentiality must be maintained.
- Passwords not displayed during entry.
- Requirement to enter old password when changing to new password.
- Storing passwords encrypted using a one way encryption algorithm.

When a user enters an incorrect userid & password combination then the system should allow no more than two further attempts before locking the user account and requiring the systems administrator to intervene.

The strength of passwords should be verified by the use of Password cracking programs such as L0phtcrack (available for NT Systems) that can be run by the Systems Administrators. Any weak passwords will be revealed quickly and can then be changed. Other threats to passwords include the use of “sniffers” which eavesdrop on the network and capture password hashes or data for cracking at a later time.

Given the relative weakness of passwords compared to Tokens or Biometrics it is strongly recommended that if a system requires a high degree of confidentiality or integrity then an authentication method **other** than passwords be used. Tokens using ‘one-time’ techniques may be appropriate.

Biometrics require careful choice, it may not be possible to enrol every person for a particular biometric and they may be unsuitable for some environments. Furthermore some biometrics may be ‘spoofed’ and some legitimate users may take several attempts to achieve a successful authentication, particularly before they are habituated, and infrequent users may never become habituated.

All user workstations should be located in secure areas. When users leave their workstations they should log off the system or lock their screen. An unattended workstation can be used by an attacker to:

- Gain unauthorised access to data,
- Be used to perform an unauthorised transaction for which the user who was logged on will be accountable,
- Insert malicious software,
- Steal the workstation or parts of it.

Inactive terminals in high risk areas should have automatic shutdown following a period of inactivity.

Network access control

ISO/IEC 27002:2007 11.4 To prevent unauthorised access to network services.

Network access control involves controlling direct access by users and access paths across network boundaries.

Network boundaries are themselves security safeguards and require that traffic across a boundary only occurs in a controlled way. Partitioning networks into controlled segments is an important means of protecting specific information assets.

The main concern is real-time traffic and the main source of unauthorised real-time traffic is unauthorised network connections. Typically these are incorrectly configured wireless devices or workstations whose user’s establish ‘feral’ connections using wireless or line modems.

There are two sources of vulnerabilities in the controlled connections between networks. First, that connection controlling devices are incorrectly configured or inappropriate for the task. Second, malware delivering exploitable vulnerabilities can be introduced through other channels. These include code downloaded from web sites, delivered by messaging, by off-line media or by mobile devices including those used for remote access. Historically these threats have been random but targeted attacks using social engineering techniques are emerging. Related threats are phishing attacks that persuade legitimate users to compromise their network access credentials or the targeted theft of mobile devices for these credentials.

Use of simple dial-in access for remote users is deprecated. Generally, virtual private networks should be used and mobile devices have robust authentication of their users.

Advance planning and monitoring should be undertaken to enable reliable functioning and performance of the networks. Changes to networks should be controlled and any impacts on existing safeguards evaluated. Documentation of the network must also be up to date so that the network can be maintained. Any changes to the configuration of any component on the network must be subject to configuration management.

A standard approach for network configuration should be established, including any special protection by firewalls. This includes a standardised approach to the server configuration throughout the agency. Servers that are used as firewalls should be dedicated to that task, ie no other software should be running on them.

A firewall is a hardware and or software device to prevent data flows prohibited by security policies. Firewalls control data flows, in either direction, between networks. There are various types of firewall, each with different strengths and weaknesses. It may be necessary to use different types in series. Some types of protocol, such as peer-to-peer, can circumvent some firewalls.

To be fully effective and trustworthy within its technical capability a firewall must have a Firewall Security Policy defining functionality, configuration and security management, and be supported by security incident response procedures, and:

- Be immune to unauthorised changes via either network.
- Filter all traffic between the networks.
- Only pass authorised traffic as defined by a firewall security policy,.
- The default firewall policies must deny connections between networks.
- Provide a trusted path for its management.
- Have software patches must be applied promptly.
- Be regularly tested for weaknesses.
- Have audit capability to detect breaches and attempted network intrusions.
- Have audit logs reviewed regularly.
- Be under effective configuration management.
- Have its policy settings periodically audited.
- Have its design and implementation independently evaluated to Common Criteria (ISO/IEC 15408).

