Controlling & Auditing Information System

IT Security

Prepared by:

Basuki Rahmad, Dr, CISA, CISM

2011

TABLE OF CONTENTS

1 Module Objective....1
2 IT Security – An Overview....1
3 IT Security Standards and Frameworks....3
4 Risk analysis....9
5 Risk management....28
6 Security policy....35
7 Organisation of Information Security....39
8 Asset classification and control....44
9 Personnel security....48
10 Systems development and maintenance....53
11 Network and Communications Controls....59
12 Compliance Controls....80
13 Audit considerations....92
Annex 1: Glossary of terms....96
Annex 2: Examples of risk analysis methodologies....98
Annex 3: Sample IT security standards....114

1 Module Objective

This module provides an introduction to information system security from an auditor's perspective. The objective is to enable the auditor to examine clients' approaches to information system security and assess whether they are doing enough to reduce the risk to their information systems to an acceptable level.

Some of the terminology used in the context of information system security is open to interpretation. Every effort has been made to make the meaning of technical terms clear in the text, but in case there is any doubt, these notes contain a glossary of terms at Annex 1.

Finally, these notes are supplemented by those on IT Controls and on Business Continuity Planning.

2 IT Security – An Overview

2.1 Introduction

2.1.1 What is IT Security?

Information held in IT systems is increasingly a critical resource in enabling organisations to achieve their goals. Additionally, individuals whose personal information is contained in IT systems have a reasonable expectation of privacy and protection from harm, while beneficiaries of IT systems have a legitimate expectation that the systems will perform their functions efficiently whilst exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards.

2.2 Management's Concern about IT Security

Management should be concerned about IT security for three principal reasons:

- Dependence on IT systems. Information systems which can provide accurate services when and where they are required are the key to the survival of most modern businesses; without computers and communications they would be unable to provide services, process invoices, contact customers or make payments; information systems also handle the organisation's secrets which, if made public, would cause embarrassment and may even lead to business failure;
- Exposure of IT systems. IT systems need a stable environment and can be wrecked by natural disasters such as fire, flood, hurricane or earthquake; failure in the air conditioning or power supply can lead to system failure; terrorist bombs can cause immense disruption; accidents or deliberate sabotage can bring down whole networks. IT systems are the key to accessing vast quantities of corporate

data; this makes them an attractive target for hackers, investigative journalists and spies, and may provide staff with a motivation for abusing their privileges by selling information to outsiders. Organisations rely upon the accuracy of information provided by their systems; once this trust is destroyed the impact on the business may be as great as that which would be caused by the destruction of the system; as a result it is important to protect data from accidental or deliberate corruption.

- Investment in IT systems. Information systems are costly both to develop and maintain, and management should protect their investment like any other valuable asset. IT assets are particularly attractive to thieves as they are portable, have a high value to weight ratio and can readily be sold.

Once senior managers are aware of their dependency on information systems and the risks that they face, there may be a tendency to overreact; no system is completely secure and, once baseline controls are in place, there tends to be a diminishing return for further investment in security measures. Protecting IT assets can be expensive and disruptive; hence, a balance has to be struck by ensuring that security is:

- **appropriate** to an organisation's business needs yet comprehensive in its coverage;
- **justified** to the extent that it will reduce perceived risks to the level that management are willing to accept; and
- **effective** against actual threats.

An emerging concept related to IT security is that of information security governance, which has been defined by the National Institute of Standards and Technology of the US Federal Government as "the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk."

2.3 Objectives of IT Security

The requirement for security is derived from the need for management to reduce to an acceptable level the risk of a significant breach of the confidentiality, integrity or availability of information systems or the data handled by them. This can be achieved by reducing threats, reducing the vulnerability to a threat or reducing the impact of a threat occurring and adversely affecting the business.

The key security objectives (the so-called C-I-A triad) are:

- **confidentiality** – ensuring that information is accessible only to those authorised to have access;

- **integrity** – safeguarding the accuracy and completeness of information and processing methods; and
- **availability** – ensuring that authorised users have access to information and associated assets when required.

Which objectives are most important will depend on the nature of the system; in systems that hold key military secrets the emphasis would be on confidentiality above all else, whereas in most other applications the main emphasis will probably be on availability followed by integrity.

Some authors have recently added an additional security objective of *non-repudiation*. This relates to proving that a given individual did in fact authorise the information in question; that it was sent at a particular time, or that it was received by a particular individual at a particular time. Measures which satisfy the non-repudiation objective would make it difficult to deny being the originator, sending information or having received it. Non-repudiation is sometimes considered to be included in the integrity objective, but it is worth considering separately because the measures needed for non-repudiation of despatch and receipt in particular are distinct from those usually associated with integrity.

Information system security objectives overlap substantially with quality of service objectives. The emphasis in quality of service tends to be focused on timely availability of services and accurate information, rather than confidentiality, but there is enough in common between quality of service and security for it to be worthwhile to consider both together.

3 IT Security Standards and Frameworks

3.1 ISO/ IEC 17799

In 2000, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) released ISO/IEC 17799 "Information technology – Security techniques – code of practice for information security management", which was based almost exclusively on the control objectives of the British standard, BS7799 "Code of Practice for Information Security". The latest version of the standard, ISO/IEC 17799:2005 was released in June 2005.

The standard contains the following twelve main sections:

- Risk assessment and treatment;
- Security policy;
- Organisation of information security;
- Asset management;
- Human resources security;

- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance

Within each section, IT security controls and their objectives are specified and outlined, and for each of the controls, implementation guidance is provided; a total of 39 main security categories are covered. The main changes in the 2005 version include

- a special introductory clause on "risk assessment and treatment";
- A new top-level clause on "information security incident management";
- Substantial changes in sections relating to security of third party services, human resources security, management of vulnerabilities, and communications and operations management;
- additional emphasis on proper definition of information security roles and responsibilities; and
- expanded detail for each control requirement (including a specification of the overall control requirement, implementation guidance, and other information).

In addition, ISO/ IEC 27001 "Information technology – Security techniques – information security management systems – Requirements" specifies the detailed requirements for establishing, implementing, maintaining and improving an information security management system consistent with the best practices outlined in ISO/ IEC 17799, and can thus be used for certification, which is granted through an accredited certification body.

3.2 COBIT

COBIT (Control Objectives for Information and Related Technology) is an IT governance framework, which was originally developed in 1994 by the Information Systems Audit and Control Association (ISACA). Version 4.0 of COBIT was released in 2005 by the IT Governance Institute (ITGI). More details are available in the module on "Introduction to IT Audit"

In COBIT 4.0, the main control objectives relevant to information security are:

- (Plan & Organise Domain) PO9 – "Assess and Manage IT Risks", which deals with creating and maintaining a risk management framework; and
- (Deliver & Support Domain) DS4 – "Ensure Continuous Service" and DS5- "Ensure Systems Security"

3.3 National Institute of Standards and Technology

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) under the US Department of Commerce has been developing several standards and guidelines for the cost-effective security and privacy of federal information systems, in particular the Special Publication 800-series reports[1]. Three documents of the NIST are noteworthy:

- SP 800-100 "Information Security Handbook: A Guide for Managers", which provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.
- SP 800-53 Revision 1 "Recommended Security Controls for Federal Information Systems", which provides guidelines for selecting and specifying security controls for information systems.
- SP 800-53A (2nd Public Draft) "Guide for Assessing the Security Controls in Federal Information Systems", which provides guidelines for assessing the effectiveness of security controls employed in information systems (as defined in the publication SP 800-53).

In particular, SP 800-53 "Recommended Security Controls for Federal Information Systems" has a fairly comprehensive security control catalog, where 171 security controls have been grouped into three general classes (management, operational and technical controls), and further into the following 17 security control families:

IDENTIFIER	FAMILY	CLASS	No. of detailed controls
AC	Access Control	Technical	20
AT	Awareness and Training	Operational	5

[1] Unlike publications by other institutes, these publications of NIST are not subject to copyright regulations (attribution would be appreciated by NIST).

AU	Audit and Accountability	Technical	11
CA	Certification, Accreditation, and Security Assessments	Management	7
CM	Configuration Management	Operational	8
CP	Contingency Planning	Operational	10
IA	Identification and Authentication	Technical	7
IR	Incident Response	Operational	7
MA	Maintenance	Operational	6
MP	Media Protection	Operational	6
PE	Physical and Environmental Protection	Operational	19
PL	Planning	Management	6
PS	Personnel Security	Operational	8
RA	Risk Assessment	Management	5
SA	System and Services Acquisition	Management	11
SC	System and Communications Protection	Technical	23
SI	System and Information Integrity	Operational	12

In respect of each control, three key components are provided:

- A control section, which provides a concise statement of the specific security capability needed to protect a particular aspect of an information system.
- A supplemental guidance section, which provides additional information related to a specific security control.
- A control enhancements section, which provides statements of security capability to (a) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

Further, to assist organisations in making the appropriate selection on security controls for their information systems, the concept of baseline controls is introduced.

Baseline controls are the minimum security controls recommended for an information system based on the system's security categorisation. Systems are categorised into low-impact, moderate-impact and high-impact systems for the security objectives of confidentiality, integrity and availability:

- Low impact systems are systems where the potential impact values in respect of all three objectives are low;
- Moderate impact systems are systems where at least one security objective is moderate, and no security objective is greater than moderate;
- High impact systems are systems where at least one security objective is high.

Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the corresponding low, moderate or high baselines; a summary of the catalog is given in Annexe-1. The security control baselines are then tailored as follows:

- Application of appropriate scoping guidance to the initial baseline;
- Specification of compensating security controls, if needed
- Specification of organization-defined parameters in the security controls, where allowed.

The tailored security control baseline is to be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The final determination of the appropriate set of security controls necessary for providing adequate security for an information system is based on an assessment of risk and local conditions, including organisation-specific security requirements, specific threat information and cost-benefit analyses. Supplemental security controls are then implemented to mitigate unacceptable risks.

3.4 Criteria for Evaluation of Trusted Computer Systems

As opposed to assessment/ audit of security controls of an information system in a particular organisational environment, there are several criteria for evaluation of the security controls of a specific hardware or software product, which are described in this section. Note that the certification of a particular product is with reference to its evaluated configuration (or assumed, specific circumstances under which the evaluation is conducted) and not in the context of its actual implementation in a specific organisation.

3.4.1 Trusted Computer System Evaluation Criteria (TCSEC)

TCSEC is a US Government Department of Defence Standard, often referred to as the "Orange Book" that sets basic requirements for assessing and classifying the effectiveness of security controls built into a computer system. TCSEC was replaced

with the development of the Common Criteria international standard published in 2005.

Under TCSEC, there are two basic security policies:

- Mandatory security policy, which enforces access control rules based directly on an individual's clearance, authorization for information and the confidentiality level of the information.
- Discretionary security policy, which enforces a consistent set of rules for controlling access on a need-to-know basis.

