LICENCE

for

HB 231:2004 Information security risk management guidelines

Licensee: Mrs Anne Botting

Date: Tuesday, February 01, 2011 4:02 PM

WEB LINKS

HB 231:2004

Information security risk management guidelines

STANDARDS AUSTRALIA

STANDARDS NEW ZEALAND
Paerewa Aotearoa

Handbook

Information security risk management guidelines

Originated as HB 231:2000.
Second edition 2004.

Jointly published by Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 5649 2

This page left intentionally blank

Preface

The vulnerability of today's information society is still not sufficiently realised: Businesses, administrations and society depend to a high degree on the efficiency and security of modern information technology. In the business community, for example, most of the monetary transactions are administered by computers in the form of deposit money. Electronic commerce depends on safe systems for money transactions in computer networks. A company's entire production frequently depends on the functioning of its data-processing system. Many businesses store their most valuable company secrets electronically. Marine, air, and space control systems, as well as medical supervision, rely to a great extent on modern computer systems. Computers and the Internet also play an increasing role in the education and leisure of minors. International computer networks are the nerves of the economy, the public sector and society. The security of these computer and communication systems is therefore of essential importance.

European Commission 1998

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities.

OECD 2002

Information security risk management forms the basis for an assessment of an organization's information security framework. With increasing electronic networking between organizations for a very wide range of applications, which impacts on most aspects of life in our society, there is a clear benefit in having a common set of reference documents for information security management. This enables mutual trust to be established between networked sites and trading partners and provides a basis for management of facilities between information users and service providers. Security for information systems is an essential requirement at organizational, national and international levels.

This handbook was revised in 2003 to be consistent with AS/NZS 7799.2:2003.

This Joint Australia/New Zealand Handbook has been prepared by Committee IT-012, Information Systems, Security and Identification Technology. This publication extends the generic work done by Committee OB/7, Risk Management to specifically address the area of information security management. Information security risk management guidelines issued by the International Organization for Standardization (ISO) as ISO/IEC TR 13335, *Information technology—Guidelines for the management of IT security* have been adapted to align with the Australian and New Zealand Standard AS/NZS 4360, *Risk management*.

AS/NZS ISO/IEC 17799 establishes a code of practice for selecting information security controls (or equivalently treating information security risks). AS/NZS 7799.2 (BS 7799.2) specifies an information security management system. Both documents require that a risk assessment process is used as the basis for selecting controls (treating risks). This Handbook complements these Standards by providing additional guidance concerning management of information security risks.

The guidance in this Handbook is not intended to be a comprehensive schedule of information security threats and vulnerabilities. It is intended to serve as a single reference point describing an information security risk management process suitable for most situations encountered in industry and commerce and therefore can be applied by a wide range of organizations. Not all of the steps described in the handbook are relevant to every situation, nor can they take account of local environmental or technological constraints, or be presented in a form that suits every potential user in an organization. Safety critical applications in particular will require additional consideration of factors specific to the circumstances and relevant Standards should be consulted in such cases. Consequently, these guidelines may require to be augmented by further guidance before they can be used as a basis (for example) for corporate policy or an inter-company trading agreement.

It has been assumed in the drafting of these guidelines, that the execution of their provisions is entrusted to appropriately qualified and experienced people.

Contents

1 Scope, Application and Definitions

1.1 Scope

This Handbook provides a generic guide for the establishment and implementation of a risk management process for information security risks.

1.2 Methodology

The risk management process involves establishing the context, identifying, analysing, evaluating, treating, communicating and monitoring of risks.

1.3 Application

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

Generally, information security risk management methods and techniques are applied to complete information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful.

This Handbook is intended for use as a reference document by three audiences:

a) managers accountable for the management of information security;

b) personnel who are responsible for initiating, implementing and/or monitoring generic risk management systems within their organizations; and

c) personnel who are responsible for initiating, implementing and/or maintaining information security within their organization.

This Handbook may be applied at all stages in the life of an activity, function, project, product or asset. Often a number of differing studies are carried out at different stages of a project. The maximum benefit is usually obtained by applying the risk management process from the beginning.

This Handbook does not provide sufficient guidance for managing information security risks in safety related systems. IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, gives requirements and guidance in this area.

AS/NZS ISO/IEC 17799 establishes a code of practice for selecting information security controls (or equivalently treating information security risks). AS/NZS 7799.2 (BS 7799.2) specifies an information security management system. Both documents require that a risk assessment process is used as the basis for selecting controls (treating risks). This Handbook complements these Standards by providing additional guidance concerning management of information security risks.

1.4 Terminology

Risk management is the term applied to a logical and systematic method of establishing the context of, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses.

1.5 Definitions

For the purpose of this Handbook, the following definitions apply.

Availability: ensuring that authorized users have access to information and associated assets when required.

Confidentiality: ensuring that information is accessible only to those authorized to have access.

Consequence: the outcome of an event expressed qualitatively or quantitatively, being a loss, injury, or disadvantage. There may be a range of possible outcomes associated with an event.

Cost: of activities, both direct and indirect, involving any negative impact, including money, time, labour, disruption, goodwill, political and intangible losses.

Event: an incident or situation, which occurs in a particular place during a particular interval of time.

Event tree analysis: a technique which describes the possible range and sequence of the outcomes which may arise from an initiating event.

Fault tree analysis: a systems engineering method for representing the logical combinations of various system states and possible causes which can contribute to a specified event (called the top event).

Frequency: a measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.

Hazard: a source of potential harm or a situation with a potential to cause loss.

Impact: see consequence.

Information security: security preservation of confidentiality, integrity and availability of information

Information Security Management System: that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Integrity: safeguarding the accuracy and completeness of information and processing methods.

Likelihood: used as a qualitative description of probability or frequency.

Loss: any negative consequence, financial or otherwise.

Monitor: to check, supervise, observe critically, or record the progress of an activity, action or system on a regular basis in order to identify change.

Organization: a company, firm, enterprise or association, or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.

Probability: the likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes. Probability is expressed as a number between 0 and 1, with 0 indicating an impossible event or outcome and 1 indicating an event or outcome is certain.

Residual risk: the remaining level of risk after risk treatment measures have been taken.

Risk: the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

Risk acceptance: an informed decision to accept the consequences and the likelihood of a particular risk.

Risk analysis: a systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk assessment: the overall process of risk analysis and risk evaluation, refer to Figure 3.1.

Risk avoidance: an informed decision not to become involved in a risk situation.

Risk control: that part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimize adverse risks.

Risk engineering: the application of engineering principles and methods to risk management.

Risk evaluation: the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Risk financing: the methods applied to fund risk treatment and the financial consequences of risk.

NOTE: In some industries risk financing only relates to funding the financial consequences of risk.

Risk identification: the process of determining what can happen, why and how.

Risk management: the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

Risk management process: the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

Risk reduction: a selective application of appropriate techniques and management principles to reduce either the likelihood of an occurrence or its consequences, or both.

Risk retention: intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organization.

Risk transfer: shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

Risk treatment: selection and implementation of appropriate options for dealing with risk.

Safeguard: see security control.

Security control: a practice, procedure or mechanism that reduces risk.

Sensitivity analysis: examines how the results of a calculation or model vary as individual assumptions are changed.

Stakeholders: those people and organizations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.

Threat: a potential cause of an unwanted event which may result in harm to a system or organization.

Vulnerability: a characteristic (including a weakness) of an information asset or group of information assets which can be exploited by a threat.

1.6 References

AS/NZS 4360:1999
Risk management (Standards Australia/Standards New Zealand, 1999)

AS/NZS ISO/IEC 17799:2001
Information technology—Code of practice for information security management (Standards Australia/Standards New Zealand, 2001)

AS/NZS 7799.2:2003 (BS 7799.2:2002)
Information security management Part 2: Specification for information security management systems (Standards Australia/Standards New Zealand, 2003)

AS/NZS ISO 14004:1996
Environmental management systems—General guidelines on principles, systems and supporting techniques (Standards Australia/Standards New Zealand, 1996)

IEC 61508 (Series)
Functional safety of electrical/electronic/programmable electronic safety-related systems

AS 13335.1-2003 (ISO/IEC TR 13335-1:1996)
Information technology—Guidelines for the management of IT Security, Part 1: Concepts and models for IT Security (Standards Australia, 2003)

AS 1335.2-2003 (ISO/IEC TR 13335-2:1997)
Information technology—Guidelines for the management of IT Security, Part 2: Managing and planning IT Security (Standards Australia, 2003)

AS 1335.3-2003 (ISO/IEC TR 13335-3:1998)
Information technology—Guidelines for the management of IT Security, Part 3: Techniques for the management of IT Security (Standards Australia, 2003)

AS 13335.4-2003 (ISO/IEC TR 13335-4:2000)
Information technology—Guidelines for the management of IT Security,
Part 4: Selection of safeguards (Standards Australia, 2003)

AS 13335.5-2003 (ISO/IEC TR 13335-5:2001)
Information technology—Guidelines for the management of IT Security,
Part 5: Management guidance on network security (Standards Australia, 2003)

2 Risk Management Framework

2.1 General

This section describes the formal process for establishing a systematic information security risk management program.

2.2 Risk management policy

The organization's executive should define and document a policy for risk management, as described in AS/NZS 4360, including objectives for and commitment to information security risk management. The policy should be relevant to the organization's strategic context, goals, objectives and the nature of its business.

The information security risk management policy should be part of the organization's overall risk management plan. If this occurs, then the information security risk management objectives must be clearly defined and identified.

Management should ensure that the policy is understood, implemented and maintained at all levels of the organization.

2.3 Planning and resourcing

2.3.1 Management commitment

The organization should ensure that:

a) a risk management system is established, implemented and maintained in accordance with AS/NZS 4360; and

b) the performance of the risk management system is reported to the organization's management for review and as a basis for improvement.

NOTE: Management must take into account any regulatory requirements for reporting risk management system performance that apply to their business environment (e.g. banking, telecommunications, etc).

2.3.2 Responsibility and authority

The responsibility, authority and the interrelationship of personnel who perform and verify work affecting risk management should be defined and documented, particularly for people who need the organizational freedom to do one or more of the following:

a) identify those areas where information security risks need management;

b) initiate action to prevent or reduce the adverse effects of risk;

c) control further treatment of risks until the level of risk becomes acceptable;

d) identify and record any problems relating to the management of risk;

e) initiate, recommend or provide solutions through designated channels;

f) verify the implementation of solutions; and

g) communicate and consult internally and externally as appropriate.

2.3.3 Resources

The organization should identify resource requirements and provide adequate resources, including the assignment of trained personnel for management, performance of work and verification activities including internal review.

2.4 Implementation program

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

a) security objectives and activities being based on business objectives and requirements and led by business management;

b) visible support and commitment from top management;

c) a good understanding of the security risks;

d) effective marketing of security to all managers and employees; and

e) distribution of comprehensive guidance on information security policy and standards to all employees and contractors.

An effective risk management process for any organization aids this success by requiring a number of steps to be logically executed. Section 4 describes the steps required to implement an effective risk management process within any organization.

2.5 Management review

An organization's executive should ensure a review of the risk management program is carried out at specified intervals, sufficient to ensure its continuing suitability and effectiveness in satisfying the requirements of this Handbook, and the organization's stated risk management policy (see Clause 2.2). Records of such reviews should be maintained.

3 Risk Management Overview

3.1 General

Management of risk is an integral part of the management process. Risk management is a multifaceted process; appropriate aspects are often best carried out by a multidisciplinary team.

Risk management can be applied at many levels in the organization. It can be applied at the strategic level and at operational levels. It may be applied to specific projects, to assist with specific decisions or to manage specific recognized risk areas.

Risk management is an iterative process that can contribute to organizational improvement. With each cycle, risk criteria can be strengthened to achieve progressively better levels of risk management. For each stage of the process adequate records should be kept, sufficient to satisfy independent audit.

Unlike some areas of risk management, information security risks are considered to have only negative outcomes. Whilst it is possible for some 'security events' to have outcomes that in part include benefits, these are not normally predictable or manageable. The discussion in this Handbook therefore focuses on management processes associated with events that could harm organizations.

3.2 Information security management models

AS/NZS 7799.2 describes a process model for information security management systems as shown in Figure 3.1. The information security risk management process encompasses all steps of the Information Security Management System (ISMS). AS/NZS 7799.2 does not pre-suppose any particular approach to risk management and has been written to be compatible with AS/NZS 4360. It is assumed that implementers of an ISMS will also use a standard such as AS/NZS 4360 to guide them in implementation of risk management processes.