Monitoring the network enables identification of weaknesses in the network configuration. Routes of messages should be regularly monitored, so that weaknesses can be identified and re-arrangements made. Monitoring also provides the ability to identify attackers and can be used to tune the network.

Connection to a public network such as the Internet raises the risks of external attack. All network connections to the Internet must be protected by a suitable Firewall.

Technical policies for email, file transfers and downloads, accessing of sites, etc, must be developed and implemented. It is strongly recommended that Web Servers are separated from the rest of the Agency's networks by an internal firewall.

Operating System Access Control

ISO/IEC 27002:2007 11.5 To prevent unauthorised access to operating systems.

From a security perspective, operating system access is privileged access and should be limited to as few people as possible.

Application Access Control

ISO/IEC 27002:2007 11.6 To prevent unauthorised access to information held in application systems.

Some applications may be considered so sensitive that they warrant running on a separate dedicated computer system. This sensitivity may be due to the sensitive nature of the held.

5.2 Information Systems Acquisition, Development and Maintenance

Using risk management, security considerations must be addressed at all stages of system procurement. This includes the procurement activities, measures to ensure that off the shelf or developed applications have appropriate security features and that any development and integration does not introduce security vulnerabilities.

Correct processing in applications

ISO/IEC 27002:2007 12.2 To prevent errors, loss, unauthorised modification or misuse of information in applications.

Application safeguards should be designed into systems to provide appropriate assurance for the accuracy and integrity of the data held. Even when developed to rigorous standards applications are still reliant on the quality of data to ensure the integrity of the processed results. It is particular important to ensure that only data within defined parameters can be entered into an application.

Other possible safeguards include:

- Check digits on important fields e.g. (Tax file numbers).
- Sequence checks e.g. (Invoice numbers should be consecutive).
- Consistency checks e.g. (Age must be > 15).
- Matching of data with master file e.g. (Customer doesn't exist on file).
- Scanning of pre-printed data e.g. (Bar codes).

Cryptographic safeguards

ISO/IEC 27002:2007 12.3 To protect the confidentiality, authenticity or integrity of information by cryptographic means.

The need for cryptographic safeguards will be decided after a risk assessment.

In circumstances where integrity of data is important, hash functions, digital signatures and integrity safeguards should be considered.

When an electronic transaction is sent by the originator and the other parties act on that transaction, a method may be required to stop the originator repudiating or denying that he sent the transaction. Non-repudiation is the process of assuring that the originator sent the message. Use of Digital signatures can provide this non-repudiation capability.

Security of system files

ISO/IEC 27002:2007 12.4 To ensure the security of system files.

From a security perspective, system file access is privileged access.

Security in development and support processes

ISO/IEC 27002:2007 12.5 To maintain the security of application system software and information.

Development and support processes provide significant opportunities to affect the future confidentiality, integrity and availability of information assets. This is particularly the case when software engineering processes and procedures are weak or informal.

Technical Vulnerability Management

ISO/IEC 27002:2007 12.6 To reduce risks resulting from exploitation of published technical vulnerabilities.

Vulnerability management should be fully integrated with change and configuration management.

Appendix A – Classification of Safeguards

This list is a guide that classifies the safeguards in clauses in ISO/IEC 27002:2007 to six control functions. The functions are:

Deter: Prevent or reduce the likelihood of an undesirable event being attempted.

Avoid: Eliminate known vulnerabilities and prevent new ones being created.
Protect: Safeguard the information assets with vulnerabilities or exposures from adverse security events.

Detect: Identify the occurrence of an undesirable security event and initiate protective, reactive or recovery safeguards.

React: Respond to or counter a security event to minimize its impact and ensure business continuity.

Recover: Restore the integrity, availability and confidentiality of information assets to their expected state.