Under TCSEC, there are two types of assurance:

- Assurance Mechanisms, which includes operational assurance (covering system architecture, system integrity, covert channel analysis, trusted facility management and trusted recovery), and life-cycle assurance (covering security testing, design specification and verification, configuration management and trusted distribution)
- Continuous Protection Assurance, to ensure that the trusted mechanisms for enforcing the basis requirements are themselves continuously protected against tampering or unauthorized changes.

The classification hierarchy specified under TCSEC (in increasing order of security) is as follows:

- D – Minimal Protection
- C – Discretionary Protection
  - C1 – Discretionary Security Protection
  - C2 – Controlled Access Protection
- B – Mandatory Protection
  - B1 – Labelled Security Protection
  - B2 – Structured Protection
  - B3 – Security Domains
- A – Verified Protection
  - A1 – Verified Design
  - Beyond A1

3.4.2 Information Technology Security Evaluation Criteria (ITSEC)

ITSEC is a structured set of criteria published by France, Germany, the Netherlands the UK for evaluating computer security within productions and systems. The target

of evaluation is subjected to a detailed examination of its security features, including functional and penetration testing. The examination is with reference to the security features documented in the Security Target documents, and the level of examination is commensurate with the desired level of confidence (defined in the form of evaluation levels ranging from E0 to E6). ITSEC has largely been replaced by the Common Criteria.

3.4.3 Common Criteria

The Common Criteria is an international standard (ISO/ IEC 15408) which provides a framework for deriving assurance as to the process of specification, implementation and evaluation of a computer security product. Under CC, claims about the security features of the Target of Evaluation are documented through:

- Protection Profile (PP), which identifies user security requirements for a particular purpose, and effectively defines a class of security devices.
- Security Functional Requirements (SFRs), which specify individual security functions which may be provided by a product, with the CC presenting a standard catalogue of such functions.
- Security Target, which identifies the specific security properties of the target of evaluation.

The target is thus evaluated against the SFRs specified in the Security Target; quality assurance is ensured through:

- Security Assurance Requirements (of which the CC has a catalogue), which describe the measures taken during development and assurance of the product to assure compliance with the claimed security functionality.
- Evaluation Assurance Level (EAL) which is a numerical rating of the extent of validation of the claimed security assurance, ranging from EAL 1 (the most basic) to EAL 7 (the most stringent).

4 Risk analysis

4.1 Overview

The objective of IT risk analysis is to identify the various ways in which data, and the information system and network which support it, are exposed to risk. This process involves assessing the possibility that each of a wide range of threats (see Annex 3) might attack a system and the impact that a successful attack would have on the business. The end result is an individual assessment - sometimes referred to as a "security requirement" - for each type of threat that could affect the system in question. Security requirements are used to provide a basis for the following "risk management" process.

4.2 The nature of "risk"

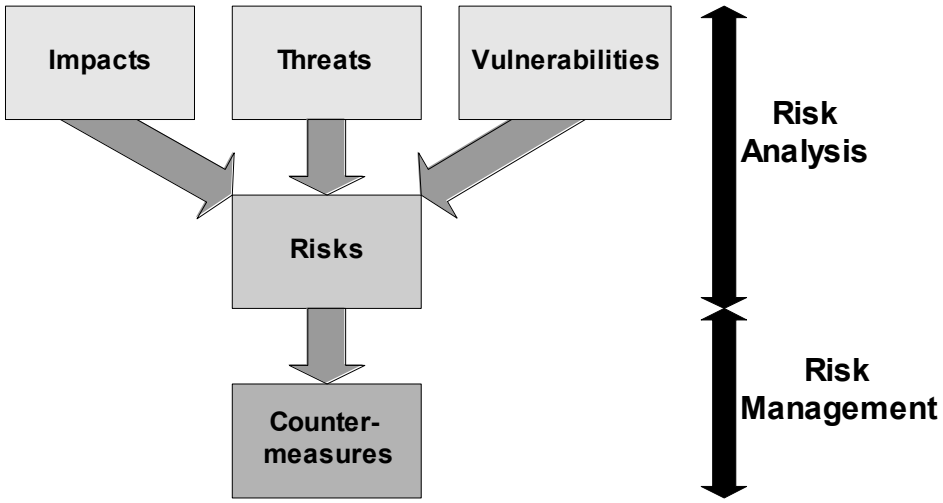
Risk is a combination of *threat, vulnerability and impact*. If there is no threat, then there is no risk.

The term ***risk*** is often used to mean either ***threat***, or the ***probability*** of a threat occurring. While threat and probability are both important components of risk, they are not the only factors to apply. In order to avoid confusion in the remainder of this section, some definitions are appropriate.

> **IT Asset** : a component part of an information system. There are four types of IT assets; physical, information, software and hardware.
>
> **Threat** : an unwanted incident (e.g. fire, malicious damage, theft) that could remove, disable, damage or destroy an IT asset.
>
> **Vulnerability** : a weakness that could be exploited by a threat.
>
> **Impact** : the consequences of a vulnerability in a system being exploited by a threat.
>
> **Probability** : in this context, the likelihood of a threat successfully attacking a computer system.
>
> **Risk** : a measure of the exposure to which a computer system is subjected. It is a function of the likelihood of a threat successfully attacking a system and the impact that would result.

Thus, in the context of IT security, ***risk*** comprises three components; ***threats***, together with their associated ***vulnerabilities*** and ***impacts***.

Figure 2 : Risk Analysis and Risk Management



Measures of risk are expressed under the headings to which they relate; for example, quite separate assessments will apply to the risks of ***fire***, ***theft*** and ***program design error*** because each of these threats is different in nature. Some approaches to risk assessment express levels of risk simply as 'high", "medium" or 'low'; more sophisticated approaches use either wider scales of assessment or use a graphical approach to compare the results of the risk analysis review with the appropriate industry norm.

4.3 Cost-effective security

Security is not free. Indeed, it can be very expensive in terms of its procurement costs, and the costs associated with installation, testing, training, operation and maintenance. Because security measures do not show a return on investment in terms of gains in operational efficiency - indeed, the need to perform security checks may reduce throughput - management tend to look very critically at their provision. The IT security practitioner must therefore be able to demonstrate that the costs involved in implementing countermeasures are fully justified in terms of the values of the IT assets that are at risk, the scale of the risks that they face, and the consequences to the business should they be compromised, disrupted or damaged in any way.

The countermeasures that are selected must also be appropriate to the type of risk in question - this is covered in "risk management" - and the level of protection that is required. For example, appropriate fire extinguishers are applicable to the risk of fire, but in an environment where there is a high risk of fire and/or a valuable IT asset is at risk, they may not on their own provide adequate fire protection. A sufficiently high measure of risk (derived from a risk analysis review) would indicate that expenditure

on more comprehensive - and expensive - countermeasures was justified; for example, on automatic fire detection, alarm and suppression systems.

Conversely, risk analysis might also identify IT assets that are over-protected. This could result from a historical error or an incorrect assumption, but is more likely to result from change. For example, if a business outsources certain of its key business processes to a third party supplier, it may no longer be necessary to commit the same level of expenditure to protecting the computer centre if it no longer supports these systems. Thus risk analysis might result in some countermeasures being scaled down or discarded altogether, and economies being made.

Risk analysis therefore identifies the types of IT risks that need to be managed together with the reasons why; and indicates the level of investment that is justified in providing an adequate level of protection by the implementation of appropriate countermeasures. Properly conducted IT risk analysis and risk management (during which appropriate countermeasures are selected) are the basis of cost-effective IT security.

4.4 The risk analysis cycle

It is important to appreciate that a risk analysis is only a snapshot in time. IT risks must be re-assessed periodically because their nature and potential severity will change with the introduction of new types of technology, changes to existing systems (e.g. the introduction of electronic trading) and working practices, and changes to the threat environment (e.g. connection to the Internet).

Change might also result from external factors that are beyond an organisation's control. For example, recent terrorist attacks have caused significant damage to computer centres located in the US and England. The risk environment has therefore changed for many businesses and other institutions located in these countries, particularly in relation to disaster recovery and the protection of their staff and equipment from exposure to explosions. Connection to the Internet - and indeed wider use of data communications systems in general - are other factors which have changed the IT risk environment in recent years.

4.5 End user involvement

A major problem for any security manager is to ensure that all staff are fully aware of the need for, and the importance of maintaining, effective IT security within the business. If there is not a good *security culture* within the workplace, the effectiveness of much of the organisation's investment in systematic countermeasures will be diminished.

End users' awareness of security problems can be heightened through their participation in the security review. Furthermore, the review team must work with the user community to identify the need for cost-effective countermeasures because:

- they know best which countermeasures are acceptable in the working environment;
- they are more likely to support the selected countermeasures if they helped to choose them;
- the most effective scheme for making sure that only cost-justified countermeasures are in place is to require user management to pay for the security they need. Users are more likely to resist paying for countermeasures if they have taken no part in their selection.