AS/NZS 4360 outlines a generic risk management process as shown in Figure 3.2. The details of a generic risk management process are fully described in Section 4 of AS/NZS 4360. The terminology used in the AS/NZS 7799.2 security management framework is consistent with that used in AS/NZS 4360. Table 3.1 shows the relationships between the two models. This Handbook follows the AS/NZS 4360 model, extended where appropriate to incorporate common practice in the area of managing information security risks.

This Handbook uses the terminology of 'controls' as a means of treating risks.

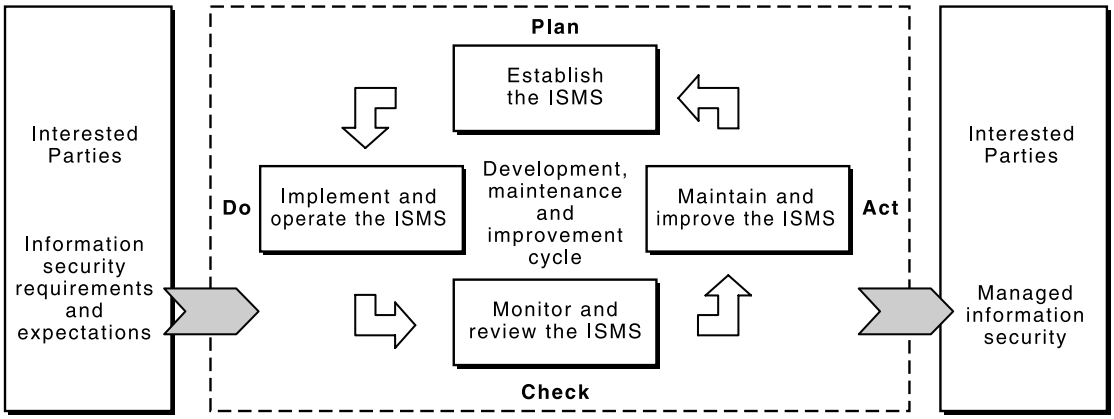

Figure 3.1 – Process model applied to ISMS

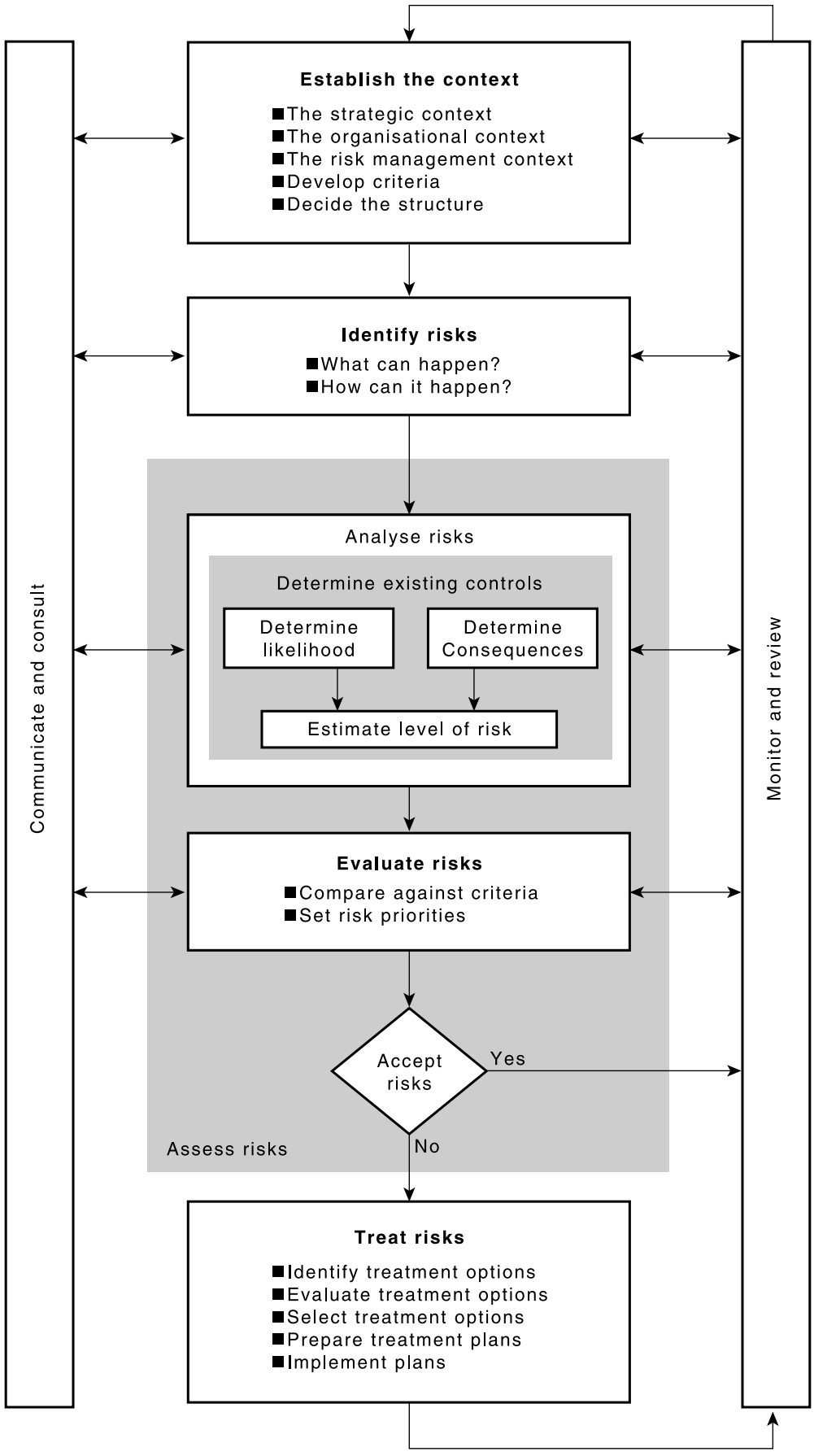

Figure 3.2 – Risk management process

Table 3.1 Comparison of AS/NZS 7799.2 and AS/NZS 4360 risk management models

PHASES OF THE AS/NZS 7799.2 MODEL	EQUIVALENT PHASES OF THE AS/NZS 4360 MODEL
Establish the ISMS All requirements of the AS/NZS 4360 'establish the context', 'identify risks', 'analyse and evaluate risks' phases are included within the 'establish' phase of AS/NZS 7799.2. The 'establish' phase of AS/NZS 7799.2 also includes some of the requirements of the 'treat risks' phase of AS/NZS 4360. Within AS/NZS 7799.2, the 'establishment' phase includes setting up the ISMS and undertaking those tasks necessary to complete risk assessment. It covers establishing security policy, objectives, targets, processes and procedures relevant to managing risk. Activities in the 'establish' phase include: determining the scope of the ISMS, defining a systematic approach to be taken for risk assessment, identifying risks, assessing risks, identifying and selecting options for treating risks, selecting control objectives and controls for the treatment of risks, and acceptance of residual risks. The risk identification phase includes identification (and valuation) of the information assets at risk.	**Establish the context** All requirements of the 'establish the context' phase are included within the plan phase of AS/NZS 7799.2. Policy definition is included within the 'establish the context' phase. Design of procedures that are to be followed is included within the 'establish the context' phase.
The AS/NZS 7799.2 model does not have a separate phase for risk identification. These requirements are included within the 'establish' phase.	**Identify risks** All requirements of the 'identify risks' phase are included within the 'establish' phase of AS/NZS 7799.2.
The AS/NZS 7799.2 model does not have a separate phase for risk analysis and evaluation. These requirements are included within the 'establish' phase.	**Analyse and evaluate risks** All requirements of the 'analyse and evaluate risks' phase are included within the 'establish' phase of AS/NZS 7799.2. Risk assessment is considered to consist of the combination of a risk analysis phase followed by a risk evaluation phase. The outcome of this phase is an understanding of risks that will be accepted and risks that require treatment.
The AS/NZS 7799.2 model does not have a separate phase for risk treatment. Identification, evaluation, and selection aspects of risk treatment are included as components of the 'establish' phase. Implementation aspects of risk treatment are included in the 'implementation' phase.	**Treat risks** Some requirements of the 'establish the context' phase are included within the 'establish' phase of AS/NZS 7799.2. The remaining, implementation oriented, aspects of risk treatment are covered in the implementation phase of AS/NZS 7799.2.

(*continued*)

Table 3.1 (*continued*)

PHASES OF THE AS/NZS 7799.2 MODEL	EQUIVALENT PHASES OF THE AS/NZS 4360 MODEL
Implement and operate the ISMS All remaining requirements of the AS/NZS 4360 'treat risks' phase are covered in the 'implement' phase of AS/NZS 7799.2. AS/NZS 7799.2 contains additional detail concerning requirements for operating controls to ensure that they are effective. It includes planning and implementation of a control plan as well as operational resource management, training, awareness, and incident detection and response.	The remaining, implementation oriented, aspects of risk treatment are covered in the implementation phase of AS/NZS 7799.2. AS/NZS 7799.2 contains operational requirements that are more explicit and comprehensive than those specified in AS/NZS 4360.
Monitor and review the ISMS All requirements of the 'monitor and review the ISMS' phase are included within the 'monitor and review' phase of AS/NZS 4360. AS/NZS 7799.2 is more specific concerning requirements.	**Monitor and review** All requirements of the 'monitor and review' phase are included within the 'monitor and review the ISMS' phase of AS/NZS 7799.2.
Maintain and improve the ISMS Those requirements of the 'maintain and improve the ISMS' phase concerning communication and consultation with stakeholders are included within the 'monitor and review' phase of AS/NZS 4360. This phase in AS/NZS 7799.2 goes beyond what is covered in AS/NZS 4360 by specifying requirements for taking corrective and preventive actions to improve the ISMS.	**Communicate and consult** All requirements of the 'communicate and consult' phase are included within the 'maintain and improve the ISMS' phase of AS/NZS 7799.2. AS/NZS 4360 contains more detail concerning the importance of communication with stakeholders.

3.3 Main elements

AS/NZS 4360 describes the main elements of the generic risk management process as the following:

a) *Establish the context*

Establish the strategic, organizational and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined. (See Clause 4.1)

b) *Identify risks*

Identify what, where and how things can arise as the basis for further analysis. (See Clause 4.2)

c) *Assess risks*

Assessment of risks enables an organization to determine which risks can be accepted and which risks require controls to reduce them. AS/NZS 7799.2 sets out requirement related to controls.

NOTE: Risk assessment may quantify exceptional information security risks requiring stronger controls that are additional to the recommendations given in AS/NZS 7799.2. These controls need to be justified on the basis of the conclusions of the risk assessment.

d) *Analyse risks*

Determine the existing controls and analyse risks in terms of consequence and likelihood in the context of these controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood may be combined to produce an estimated level of risk. (See Clause 4.3)

Analysis of risks depends on the following factors:

i) the nature of the business information and systems;

ii) the business purpose for which the information is going to be used;

iii) the environment in which the system is used and operated; and

iv) the protection provided by the controls in place.

e) *Evaluate risks*

Compare estimated levels of risk against the pre-established criteria. This enables risks to be ranked so as to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required. (See Clause 4.4)

f) *Treat risks*

Accept and monitor low-priority risks. For other risks, develop and implement a specific management plan that includes consideration of funding. (See Clause 4.5)

g) *Monitor and review*

Monitor and review the performance of the risk management system and changes that might affect it. (See Clause 4.7)

h) *Communicate and consult*

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole. (See Clause 4.8)

3.4 Information security risks

3.4.1 Assets

An asset is something to which an organization directly assigns value and, hence, for which the organization requires protection. The proper management of and accountability for assets is vital in order to maintain appropriate protection of the organization's assets. These two aspects should be a major responsibility of all management levels. It is important that an inventory is drawn up of the major assets associated with each information security management system. Each asset should be clearly identified and appropriately valued, and its ownership and security classification agreed and documented. Examples of assets include:

a) ***information assets:*** databases and data files, voice records, image files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;

b) ***paper documents***: contracts, guidelines, company documentation, documents containing important business results;

c) ***software assets***: application software, system software, development tools and utilities;

d) ***physical assets***: computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;

e) ***marketing assets***: company image and reputation; and

f) ***services***: computing and communications services, other technical services (heating, lighting, power, air-conditioning).