Control Name	ISO/IEC 27002:2007	Control Function					
		Deter	**Avoid**	**Pro-tect**	**De-tect**	**React**	**Re-cover**
Security policy	**5**						
Information Security Policy	**5.1**						
Information security policy document	5.1.1	✓	✓	✓		✓	✓
Review of the information security policy	5.1.2	✓	✓	✓		✓	✓
Organisation and information security							
Internal organisation	**6.1**						
Management commitment to information security	6.1.1	✓	✓	✓		✓	✓
Information security co-ordination	6.1.2		✓	✓		✓	✓
Allocation of information security responsibilities	6.1.3		✓	✓	✓	✓	✓
Authorisation process for information processing facilities	6.1.4		✓				
Confidentiality agreements	6.1.5		✓	✓			
Contact with authorities	6.1.6		✓			✓	
Contact with special interest groups	6.1.7		✓	✓	✓		
Independent review of information security	6.1.8		✓	✓	✓	✓	✓
External parties	**6.2**						
Identification of risks related to external parties	6.2.1	✓	✓	✓			
Addressing security when dealing with customers	6.2.2	✓	✓	✓			
Addressing security in third party agreements	6.2.3	✓	✓	✓	✓	✓	✓
Asset management	**7**						
Responsibility for assets	**7.1**						
Inventory of assets	7.1.1		✓	✓			✓
Ownership of assets	7.1.2		✓	✓	✓	✓	✓
Acceptable use of assets	7.1.3		✓	✓			
Information calssification	**7.2**						
Classification guidelines	7.2.1		✓				
Information labelling and handling	7.2.2	✓		✓	✓		
Human resources security	**8**						
Prior to employment	**8.1**						

Control Name	ISO/IEC 27002:2007	Control Function					
		Deter	Avoid	Pro-tect	De-tect	React	Re-cover
Roles and responsibilities	8.1.1	✓	✓	✓			
Screening	8.1.2	✓	✓				
Terms and conditions of employment	8.1.3	✓	✓				
During employment	**8.2**						
Management responsibilities	8.2.1	✓	✓	✓	✓		
Information security awarensss, education and training	8.2.2	✓	✓	✓	✓		
Disciplinary process	8.2.3	✓	✓	✓	✓		
Termination or change of employment	**8.3**						
Termination of responsibilities	8.3.1		✓	✓			
Return of assets	8.3.2		✓				
Removal of access rights	8.3.3		✓	✓			
Physical and environmental security	**9**						
Secure areas	**9.1**						
Physical security perimeter	9.1.1	✓	✓	✓			
Physical entry safeguards	9.1.2	✓	✓	✓	✓		
Securing offices, rooms and facilities	9.1.3	✓	✓	✓	✓		
Protecting against external and environmental threats	9.1.4		✓	✓			
Working in secure areas	9.1.5	✓		✓			
Public access, delivery and loading areas	9.1.6	✓	✓	✓			
Equipment security	**9.2**						
Equipment siting and protection	9.2.1		✓	✓	✓		
Supporting utilities	9.2.2		✓	✓		✓	✓
Cabling security	9.2.3			✓			
Equipment maintenance	9.2.4		✓	✓	✓		
Security of equipment off-premises	9.2.5		✓				
Security disposal or re-use of equipment	9.2.6	✓	✓	✓			
Removal of property	9.2.7	✓	✓	✓	✓		
Communications and operations management	**10**						
Operatinal procedures and responsibilities	**10.1**						
Documented operating procedures	10.1.1		✓	✓		✓	✓
Change management	10.1.2	✓	✓	✓			
Segregation of duties	10.1.3	✓	✓	✓			
Separation of development, test and operational facilities	10.1.4	✓	✓	✓			
Third party service delivery management	**10.2**						
Service delivery	10.2.1	✓	✓	✓	✓	✓	✓
Monitoring and review of third party services	10.2.2				✓		
Managing changes to third party services	10.2.3		✓	✓			
System planning and acceptance	**10.3**						
Capacity management	10.3.1		✓				
System acceptance	10.3.2			✓	✓		
Protection against malicious and mobile code	**10.4**						
Safeguards against malicious code	10.4.1	✓		✓	✓	✓	✓
Safeguards against mobile code	10.4.2		✓	✓			
Back-up	**10.5**						
Information back-up	10.5.1		✓	✓			✓