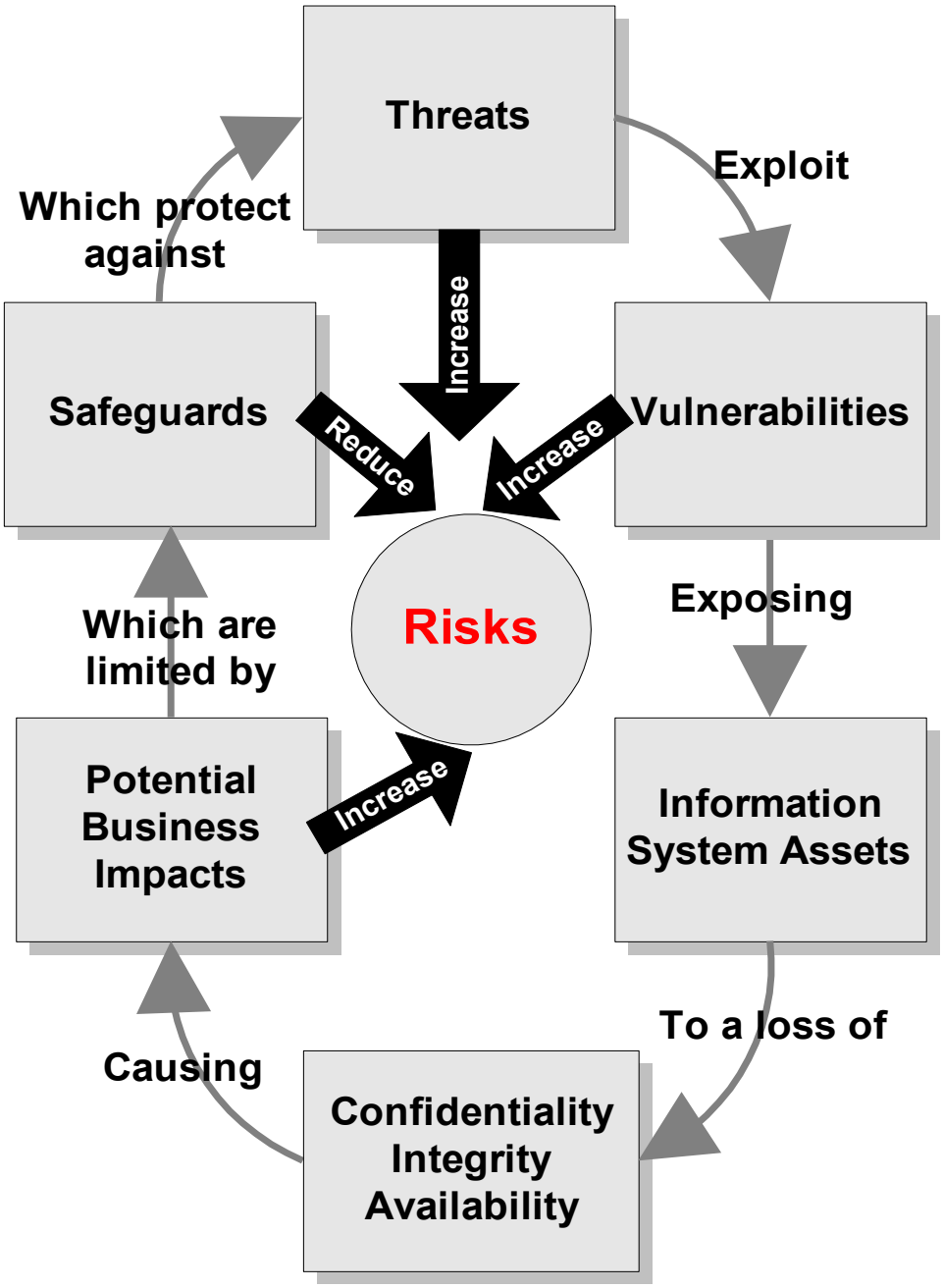
4.6 Risk analysis principles

Risk analysis involves:

- **business modelling** to determine which information systems support which business functions;
- **impact analysis** to determine the sensitivity of key business functions to a breach of confidentiality, integrity or availability;
- **dependency analysis** to determine points of access to information systems and assets that must be in place to deliver a service to a business function; and
- **threat and vulnerability analysis** to determine points of weakness in the system configuration and the likelihood of events that would exploit the weaknesses identified to cause impacts in terms of a breach of confidentiality, integrity or availability.

The following diagram illustrates the relationship between the various aspects of security that need to be considered in order to reduce the risk to an acceptable level.

Figure 3 : The Components of IT Risk



4.7 Business modelling

The first stage in managing risks to an organisation's information system is to build a business model that identifies which business processes rely upon which information

systems. The auditor would not normally expect to have to build the business model - this is a management function. The outline below is intended to provide basic information for the auditor to advise clients on building a business model and to assess the completeness of business models that clients have developed.

The purpose of the business model is to show clearly what the organisation is trying to achieve and to map information systems onto this framework.

4.7.1 Objectives

Organisations are driven by objectives - what they are trying to achieve. The top-level objectives may be defined externally by, for example, legislation or by the head of the senior management of the organisation. Objectives usually form a hierarchy with a single main aim or "mission". A mission statement for a railway company might be to:

> "maintain, develop and use railway assets to transport customers and goods with a minimum of inconvenience commensurate with the need for economy and efficiency."

Once the mission of the organisation has been established, it should be broken down into high-level objectives that contribute to the mission. These may, in turn, be broken down to lower level objectives until operational aims and objectives are clear enough for managers to act upon them. There is no absolute rule as to the number of objectives that should be stated at each level of the hierarchy or the number of levels that are required but it is generally reckoned to be poor practice to break a single objective down into more than eight objectives at the next level down in the hierarchy. The desirable size and detail of the hierarchy of objectives is a matter of judgement in the light of the complexity of the client's business.

For the purposes of business modelling it is usually sufficient to examine the top two levels of the hierarchy of objectives. The resulting analysis will take a form like the following:

1. Mission
1.1 top-level objective contributing to mission
1.1.1 second-level objective contributing to 1.1
1.1.2 second-level objective contributing to 1.1
1.2 top-level objective contributing to mission
1.2.1 second-level objective contributing to 1.2
and so on.

Each objective should have an "owner". The owner will be someone who is responsible for monitoring performance against a particular objective, defining lower level objectives and reporting on progress. The owner of the mission should be the head of the organisation.

4.7.2 Prioritisation

Objectives do not all have the same importance. The client may have already attached a weighting to each objective to express its importance. If no weightings have been applied, then the auditor will find it useful to establish the importance of each of the objectives identified. One method for analysing the importance of objectives is to assign 100 points to the mission statement of the organisation and then ask the head of the organisation to assign the 100 points to the top-level objectives. The owners of the top level objectives can then be asked to assign the points that they were awarded to the objectives at the next level down the hierarchy. If this is repeated for all of the objectives in the hierarchy then a picture will be built up of the importance of each objective.

The result might look like this:

1.	100
1.1	40
1.1.1	30
1.1.2	10
1.2	60
1.2.1	15
1.2.2	45

This table provides some useful information. The bottom level objective 1.2.2 turns out to be more important than the higher level objective 1.1. This may have been overlooked if points had not been allocated to objectives.

4.7.3 Organisation

Analysis of objectives clarifies **what** an organisation is aiming to do. Analysis of the organisation and management of an organisation reveals **how** it proposes to meet its objectives. The auditor should undertake a high level review of policies, standards and controls to determine whether they are appropriate and adequate. Any weaknesses should be noted as potential risks to security.

Organisational **culture** is a subjective area but questions of organisational culture are worth exploring, particularly the attitudes of top management; their stance on whether the organisation should be entrepreneurial or bureaucratic; centralised or devolved; customer or product based can all potentially impact upon security.

The auditor should also consider the financial control environment. What are senior management attitudes to regularity, probity and governance? Senior management attitudes are likely to influence those of the whole organisation and may give rise to security concerns.

The structure of an organisation can be modelled with an organisation chart. The business model should identify the staff involved in particular **activities** such as policy, finance, service delivery, and sales. A hierarchy should be built up which can be mapped onto the hierarchy of objectives. Try to cross reference activities to objectives. If there are activities that seem to serve no objective then this suggests either that the objectives are wrong or that the activity should cease.

Activities inherit their importance from the objectives that they contribute to. Using the example method above, owners of objectives could be asked to allocate their objective points to activities that support their objectives. The sum of the allocated points provides a measure of the importance of the activity.

For each main activity the auditor should consider the competence of the staff, whether they are complying with organisational standards and policies and whether they have a clear view of the objectives that they are trying to achieve.

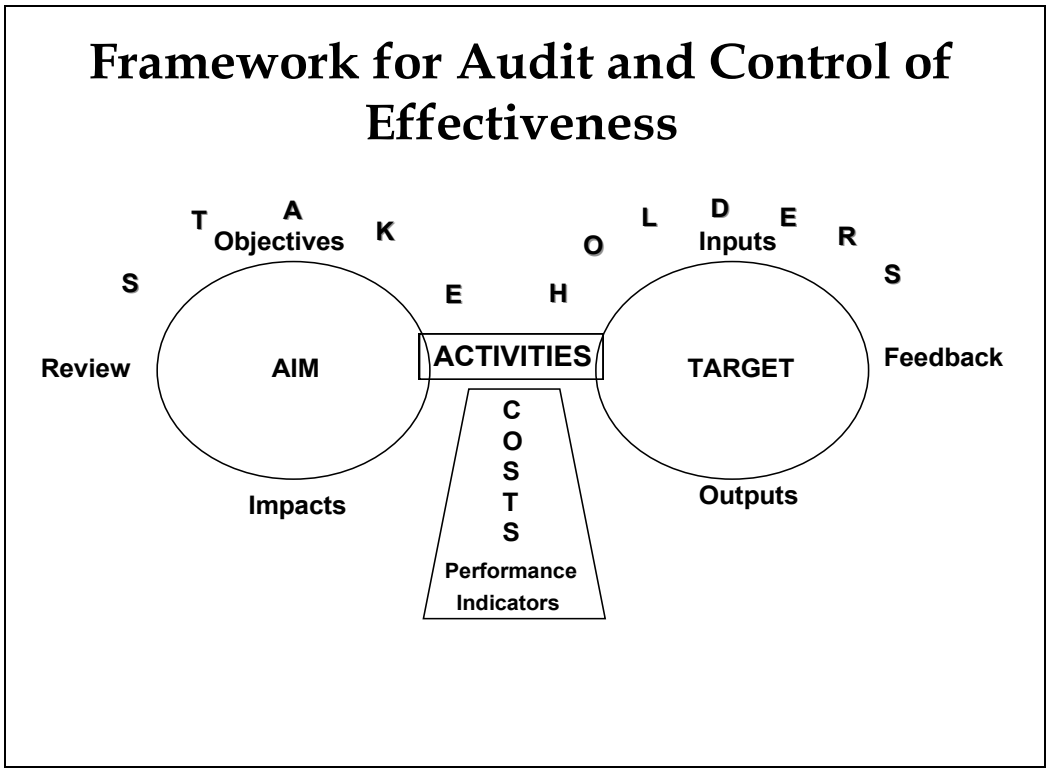
The sections above provide a framework for the collection of a vast array of information about the client objectives, activities, performance and stakeholders. This information can be considered in a number of different ways to highlight areas of the business that have failed or are failing.

The auditor may focus on:

- does the client know what they are trying to do?
- does the client know how they achieve their objectives/key activities?
- can the client identify key information systems?

The following diagram shows the relationship between the business model components. The stakeholders should have oversight of the entire business process. The business itself should be driven by its aim or mission which should be reflected in the process of refinement of objectives represented by the left hand cycle. The right hand cycle represents operational activities which should be tied to, and driven by, objectives. Activities connect the two cycles in that they are the result of objectives and the purpose of operations; they are also the focus for determining security requirements.

Figure 4



Information systems serve two main purposes:

- they provide information on plans, resource allocation, resource usage and performance; and
- they support activities.

The importance of information systems is derived from the importance of the business activities that they support.

4.8 Impact analysis

The security requirement for a given system will depend on the value of the information handled by the system and the activities that depend upon the system. For security purposes, the value of a system is expressed in terms of the consequences to the organisation of a service offered by the system being unavailable or the data handled by the system being disclosed or modified in an unauthorised fashion. There are a wide range of impacts that might be caused by the breach of the security of an information system; these include:

- embarrassment to the organisation;
- loss of credibility;
- compromise of confidential information;

- compromise of personal information;
- financial loss;
- personal safety (such as hospital patient care systems);
- disruption to the business; and
- legal liability.

It is possible to quantify impacts by expressing them in financial terms. Where there is no direct financial impact a figure is derived from a management consideration of how much it is worth to avoid the impact identified.

The business modelling process outlined above is a good starting point for identifying systems where the impact of unavailability or loss of integrity would have serious business consequences. Impact analysis goes beyond this in considering a wider range of impact than just business disruption and also considering the impact of a breach of confidentiality.

An alternative to expressing impacts in financial terms is to agree descriptions of high, medium and low impact scenarios with senior management and use these descriptions to assign a high, medium or low score to the impact of a breach of confidentiality, integrity or availability.