3.4.2 Asset values (and potential impacts)

In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business. These values are usually expressed in terms of the potential business impacts of unwanted incidents such as loss of confidentiality, integrity and/or availability. This could, in turn, lead to financial losses, loss of revenue, market share, or company image. In order to assess these potential losses consistently and to relate them appropriately, a value scale for assets should be applied. For each of the assets and each of the possible losses, i.e. loss of confidentiality, integrity and availability, a value should be assigned.

3.4.3 Threats

Assets are subject to many kinds of threats. A threat has the potential to cause an unwanted incident that may result in harm to a system or organization and its assets. This harm can occur from a direct or an indirect attack on an organization's information e.g. its unauthorized destruction, disclosure, modification, corruption, and availability or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit a vulnerability of the systems, applications or services used by the organization in order to successfully cause harm to the asset. (Refer to Clause 4.3.4.3.)

NOTE: Appendix A provides examples of possible threat types.

3.4.4 Vulnerabilities

Vulnerabilities are weaknesses associated with an organization's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to these assets. Vulnerability in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an asset. (Refer to Clause 4.3.4.3.)

NOTE: Appendix B provides examples of common information security vulnerabilities.

3.4.5 Security risks

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

3.4.6 Security requirements

3.4.6.1 *Sources of requirement*

There are three main sources of security requirements to be documented in an ISMS as follows:

a) unique security risks which could lead to significant losses in business if they occur;

b) statutory and contractual obligations which have to be satisfied by the organization, its trading partners, contractors and service providers; and

c) unique principles, objectives and obligations that an organization has developed to support its business operations and processes, and which apply to the organization's information systems.

Once these security requirements have been identified, it is helpful to formulate them in terms of requirements for confidentiality, integrity and availability.

3.4.6.2 *Security issues*

When identifying the security requirements, it is important to understand what damage the security risks can do to a business. A method is to consider the following list of questions when establishing the context, identifying potential risks, and valuing assets.

a) What are the most important parts of the business, how are they supported by using or processing information, and how essential is this support?

b) What essential decisions depend on the accuracy, integrity, or availability of information, or on how up-to-date this information is?

c) What confidential information needs to be protected?

d) What are the implications of security incidents (related to information) for the business or the organization?

AS 13335.1 and AS 13335.2 provide additional information concerning basic concepts for managing IT security as well as management and planning guidelines.

3.4.6.3 *Legal, regulatory and contractual requirements*

The security requirements specifying the set of statutory and contractual obligations that an organization, its trading partners, contractors and service providers have to satisfy should be documented in an ISMS. It is important e.g. for the control of proprietary software copying, safeguarding of organizational records, or data protection, that the ISMS supports these requirements. It is also vital that the implementation of, or absence of security controls in each of the information systems does not breach any statutory, criminal or civil obligations, or commercial contracts. AS/NZS ISO/IEC 17799 provides more information on this topic.

3.4.6.4 *Organizational principles, objectives and requirements*

The security requirements relating to the organization-wide principles, objectives and requirements for information processing to support its business operations should also be documented in an ISMS. It is important, e.g. for competitive edge, cash flow and/or profitability, that the ISMS supports these requirements, and vital that the implementation of, or absence of security controls in each of the information systems does not impede efficient business operations. Each of these security requirements should be translated in terms of the confidentiality, integrity and/or availability of the information encompassed by the ISMS.

3.4.7 Security controls

Security controls, such as those defined in AS/NZS ISO/IEC 17799 and AS/NZS 7799.2 are practices, procedures or mechanisms which may protect against threats, reduce vulnerabilities, limit the impact of an incident, or protect against risks in any other way. Effective security usually requires a combination of controls which can perform one or more of the following functions: detection, deterrence, prevention, limitation, correction, recovery, monitoring and awareness.

Expenditure on information security controls needs to be balanced against, and appropriate to, the value of the information and other business assets at risk, and the business harm likely to result from security failures.

3.4.8 Relationship between risk components

This Clause describes the set of components relevant to whatever risk analysis approach is selected. Figure 3.3 below illustrates what these components are and the relationship between each component.

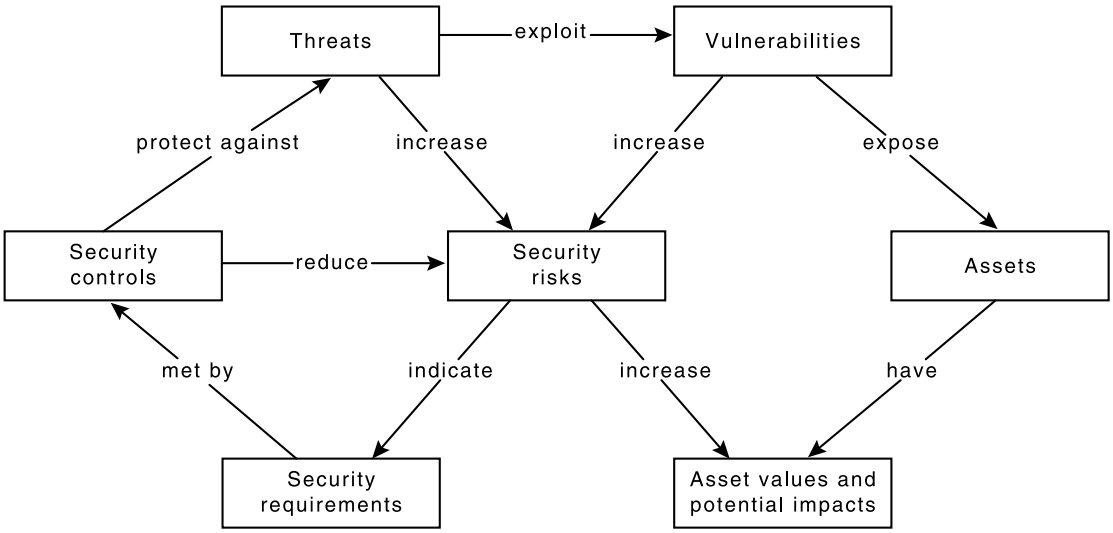

Figure 3.3 – Risk concept relationships

4 Risk Management Process

4.1 Establish the context

4.1.1 General

Organizations rely heavily on the use of information to conduct their business activities. Loss of confidentiality, integrity and availability of information and services can have an adverse impact. Consequently there is a critical need to protect information and manage the security of information technology (IT) systems within organizations. This requirement is particularly important in today's environment because many organizations are internally and externally connected by networks of IT systems.

The risk management process occurs within the framework of an organizational and risk management context. This process needs to be established to define the basic parameters within which risks must be managed and to provide guidance for decisions within more detailed risk management studies. This sets the scope for the rest of the risk management process. It must be remembered that few risks remain static. Ongoing monitoring and review is necessary to ensure that the context, identified risks, risk analysis, risk evaluation and risk treatment remain appropriate to the circumstances.

A careful definition of boundaries at this stage avoids unnecessary work and improves the quality of the risk analysis. The boundary description should clearly define which of the following have to be considered when carrying out the risk analysis for the considered information asset:

a) IT assets (e.g. hardware, software, information);

b) people (e.g. staff, subcontractors, other external personnel);

c) environments (e.g. buildings, facilities), or geographical location; and

d) activities (operations).

AS/NZS 4360 specifies a generic risk management process. AS/NZS 7799.2 specifies an information security risk management system to implement this process for information security risks. Depending on the organization's overall risk management philosophy, culture and structure, it may be possible to combine or omit certain steps. However, all underlying concepts should receive consideration.

4.1.2 Establish the strategic context

Establish the relationship between the organization and its environment, identifying the organization's strengths, weaknesses, opportunities and threats. The strategic context includes the financial, operational, competitive, political (public perceptions/image), social, client, cultural and legal aspects of the organization's functions.

Identify the internal and external stakeholders, and consider their objectives, take into account their perceptions and establish communication policies with these parties.

This step is focused on the environment in which the organization operates. The organization should seek to determine the crucial elements that might support or impair its ability to manage the information security risks it faces.

Strategic analysis must be undertaken. It should be endorsed at the executive level, set the basic parameters and provide guidance for the more detailed information security risk management processes. There should be a close relationship between an organization's mission or strategic objectives and its management of all the identified risks to which it is exposed.

4.1.3 Establish the organizational context

Before a risk management study is commenced, it is necessary to understand the organization and its capabilities, as well as its goals and objectives and the strategies that are in place to achieve them.

This is important for the following reasons:

a) Information security risk management takes place in the context of the wider goals, objectives and strategies of the organization.

b) Failure to achieve the objectives of the organization or the specific activity, or project being considered is one set of information security risks which should be managed.

c) The organizational policy and goals help define the criteria by which it is decided whether an information security risk is acceptable or not, and form the basis of options for treatment.

For example, privacy of customer information is very important for organizations involved in electronic commerce. Customers have shown reluctance to do business over the Internet if they are not confident that their privacy will be respected. In this case, organizations need to:

i) understand the importance of the privacy of customer information to their business plan;

ii) understand the potential impact of breaches of customer information privacy (to both customers and their business); and

iii) put in place appropriate organizational policies and procedures to ensure that such privacy risks are acceptable.

4.1.4 Establish the risk management context

The goals, objectives, strategies, scope and parameters of the activity, or part of the organization, to which the risk management process is being applied, should be established. The process should be undertaken with full consideration of the need to balance costs of controls and risk reduction benefits. The resources required and the records to be kept should also be specified.

Setting the scope and boundaries of an application of the information security risk management process involves:

a) defining the project or activity and establishing its goals and objectives;

b) defining the extent of the project in time and location;

c) identifying any studies needed and their scope, objectives and the resources required. Generic sources of risk and areas of impact may provide a guide for this; and

d) defining the extent and comprehensiveness of the risk management activities to be carried out.

Specific issues that may also be discussed include the following:

i) the roles and responsibilities of various parts of the organization participating in managing risk; and

ii) the relationship between the project and other projects, or parts of the organization.

4.1.5 Develop risk evaluation criteria

Decide the criteria against which information security risk is to be evaluated. Decisions concerning risk acceptability and risk treatment may be based on the operational, technical, financial, legal, social, humanitarian or other criteria. These often depend on an organization's internal policy, goals, objectives and the interests of stakeholders.

Internal and external perceptions and legal requirements may affect criteria. It is important that appropriate criteria be determined at the outset and continually reviewed throughout the risk management process. Although risk criteria are initially developed as part of establishing the risk management context, they may be further developed and refined subsequently as particular risks are identified and risk analysis techniques are chosen i.e. the risk criteria must correspond to the type of risks and the way in which the levels are expressed.

Criteria for evaluation of information security risks are typically (but not limited to) financial consequences associated with:

a) customer perceptions and regulatory impacts of breaches of privacy;

b) operational and business impacts of unavailability;

c) business impacts of loss of confidentiality; and

d) operational and business impacts of loss of integrity.

An organization has to define its own limits for damages like 'low' or 'high'. For example, financial damage that might be disastrous for a small company might be low or even negligible for a very big company.

4.1.6 Define the structure

This involves separating the activity or project into a set of elements. Those elements provide a logical framework for identification and analysis that helps to ensure that significant risks are not overlooked. The structure chosen depends on the nature of the risks and the scope of the project or activity. For example, the structure could be based on the different types of information assets as listed in Clause 3.4.1.

4.1.6.1 *Structured identification of information assets*

An asset is a component or part of a total system to which an organization directly assigns value and hence for which the organization requires protection. For the identification of assets it should be borne in mind that information needs to be considered in a wider context than just an IT system and its associated hardware and software. Thus, it may be appropriate to structure risk management activities based on the type of asset involved. For example, asset types (in no particular order) can be any of the following:

a) information/data (e.g. files containing payment details, voice records, image files, product information);

b) hardware (e.g. computer, printer);

c) software, including applications (e.g. text processing programs, programs developed for special purposes);

d) communications equipment (e.g. telephones, copper cable, fibre);

e) firmware (e.g. floppy discs, CD Read Only Memories, Programmable ROMs);

f) documents (e.g. contracts);

g) funds (e.g. in Automatic Teller Machines);

h) manufactured goods;

i) services (e.g. information services, computing resources);

j) confidence and trust in services (e.g. payment services);

k) environmental equipment;

l) personnel; and

m) image of the organization.

All assets within the risk management context must be identified. Conversely, any assets to be excluded from a review boundary, for whatever reason, need to be assigned to another review to ensure that they are not forgotten or overlooked.

It should be noted that different structures may sometimes be appropriate. For example in some cases a structure based on business processes (or organizational structure) may be simpler to implement that a structure based on asset type.