Control Name	ISO/IEC 27002:2007	Control Function					
		Deter	Avoid	Pro-tect	De-tect	React	Re-cover
Network security management	**10.6**						
Network controls	10.6.1			✓			
Security of network services	10.6.2		✓	✓	✓		
Media handling	**10.7**						
Management of removable media	10.7.1	✓	✓	✓			
Disposable of media	10.7.2		✓	✓			
Infromation handling procedures	10.7.3		✓	✓			
Security of system documentation	10.7.4			✓			
Exchange of information	**10.8**						
Information exchange policies and procedures	10.8.1		✓	✓			
Exchange agreements	10.8.2		✓	✓			
Physical media in transit	10.8.3		✓	✓			
Electronic messaging	10.8.4	✓		✓			
Business information systems	10.8.5	✓		✓			✓
Electronic commerce services	**10.9**						
Electronic commerce	10.9.1	✓	✓	✓			
On-line transactions	10.9.2	✓	✓	✓			
Publicly available information	10.9.3			✓			
Monitoring	**10.10**						
Audit logging	10.10.1	✓			✓	✓	
Monitoring system use	10.10.2	✓			✓	✓	
Protection of log information	10.10.3	✓	✓	✓			
Administrator and operator logs	10.10.4	✓			✓		
Fault logging	10.10.5				✓		✓
Clock synchronisation	10.10.6		✓	✓			
Access control	**11**						
Business requirments for access control	**11.1**						
Access control policy	11.1.1	✓		✓			
User access management	**11.2**						
User registration	11.2.1	✓	✓				
Priviledge management	11.2.2		✓	✓			
User password management	11.2.3			✓			
Review of user access rights	11.2.4	✓		✓	✓		
User responsibilities	**11.3**						
Password use	11.3.1		✓	✓			
Unattended user equipment	11.3.2	✓		✓			
Clear desk and clear screen policy	11.3.3		✓	✓			
Network access control	**11.4**						
Policy on use of network services	11.4.1		✓	✓			
User authenrication for external connection	11.4.2	✓	✓	✓			
Equipment identification in networks	11.4.3	✓	✓	✓			
Remote diagnostic and configuration port protection	11.4.4		✓	✓			
Segregation of networks	11.4.5	✓		✓			
Network connection control	11.4.6	✓		✓			
Network routing control	11.4.7	✓		✓			
Operating system access control	**11.5**						
Secure Logon Procedures	11.5.1	✓	✓	✓			

Control Name	ISO/IEC 27002:2007	Control Function					
		Deter	Avoid	Pro-tect	De-tect	React	Re-cover
User identification and authentication	11.5.2	✓		✓			
Password management system	11.5.3	✓		✓			
Use of system utilities	11.5.4			✓			
Session time-out	11.5.5	✓		✓		✓	
Limited connection time	11.5.6	✓	✓				
Application and information access control	**11.6**						
Information access restriction	11.6.1	✓		✓			
Sensitive system isolation	11.6.2	✓		✓			
Mobile computing and teleworking	**11.7**						
Mobile computing and communications	11.7.1			✓			
Teleworking	11.7.2			✓			
Information systems acquisition, development and maintenance	**12**						
Security requirements of information systems	**12.1**						
Security requirements analysis and specification	12.1.1		✓				
Correct processing in applications	**12.2**						
Input data validation	12.2.1		✓				
Control of internal processing	12.2.2			✓			
Message integrity	12.2.3		✓				
Output data validation	12.2.4			✓			
Cryptographic safeguards	**12.3**						
Policy on the use of cryptographic Safeguards	12.3.1		✓				
Key management	12.3.2		✓				
Security of system files	**12.4**						
Control of operational software	12.4.1		✓				
Protection of system test data	12.4.2			✓			
Access control to program source code	12.4.3		✓	✓			
Security in development and support processes	**12.5**						
Change control procedures	12.5.1		✓				
Technical review of applications after operating system changes	12.5.2				✓		
Rectrictions on changes to software packages	12.5.3		✓	✓			
Information leakage	12.5.4		✓	✓			
Outsourced software development	12.5.5	✓	✓	✓			
Technical Vulnerability Management	**12.6**						
Control of technical vulnerabilities	12.6.1		✓				
Information security incident management	**13**						
Reporting informatin security events and weaknesses	**13.1**						
Reporting information security events	13.1.1				✓	✓	
Reporting security weaknesses	13.1.2	✓			✓		
Management of information security incidents and improvements	**13.2**						
Responsibilities and procedures	13.2.1					✓	✓
Learning from information incidents	13.2.2		✓				✓
Collection of evidence	13.2.3	✓		✓		✓	
Business continuity management	**14**						