Whichever method is used, the auditor should ensure that senior management has agreed to the basis of impact analysis as this is fundamental to the determination of the security requirement and subsequently to the consideration of the level of protection that is appropriate for a given system.

The results of impact analysis will be a ranked list of systems which will reveal those most sensitive to a loss of availability, integrity or confidentiality. It is important to consider the three security objectives separately as the measures required to address each objective are different and may conflict. Encryption and strong access controls may reduce vulnerability to unauthorised disclosure but increase vulnerability to unavailability of information.

This analysis will highlight those systems where exceptional protection may be justified and help to identify systems where a full risk analysis is required.

4.9 Dependency analysis

Business modelling and impact analysis identifies key information systems by reference to the importance of the business functions that they support and the consequences of a breach of system security. The next stage in risk analysis is to map out the information system assets that must be in place for the information system to continue to provide a reliable and accurate service to the business functions; this will identify key assets from the point of view of integrity and availability. From the confidentiality point of view the concern is rather to identify all possible routes to the information that needs to be protected. The difference is illustrated by considering a

system with no backup, a single storage device and only one terminal. From the point of view of availability this system is very poor as it has many single points of failure that would deny service to the user but from the confidentiality point of view this system looks good since there are few points of access so it is easier to protect.

Infrastructure such as network cabling and devices, mainframe computers and office accommodation will be shared by many applications. Two implications follow from this:

- the security requirement of shared infrastructure may exceed that of any one information system that depends on it; and
- the security requirement of shared infrastructure will be at least as great as the most sensitive application that uses it.

The auditor should ensure that clients have considered and documented their system configurations, identified the dependency of key information systems on system components and considered points where information may be disclosed in an unauthorised fashion.

4.10 Threats and vulnerabilities

Dependency analysis and impact analysis identifies key system components. Threat and vulnerability analysis involves considering adverse events which could exploit security weaknesses to bring about adverse consequences. There are two main types of threat:

- **accidental** such as natural disasters, programming errors, user errors and equipment failure; and
- **deliberate** such as sabotage, espionage, fraud, hacking and theft.

The process of establishing key weaknesses involves examining each key information system component from the point of view of a malevolent deity who wants to breach system security and can control both accidents and people. A security officer has to follow through the configuration of key systems and think about what could go wrong; how could a malevolent deity bring about a breach of confidentiality, integrity or availability?

Threats exploit system **vulnerabilities** to cause **impacts**. The combination of these three components provides a measure of risk. The impact analysis and dependency modelling identifies system components where the impact of a breach of security is high. Threat and vulnerability analysis tries to establish the likelihood of such a breach; this is related to:

- the probability of the threat (adverse event) occurring; and
- the likelihood of a breach of security given that the threat does occur.

It is very difficult to assess precisely the probability of a threat occurring or of it succeeding in bringing about adverse consequences. It is sufficient for the security officer to use agreed criteria to assign a value of high, medium or low to both the threats and the vulnerabilities. The agreed criteria need to be embodied in threat and vulnerability questionnaires that ask questions appropriate to the type of asset and the types of threat that it could face. The results of threat and vulnerability analysis, together with the results of impact analysis, will be used to justify recommendations on protective measures that should be put in place; senior management will not accept the recommendations unless they have signed up to the method used for threat and vulnerability analysis.

The magnitude of a deliberate threat will be related to motivation, opportunity and the likelihood of detection and punishment. The magnitude of an accidental threat can only be assessed on the basis of past experience.

Components cannot be considered in isolation; a weakness in one component may be addressed by a strength in another component. It may, for example, be quite acceptable to have a terminal in a public place if it can only be used by people who have an access control card and also know a personal identification number. It might be equally acceptable for the same system to be accessible from a terminal that requires no card or personal identification number but is situated in a locked booth that can only be accessed by cardholders.

The easiest way to approach the analysis is to agree a list of threats and then to consider each sensitive system with a view to finding opportunities for the threat to cause a business impact. A typical list of threats might be:

Threat	Asset types	Disclosure / Confidentiality	Modification / Integrity	Destruction / Availability
Fire, flood, hurricane, earthquake	Buildings, communication towers	Physical access controls may be abandoned during disaster recovery and discarded assets may hold confidential information		All services may be disrupted and data may be lost
Environmental failure including power loss	Hardware			Services will be lost and hardware may be damaged.
Theft	Valuable, portable assets	Stolen assets may hold confidential information		Services may be disrupted and data may be lost
Viruses	Software and Information		Data may be corrupted by viruses	Computers infected with viruses might crash or delete vital data.
Hacking	All networked systems	Surveys suggest that most attempts at unauthorised access are initiated by staff rather than outsiders but the trend towards connection to public information systems may alter this balance. The most common motivation for hacking is unauthorised disclosure of information but the hacker may decide to modify data or destroy it.		
Hidden code	All software and information	Unauthorised code may reveal sensitive information such as passwords	Hidden program functions may manipulate data.	Programs may be designed to destroy data or deny authorised access to services
Hardware failure	All hardware	Failed hardware may be discarded	Data may be corrupted when	Denial of service

		or sent for maintenance without purging sensitive information	hardware fails	
Software failure	Software and information		Data may be corrupted	Services will be unavailable
Personnel error	All systems	Staff may inadvertently disclose sensitive information by, for example, printing to the wrong printer	Staff may enter data incorrectly	Staff may destroy information accidentally, crash systems through configuration errors or damage hardware.

The table above identifies some common threats. The auditor should seek evidence that the client has considered the range of threats to their key systems and identified the parts of their systems that are at greatest risk by considering the level of threat, system vulnerabilities and the impact that would be caused by a breach of confidentiality, integrity or availability.

4.11 Reviewing IT risks

In general, IT risk analysis involves identifying IT assets that are at risk, and then asking the following questions:

- what type of threats do they face?
- what are their likely causes and their probable impact(s)?
- what is the likelihood of the threat succeeding?
- how would we know if the threat did succeed?
- what can we do to prevent the impact?
- what can we do to recover if the threat does succeed?
- will alternative courses of action produce other risks? If so, are these more or less severe?

A number of steps are necessary to provide the answers to these questions, and the overall process is rarely straightforward. Much information needs to be collected and assimilated, and estimates, judgements and compromises will need to be made.

The initial risk analysis process can be very expensive and time-consuming to carry out but, providing that good quality records are kept, future reviews carried out to

assess the impact of system changes will be able to build on earlier results, and should therefore be much quicker and cheaper to conduct.

4.11.1 Establishing the review boundary

It is essential that the boundary of an IT risk analysis review be agreed with management at the start. This will involve clearly and unambiguously defining the overall objective of the review, and agreeing which IT assets are to be covered and which are not. The aim is to:

- understand clearly what the review is intended to achieve;
- provide a framework for project planning and conducting the analysis;
- avoid delivering a false sense of security by over-looking IT assets that are essential to the successful functioning of the system.

In some systems, particularly small dedicated systems, a logical boundary to the review may be obvious. But large, inter-connected systems can pose much more difficult problems, particularly if resource and time constraints are tight. In this situation, it may be necessary to review representative parts of the system and gather sufficient information to create a range of models on which to base risk management.

Inaccessible areas within the review boundary are another complicating factor that might need to be taken into account. The most common example is where data communication links enter the domain of the telecommunications authority. It will probably be impossible for the reviewers to judge whether the authority maintain an adequate level of security within their domain. Other examples are the systems operated by value added network suppliers (e.g. the Internet, electronic data interchange), utility supply companies (maintaining the power and water supplies), and organisations involved with mail collection/delivery, refuse collection, meter reading, etc.

A good standard of system documentation will also be necessary for establishing the review boundary. This will need to include:

- information on the system's function(s), components, and owners;
- lists of the physical assets that make up the system, together with their replacement costs;
- lists of all data and software assets;
- organisation structure, and the identities of personnel who can talk with authority on both the business and technical aspects of the system(s) to be reviewed;
- details of existing countermeasures.

4.11.2 CVE Vulnerability Naming Scheme

The Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme is an emerging industry standard, representing a dictionary of common names for publicly known IT system vulnerabilities and security exposures. While CVE is a dictionary, and not a database, it still provides a comprehensive list of publicly known exposures and an analysis of the authenticity of newly published vulnerabilities. Further, CVE attempts to make it easier to share data across different security tools and vulnerability databases, through the use of a common name.

4.11.3 Risk analysis methodologies

Gaining an estimate of probability of a security incident affecting an organisation is even more problematic that that of valuing IT assets. Such estimates require considerable expertise and experience of risk assessment. Methodologies provide some help in getting around these problems, but regardless of what the writers of the methodologies claim, they still require considerable expertise, together with an aptitude for the task, if they are to be used effectively.

There are a number of risk analysis methodologies on the market, some of which have been implemented in PC software. They fall into two broad categories, quantitative and qualitative.

Quantitative methods aim to balance the costs of implementing security against the possible cost of failing to implement it, as expressed by an Annual Loss Expectancy (**ALE**).

ALE is based upon the concept that in any rolling twelve month period ‘n’ incidents will occur for any particular type of threat (‘n’ might be fractional for incidents that have arisen less frequently). If each incident results in an average loss ‘i’, then ALE will be the product of the two, ‘ni’. Investment in countermeasures with an annualised cost ‘$’ will therefore be justified if this is expected to result in a reduction of the ALE that is greater than ‘$’.

A problem with the ALE approach is that, to be effective, a comprehensive history of security incidents and their related impacts is required. If this does not exist, the ALE calculations have to be based on the experience of comparable organisations if this is available which may not be representative. The approach also requires impacts to be measured in monetary terms, which is not always realistic.

Qualitative methods are based on scoring questionnaires that have been designed to assess the likely levels of a range of threats and their associated vulnerabilities.

In common with any questionnaire-driven approach, the relevance of some of the questions will vary according to circumstances, while the questionnaire itself may not be sufficiently comprehensive or relevant in unusual situations. This means that the

reviewer may need to adjust the questionnaire's standards markings, and this could introduce a risk of distortion in the method.

Risk analysis involves a major data collection, collation, computation and reporting task. A number of commercially available methodologies (e.g. CRAMM, MARION, RISKCALC) are supported by PC software packages which greatly reduces the manual effort and the paperwork. Automated tools also build databases of information that greatly reduce the cost of future work, and are indispensable for a detailed risk analysis review. However, they do require complex navigation through a number of layers of menus and formal training in their use will be necessary.

Paper-based approaches to risk analysis offer some advantages for initial, high-level risk studies that are designed to act as a pilot for more in-depth reviews. They require less initial training and are generally more flexible to use. However, such methods produce large volumes of paper as the degree of detail in the review increases, and they become slow and cumbersome as a result.

4.11.4 Summary

Risk analysis is an assessment of each type of "threat" that might attack "IT assets" within a defined boundary; the likelihood of an attack being successful ("vulnerability"); the business consequences that could result ("impact"). The "quantitative" approach to risk analysis multiplies the probability of an incident occurring (based on experience) with its estimated financial impact to compute an expected annual value of loss for each type of threat. The "qualitative" approach to risk analysis relates assessed levels of threat, vulnerability and impact empirically to produce an overall level of risk, or "security requirement".