4.2 Risk identification

4.2.1 General

This step is to identify the information security risks to be managed and the most appropriate approach to their treatment. In some cases, risks will be similar to those in other systems or organizations and can be treated using a baseline approach. In other cases, specific analysis of risks on a case by case basis will be necessary. Comprehensive identification using a well-structured systematic process is critical, because a potential risk not identified at this stage is excluded from further analysis. Identification should include all risks whether or not they are under the control of the organization.

4.2.2 What can happen

The aim of this step is to generate a comprehensive list of events that might affect each element of the structure referred to in Clause 4.1.6. These are then considered in more detail to identify what can happen.

4.2.3 How and why it can happen

Having identified a list of events, it is necessary to consider possible causes and scenarios. There are many ways an event can be initiated. It is important that no significant causes are omitted.

4.2.4 Tools and techniques

Approaches used to identify risks include:

a) checklists;

b) judgements based on experience and records;

c) flowcharts;

d) brainstorming;

e) systems analysis;

f) scenario analysis; and

g) systems engineering techniques.

Techniques include:

i) structured interviews with experts in the area of interest;

ii) use of multidisciplinary groups of experts;

iii) individual evaluations using questionnaires;

iv) use of computer and other modelling; and

v) use of fault tree analysis and event tree analysis.

4.3 Risk analysis

4.3.1 General

The objectives of analysis are to separate the minor acceptable risks from the major risks, and to provide data to assist in the evaluation and treatment of risks. Risk analysis involves consideration of the sources of risk, determination of the consequences of realizing these risks and the likelihood that those consequences may occur. Factors that affect the consequences and likelihood may also be identified. Risk is analysed by combining estimates of consequences and likelihood in the context of existing control measures.

The risk analysis phase can be made very brief if previous work has established a baseline (or code of practice) for the treatment of specific types of risk. Appendix C provides guidance for using this approach. Baseline controls can be used to treat common risks. Where large or unusual risks are identified, it is necessary to complete risk analysis and evaluation as discussed below to determine appropriate treatment options. More details of this approach can be found in AS 13335.3.

A preliminary analysis can be carried out so that similar or low-impact risks are excluded from detailed study. Excluded risks should, where possible, be listed to demonstrate the completeness of the risk analysis.

4.3.2 Determine existing controls

Identify the existing management, technical mechanisms and procedures to control risk and assess their strengths and weaknesses. Tools used in Clause 4.2.4 may be appropriate, as well as approaches such as inspections and control self-assessment techniques.

4.3.3 Consequences and likelihood

The magnitude of consequences of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls. Consequences and likelihood are combined to produce a level of risk. Consequences and likelihood may be determined using statistical analysis and calculations. Alternatively, where no past data is available, subjective estimates may be made which reflect an individual's or group's belief that a particular event or outcome will occur.

To avoid subjective biases, the best available information sources and techniques should be used when analysing consequences and likelihood. Sources of information may include the following:

a) past records;

b) relevant experience;

c) industry practice and experience;

d) test marketing and market research;

e) experiments and prototypes;

f) economic, engineering or other models; and

g) specialist and expert judgements.

Wherever possible, the confidence placed on estimates of levels of risk and its determining factors should be included.

4.3.4 Methods of analysis

A detailed risk analysis for an information system involves the identification of the related risks, and an assessment of their magnitude. The need for a detailed risk analysis can be determined without unnecessary investment in time and money when high level reviews are conducted for all systems, followed by detailed risk analysis reviews only on high risk or critical systems.

The risk analysis is done by an identification of potential adverse business impacts of unwanted events and the likelihood of their occurrence in a given timeframe. Unwanted events can adversely impact the business, persons or any other valuable entity of the organization. The adverse impact of an unwanted event is a composite of possible damages related to the value of the assets at risk. The likelihood of occurrence is dependent on how attractive the asset is for a potential attacker, the likelihood of threats occurring, and the ease with which the vulnerabilities can be exploited. The results of the risk analysis lead to the identification and selection of controls that can be used to reduce the identified risks to an acceptable level.

A number of incidents and external influences which may affect the security requirements of the system can make it necessary to reconsider parts of or the whole risk analysis. Those influences could be:

a) recent significant changes to the system;

b) planned changes; or

c) the consequences of incidents which need to be dealt with.

A variety of methods exist for the performance of a risk analysis ranging from checklist based approaches to structured analysis based techniques. As discussed in AS/NZS 4360, analysis may be qualitative, semi-quantitative, or quantitative. (AS/NZS 4360 Appendices E and F give examples of qualitative and quantitative measures and scales.) Automated (computer assisted) or manual based products can be used. Whatever method or product is used by the organization, it should at least address the topics identified in the following clauses. It is also important that the methods used fit with the organization's culture.

Once a detailed risk analysis review for a system has been completed for the first time, the results of the review—assets and their values, threat, vulnerability and risk levels, and controls identified—should be saved, for example, in a database. Obviously, methods with software support tools make this activity much easier. This representation, sometimes referred to as a model, can be utilized to significant effect as changes occur over time, be they to configuration, information types processed, threat scenarios, etc. Only the changes are needed as input in order to ascertain the effect on the necessary controls. Further, such models can be quickly used to examine different options, say during the development of a new system, as well as being used for other systems that are similar in nature.

Appendix D provides examples of different methods commonly used to analyse information security risks.

4.3.4.1 *Valuation of information assets and establishment of interdependencies*

After fulfilling the objective of asset identification by listing all assets of the context under review, values should be assigned to these assets. These values represent the importance of the assets to the business of the organization. This may be expressed in terms of security concerns such as the potential adverse business impacts from the disclosure, modification, non-availability and/or destruction of information, and other IT system assets. Thus asset identification and valuation, based on the business needs of an organization, is a major factor in the determination of risks.

The input for the valuation of assets should be provided by owners and users of the assets. The person(s) carrying out the risk analysis will list the assets. They should seek assistance from those involved in business planning, finance, information systems and other relevant activities in order to identify values for each of these assets. The values assigned should be related to the cost of obtaining and maintaining the asset, and the potential adverse business impacts from loss of confidentiality, integrity, availability, accountability, authenticity and reliability. Each of the assets identified should be of value to the organization. However, there will not be a direct or easy way to establish financial value for all. It is also necessary to establish the value or extent of importance in non-financial, i.e. qualitative, terms to the organization. Otherwise it will be difficult to identify the level of protection and the amount of resources the organization should devote to protect the assets. An example for such a valuation scale could be a distinction between low, medium and high, or, in more detail:

negligible → low → medium → high → very high

Regardless of which scale is used, issues to be considered in this valuation could be the possible damages resulting from:

a) violation of legislation and/or regulation;

b) impairment of business performance;

c) loss of goodwill/negative effect on reputation;

d) breach of confidentiality associated with personal information;

e) endangerment of personal safety;

f) adverse effects on law enforcement;

g) breach of commercial confidentiality;

h) breach of public order;

i) financial loss;

j) disruption to business activities; and

k) endangerment of environmental safety.

It should be emphasized at this stage that the method for analysis must allow not only quantitative valuation, but also qualitative valuation where quantitative valuation is impossible or illogical (for example, the potential for loss of life, or loss of business goodwill). Explanation should be given of the valuation scale used.

Dependencies of assets on other assets should also be identified, since this might influence the values of the assets. For example, the confidentiality of data should be kept throughout its processing; i.e. the security needs of a data processing program should be directly related to the value representing the confidentiality of the data processed. Also, if a business process is relying on the integrity of certain data being produced by a program, the input data of this program should be of appropriate reliability. Moreover, the integrity of information will be dependent on the hardware and software used for its storage and processing. Also, the hardware will be dependent on the power supply and possibly the air conditioning. Thus information about dependencies will assist in the identification of relevant threats and particularly vulnerabilities. It will also help to assure that the true value of the assets (through the dependency relationships) is given to the assets, thereby ensuring an appropriate level of protection.

The values of assets on which other assets are dependent may be modified in the following way:

i) if the values of the dependent assets (e.g. data) are lower or equal to the value of the asset considered (e.g. software), its value remains the same; and

ii) if the values of the dependent asset (e.g. data) are greater, then the value of the asset considered (e.g. software) should be increased according to:
   A) the degree of dependency; and
   B) the values of the other assets.

An organization may have some assets that are available more than once, like copies of software programs or the same type of PC used in most of the offices. It is important to consider this fact when doing the asset valuation. On one hand, these copies are overlooked easily, so care must be taken to identify all of them; on the other hand, they could be used to reduce availability problems.

The final output of this step is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity), non-availability and destruction (preservation of availability), and replacement cost.

4.3.4.2 *Threat assessment*

A threat has the potential to harm the information assets under review. If a threat occurred, it could impinge on information in some way to cause unwanted incidents and thus adverse impacts. Threats may be of natural or human origin, and could be accidental or deliberate. Both accidental or deliberate threat sources should be identified and the likelihood of their occurrence should be assessed. It is essential that no relevant threat is overlooked, since this could result in failure or weaknesses in the information security.

Input to the threat assessment should be obtained from the asset owners or users, from personnel department staff, from facility planning and IT specialists, as well as from people responsible for the protection of the organization. Other organizations like legal bodies and national government authorities may be able to assist, for example by providing threat statistics.

A list of generally possible threats is helpful to perform the threat assessment. An example of threat types is given in Appendix A. Nevertheless it might be worthwhile to consult other threat catalogues (maybe specific to your organization or business) since no list can be exhaustive. Some of the most common manifestations of threats are:

a) errors and omissions;

b) fraud and theft;

c) employee sabotage;

d) loss of physical and infrastructure support;

e) malicious hacking, e.g. through masquerading;

f) malicious code; and

g) industrial espionage.

When using threat catalogues or the results of earlier threat assessments, one should be aware that threats are continually changing, especially if the business environment or the IT environment changes. For example, the viruses of the 90s were significantly more complex than those of the 80s. It is also interesting to note that the implementation of controls such as virus checking software always seem to lead to the development of new viruses which are resistant to current controls.

After identifying the threat source (who and what causes the threat) and the threat target (i.e. what elements of the system may be affected by the threat), it is necessary to assess the likelihood of the threats. This should take account of:

i) the threat frequency (how often it might occur, according to experience, statistics etc.), if statistics can be applied;

ii) the motivation, the capabilities perceived and necessary, resources available to possible attackers, and the perception of attractiveness and vulnerability of information assets for the possible attacker, for deliberate threat sources; and

iii) geographical factors such as proximity to chemical or petroleum plants, the possibility of extreme weather conditions, and factors that could influence human errors and equipment malfunction, for accidental threat sources.

Depending on the need for accuracy, it might be necessary to split assets into their components and relate the threats to the components. For instance, a physical asset might initially be considered to be ‘central data servers’, but when it is identified that these servers are in different geographic locations, it would be split into ‘central data server 1’ and ‘central data server 2’ because some threats may be different, and others may be at different levels. Similarly, a software asset might first be regarded as ‘application software’ but later broken down into two or more instances of ‘application software’. An example with regard to a data asset could be where it is first determined as ‘criminal record’ but later split into ‘criminal record text’ and ‘criminal record image’.

At the completion of the threat assessment, there will be a list of threats identified, the assets or groups of assets they would affect, and measures of the likelihood of threats occurring on a scale such as high, medium, or low.

4.3.4.3 *Vulnerability assessment*

This assessment includes identifying weaknesses in the physical environment, organization, procedures, personnel, management, administration, hardware, software or communications equipment, that may be exploited by a threat source to cause harm to the assets, and the business they support. The presence of a vulnerability does not cause harm in itself as there must be a threat present to exploit it. A vulnerability that has no corresponding threat does not require the implementation of a control, but should be recognized and monitored for changes. It should be noted that incorrectly implemented or malfunctioning controls, or controls being used incorrectly, could in themselves be vulnerability.

Vulnerabilities can be related to properties or attributes of the asset that can be used in a way, or for a purpose, other than that intended when the asset was purchased or made. For example, one of the properties of an EEPROM (Electronically Erasable Programmable Read Only Memory) is that the information stored on it can be erased and replaced. This is one of the design criteria of an EEPROM. However, this property also means that the unauthorized destruction of information stored on the EEPROM is possible. This can be vulnerability.

This assessment identifies vulnerabilities that may be exploited by threats and assesses their likely level of weakness, i.e. ease of exploitation. For example, some assets are easily disposed of, easily concealed or transported—all of these properties can relate to vulnerabilities. Input for the vulnerability assessment should be obtained from the asset owners or users, from facility specialists, and IT systems experts on hardware and software. Examples of vulnerabilities are:

a) unprotected connections (for example to the Internet);

b) processes for identifying remote users;

c) untrained users;

d) wrong selection and use of passwords;

e) no proper access control (logical and/or physical);

f) no back-up copies of information or software; and

g) location in an area susceptible to flooding.