Control Name	ISO/IEC 27002:2007	Control Function					
		Deter	Avoid	Protect	Detect	React	Recover
Information security aspects of business continuity management	**14.1**						
Including information security in the business continuity management process	14.1.1		✓			✓	✓
Business continuity and risk assessment	14.1.2		✓			✓	✓
Developing and implementing continuity plans including information security	14.1.3						✓
Business continuity planning framework	14.1.4					✓	✓
Testing, maintaining and re-assessing business continuity plans	14.1.5					✓	✓
Compliance	**15**						
Compliance with legal requirements	**15.1**						
Identification of applicable legislation	15.1.1			✓			
Intellectual property rights (IPR)	15.1.2			✓			
Protection of organisational records	15.1.3			✓		✓	✓
Data protection and privacy of personal information	15.1.4			✓			
Prevention of misuse of information processing facilities	15.1.5	✓		✓			
Regulation of cryptographic safeguards	15.1.6			✓			
Compliance withg security policies and staandards, and technical compliance	**15.2**						
Compliance with security policies and standards	15.2.1	✓			✓		
Technical compliance checking	15.2.2					✓	
Information systems audit considerations	**15.3**						
Information system audit safeguards	15.3.1	✓			✓		
Protection of information systems audit tools	15.3.2			✓	✓		

Appendix B - Safeguards by Security Concern

This Appendix lists the standard safeguards against the security concerns.

Control Name	ISO/IEC 27001:2007	Security Concern		
		Confid-entiality	Integrity	Availab-ility
Security policy	**5**			
Information Security Policy	**5.1**			
Information security policy document	5.1.1	✓	✓	✓
Review of the information security policy	5.1.2	✓	✓	✓
Organisation and information security	**6**			
Internal organisation	**6.1**			
Management commitment to information security	6.1.1	✓	✓	✓
Information security co-ordination	6.1.2	✓	✓	✓
Allocation of information security responsibilities	6.1.3	✓	✓	✓
Authorisation process for information processing facilities	6.1.4	✓	✓	✓
Confidentiality agreements	6.1.5	✓		
Contact with authorities	6.1.6	✓	✓	✓
Contact with special interest groups	6.1.7	✓	✓	✓
Independent review of information security	6.1.8	✓	✓	✓
External parties	**6.2**			
Identification of risks related to external parties	6.2.1	✓	✓	✓
Addressing security when dealing with customers	6.2.2	✓	✓	✓
Addressing security in third party agreements	6.2.3	✓	✓	✓
Asset management	**7**			
Responsibility for assets	**7.1**			
Inventory of assets	7.1.1	✓	✓	✓
Ownership of assets	7.1.2	✓	✓	✓
Acceptable use of assets	7.1.3	✓	✓	✓
Information calssification	**7.2**			
Classification guidelines	7.2.1		✓	✓
Information labelling and handling	7.2.2	✓	✓	✓
Human resources security	**8**			
Prior to employment	**8.1**			
Roles and responsibilities	8.1.1	✓	✓	
Screening	8.1.2	✓	✓	✓
Terms and conditions of employment	8.1.3	✓	✓	✓
During employment	**8.2**			
Management responsibilities	8.2.1	✓	✓	✓
Information security awarenss, education and training	8.2.2	✓	✓	✓
Disciplinary process	8.2.3	✓	✓	✓
Termination or change of employment	**8.3**			
Termination of responsibilities	8.3.1	✓	✓	✓
Return of assets	8.3.2	✓	✓	✓
Removal of access rights	8.3.3	✓	✓	✓
Physical and environmental security	**9**			
Secure areas	**9.1**			
Physical security perimeter	9.1.1	✓	✓	✓