It must be stated that there is a divergence of view on which approach should be taken, or methodology followed, for risk analysis; but regardless of approach, a risk analysis ought to be led by a person who has:

- a sound appreciation of the role and importance of IT within the organisation;
- an information technology background;
- good experience of the principles and practice of IT security management and methods;
- experience of the risk analysis methodology to be employed, together with a knowledge of its limitations.

Risk analysis methodologies have an important part to play. Software assisted methodologies are essential for supporting anything more than a high level risk analysis because of the large volume of data to be collected, stored, collated, processed and reported on. However, methodologies are not a substitute for experienced staff, and do not therefore provide business solutions in themselves. They only provide a framework in which to work.

5 Risk management

5.1 Overview

The preceding section dealt with the identification of threats, vulnerabilities and impacts. The combination of threat, vulnerability and impact analysis provides an indication of the level of risk to which an organisation's information systems are exposed.

Risk management follows risk analysis; it involves the identification, selection and implementation of countermeasures that are designed to reduce the identified levels of risk to acceptable levels. It is impossible to reduce all risks to zero; and even if it were possible, the cost would be astronomic and the resulting system quite unworkable. Risk management is therefore very much a matter of compromise between what is desirable, what is workable and what is affordable. It involves both technical skill, a good knowledge of the business and its workforce, and good judgement.

5.2 Countermeasures

5.2.1 Overview

A countermeasure is a check or restraint on a system that is designed to enhance its security.

Countermeasures fall into a number of different types and act in different ways. A good security environment will have a mixture of countermeasures that overlap to provide "security in depth". Thus, if one countermeasure fails there is a good chance that another will compensate. For example, if a hacker succeeds in gaining access to a system, individual security profiles, data encryption and logging (together with log review!) will continue to provide a good measure of protection and should, if properly implemented, alert management to the failure in controls.

Computer security countermeasures fall into the following broad categories:

- **physical:** (sometimes referred to as environmental countermeasures) designed to protect a system against physical threats. These include damage from fire, water, lightening strikes; from failure to maintain an adequate operating environment in terms of its temperature, humidity, cleanliness, quality of the power supply; and from incidents that stem from physical access, such as theft and malicious damage to equipment;
- **technical (or logical)**: are those implemented by computer software. Technical countermeasures are used to restrict access to, and the use of, the computer's operating system, networks, utility programs (such as editors and compilers) and applications programs;

- **procedural** countermeasures are those that are carried out manually. For example, there may be a need to verify that all people who wish to enter the computer room are authorised to do so. This requirement could be implemented as a procedural countermeasure by placing a guard on the door whose job is to carry out the necessary checks, and to record the names, times, dates, etc of all those who are admitted. A line manager might be required to check the validity of all computer input - after it has been entered into the system, but before it is processed - in order to confirm that it is complete and does not contain any unauthorised or invalid items.

Where one or more of these categories of countermeasures are absent, an unmanaged risk will exist. It is of course for management to decide whether this situation is acceptable; but a system should have some value to the organisation (otherwise why have it?), and as a result there should be some justification for protecting it by at the least the basic countermeasures that are accepted good practice.

Within each of the broad categories described above, different types of countermeasures will act in different ways. Although in-depth security requires a mix of countermeasure types, some types will provide more effective protection than others. The following list shows countermeasure types in their descending order of effectiveness. These countermeasures act to:

- **reduce the threat** that an incident will occur. For example, effective password control coupled with individual security profiles (if properly managed) will reduce the threat of unauthorised access to a system;
- **reduce the vulnerability** of the system to a particular threat. Countermeasures in this category aim to reduce the likelihood that a threat, if it occurs, will succeed in damaging the system. For example a building constructed of materials that have good fire retarding properties should be less vulnerable to the threat of fire than say a wooden building;
- **reduce the impact** should a threat succeed in attacking the system. For example, distributing sensitive data across a number of separate databases, each with its own access controls, would mean that any one security failure would result in a limited amount of information being disclosed. Another approach to reducing impact would be to remove the most sensitive information from the computer system altogether;
- **detect an incident** should it occur. Countermeasures in this category are designed to detect either attempted or actual security breaches. Computer logs can be used to record how a computer system is being used, and software can be designed to raise an alarm automatically if any one of a specified range of events occurs (e.g. repeated unsuccessful

attempts to log on). Other countermeasures of this type include those designed to detect fire, water leakage and intruders;

- **recover from the impact.** Countermeasures in this category are the last line of defence. They are designed to restore normal service after all preceding controls have failed and an incident has succeeded in damaging the system. Procedures for backing up the system, system recovery, disaster planning and change controls come within this category.

A final sub-division of countermeasure types that is worth referring to is that between procedural and systematic countermeasures.

Procedural countermeasures (described above) might be informal; however, they are more likely to be carried out correctly and consistently (and be auditable) if they are described in detailed instructions (sometimes referred to as *secure operating procedures*), which have been formally endorsed by senior management as a business requirement. And as it is not always apparent after the event whether a procedural control has been properly carried out, some form of record should be kept of who carried out the procedure, when, what resulted, and any action that was necessary.

Systematic (or **Technical**) countermeasures comprise some form of hardware (in its broadest sense) or software. A door lock and key is a simple example of a systematic access control countermeasure; other examples of systematic countermeasures are passwords, heat and moisture detectors, closed circuit television monitoring systems (CCTV), and software designed to generate and validate digital signatures. In general, systematic countermeasures are more expensive to implement than purely procedural countermeasures, but if properly managed they provide an advantage in their speed, span and consistency of operation.

Although procedural countermeasures can be freestanding, systematic countermeasures must have procedural countermeasures associated with them if they are to operate correctly. This requirement must be taken into account when systematic countermeasures are being considered not only because supporting procedures increase their cost of operation, but because inadequate supporting procedures might easily result in a systematic countermeasure becoming ineffective and providing a false sense of security.

An example of a common failing in supporting a systematic countermeasure is inadequate password management procedures. Password software can generally be relied upon to verify a password against its associated identifier, but for the check to be fully effective there must also be procedures to ensure that:

- users appreciate the importance of passwords and the need to keep them secret;
- passwords are difficult to guess - their format should therefore comply with a minimum standard (e.g. 6 digit alpha numeric);

- an enforced password change takes place periodically, or whenever security is breached, to reduce the risk of damage from passwords that have already been compromised;
- new users and those who forget their passwords are allocated passwords in a manner which prevents others from intercepting them and gaining unauthorised access to the system;
- a group of users that are re-issued passwords at the same time are not given similar temporary passwords that can easily be guessed by others;
- default passwords are changed immediately - when systems are changed or software is re-installed, default passwords that are commonly known may unwittingly be put back into effect;
- repeated failed login attempts are promptly detected and investigated in order to alert management to a possible attack on the system by *password guessing*;
- redundant passwords are promptly removed from the system to make it less vulnerable to unauthorised use.

Similarly, where individual security profiles are concerned, the software can generally be relied upon to enforce whatever security profile is created, but manual procedures are necessary to ensure that individuals' security profiles are set up correctly in the first place, are kept up-to-date, and are promptly removed when they are no longer required.

5.2.2 Countermeasure selection

Countermeasure selection requires a number of factors to be considered:

- what countermeasures are already in place?
- how effective are existing countermeasures?
- are any existing countermeasures unnecessary?
- what additional countermeasures are required?
- what is the most cost-effective solution to providing additional protection?
- which cost-effective solutions are likely to be acceptable to the work-force?

The software that drives automated methodologies, such as CRAMM and MARION (see Annex 2), establishes links between the types and levels of risks revealed during risk analysis. This information enables the software to select and prioritise appropriate countermeasures automatically using a database built into the package; that built into CRAMM contains well over 1,500 different countermeasures. Automatic countermeasure selection simplifies the risk management process considerably.

Although manual risk analysis methods are sometimes supplemented with checklists to assist with the countermeasure selection process, such methods rely much more heavily than automated methods on the knowledge and experience of the review team.

During the risk analysis the review team should record the countermeasures that they find in place and an assessment of whether they appear to be effective, or indeed necessary (organisational and system changes may have reduced risks in some areas leaving an expensive over-provision of security). During the risk management phase of the review, the team will need to refer back to their records of existing countermeasures when deciding whether any additional protection is required to reduce risks to acceptable levels.

In general the selection of countermeasures will be influenced by a number of factors:

- how effective a particular countermeasure is likely to be in any particular situation;
- its cost, in terms of procurement, installation, training and maintenance - and where software is involved, licensing fees may also increase cost;
- the number of IT assets that the countermeasure will protect against any particular threat;
- the level of risk which the countermeasure provides protection against;
- the number of impacts it covers;
- the type of countermeasure (i.e. reduce threat, reduce vulnerability, reduce impact, detect, recover).

Comprehensive protection requires security to be "built in depth". This means that physical, logical and procedural countermeasures must all be considered; and as no security system will ever be perfect there must be recognition that a security incident - either accidental, deliberate or naturally occurring - will impact on a system sooner or later. Countermeasures therefore need to be balanced between those that act to prevent threats occurring, those that detect threats that have succeeded, and those that enable recovery from the resulting impact(s). However, where a choice has to be made (generally because of budgetary restrictions), preventive countermeasures will provide more effective protection than those that are primarily detective or corrective in character.

Some countermeasures will reduce the exposure to more than one threat; the number of threats that a countermeasure if effective in controlling is referred to as its "span of control". Span of control is an important point to consider when selecting countermeasures that achieve the widest coverage at the lowest cost. For example, unauthorised access to data is often controlled by password systems. This threat could also be controlled (although less effectively) by holding system users accountable for their actions. Thus a system of unique personal identifiers (i.e. individual logon IDs) and automatic computer logs, coupled with periodic reviews of the logs produced by

the system, can on its own control limit misconduct if personnel are aware that anything they do can be traced back to them. In addition, computer logs can also be used to control other problems such as tracing the cause of hardware, software and data communications malfunctions, and analysing program performance. Thus, the sensible use of computer logs can have a wider span of control than passwords.

While technical controls should not be avoided if they appear to be necessary, they will generally be more expensive to buy and maintain than procedural controls. It is therefore important to balance their costs and span of control against levels of risks; and it is here that automated security methodologies can offer a distinct advantage in performing these calculations.

5.3 Information security starting point

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security.

Some basic aspects of such controls are:

- These controls apply to most organisations and in most environments.
- Although all these controls are important, the relevance of any control should be determined in the light of the specific risks an organisation is facing.
- Though these controls constitute a good starting point, it does not replace selection of controls based on a risk assessment.

5.3.1 IS starting point - legislative

The controls that are considered to be essential to an organisation from a legislative point of view are:

Data protection and privacy of personal information:

- A number of countries have introduced legislation placing controls on the processing and transmission of personal data.
- Compliance with legislation could be best achieved by the appointment of a data protection officer.