More examples of common vulnerabilities can be found in Appendix B.

It is important to assess how severe the vulnerabilities are, in other words how easily they may be exploited. A vulnerability should be assessed in relation to each threat that might exploit it in a particular situation. For instance, a system may have a vulnerability to the threats of masquerading of user identity and misuse of resources. The vulnerability to masquerading of user identity may be high because of lack of user authentication. On the other hand, the vulnerability to misuse resources may be low because even with lack of user authentication the means by which resources might be misused are limited.

The result of this step should be a list of vulnerabilities and assessments of the ease of exploitation, e.g. on a scale high, medium, and low.

4.4 Risk evaluation

Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria.

Risk analysis and the criteria against which risks are compared in risk evaluation should be considered on the same basis. Thus, qualitative evaluation involves comparison of a qualitative level of risk against qualitative criteria, and quantitative evaluation involves comparison of numerical level of risk against criteria that may be expressed as a specific number, such as frequency, duration or outage, or monetary value.

Tables 4.1 and 4.2 give examples of measures that might be used for likelihood and impact/consequence of events subject to risk analysis. It is noted that the details will depend on the business context and the types of risks being considered. The examples may be relevant to events with potentially large consequences in a large organization. In other cases risks with consequences less than $1M may be critical, for example.

Table 4.1: Example of qualitative risk quantification

Likelihood	*Impact/Consequence*
A = Almost Certain L = Likely M = Moderate U = Unlikely	C = Critical H = High M = Medium L = Low

Table 4.2: Example of semi-quantitative risk evaluation

Likelihood	*Impact/Consequence*
A = within 12 months L = within 1 to 2 years M = within 2 to 5 years U = Unlikely	C > $10M H = $5M to $10M M = $1M to $5M L < $1M

After applying the simplified example of Method 3 (Table D5) given in Appendix D, the quantification of likelihood and impact can be stated as an assessment of risk:

Table 4.3: Example of risk assessment

Risk Assessment
H = High M = Medium L = Low

The result of a risk evaluation (for example using one of the methods described in Appendix D) is a priority list of risks for further action.

Decisions should take into account the wider context of the risk and include consideration of the tolerability of the risks borne by parties other than the organization that benefits from it.

If the resulting risk falls into the low or acceptable risk categories it may be accepted with minimal further treatment. Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable.

If risks do not fall into the low or acceptable risk category, they should be treated using one or more of the options considered in Clause 4.5.

4.5 Risk treatment

Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them.

4.5.1 Identifying options for risk treatment

Figure 4.1 illustrates the risk treatment process.

Options, which are not necessarily mutually exclusive or appropriate in all circumstances, include the following:

a) risk avoidance;

b) reduction of likelihood;

c) reduction of consequences;

d) risk transference; and

e) risk retention.

4.5.1.1 *Risk avoidance*

Risks can be avoided by deciding not to proceed with the activity likely to generate risk (where this is practicable).

For example, an organization might choose not to allow networked access to its corporate financial systems because the consequences of a successful hacker attack could put it out of business.

Risk avoidance can occur inappropriately because of an attitude of risk aversion, which is a tendency of many people (often influenced by an organization's internal system). Inappropriate risk avoidance may increase the significance of other risks.

Risk aversion results in:

a) decisions to avoid or ignore risks regardless of the information available and costs incurred in treating those risks;

b) failure to treat risk;

c) leaving critical choices and/or decisions up to other parties;

d) deferring decisions which the organization cannot avoid; or

e) selecting an option because it represents a potential lower risk regardless of benefits.

4.5.1.2 *Reduction of likelihood*

The likelihood of occurrence of 'risk' events may be reduced by reducing threats or vulnerabilities. (See Clauses 3.4.3 and 3.4.4.)

For example, use of hardware tokens to authenticate users accessing a corporate network over the Internet can reduce the likelihood of unauthorized access.

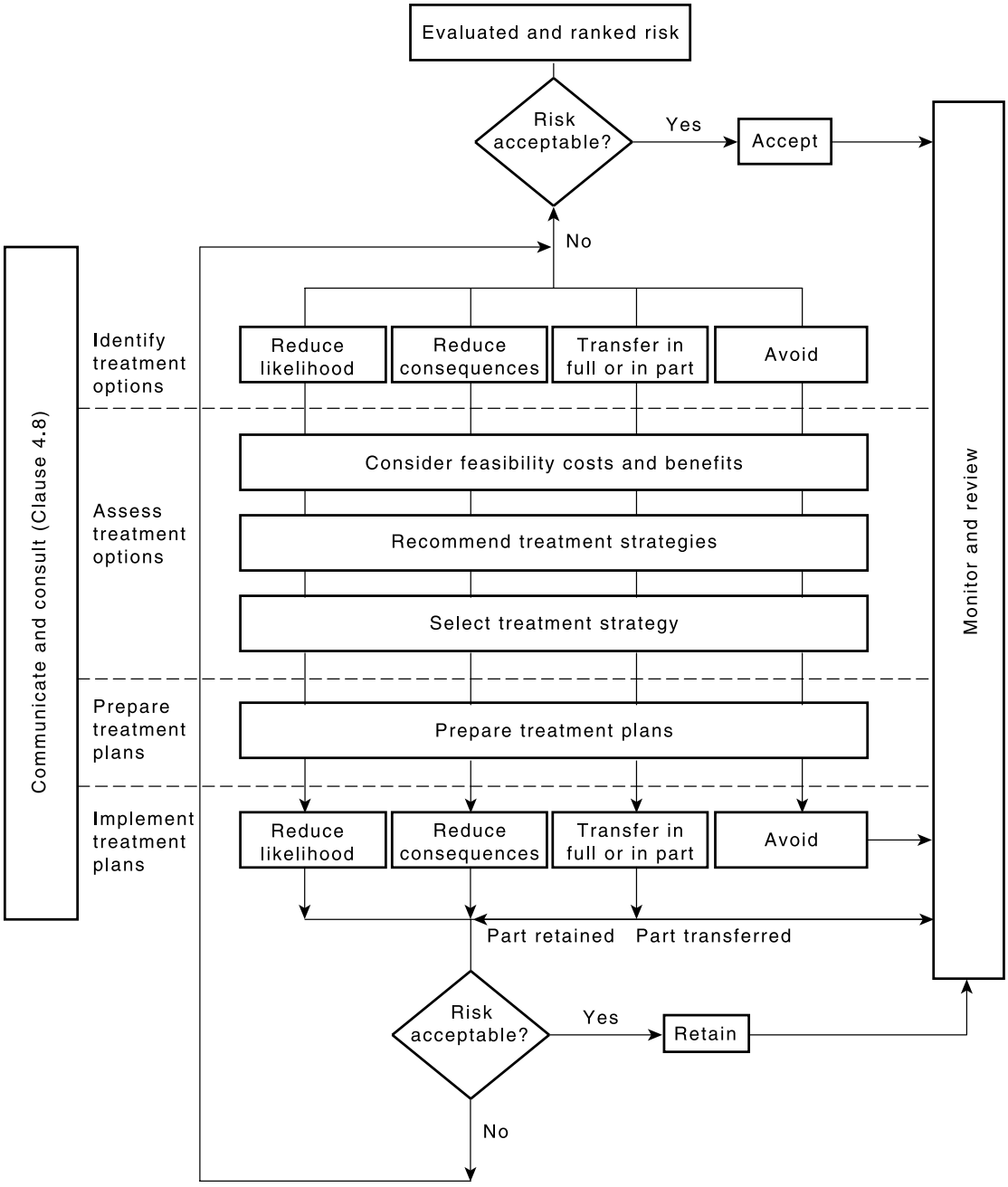

Figure 4.1 – Risk treatment process

4.5.1.3 *Reduction of consequences*

The consequences of 'risk' events may be reduced by reducing threats or vulnerabilities or modification of the assets at risk in some other way.

For example, separation of development and operational facilities can reduce the consequences of unauthorized access to development and testing environments.

4.5.1.4 *Risk transference*

Another party can bear or share some part of the risk. Mechanisms include the use of contracts, insurance arrangements and organizational structures such as partnership and joint ventures.

For example, outsourcing IT operations can be used to transfer availability risks to a supplier on a contractual basis.

The transfer of a risk to other parties, or physical transfer to other places, will reduce the risk for the original organization, but may not diminish the overall level of risk to the organization.

Where risks are transferred in whole or in part, the organization transferring the risk has acquired a new risk, in that the organization to which the risk has been transferred may not manage the risk effectively.

4.5.1.5 *Risk retention*

After unacceptable risks have been reduced or transferred, there may be residual risks that are retained. Plans should be put in place to manage the consequences of these risks if they should occur, including identifying a means of financing the risk. Risks can also be retained by default, i.e. when there is a failure to identify and/or appropriately transfer or otherwise treat risks.

In some cases, residual risks of potentially high impact but low likelihood will remain. It may be an acceptable risk management strategy to accept such residual risks. However, in such cases an organization should make business continuity plans to recover from high impact incidents if they occur. Such a business continuity management strategy should ensure that key business objectives continue to be met and key business activities continue during the recovery process. Additional guidance concerning Business Continuity Management can be found in AS/NZS ISO/IEC 17799.

4.5.2 Risk control

Reduction of consequences and likelihood may be referred to as risk control. Risk control involves determining the relative benefit of new controls. Controls may involve effectiveness policies, procedures or physical changes.

4.5.3 Assessing risk treatment options

Options should be assessed on the basis of the extent of risk reduction, and the extent of any additional benefits or opportunities created, taking into account the criteria developed in Clause 4.1.5. A number of options may be considered and applied either individually or in combination.

Selection of the most appropriate option involves balancing the cost of implementing each option against the benefit derived from it. In general, the cost of managing risks needs to be commensurate with the benefits obtained.

When large reductions in risks may be obtained with relatively low expenditure, such options should be implemented. Further options for improvements may be uneconomic and judgement needs to be exercised as to whether they are justifiable. This is illustrated in Figure 4.2.

Decisions should take account of the need to carefully consider rare but severe risks, which may warrant risk reduction measures that are not justifiable on strictly economic grounds.

In general the adverse impacts of risks should be made as low as reasonably practicable, irrespective of any absolute criteria.

If the level of risk is high, but considerable opportunities could result from taking the risk, such as the use of a new technology, then acceptance of the risk needs to be based on an assessment of the costs of risk treatment, and the costs of rectifying the potential consequences versus the opportunities afforded by taking the risk.

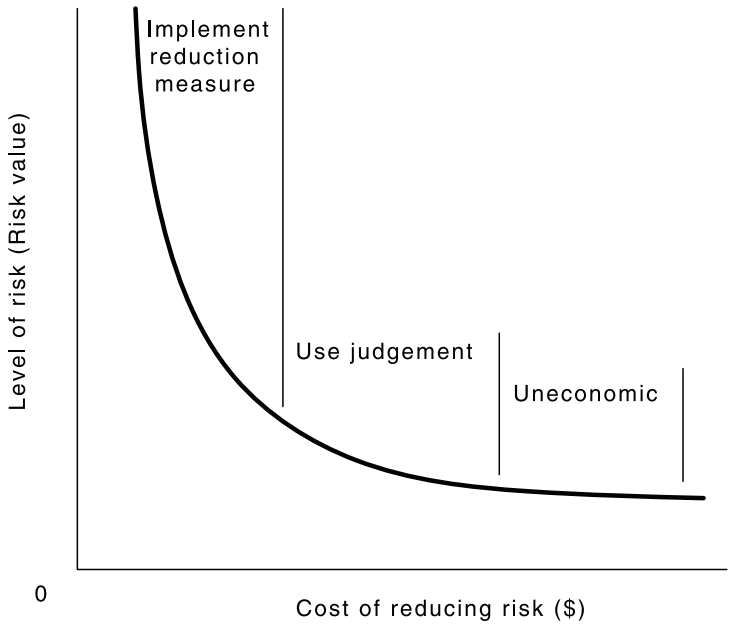

Figure 4.2 – Cost of risk reduction measures

In many cases, it is unlikely that one risk treatment option will be a complete solution for a particular problem. Often the organization will benefit substantially by a combination of options such as reducing the likelihood of risks, reducing their consequences, and transferring or retaining any residual risks. An example is the effective use of contracts and risk financing supported by a risk reduction program.