Physical entry safeguards	9.1.2	✓	✓	✓
Securing offices, rooms and facilities	9.1.3	✓	✓	✓
Protecting against external and environmental threats	9.1.4			✓
Working in secure areas	9.1.5	✓	✓	✓
Public access, delivery and loading areas	9.1.6	✓	✓	✓
Equipment security	**9.2**			
Equipment siting and protection	9.2.1	✓	✓	✓
Supporting utilities	9.2.2			✓
Cabling security	9.2.3	✓		✓
Equipment maintenance	9.2.4		✓	✓
Security of equipment off-premises	9.2.5	✓	✓	✓
Security disposal or re-use of equipment	9.2.6	✓		
Removal of property	9.2.7	✓	✓	✓
Communications and operations management	**10**			
Operatinal procedures and responsibilities	**10.1**			
Documented operating procedures	10.1.1	✓	✓	✓
Change management	10.1.2	✓	✓	✓
Segregation of duties	10.1.3	✓	✓	✓
Separation of development, test and operational facilities	10.1.4	✓	✓	✓
Third party service delivery management	**10.2**			
Service delivery	10.2.1	✓	✓	✓
Monitoring and review of third party services	10.2.2	✓	✓	✓
Managing changes to third party services	10.2.3	✓	✓	✓
System planning and acceptance	**10.3**			
Capacity management	10.3.1			✓
System acceptance	10.3.2			✓
Protection against malicious and mobile code	**10.4**			
Safeguards against malicious code	10.4.1		✓	✓
Safeguards against mobile code	10.4.2		✓	✓
Back-up	**10.5**			
Information back-up	10.5.1		✓	✓
Network security management	**10.6**			
Network controls	10.6.1	✓	✓	✓
Security of network services	10.6.2	✓	✓	✓
Media handling	**10.7**			
Management of removable media	10.7.1	✓	✓	✓
Disposable of media	10.7.2	✓	✓	✓
Infromation handling procedures	10.7.3	✓	✓	✓
Security of system documentation	10.7.4	✓	✓	
Exchange of information	**10.8**			
Information exchange policies and procedures	10.8.1	✓	✓	✓
Exchange agreements	10.8.2	✓	✓	
Physical media in transit	10.8.3			✓
Electronic messaging	10.8.4	✓	✓	✓
Business information systems	10.8.5	✓	✓	
Electronic commerce services	**10.9**			
Electronic commerce	10.9.1	✓	✓	
On-line transactions	10.9.2	✓	✓	
Publicly available information	10.9.3		✓	