Safeguarding of organisational records:

- Some organisational records may need to be securely retained to meet statutory requirements.
- The time period and data content of such records may be defined by national law.
- A retention schedule should be drawn up identifying essential records and the period of time for which they should be retained.

Intellectual property rights:

- Ensure compliance with legal restrictions on use of material in respect of which there may be copyright, design rights, trade marks.
- Controls necessary to ensure that software copyrights associated with proprietary software are fulfilled.

5.3.2 IS Starting point – Best practices

Controls considered to be common best practice for information security include:

Information security policy document:

- Management should set a clear policy direction and demonstrate support for information security;
- IS policy document should be approved by management
- Policy should have a owner who should be responsible for its maintenance and review

Allocation of information security responsibilities:

- Responsibilities for protection of individual assets and for carrying out specific security process should be clearly defined.
- Information security manager could be appointed to take overall responsibility
- Owner for each information asset could be appointed who then becomes responsible for day to day security.

Information security education and training:

- All employees and where relevant third party users should receive appropriate training in information security before access to information or services is granted.
- Training should cover correct use of processing facilities e.g. log-on procedure, use of software packages

Reporting security incidents:

- Security incidents should be reported through appropriate management channels as quickly as possible.
- Formal reporting procedure is to be established together with an incident response procedure, setting out the action to be taken on receipt of an incident report.
- Suitable feedback process should be established to ensure that those reporting incidents are notified of results after the incident has been dealt with.

Business continuity management:

- Business continuity management process should be implemented to reduce the disruption caused by disasters and security failures.
- Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents and ensure the timely resumption of essential operations.

5.4 Risk Management process

A number of steps are involved in the risk management process. These are:

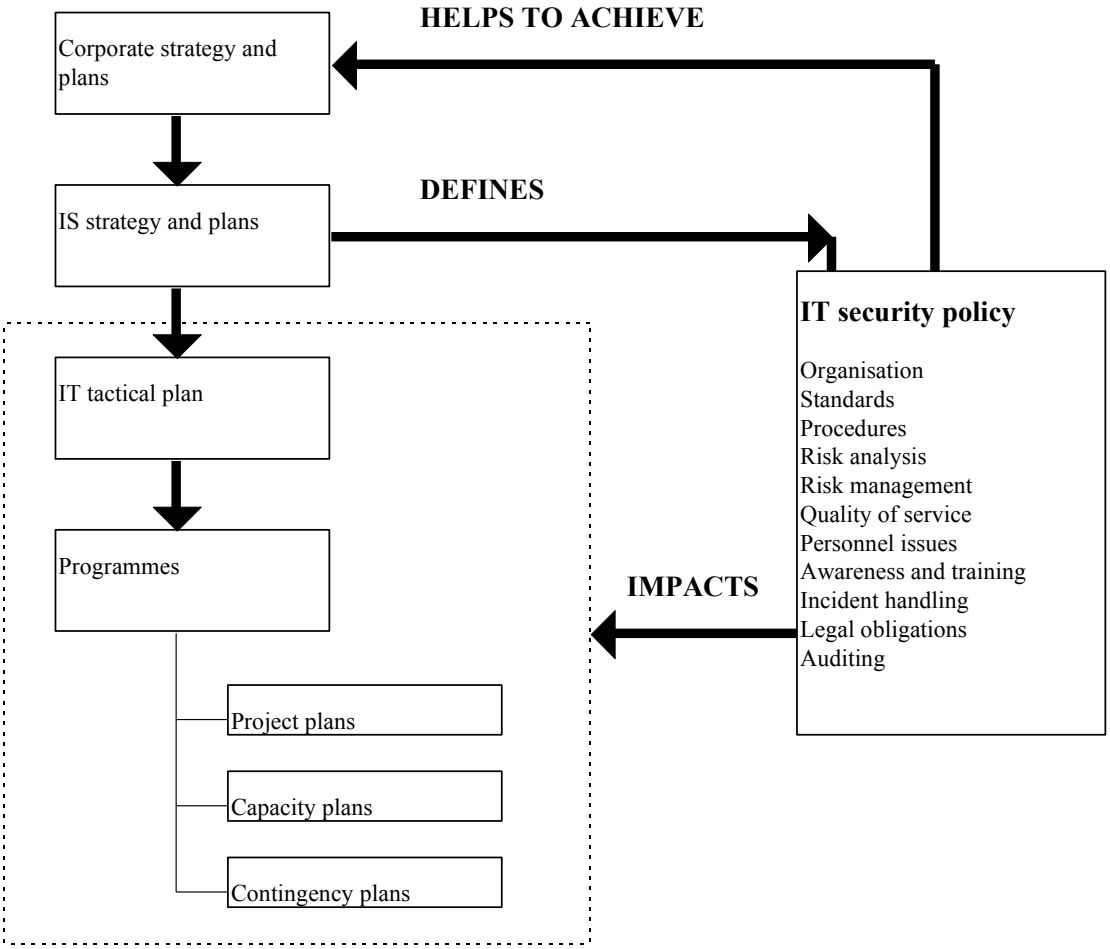
- Prioritize actions: Based on the risk levels presented in the risk assessment report, the implementation actions are prioritized.
- Evaluate recommended control actions: The technical feasibility and effectiveness of all identified controls should be evaluated so that the most appropriate control is chosen.
- Conduct cost-benefit analysis: To allocate resources and implement cost-effective solutions, organisations should conduct a cost-benefit analysis for each proposed control.
- Select control: On the basis of the results of the cost-benefit analysis, management selects the cost-effective controls for reducing risks.
- Assign responsibility: Responsibility should be assigned to in-house experts or an outside agency which have the appropriate skill set and expertise to implement the selected control.
- Develop safeguard implementation plan: The safeguard implementation plan prioritizes the implementation actions and projects the start dates and the target completion dates.
- Implement selected controls: The selected controls should be implemented so that the risks are brought down within the acceptable levels. Where an organisation has decided to accept risks that are higher than the acceptance level, sign-off from management should be obtained.

6 Security policy

The commitment to protect information systems must come from the highest level of an organisation; it will be driven by a recognition that serious problems could result from the disclosure, modification or unavailability of information or from possible repudiation of origin (submission, delivery, or receipt). This commitment should be expressed in a formal IT security policy that should be set in the context of the objectives and business functions of the organisation.

Although there are concerns which are specific to IT systems, the IT security policy must recognise, and be integrated with, the organisation's wider business and security policies; many of the risks to IT security arise from threats such as fire and unauthorised access, which apply equally to sensitive paper based systems. The following diagram shows the relationship between IT security and other components of corporate policy and planning:

Figure 1 : IT Security Policy



The top level IT security policy should be endorsed by senior management. Although it should be comprehensive it should concentrate on matters of principle rather than of detail. The result should be a clear, concise and stable statement of corporate security objectives - two pages is a good target.

The IT security policy should set out the principles governing the manner in which the organisation aims to distribute, protect, manage and monitor its information system assets. There should be an introductory statement setting the policy in context, explaining the organisation's reliance on IT systems and the major perceived threats. The policy should set out responsibilities in terms of roles rather than individuals so that it is generally applicable and unaffected by changes in personnel.

Specific areas that should be covered in a corporate IT security policy include:

- who will be responsible and accountable for security at all levels in the organisation and what the reporting lines will be;

- a reference to agreed minimum standards to be applied to all corporate information systems and guidance on the use of risk analysis to identify those systems where the security requirement justifies the application of additional measures;
- recognition that effective IT security has to be designed into IT systems, rather than bolted on, and hence that IT security should be considered in business cases for new systems and will be a major concern throughout the system development life cycle;
- the principle that IT security should be built into operational procedures including access controls and that internal audit will review the adequacy of system controls;
- the approach to personnel issues such as background security checks and handling of security violations;
- the importance of good training programmes to raise awareness of IT security issues;
- a reference to procedures for controlling proprietary and copyright materials;
- a reference to procedures for registration and accreditation of systems and data and arrangements to ensure compliance with applicable legislation;
- policy on connection to external systems;
- policy on the reporting and investigation of security incidents; and
- business continuity planning requirements.

The IT Security Policy should not be static; in order to remain effective it needs to respond to changing threats and business needs. A strong life-cycle is important for ensuring that the policy remains up to date. The auditor should look for a formal process of:

- security requirement analysis;
- policy formulation;
- policy promulgation;
- implementation;
- monitoring incidents and changes in threats; and
- policy review and update at appropriate frequencies.

An example of an IT security policy document is at Annex 3.

7 Organisation of Information Security

Organisational security refers to the security of information processing facilities and information assets. It deals with security of assets within the organisation, when accessed by third parties and when processing of information is outsourced to another organisation The three components of organisational security are:

- Information security structure: The objective is to deal with management of information security within the organisation. A management framework should be established to initiate and control the implementation of information security within the organisation;
- Security of third party access: the objective is to maintain security of organisational information processing facilities accessed by third parties. Access to organisation's information processing facilities by third parties should be controlled
- Outsourcing: The Objective is to maintain security of information when responsibility for processing is outsourced.

These three controls are being described exhaustively below:

7.1 Information security structure

The various common controls under information security structure are:

7.1.1 Management IS Forum

A management forum should be constituted to ensure that there is clear direction and visible management support for security initiatives. The forum may be part of an existing management body. One manager should be responsible for all security related activities. Such a forum undertakes the following:

- Reviewing and approving policy and overall responsibilities
- Monitoring significant changes in the exposure of information assets to major threats
- Reviewing and monitoring security incidents
- Approving major initiatives to enhance security

7.1.2 Information Security co-ordination

In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate the implementation of security controls. Typically such a forum:

- Agrees specific roles and responsibilities for information security across the organisation
- Agrees specific methodologies and processes for information security e.g. risk assessment, security classification system
- Agrees and supports security initiatives
- Ensures that security is a part of the information planning process
- Assesses the adequacy and co-ordinates implementation of specific controls
- Reviews security incidents
- Promotes visibility of business support for information system throughout the organization.

7.1.3 Allocation of responsibilities

Responsibilities for protection of individual assets and for carrying out specific security processes should be clearly defined. Information security policy should provide general guidance on the allocation of security roles and responsibilities in the organization. This should be supplemented with more detailed guidance for specific sites, systems or services. Owner may delegate security responsibilities to individual managers or service providers, but remains ultimately responsible for the security of the IT asset.

In many organizations an information security manager will be appointed to take overall responsibility for development and implementation of security. However, responsibility for resourcing and implementing the controls will rest with the individual managers. One common practice is to appoint an owner for each information asset who then becomes responsible for its day-to-day security.

It is essential that areas for which each manger is responsible are clearly stated, in particular the following should take place:

- Definition of assets and security processes associated with individual systems
- Manager responsible for each asset or security process should be agreed and details of this responsibility should be documented
- Authorization levels should be clearly defined and documented

7.1.4 Authorisation of processing

Management authorisation process for new processing facilities should be established. Following controls may be considered:

- New facilities should have appropriate user management approval, authorizing their purpose and use. Approval should also be obtained from the manager

responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met.