Where the cumulative costs of implementing all risk treatments exceeds the available budget, the plan should clearly identify the priority ordering in which individual risk treatments should be implemented. Priority ordering can be established using various techniques, including risk ranking and cost-benefit analysis. Risk treatments which cannot be implemented within the limit of the available budget must either wait until the availability of further financial resources or, if for whatever reason any or all of the remaining treatments are considered important, a case must be made to secure additional finances.

Risk treatment options should consider how risk is perceived by affected parties and the most appropriate ways to communicate to those parties.

4.5.3.1 *Selection of controls*

Risk treatment controls (safeguards or chosen options) selected to either reduce the likelihood of occurrence of security incidents or reduce the consequences should be additional to any already existing and planned controls. It is important that such existing and planned controls are identified as part of this process to avoid unnecessary work or cost, e.g., in the duplication of controls. It might also be identified that an existing or planned control is not justified. In this case, it should be checked whether the control should be removed, replaced by another, more suitable, control, or whether it should stay in place (for example, for cost reasons).

In order to select controls that effectively protect against the assessed risks, the results of the risk analysis should be considered. The vulnerabilities to associated threats indicate where additional protection may be needed, and what form it should take.

There might be alternatives, which are decided on according to the costs of the considered controls. Areas where controls are applicable include:

a) security policy;
b) security organization;
c) personnel;
d) physical and environment;
e) communication and operations management;
f) access control;
g) systems development and maintenance;
h) business continuity management; and
i) compliance.

Where a baseline approach is used, the selection of controls is relatively simple. Control catalogues suggest a set of controls to protect information against the most common threats. These recommended controls are compared with the existing or planned controls, and the ones not already in place or planned for form a list of controls to be implemented to obtain baseline protection.

Control selection should always include a balance of operational (non-technical) and technical controls. Operational controls include those that provide physical, personnel, and administrative security.

Physical security

Physical security controls include strength of internal building walls, key coded door locks, fire suppression systems, and guards. Personnel security covers personnel recruitment checks, (especially people in 'positions of trust'), staff monitoring, and security awareness programs.

Procedural security

Procedural security includes secure operating procedures documentation, application development and acceptance procedures as well as procedures for incident handling. Related to this category, it is very important that an appropriate business continuity plan, including contingency planning/ disaster recovery strategy, is developed for each system. The plan should include details of the key functions and priorities for recovery, processing needs, and the organizational procedures to follow if a disaster or service interruption occurs. Such plans must include the steps required to control sensitive information being processed, while still permitting the organization to conduct business.

Technical security

Technical security encompasses hardware and software security as well as communications controls. These controls are selected according to the risks to provide security functionality and assurance. The functionality will cover, for example, identification and authentication, logical access control requirements, audit trail/security logging needs, dial-back security, message authentication, encryption, and so on. Assurance requirements document the level of trust needed in security functions and thus the amount and type of checking, security testing, etc., necessary to confirm that level. In deciding on the complementary blend of operational and technical controls, there will be different options for implementing the technical security requirements. A technical security architecture should be defined for each option to help in identifying that security can be provided as required, and also that it is feasible with available technology.

Evaluated products

An organization may chose to make use of evaluated products and systems as part of the final system solution. Evaluated products are those which have been examined by a third party. The third party may be another part of the same organization or an independent organization specializing in product and system evaluation. The evaluation may be performed against a set of predetermined criteria that are created specifically for the system being built or it may be a generalized set of criteria that can be used in a variety of situations. The evaluation criteria may specify functional requirements and/or assurance requirements. A number of evaluation schemes are in existence, many of them sponsored by government and international standards organizations. An organization could decide to make use of evaluated products and systems when it requires confidence that the set of functionality implemented is what is required, and when it needs to trust in the correctness and completeness of the implementation of that functionality. Alternatively, focused pragmatic security testing could provide assurance of confidence in the security provided.

Factors influencing control selection

When selecting controls for implementation, a number of factors should be considered including:

i) ease of use of the control;

ii) transparency to the user;

iii) proximity of the control to the asset being protected;

iv) the help provided to the users to perform their function;

v) the relative strength of the controls; and

vi) the types of functions performed—prevention, deterrence, detection, recovery, correction, monitoring, and awareness.

Generally, a control will fulfil more than one of these functions - the more it can fulfil the better. When examining the overall security, or set of controls to be used, a balance should be maintained between the types of functions if at all possible. This helps the overall security to be more effective and efficient. A cost/benefit analysis may be required as well as a trade-off analysis (a method of comparing competing alternatives using a set of criteria which are weighted for relative importance in regard to the particular situation).

Cost of controls

An important aspect of control selection is the cost factor. It would be inappropriate to recommend controls that are more expensive to implement and maintain than the value of the assets they are designed to protect. It may also be inappropriate to recommend controls that are more expensive than the budget that the organization has assigned for security. However, great care should be taken if the budget reduces the number or quality of controls to be implemented since this can lead to the implicit acceptance of a greater risk than planned. The established budget for controls should only be used as a limiting factor with considerable care.

The existing and planned controls should be assessed in terms of cost comparisons, including maintenance, with a view to removing (or not implementing) or improving them if they are not effective enough. Here it should be noted that sometimes it is more expensive to remove an inappropriate control than to leave it in place, and maybe add another control. It is possible as well that a control may provide protection to assets outside of the current review boundary.

Control compatibility

A check needs to be made to determine whether the controls selected following the risk analysis are compatible with existing and planned controls, i.e. that the controls being selected and existing controls should not hinder each other.

Existing controls

While identifying the existing controls, a check should be made to ensure that the controls are working correctly. A control that is relied on to work correctly, but does not function in the business process, is a source of possible vulnerability.

The result of this step is a list of all existing and planned controls, and their implementation and use status.

Additional advice on the selection of controls can be found in AS 13335.4.

4.5.3.2 *Security architecture*

A security architecture describes how the requirements for security are to be satisfied. Therefore, it is important to consider the security architecture during the process of control selection.

A security architecture can be used in the development of new systems and when major changes are made to existing systems. Based on the results of the risk analysis or baseline approach, it takes the requirements for security and refines them into a set of technical security services for the system that will satisfy those requirements. In some cases, particularly when changes are being made to existing systems, some of the requirements may be in the form of specific controls that are to be used.

A security architecture focuses on technical security services and how they will fulfil the security objectives. In doing this, related non-technical security controls are taken into account. Even though the architecture can be built from a number of different perspectives and approaches, one fundamental principle should be taken into account. A security problem in a unique security domain (an area of the same or similar security requirements and controls) must not be permitted to adversely impact the security of another unique security domain. A security architecture will normally consist of one or more security domains. The security domains should follow the business domains that the organization is using and has established, as closely as is practical. These business domains may follow particular business functional divisions such as payroll, manufacturing, or customer service, or they may follow business services divisions such as e-mail services or office services.

Security domains are differentiated by one or more of the following attributes:

a) levels, categories or types of information accessible within the domain;

b) operations applicable to the domain;

c) communities of interest (COI) associated within the domain;

d) relationships to other domains and environments; and

e) types of functions or information access required by COI within the domain.

In constructing a security architecture, the issues that should be addressed include:

i) interrelationships and interdependencies between unique security domains;

ii) impacts or implications of interrelationships and interdependencies weakening security services; and

iii) extra services or precautions required to correct, control or counter any weakness.

A security architecture does not stand alone, rather it relies on and interfaces with other documents. The most important of these is the system architecture and the other associated architectures such as hardware, communications and applications. A security architecture will not contain a complete description of the system, it will address technical aspects and elements related to the security only. A security architecture should aim to adversely impact users as little as possible while ensuring that the environment has the optimum protection in place.

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

A) security design;
B) security operational concept;
C) security plan;
D) security policy; and
E) certification and accreditation documentation, if required.

4.5.3.3 *Identification/review of constraints*

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

Time constraints

Many types of time constraints can exist. For example, controls should be implemented within a time period acceptable for management. Another type of time constraint is whether a control can be implemented within the lifetime of the system. A third type of time constraint may be the period of time management decides is an acceptable period to leave the system exposed to a particular risk.

Financial constraints

Controls should not be more expensive to implement than the value of assets they are designed to protect. Every effort should be made not to exceed assigned budgets. However, in some cases it may not be possible to achieve the desired security and level of risk acceptance within those budget constraints. The resolution of this situation becomes a management decision.

Technical constraints

Technical problems, like the compatibility of programs or hardware, can easily be avoided if account is taken of them during the selection of controls. Also, the retrospective implementation of controls to an existing system is often hindered by technical constraints. These difficulties may move the balance of controls towards the procedural and physical aspects of security.

Sociological constraints

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

Environmental constraints

Environmental factors may influence the selection of controls; for example, space availability, extreme climate conditions, surrounding natural and urban geography.

Legal constraints

Legal factors like personal data protection or criminal code provisions for information processing could affect the selection of controls. Non IT specific laws and regulations like fire department regulations and labour relations laws could also affect control selection.

People and skill constraints

Some controls may require availability of specialist skills to implement them or operate them. Such factors may be constraints if people with the necessary skills are not available.

4.5.4 Preparing treatment plans

Plans should document how the controls should be implemented.

The treatment plan should identify responsibilities, schedules, the expected outcome of treatments, budgeting performance measures and the review process to be set in place.

The plan should also include a mechanism for assessing the implementation of the options against performance criteria, individual responsibilities and other objectives, and to monitor critical implementation milestones.

4.5.5 Implementing treatment plans

Ideally, responsibility for treatment of risks should be borne by those best able to control the risk. Responsibilities should be agreed between the parties at the earliest possible time.

The successful implementation of the risk treatment plan requires an effective management system which specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria.

If after treatment there is a residual risk, a decision should be taken as to whether to retain this risk or repeat the risk treatment process.

4.6 Risk acceptance

After the implementation of the selected controls, there will always be residual risks. This is because an organization's information systems can never be made absolutely secure. It may also be that certain assets may have been left unprotected intentionally (e.g., because of assumed low risk or the high costs of the recommended control).

Risk acceptance involves a review of the controls selected in order to identify and assess all residual risks. This involves a judgement of how much the controls selected reduce the risks, for example, by reducing the threats and/or vulnerabilities. These residual risks are categorized according to those that are considered 'acceptable' and those that are considered 'unacceptable' to the organization. It is generally good practice that unacceptable risks should not be tolerated, thus additional controls reducing those risks should be considered. For each of these unacceptable risks, a business decision must be made. Either the risk is finally accepted, or the expense of additional controls must be approved to reduce the risk to an acceptable level.

4.7 Monitoring and review

It is necessary to monitor risks, the effectiveness of the risk treatment plan, strategies and the management system that is set up to control implementation. Risks and the effectiveness of control measures need to be monitored to ensure changing circumstances do not alter risk priorities. Few risks remain static.

Ongoing review is essential to ensure that the management plan remains relevant. Factors which may affect the likelihood and consequences of an outcome may change, as may the factors which affect the suitability or cost of the various treatment options. It is therefore necessary to regularly repeat the risk management cycle. Review is an integral part of the risk management treatment plan. Results of monitoring and review activities should be fed back into the risk management system.

4.8 Communication and consultation

Communication and consultation are an important consideration at each step of the risk management process. It is important to develop a communication plan for both internal and external stakeholders at the earliest stage of the process. This plan should address issues relating to both the risk itself and the process to manage it.

Communication and consultation involve a two-way dialogue between stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision-maker to other stakeholders.

Effective internal and external communication to all stakeholders is important as it may have a significant impact on decisions made. This communication will ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required.

Perceptions of risk can vary due to difference in assumptions and concepts and the needs, issues and concerns of stakeholders as they relate to the risk or the issues under discussion. Stakeholders are likely to make judgements on the acceptability of the risk based on their perception of risk. This is especially important to ensure that the stakeholders perceptions of risk, as well as their perceptions of benefits, can be identified and documented and the underlying reasons clearly understood and addressed.

5 Documentation

5.1 General

Each stage of the risk management process should be documented. Documentation should include assumptions, methods, data sources and results.

Documentation should be maintained to be up to date and available for routine operations within an information security management system or for status review. Obsolete documentation should be withdrawn but retained if necessary for traceability of decisions. Version control should be applied to documentation, and all documents should include the date of effect and the name of the accountable person.

All documentation shall be made available as required by the ISMS and Risk Management policy. Where a quality management system is in operation, risk management documentation should be managed under the same management system.