Monitoring	**10.10**			
Audit logging	10.10.1	✓	✓	✓
Monitoring system use	10.10.2	✓	✓	
Protection of log information	10.10.3	✓	✓	✓
Administrator and operator logs	10.10.4	✓	✓	✓
Fault logging	10.10.5			✓
Clock synchronisation	10.10.6		✓	
Access control	**11**			
Business requirments for access control	**11.1**			
Access control policy	11.1.1	✓	✓	
User access management	**11.2**			
User registration	11.2.1	✓	✓	
Priviledge management	11.2.2	✓	✓	
User password management	11.2.3	✓	✓	
Review of user access rights	11.2.4	✓	✓	
User responsibilities	**11.3**			
Password use	11.3.1	✓	✓	
Unattended user equipment	11.3.2	✓	✓	
Clear desk and clear screen policy	11.3.3	✓		
Network access control	**11.4**			
Policy on use of network services	11.4.1	✓	✓	
User authenrication for external connection	11.4.2	✓	✓	
Equipment identification in networks	11.4.3	✓	✓	
Remote diagnostic and configuration port protection	11.4.4	✓	✓	✓
Segregation of networks	11.4.5	✓	✓	
Network connection control	11.4.6	✓	✓	
Network routing control	11.4.7	✓	✓	
Operating system access control	**11.5**			
Secure Logon Procedures	11.5.1	✓	✓	
User identification and authentication	11.5.2	✓	✓	
Password management system	11.5.3	✓	✓	
Use of system utilities	11.5.4	✓	✓	✓
Session time-out	11.5.5	✓	✓	
Limited connection time	11.5.6	✓	✓	
Application and information access control	**11.6**			
Information access restriction	11.6.1	✓	✓	
Sensitive system isolation	11.6.2	✓	✓	
Mobile computing and teleworking	**11.7**			
Mobile computing and communications	11.7.1	✓	✓	✓
Teleworking	11.7.2	✓	✓	
Information systems acquisition, development and maintenance	**12**			
Security requirements of information systems	**12.1**			
Security requirements analysis and specification	12.1.1	✓	✓	✓
Correct processing in applications	**12.2**			
Input data validation	12.2.1		✓	
Control of internal processing	12.2.2		✓	
Message integrity	12.2.3		✓	
Output data validation	12.2.4		✓	

Cryptographic safeguards	**12.3**			
Policy on the use of cryptographic Safeguards	12.3.1	✓	✓	
Key management	12.3.2	✓	✓	
Security of system files	**12.4**			
Control of operational software	12.4.1	✓	✓	✓
Protection of system test data	12.4.2		✓	
Access control to program source code	12.4.3		✓	
Security in development and support processes	**12.5**			
Change control procedures	12.5.1		✓	✓
Technical review of applications after operating system changes	12.5.2		✓	
Rectrictions on changes to software packages	12.5.3		✓	
Information leakage	12.5.4	✓		
Outsourced software development	12.5.5	✓	✓	
Technical Vulnerability Management	**12.6**			
Control of technical vulnerabilities	12.6.1		✓	
Information security incident management	**13**			
Reporting informatin security events and weaknesses	**13.1**			
Reporting information security events	13.1.1	✓	✓	✓
Reporting security weaknesses	13.1.2	✓	✓	✓
Management of information security incidents and improvements	**13.2**			
Responsibilities and procedures	13.2.1	✓	✓	✓
Learning from information incidents	13.2.2	✓	✓	✓
Collection of evidence	13.2.3	✓	✓	✓
Business continuity management	**14**			
Information security aspects of business continuity management	**14.1**			
Including information security in the business continuity management process	14.1.1			✓
Business continuity and risk assessment	14.1.2			✓
Developing and implementing continuity plans including information security	14.1.3			✓
Business continuity planning framework	14.1.4			✓
Testing, maintaining and re-assessing business continuity plans	14.1.5			✓
Compliance	**15**			
Compliance with legal requirements	**15.1**			
Identification of applicable legislation	15.1.1	✓	✓	✓
Intellectual property rights (IPR)	15.1.2	✓		
Protection of organisational records	15.1.3	✓	✓	✓
Data protection and privacy of personal information	15.1.4	✓		
Prevention of misuse of information processing facilities	15.1.5			✓
Regulation of cryptographic safeguards	15.1.6	✓		
Compliance withg security policies and standards, and technical compliance	**15.2**			
Compliance with security policies and standards	15.2.1	✓	✓	✓
Technical compliance checking	15.2.2	✓	✓	
Information systems audit considerations	**15.3**			
Information system audit safeguards	15.3.1			✓
Protection of information systems audit tools	15.3.2		✓	