- Hardware and software to be checked to ensure compatibility with other system components.
- The use of personal processing facilities for business processing business information and any necessary controls should be authorized.
- The use of personal information processing facilities in the work place may cause new vulnerabilities and should therefore be assessed and authorized.

7.1.5 Specialist information security advice

Specialist security advice is required by many organizations. Ideally an experienced in-house security advice should provide the specialist advice. However, not all organizations may wish to employ a specialist adviser. When the organization does not have a specialist adviser, then a specific individual should be identified to co-ordinate in-house knowledge and experiences to ensure consistency and provide help in decision making.

There should be access to suitable external advisers to provide specialist advice. The quality of their assessment of security threats and advice on controls will determine the effectiveness of the organisation's information security. The information security adviser or equivalent point of contact should be consulted at the earliest possible stage following a suspected security incident or breach to provide a source of expert guidance or investigative resources.

7.1.6 Co-operation between organizations

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators should be maintained to ensure that appropriate action can be quickly taken, and advice obtained, in the event of a security incident. Similarly, membership of security groups and industry forums should be considered.

Exchanges of security information should be restricted to ensure that confidential information of the organization is not passed to unauthorized person.

7.1.7 Independent review of information security

The information security policy document sets out the policy and responsibility for information security. Its implementation should be reviewed independently to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.

Such a review may be carried out by the internal audit function, an independent manager or a third party organization specializing in such reviews.

7.2 Security of third party access

The objective of security of third party access is to maintain the security of organizational information processing facilities and information assets accessed by third parties. Access to information processing facilities by third parties should be controlled.

This involves the following two main activities:

7.2.1 Identification of risks from third part access

The risks associated with access to organizational information processing facilities by third parties should be assessed and appropriate security controls should be implemented. Identification of risks from third party access involves the following:

- Identification of types of access: The types of access given to a third party are of special importance. For example, the risks of access across a network connection are different from risks resulting from physical access. Types of access that should be considered are
  - Physical access, e.g. to offices, computer rooms, filing cabinets
  - Logical access, e.g. to an organisation's databases, information systems
- Identification of reasons for access: Third parties may be granted access for a number of reasons. For example, there are third parties that provide services to an organization and are not located on-site but may be given physical and logical access, such as
  - Hardware and software support staff, who need access to system level or low level application functionally;
  - Trading partners or joint ventures, who may exchange information, access information systems or share databases.

  Information might be put at risk by access from third parties with inadequate security management. Where there is a business need to connect to a third party location a risk assessment should be carried out to identify any requirements for specific controls. It should take into account the type of access required, the value of the information, the controls employed by the third party and implications of this access to the security of the organisation's information.
- Assessment of risks from On-site contractors: Third parties that are located on-site for a period of time as defined in their contract may also give rise to security weaknesses. Examples of on-site third party include:
  - Hardware and software maintenance and support staff;
  - Cleaning, catering, security guards and other outsourced support services;

- Student placement and other casual short term appointments
- consultants

It is essential to understand what controls are needed to administer third part access to information processing facilities. Access to information and information processing facilities by third parties should not be provided until the appropriate controls have been implemented and a contract has been signed defining the terms for the connection of access.

7.2.2 Security requirements in third party access

Arrangements involving third party access to organizational information processing facilities should be based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards. The contract should ensure that there is no misunderstanding between the organization and the third party. The following terms should be considered for inclusion in the contract:

- general policy on information security;
- asset protection, including:
  - Procedures to meet organizational assets, including information and software;
  - Procedures to determine whether any compromise of the assets, e.g. loss of modification of data, has occurred
  - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the contract;
  - Integrity and availability
  - Restrictions on copying and disclosing information
- Description of each service to be made available
- Target level of service and unacceptable levels of service
- Respective liabilities of the parties to the agreement
- Responsibilities with respect to legal matters, e.g. data protection legislation
- Intellectual property rights and copyright assignments
- Access control agreements, covering permitted access methods, an authorization process for user access and privileges
- Right to monitor and revoke user security
- Right to audit contractual responsibilities
- Establishment of an escalation process for problem resolution

- Responsibilities regarding hardware and software maintenance
- A clear reporting structure and agreed reporting formats
- Any required physical protection controls and mechanism to ensure that such controls are followed
- User and administrative training in methods, procedures and safety
- Arrangements for reporting, notification and investigation of security incidents and security breaches

7.3 Outsourcing

The objective of outsourcing control is to maintain the security of information when the responsibility for information processing has been outsourced to another organization. The important issues to be covered in outsourcing are:

- Maintaining security of information when responsibility for processing has been outsourced
- Outsourcing arrangements should be covered by a contract between the parties and address risks, security controls and procedures for information systems and networks.

Outsourcing controls is discussed in greater detail in the IT Controls module.

8 Asset classification and control

The objectives of asset classification and control are to maintain appropriate protection of organisational assets and to ensure that information assets receive an appropriate level of protection. This can be achieved by classification the information assets and by following proper procedures for labelling and handling of information. The two main controls that would be discussed in the session are accountability for assets and information classification. These are discussed below:

8.1 Accountability for assets

The objective of accountability of assets is to ensure that information assets receive an appropriate level of protection. This would involve the following:

- Prescribing classification guidelines taking into account business needs for sharing or restricting information and the business impacts associated with such needs
- Defining and following a set of procedures for information labelling and handling in accordance with classification scheme adopted by the organisation.

However, before discussing the controls, it is necessary to know the types of information assets.

8.1.1 Types of assets

The different types of assets associated with information systems are:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information
- Software assets: application software, system software, development tools and utilities
- Physical assets: computer equipment (processors, monitors, laptops, modems), communication equipment (routers, PABX, fax machines), magnetic media (tapes and disks), furniture
- Services: computing and communication services, general utilities, e.g. heating, lighting, power, air-conditioning

8.1.2 Inventory of assets

Inventories of assets help ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial reasons. The process of compiling an inventory of assets is an important aspect of risk management. The following points should be considered while maintaining inventory:

- The inventory should cover all important assets associated with each information system
- Each asset should be clearly identified and its ownership and security classification agreed and documented together with its current location
- The relative value and importance of the assets needs to be identified so that the organisation can provide levels of protection commensurate with the value and importance of the asset.

8.2 Information classification

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorised access or damage to the information. In general, the classification given ton information is a shorthand way of determining how this information is to be handed or protected. Some points to consider while classifying information are:

- Not all data is equally sensitive. Therefore, classification and protection of information should be according to their value and sensitivity
- Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account as over-classification can lead to unnecessary expense.
- Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic in use or prove impractical.
- Care should be taken in interpreting classification labels on documents from other organisations which may have different definitions for the same or similarly named labels.
- The responsibility for defining the classification of an item of information, e.g. for a document, data record, data file or diskette, and for periodically reviewing that classification should remain with the originator or nominated owner of the information.

8.2.1 Types of classification

The different types of commonly used classification of information are as follows:

- Unclassified: data that does not fall into any of the classification given below. This data may be made generally available without specific data custodian approval.
- Operational use only: data whose loss, corruption or unauthorised access may not cause any financial or legal loss but which is mad available to data custodian approved users only
- Private: data whose disclosure would not result in any financial or legal loss to the organisation but involves issues of personal credibility, loss of reputation or other issues of personal secrecy
- Restricted: data whose loss, corruption or unauthorised disclosure would tend to impair the functioning of the organisation or result in financial or legal loss.
- Confidential: data whose laws, corruption or unauthorised disclosure would be a violation of law.

Another accepted method of classification, referred to in the US Federal Information Processing Standard 199 (FIPS 199), categorises information on all three security objectives – confidentiality, integrity and availability – into low impact, moderate impact and high impact systems; this has been covered under the section on NIST Security frameworks.

8.2.2 Costs and benefits of classification

The advantages and disadvantages of classifying data compared with applying a uniform standard to the protection of all data are as follows:

Advantages:

- less spent in protecting low sensitivity data - resources focused on areas of most need;
- security less of an obstacle to operational efficiency (most data likely to be low sensitivity);
- segregating sensitive data in separate systems and networks reduces the numbers of potential users and the threat of unauthorised access.

Disadvantages:

- segregating sensitive data to separate systems can draw attention it;
- cost of maintaining classification scheme and vetting potential users;
- difficulty in maintaining appropriate security on equipment shared by other systems;
- may result in need to classify networks and devices (discs, printers, etc)

NIST's approach of having baselines for security controls based on their classification (into low impact, moderate and high impact systems), and then tailoring/ supplementing the baseline controls to suit organisation-specific requirements, is another approach managing to combine both classification and customisability.

8.2.3 Labelling and handling

It is important that an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by the organisation. These procedure need to cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover:

- copying,
- storing,
- transmission by post, fax and electronic mail
- transmission by spoken word, including mobile phone, answering machines
- destruction

Labelling should reflect the classification according to the rules established in the classification guidelines. Physical labels are generally the most appropriate form of

labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling should be used.

9 Personnel security

Care should be exercised while recruiting users of IT systems and adequate training should be imparted to the users in information security before they access the IT facilities. There should be well established procedures for reporting and following up of security incidents. The three important controls for personnel security are:

- Security in personnel policy, job definition and resourcing: The objective of this control is to reduce the risks of human error, theft, fraud or misuse of facilities.
- User awareness and training: The objective is to ensure that users are aware of information security threats and concerns, and are equipped to support organisational policy in the course of their normal work.
- Responding to security incidents and malfunctions: The objective of this control is to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

These controls are discussed in detailed in the ensuing paragraphs.

9.1 Security in personnel policy, job definition

The objective of this control is to reduce the risks of human error, fraud, theft or misuse of facilities. To achieve this, the following controls are necessary:

9.1.1 Personnel Security Policy

The organisation should have a documented personnel security policy, which addresses purpose, scope, roles, responsibilities, and compliance; this should be supported by documented procedures to ensure compliance. Such a policy should also cover the formal disciplinary process for personnel failing to comply with established security policies and procedures.

9.1.2 Including security in job definitions

Security roles and responsibilities as laid down in the organisation's security policy should be documented where appropriate. They should include any general responsibilities for implementing or maintaining security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

Further, the organisation should assign risk designations for all positions, and establish screening criteria for individuals filling those positions (especially for high risk positions).

9.1.3 Personnel screening

Verification checks on permanent staff should be carried out at the time of job applications. This should include the following controls:

- Availability of satisfactory character references, e.g. one business and one personnel
- A check (for completeness and accuracy) of the applicant's curriculum vitae
- Confirmation of claimed academic and professional qualifications
- Independent identity check

Where a job either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the organisation should carry out a credit check. For staff holding positions of considerable authority this check is to be repeated periodically.

A screening process should be carried out for contractors and temporary staff. Where these staff are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern.

Management should evaluate the supervision required for new and inexperienced staff with authorisation for access to sensitive systems. The work of all staff should be subject to periodic review and approval procedures by a more senior member of staff.