The extent of the documentation can differ from one organization to another owing to:

a) the size of the organization and the type of its activities; and

b) the scope and complexity of the security requirements and the system being managed.

Documents and records may be in any form or type of medium.

5.2 Reasons for documentation

The reasons for documentation are as follows:

a) to demonstrate the process is conducted properly;

b) to provide evidence of a systematic approach to risk identification and analysis;

c) to provide a record of risks and to develop the organization's knowledge database;

d) to provide the relevant decision makers with a risk management plan for approval and subsequent implementation;

e) to provide an accountability mechanism and tools;

f) to facilitate continuing monitoring and review;

g) to provide an audit trail; and

h) to share and communicate information.

5.3 Security policy

Information security policies set out the goals and objectives of the information security management system and define the structure and management processes to manage risk within the organization.

The content of security policies should be relevant and specific to the nature of the organization, its activities and functions, and its operational environment.

AS/NZS 7799.2 documents the matters that must be covered in an information security policy. It specifically requires that policies be framed and applied to reduce risks to acceptable levels and be developed to:

a) establish the strategic organizational and risk management context;

b) establish the criteria against which risk will be evaluated; and

c) establish the structure of the risk assessment process.

The security policy must also identify the criteria for determining whether documents require special or restricted handling and set out the operational methods for marking and handling those documents. This is especially important for risk management documents, which may contain commercially sensitive information or details of physical and technical vulnerabilities within the organization.

5.4 Scope and context of the information security management system

An information security management system may include all or part of an organization. The scope should clearly define what must be considered in the context of the business processes and information assets under review:

Scope documentation should cover the context as described in Clause 4.1 and provide:

a) clearly defined boundaries for the operational activities and business processes of the organization that are within the scope of the ISMS;

b) the roles and responsibilities of third parties, including trading partners, customers, suppliers, service providers, and other organizations with regard to the assumption and treatment of risk; and

c) detailed inventories, definitions, or specifications of IT assets, people, environments, and activities within scope.

This may be based on information security services, controls, and policies that are in place or externally implemented.

Clear definition of the scope is particularly relevant if only part of an organization is within the scope, or if business processes and activities within scope are closely coupled with third parties. The scope may be divided in some way, for example into domains that will make subsequent risk management tasks simpler.

The context of the ISMS includes the business or operational environment, relevant legal and regulatory regimes, and the specific methods and processes selected to manage risk.

Documentation of the context should cover:

i) the strategic objectives and operating environment of the organization;

ii) the business information security, legal and regulatory requirements;

iii) the methods selected and applied to risk assessment;

iv) the measures and criteria for risk evaluation; and

v) the processes, accountabilities, and criteria for assessing the effectiveness of risk treatment strategies.

5.5 Risk identification and assessment

Risk assessment documentation should cover analysis performed as described in Clauses 4.2, 4.3 and 4.4. It is essential that decisions and their rationale are clearly documented. The tools and techniques used should be described and the rationale for their choice documented. The documentation should also indicate how such tools were used. Documentation based on a 'risk register' is one approach that can be used.

Risk assessment documentation should contain sufficient detail to allow a reviewer to assess:

a) whether the chosen approach, tools and techniques were suitable for the chosen scope and risks;

b) whether the chosen approach, tools and techniques were correctly used to produce valid results; and

c) whether the proposed treatment plan is adequate to achieve the nominated risk management objectives.

5.6 Risk treatment plan

The risk treatment plan is a coordination document defining the actions to be undertaken to implement the required controls to protect information. The plan should include a schedule and priorities, a detailed work plan and responsibilities for the implementation of controls.

This plan should contain the results of the risk assessment, the actions to be undertaken within short, medium and long time frames to mitigate the risk to an acceptable level, the costs, and an implementation schedule. It should include for each identified risk:

a) the method selected for treating the risk;

b) what controls are in place;

c) what additional controls are proposed;

d) the time frame over which the proposed controls are to be implemented.

The plan should also include:

i) the reasons for choosing the selected controls in terms of threats and vulnerabilities to be addressed. (Controls may be grouped together insofar as they address common threats and vulnerabilities);

ii) priorities for the implementation of the selected controls and the upgrading of existing controls;

iii) implementation and operational guidelines for the selected controls;

iv) estimates of the installation and running costs for these controls;

v) estimates of manpower resources for the implementation of these controls, and for follow-up actions;

vi) a detailed workplan for the implementation, containing:

A) priorities;

B) an implementation schedule in relation to priorities;

C) the budget needed; and

D) responsibilities,

vii) the security awareness and training procedures for staff and end users to ensure the effectiveness of the controls;

viii) a schedule for approval processes to take place where needed; and

ix) a schedule for follow-up procedures.

The risk treatment plan must also identify individuals with sufficient seniority to be accountable for the successful execution of the plan.

5.7 Implementation and operational procedures

These procedures should describe implementation of the risk treatment plan, including a description of the management framework and responsibilities of the people with implementation or operational roles. They should also include a description of procedures for the management and operation of the controls in the ISMS and processes for ongoing review of risks and their treatment in the light of changing technology, threats, or functions.

5.8 Statement of Applicability

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

The Statement of Applicability should be signed off by the person (or people) accountable for the security domain(s) covered by it.

5.9 Records

Records must be kept and maintained to provide evidence of compliance with risk management and security policies and processes. Records also need to be kept and maintained as evidence of the implementation of the risk management process and risk treatment plans.

Records must be controlled, in that operational procedures are in place for the creation, storage, and management of records. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records must be documented. All legal and regulatory requirements for the keeping and retention of records must be met. Records shall remain legible, readily identifiable and retrievable.

Management reviews will determine the need for and extent of records.

APPENDIX

A Examples of possible threat types

The following list gives examples of typical threats. The list can be used during the threat assessment process. Threats can be caused by one or more of deliberate, accidental or environmental (natural) events. The following list indicates for each threat type where D (deliberate), A (accidental), E (environmental) are relevant. D is used for all deliberate actions aimed at information assets, A is used for all human actions which accidentally can damage information assets, E is used for all incidents which are not based on human actions.

Earthquake	E
Flooding	D, A, E
Hurricane	E
Lightning	E
Industrial action	D, A
Bomb attack	D, A
Use of arms	D, A
Fire	D, A
Willful damage	D
Failure of power supply	A
Failure of water supply	A
Air conditioning failure	D, A
Hardware failures	A
Power fluctuation	A, E
Extremes of temperature and humidity	D, A, E
Dust	E
Electromagnetic radiation	D, A, E
Electrostatic charging	E
Theft	D
Unauthorized use of storage media	D
Deterioration of storage media	E
Operational staff error	D, A
Maintenance error	D, A
Software failure	D, A
Use of software by unauthorized users	D, A
Use of software in an unauthorized way	D, A
Masquerading of user identity	D
Illegal use of software	D, A
Malicious software	D, A

Illegal import/export of software	D
Operational staff error	D, A
Maintenance error	D, A
Network access by unauthorized users	D
Use of network facilities in an unauthorized way	D
Technical failure of network components	A
Transmission errors	A
Damage to lines	D, A
Traffic overloading	D, A
Eavesdropping	D
Communications infiltration	D
Traffic analysis	D
Misrouting of messages	A
Rerouting of messages	D
Repudiation	D
Failure of communications services (i.e. network services)	D, A
Staff shortage	D, A
User errors	D, A
Misuse of resources	D, A

APPENDIX

B Examples of common vulnerabilities

The following lists give examples for vulnerabilities in various security areas, including examples of threats that might exploit these vulnerabilities. The lists can provide help during the assessment of vulnerabilities. It is emphasized that in some cases other threats may also exploit these vulnerabilities.

Vulnerabilities can be demonstrated through the use of the following examples:

a) Single point of failure

(could be exploited by, for example, the threat of failure of communications services)

b) Inadequate service maintenance response

(could be exploited by, for example, the threat of hardware failures)

B1 Environment and infrastructure

Lack of physical protection of the building, doors, and windows

(could be exploited by, for example, the threat of theft)

Inadequate or careless use of physical access control to buildings, rooms

(could be exploited by, for example, the threat of willful damage)

Unstable power grid

(could be exploited by, for example, the threat of power fluctuation)

Location in an area susceptible to flood

(could be exploited by, for example, the threat of flooding)

B2 Hardware

Lack of periodic replacement schemes

(could be exploited by, for example, the threat of deterioration of storage media)

Susceptibility to voltage variations

(could be exploited by, for example, the threat of power fluctuation)

Susceptibility to temperature variations

(could be exploited by, for example, the threat of extremes of temperature)

Susceptibility to humidity, dust, soiling

(could be exploited by, for example, the threat of dust)

Sensitivity to electromagnetic radiation

(could be exploited by, for example, the threat of electromagnetic radiation)

Insufficient maintenance/faulty installation of storage media

(could be exploited by, for example, the threat of maintenance error)

Lack of efficient configuration change control

(could be exploited by, for example, the threat of operational staff error)

B3 Software

Unclear or incomplete specifications for developers

(could be exploited by, for example, the threat of software failure)

No or insufficient software testing

(could be exploited by, for example, the threat of use of software by unauthorized users)

Complicated user interface

(could be exploited by, for example, the threat of operational staff error)

Lack of identification and authentication mechanisms like user authentication

(could be exploited by, for example, the threat of masquerading of user identity)

Lack of audit-trail

(could be exploited by, for example, the threat of use of software in an unauthorized way)

Well-known flaws in the software

(could be exploited by, for example, the threat of use of software by unauthorized users)

Unprotected password tables

(could be exploited by, for example, the threat of masquerading of user identity)

Poor password management (easily guessable passwords, storing of passwords in clear view, insufficient frequency of change)

(could be exploited by, for example, the threat of masquerading of user identity)

Wrong allocation of access rights

(could be exploited by, for example, the threat of use of software in an unauthorized way)

Uncontrolled downloading and using software

(could be exploited by, for example, the threat of malicious software)

No 'logout' when leaving the workstation

(could be exploited by, for example, the threat of use of software by unauthorized users)

Lack of effective change control

(could be exploited by, for example, the threat of software failure)

Lack of documentation

(could be exploited by, for example, the threat of operational staff error)

Lack of back-up copies

(could be exploited by, for example, the threat of malicious software or the threat of fire)

Disposal or reuse of storage media without proper erasure

(could be exploited by, for example, the threat of use of software by unauthorized users)

B4 Communications

Unprotected communication lines

(could be exploited by, for example, the threat of eavesdropping)

Poor joint cabling

(could be exploited by, for example, the threat of communications infiltration)

Lack of identification and authentication of sender and receiver

(could be exploited by, for example, the threat of masquerading of user identity)

Transfer of passwords in clear view

(could be exploited by, for example, the threat of network access by unauthorized users)

Lack of proof of sending or receiving a message

(could be exploited by, for example, the threat of repudiation)

Dial-up lines

(could be exploited by, for example, the threat of network access by unauthorized users)

Unprotected sensitive traffic

(could be exploited by, for example, the threat of eavesdropping)

Inadequate network management (resilience of routing)

(could be exploited by, for example, the threat of traffic overloading)

Unprotected public network connections

(could be exploited by, for example, the threat of use of software by unauthorized users)

B5 Documents

Unprotected storage

(could be exploited by, for example, the threat of theft)

Lack of care at disposal

(could be exploited by, for example, the threat of theft)

Uncontrolled copying

(could be exploited by, for example, the threat of theft)

B6 Personnel

Absence of personnel

(could be exploited by, for example, the threat of staff shortage)

Unsupervised work by outside or cleaning staff

(could be exploited by, for example, the threat of theft)

Insufficient security training

(could be exploited by, for example, the threat of operational staff error)

Lack of security awareness

(could be exploited by, for example, the threat of user errors)

Incorrect use of software and hardware

(could be exploited by, for example, the threat of operational staff error)

Lack of monitoring mechanisms

(could be exploited by, for example, the threat of use of software in an unauthorized way)

Lack of policies for the correct use of telecommunications media and messaging

(could be exploited by, for example, the threat of use of network facilities in an unauthorized way)

Inadequate recruitment procedures

(could be exploited by, for example, the threat of willful damage)

APPENDIX

C Combined approach for risk identification, assessment and treatment

This Appendix provides guidance for implementing a combined risk treatment strategy.

This approach begins with risk identification. Identified risks are then separated into two categories;

a) risks that are common and/or for which there is an established treatment code of practice (or baseline); and

b) risks that are unusual and potentially serious.

The first category of risk is treated by implementing controls from a baseline standard or code of practice. The second category of risk requires assessment and treatment as discussed in Clauses 4.4 and 4.5.

The advantage of combining baseline and risk assessment approaches to risk treatment is that attention and risk assessment resources can be focused on just those risks that are unusual or serious. This can be much more efficient than adopting an assessment oriented approach for all risks because there are typically a large number of information security risks, many of which have widely accepted treatment solutions.

For example, the risk of unauthorized access to information on in-house networks can be treated by a well managed, password based, user authentication system. Whilst assessment methods could be used to optimize parameters such as password length, password composition, and user guidelines for password handling, the effort required for such analysis is not worthwhile. There is a code of practice for such details that has been proven effective. (See AS/NZS ISO/IEC 17799 for details.)

More information about this approach and advantages over alternative approaches can be found in AS 13335.3.

C1 High level risk identification

First it is necessary to conduct an initial high level risk identification review. This review considers the business values of the IT systems and the information handled, and the risks from the organization's business point of view. Input for the decision as to which risk treatment approach is suitable can be obtained from consideration of the following:

a) the business objectives to be achieved by using an information system;

b) the degree to which the organization's business depends on the information system, i.e. whether functions that the organization considers critical to its survival or the effective conduct of business are dependent on this system, or on the confidentiality, integrity, availability, accountability, authenticity, and reliability of the information processed on this system;

c) the level of investment in an IT system, in terms of developing, maintaining, or replacing the system; and

d) the assets of the information system, for which the organization directly assigns value.

When these items are assessed, the decision is generally easy. If the objectives of a system are important to an organization's conduct of business, if system replacement costs are high, or if the values of the assets are at high risk, then a detailed risk analysis is necessary for the system. Any one of these conditions may be enough to justify conducting a detailed risk analysis.

A general rule to apply is: if the lack of information security can result in significant harm or damage to an organization, its business processes or its assets, then a detailed risk analysis is necessary to identify suitable treatment options. In all other cases, the application of a baseline approach provides appropriate protection.

C2 Baseline (code of practice) risk treatment

The objective of baseline (code of practice) protection is to establish a minimum set of controls to protect all or some of an organization's information. Using this approach, it is possible to apply baseline protection organization-wide, and, as reflected in Paragraph C1, additionally use detailed risk analysis reviews to protect information systems at high risk or systems critical to the business. The use of the baseline approach reduces the investment that the organization has to make in the performance of risk analysis reviews.

The appropriate baseline protection can be achieved through the use of control catalogues that suggest a set of controls to protect an information system against the most common threats. The level of baseline security can be adjusted to the needs of the organization. A detailed assessment of threats, vulnerabilities and risks is not necessary. All that has to be done to apply baseline protection is to select those parts of the control catalogue which are relevant for the context considered. After identifying the controls already in place, a comparison is made with those controls listed in the baseline catalogue. Those that are not already in place, and are applicable, should be implemented.

Baseline catalogues may specify controls to be used in detail, or they may suggest a set of security requirements to be addressed with whatever controls are appropriate to the system under consideration. Both approaches have advantages. Catalogues of both types can be found in AS 13335.3. One of the objectives of the baseline approach is consistency of security controls throughout the organization, which can be achieved by both approaches.

Several documents are already available which provide sets of baseline controls. Also, sometimes a similarity of environments can be observed among companies within the same industrial sector. After the examination of the basic needs, it may be possible for baseline control catalogues to be used by a number of different organizations. For example, catalogues of baseline controls could be obtained from:

a) international and national standards organizations;

b) industry sector standards or recommendations; or

c) some other company, preferably with similar business objectives, and of comparable size.

An organization may, of course, also generate its own baseline, established commensurate with its typical environment, and with its business objectives.

C3 Assessment and treatment of unusual or potentially serious risks

Unusual or potentially serious security risks require treatment based on the results of risk analysis and evaluation as described in Clauses 4.3, 4.4 and 4.5.

APPENDIX

D Example risk analysis methods

The analysis of risks has a number of stages that have been discussed in this Appendix and the other parts of this Handbook. Those stages are:

a) asset identification and valuation (potential adverse business impact assessment);

b) threat assessment;

c) vulnerability assessment;

d) existing/planned control assessment; and

e) risk evaluation.

The final stage is to assess the overall risks which is the focus of this Appendix. As identified earlier, assets that have value and have some degree of vulnerability are at risk whenever a threat to the assets exists. The analysis of the risks is a combination of the potential adverse business impacts of unwanted incidents, and the level of assessed threats and vulnerabilities. The risks are in effect measures of the exposure to which a system, and the associated organization, may be subjected. Risks are a function of:

i) the asset values;

ii) the threats, and their associated likelihood of the occurrence, that may threaten the assets;

iii) the ease of exploitation of vulnerabilities by threats to cause unwanted impacts; and

iv) the existing or planned controls, which might reduce the severity of vulnerabilities, threats and impacts.

The objective of risk analysis is to identify and assess the risks to which the information system and its assets are exposed, in order to identify and select appropriate and justified security controls. When assessing the risks, several aspects are considered including impact and likelihood.

The impact may be assessed in several ways, including using quantitative, e.g. monetary, and qualitative measures (which can be based on the use of adjectives such as moderate or severe), or a combination of both. To assess the likelihood of threat occurrence, the time frame over which the asset will have value or needs to be protected should be established. The probability of a threat occurring is affected by the following:

A) the attractiveness of the asset, applicable when a deliberate human threat is being considered;

B) the ease of conversion of the asset into reward, applicable if a deliberate human threat is being considered;

C) the technical capabilities of the threat agent, applicable to deliberate human threats;
D) the likelihood of the threat; and
E) the susceptibility of the vulnerability to exploitation, applicable to both technical and non-technical vulnerabilities.

Many methods make use of tables, and combine subjective and empirical measures. Currently, there is no right or wrong method to use. It is more important that the organization uses a method with which they are comfortable, have confidence in and that will produce repeatable results. Three stand alone examples of table based techniques are given below.

Example 1 - Matrix with predefined values

In risk analysis methods of this type, actual or proposed physical assets are valued in terms of replacement or reconstruction costs (i.e. quantitative measurements). These costs are then converted onto the same qualitative scale as that used for data assets (see below). Actual or proposed software assets are valued in the same way as physical assets, with purchase or reconstruction costs identified and then converted to the same qualitative scale as that used for data assets. Additionally, if any application software is found to have its own intrinsic requirements for confidentiality or integrity (for example if source code is itself commercially sensitive), it is valued in the same way as for data assets.

The values for data assets are obtained by interviewing the selected business personnel (the 'data owners') who can speak authoritatively about the data, to determine the value and sensitivity of the data actually in use, or to be, stored, processed or accessed. The interviews facilitate assessment of the value and sensitivity of the data assets in terms of the worst case scenarios that could be reasonably expected to happen from adverse business impacts due to unauthorized disclosure, unauthorized modification, repudiation, non-availability for varying time periods, and destruction.

The valuation is accomplished using data asset valuation guidelines, which cover such issues as:

a) personal safety;
b) personal information;
c) legal and regulatory obligations;
d) law enforcement;
e) commercial and economic interests;
f) financial loss/disruption of activities;
g) public order;
h) business policy and operations; and
i) loss of goodwill.

The guidelines facilitate identification of the values on a numeric scale, such as the 0 to 4 scale shown in the example matrix in Table D1, thus enabling the recognition of quantitative values where possible and logical, and qualitative values where quantitative values are not possible, e.g. for endangerment of human life.

The next major activity is the completion of pairs of questionnaires for each threat type, for each grouping of assets that a threat type relates to, to enable the assessment of the levels of threats (likelihood of occurrence) and levels of vulnerabilities (ease of exploitation by the threats to cause adverse impact). Each question answer attracts a score. These scores are accumulated through a knowledge base and compared with ranges. This identifies threat levels on say a high to low scale, and vulnerability levels similarly, as shown in the example matrix below, differentiating between the impact types as relevant. Information to complete the questionnaires should be gathered from interviews with appropriate technical, personnel and accommodation people, and physical location inspections and reviews of documentation.

Threat types to be considered are broadly grouped under: deliberate unauthorized actions by people, acts of god, errors by people, and equipment/software/line failure.

The asset values, and the threat and vulnerability levels, relevant to each impact type, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 1 to 8. The values are placed in the matrix in a structured manner. An example is given below:

Table D1 Example 1 – Matrix with predefined values

Levels of Threat		**Low**			**Medium**			**High**		
Levels of Vulnerability		**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

For each asset, the relevant vulnerabilities and their corresponding threats are considered. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes!). Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the severity of the threat and the vulnerability. For example, if the asset has the value **3**, the threat is '**high**' and the vulnerability '**low**', the measure of risk is **5**. Assume an asset has a value of **2**, e.g. for modification, the threat level is '**low**' and the vulnerability is '**high**', then the measure of risk is **4**. The size of the matrix, in terms of the number of threat severity categories, vulnerability severity categories, and the number of asset valuation categories, can be adjusted to the needs of the organization. Additional columns and rows will necessitate additional risk measures. The value of this approach is in ranking the risks to be addressed.

Example 2 - Assessing a value for the frequency and the possible damage of risks

In this example, the emphasis is placed on the impact of unwanted incidents and on determining which systems should be given priority. This is done by assessing two values for each asset and risk, which in combination will determine the score for each asset. When all the asset scores for the system are summed, a measure of risk to that information system is determined.

First, a value is assigned to each asset. This value relates to the potential damage that can arise if the asset is threatened. For each applicable threat to the asset, this asset value is assigned to the asset.

Next a frequency value is assessed. This is assessed from a combination of the likelihood of the threat occurring and the ease of exploitation of the vulnerability, as shown in Table D2.

Table D2 Example 2 – Assessing a value for the frequency and the possible damage of risks

Levels of Threat	Low			Medium			High		
Levels of Vulnerability	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Frequency Value (or likelihood)	0	1	2	1	2	3	2	3	4

Next, an asset/threat score is assigned by finding the intersect of asset value and frequency value in Table D3. The asset/threat scores are totalled to produce an asset total score. This figure can be used to differentiate between the assets forming part of a system.

Table D3 Example 2 – Assessing a value for the frequency and the possible damage of risks

Frequency Value (or likelihood)	Asset Value (or impact)				
	0	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

The final step is to total all the asset total scores for the assets of the system, producing a system score. This can be used to differentiate between systems and to determine which system's protection should be given priority.

In the following examples all values are randomly chosen.

Suppose System S has three assets A1, A2 and A3. Also suppose there are two threats T1 and T2 applicable to System S. Let the value of A1 be 3, similarly let the asset value of A2 be 2 and the asset value of A3 be 4.

If for A1 and T1 the threat likelihood is low and the ease of exploitation of the vulnerability is medium, then the frequency value is 1 (see Table D2).

The asset/threat score A1/T1 can be derived from Table D3 as the intersection of asset value 3 and frequency value 1, i.e. 4. Similarly, for A1/T2 let the threat likelihood be medium and the ease of exploitation of a vulnerability be high, giving an A1/T2 score of 6.

Now the total asset score A1T can be calculated, i.e., 10. The total asset score is calculated for each asset and applicable threat. The total system score is calculated by adding A1T + A2T + A3T to give ST.

Now different systems can be compared to establish priorities, and also different assets within one system.

A simplified case of this approach follows where three levels of risk are used (low, medium and high), and these are directly associated with different levels of asset value (impact) and frequency value (likelihood) based on experience.

Table D4 Example 2 – Assessing a value for the frequency and the possible damage of risks

Likelihood	Impact			
	Critical	**High**	**Medium**	**Low**
Almost certain	High risk	High risk	Medium risk	Low risk
Likely	High risk	High risk	Medium risk	Low risk
Moderate	High risk	High risk	Medium risk	Low risk
Unlikely	Low risk	Low risk	Low risk	Low risk

Example 3 - Distinction between tolerable and intolerable risks

Another way of measuring the risks is to only distinguish between tolerable (T) and non-tolerable (N) risks. The background of this is that the measures of risks are only used to rank the risks in terms of where action is needed most urgently, and the same can be achieved with less effort.

With this approach, the matrix used simply does not contain numbers but only **T**s and **N**s stating whether the corresponding risk is tolerable or not tolerable. For example, the matrix of Method 3 could be changed into:

Table D5 Example 3 – Distinction between tolerable and intolerable risks

Frequency Value	Damage Value				
	0	**1**	**2**	**3**	**4**
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Again, this is only an example, and it is left to the reader where to draw the line between tolerable and intolerable risks.

ISBN 0 7337 5649 2