Managers should be aware that personal circumstances of their staff may affect their work. Personal or financial problems, changes in their behaviour or lifestyle, recurring absences and evidence of stress or depression might lead to fraud, theft or security implications. This information should be handled in accordance with any appropriate legislation existing in the relevant jurisdiction.

9.1.4 Confidentiality agreements

Confidentiality or non-disclosure agreements are used to give notice that information is confidential or secret. Employees should normally sign such an agreement as part of their initial terms and conditions of employment.

Casual staff and third party users:

- Casual staff and third party users not already covered by an existing contract(containing the confidentiality agreement) should be required to sign a confidentiality agreement prior to being given access to information processing facilities.

Review of confidentiality agreements:

- Confidentiality agreements should be reviewed when there are changes to terms of employment or contract, particularly when employees are due to leave the organisation or contracts are due to end.

9.1.5 Terms and conditions of employment

The terms and conditions of employment should state the employee's responsibility for information security. The important aspects to be covered in the terms and conditions are:

- The responsibilities should continue for a defined period of time after the end of employment.
- The action to be taken if the employee disregards security requirements should be specified.
- The employee's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation, should be clarified and included.
- Responsibility for classification and management of the employer's data should also be included.
- Wherever appropriate the terms should state that the responsibilities are extended outside the organisation's premises and outside normal working hours, e.g. in the case of home-working.

9.1.6 Personnel Transfer and Termination

The organisation should have adequate and effective procedures to ensure that upon termination/ transfer of personnel:

- Information system access is terminated or appropriately re-authorised.
- System related property e.g. keys, identification cards, building passes etc. are returned/ deactivated.
- Appropriate personnel have access to official records created by the terminated/ transferred employee that are stored on organizational information systems.

9.2 User awareness and training

The objective of user training is to ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work. The following aspects should be considered while imparting training to users:

- All employees of the organisation and where relevant, third party users, should be imparted appropriate training and regular updates in organisational policies and

procedures relating to IT security. The training should cover the correct use of information processing facilities e.g. log-on procedure, use of software packages, before access to information or services is granted.

- Personnel with significant IT security responsibilities should be provided security training, especially on initial appointment and after major system changes.

Further, the organisation should also consider maintaining contacts with special interest groups, professional associations and/or peer groups of security personnel, to stay upto date with the latest security-related information including threats, vulnerabilities and incidents.

9.3 Incident Response

9.3.1 Introduction

The organisation should have strong procedures to ensure that the preparation, detection and analysis, containment, eradication and recovery/ follow-up action of security incidents is appropriate and adequate. Ensuring adequate and effective security incident response capability would involve:

- Establishing incident response policies and procedures
- Structuring an incident response team
- Handling incidents from initial preparation through to follow-up and "lessons learned"
- Drawing up written guidelines for prioritizing incidents
- Handling specific types of incidents e.g.
  - Denial of Service (DOS)
  - Malicious code
  - Unauthorised access and hacking
  - Inappropriate usage

9.3.2 Reporting security incidents and weaknesses

Procedures should be built in to minimise the damages from security incidents and weaknesses by ensuring their timely reporting. This would require the following controls:

9.3.2.1 Reporting security incidents:

- Security incidents should be reported through appropriate management channels as quickly as possible.

- A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report.
- All employees and contractors should be aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible.
- Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed. These incidents can be used in user awareness training of what could happen and how to respond to such incidents.

9.3.2.2 Reporting security weaknesses:

- Users of information services should be required to note and report any observed or suspected security weaknesses in, or threats to systems or services.
- Users should be informed that they should not, in any circumstances attempt to prove a suspected weaknesses. This is for their own protection as testing weaknesses might be interpreted as misuse of the system.

9.3.3 Reporting software malfunctions

Procedures should be established for reporting software malfunctions. The following action should be considered:

- The symptoms of the problem and any message appearing on the screen should be noted.
- The computer in which the software malfunctioned should be isolated, if possible, and use of it should be stopped. The appropriate contact should be altered immediately. If equipment is to be examined, it should be immediately disconnected from the network. Diskettes used in that computer should not be transferred to other computers.
- The matter should be reported immediately to the information security manager.
- Users should be instructed not to remove the suspected software or to correct it. Only appropriately trained staff should carry out recovery.

9.3.4 Follow-up of incident

The follow-up action to an incident is as important as the reporting of an incident and its recovery. The two important controls relating to follow-up are:

9.3.4.1 Learning from the incident:

There should be mechanisms in place to enable the types, volumes and costs of incidents to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, and cost of occurrence.

9.3.4.2 Disciplinary process:

There should be a formal disciplinary process for employees who have violated organisational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. The process should ensure correct, fair treatment to employees who are suspected of committing errors or persistent breaches of security.

10 Systems development and maintenance

It is essential to ensure that security concerns are taken into account during system development and that the maintenance of systems reckons security issues. The following five controls would take care of security requirements in systems development and maintenance:

Security requirements of systems:

- Business requirements for new systems or enhancements to existing systems should specify the requirements for controls.

Security in application systems:

- The objective is to prevent loss, modification or misuse of user data in application systems.

Cryptographic controls:

- The objective is to protect the confidentiality, authenticity or integrity of information.

Security of system files:

- To ensure that It projects and support activities are conducted in a secure manner.

Security in development and support process:

- To maintain the security of application system software and information.

10.1 Security requirements of systems

When a new system is being planned and the user requirements specification is being considered, the users tend to focus on the appearance and ease of use of the new system. It is not uncommon for the less obvious requirements, such as access controls, data processing controls, back up and recovery, check-pointing, to be overlooked. When the new system becomes operational the absence of such facilities becomes apparent. At this stage it is very expensive to re-design the system to incorporate the deficiencies; and it may not be technically feasible. For example, if a new system does not provide an adequate audit trail, it may be impossible for the external auditor to provide an unqualified opinion on the organisation's accounts. This deficiency will probably be extremely expensive to remedy. The important aspects to be kept in mind are:

- IT security requirements must be considered as a design issue. Statements of requirements for new systems, or enhancements to existing systems should specify the requirements of controls.
- Such specifications should consider automated controls to be incorporated in the system, as well as the need for supporting manual controls.

10.2 Security in application systems

The objective of security in application systems is to prevent loss, modification or misuse of user data in application systems. This can be achieved through different types of application controls. The commonly used application controls are:

Input data validation:

- The objective is to ensure that data input to application systems are validated so that they are correct and appropriate

Control of internal processing:

- To ensure that validation checks are incorporated into systems to detect any corruption of the data processed.

Message authentication:

- To use message authentication for application where there is a security requirement to protect the integrity of the message content.

Output data validation:

- Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

These controls are discussed exhaustively in the IT Controls module.

10.3 Cryptographic controls

Cryptographic controls or those controls which transform data in such a way that information it contains is hidden and it reveals any attempts to change it. Such controls are used to protect the confidentiality, authenticity or integrity of information. The different cryptographic controls are:

Policy on the use of cryptographic controls:

- A policy on the use of cryptography for protection of information is to be developed in the organisation.

Encryption:

- Encryption shall be used to protect the confidentiality of sensitive or critical information.

Digital signature:

- Digital signatures shall be used to protect the authenticity and integrity of electronic information.

Non-repudiation services:

- Non-repudiation services shall be used to resolve disputes about the occurrence or non-occurrence of an event or action.

Key Management:

- A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.

These issues are explained later in this module.

10.4 Security of system files

The objective of this control is to ensure that IT projects and support services are conducted in a secure manner. This can be achieved with the help of following controls:

10.4.1 Control of operational software

The objective of this control is to ensure that procedures are in place to control the implementation of software on operation systems. To minimise the risk of corruption of operational systems, the following controls should be considered:

- Updating of program libraries should be done only by the nominated librarian upon appropriate management authorisation
- If possible, operating systems should only hold executable code

- Executable code should not be implemented on an operational system until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated
- An audit log should be maintained of all updates to operational program libraries
- Previous versions of software should be retained as a contingency measure
- Vendor supplied software used in operational systems should be maintained at a level supported by the supplier
- Physical or logical access to operational software should only be given to suppliers for support purposes when necessary and with management approval.

10.4.2 Protection of test data

Test data is to be protected and controlled. System and acceptance testing requires substantial volumes of test data that are as close as possible to operational data. The following controls should be applied to protect operational data when used for testing purposes:

- The access control procedures, which apply to operational application systems should also apply to test application systems
- There should be separate authorisation each time operational information is copied to a test application system
- The use of operational database containing personal information should be avoided. If such information is used, it should be depersonalised before use.
- Operational information should be deleted from a test application system immediately after the testing is complete.
- The copying and use of operational information should be logged to provide an audit trail.

10.4.3 Access control to program source library

The objective of this control is to reduce the potential for corruption of computer programs. This can be achieved by maintaining strict control over access to program source libraries as follows:

- Where possible program source libraries should not be held in operational systems
- A program librarian should be nominated for each application
- IT support staff should not have unrestricted access to program libraries.
- Programs under development or maintenance should not be held in operational program source libraries

- The updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorsiation from the IT support manager for the application
- Program listing should be held in a secure environment
- An audit log should be maintained of all accesses to program source libraries
- Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, data definitions and procedures.
- Maintenance and copying of program source libraries should be subject to strict change control procedures.

10.5 Security in development and support processes

The objective of this control is to maintain the security of application system software and information. This can be achieved through the following controls:

10.5.1 Change control procedures

Changes to operational programs are almost inevitable even if the programs are written very well. Such changes may be necessary due to changes in legislation, changes in working practices in the organisation etc. The objective of this control is to ensure implementation of changes by the use of a formal change control procedure. The change control procedure covers controls to ensure that all changes to systems configurations are

- Authorisedtested documentedcontrolled andthat there is an adequate audit trail of changes. **Technical review of operating system changes**

Periodically it may be necessary to change the operating system, e.g. to install a newly supplied software release or patches. When changes occur, the application system should be reviewed and tested to ensure that there is no adverse impact on operation of security. This process should cover:

- review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes
- ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes
- ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation
- ensuring that appropriate changes are made to the business continuity plans

10.5.3 Restrictions on changes to software packages

Modifications to software packages should be discouraged. As far as possible, vendor supplied software packages should be used without modification. Where it is deemed essential to modify a software package, the original software should be retained and the changes applied to a clearly identified copy. All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades. The following points should be considered before making changes to the software:

- the risks of built-in controls and integrity processes being compromised.
- Whether the consent of the vendor should be obtained.
- The possibility of obtaining the required changes from the vendor as standard program updates and
- The impact if the organisation becomes responsible for future maintenance of the software as a result of the changes.

10.5.4 Covert channels and Trojan code

A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter by both secure and insecure elements of a computing system, or by embedding information into a data stream. Trojan code is designed to affect a system in a way that is not authorised and not readily noticed and not required by the recipient or user of the program. Covert channels and Trojan code rarely occur by accident. The following controls may take care of the concerns of covert channels and Trojan horse:

- Buying programs only from a reputable source
- Buying programs in source code so the code may be verified
- Using evaluated products
- Inspecting all source codes before operational use
- Controlling access to and modifications of code, once installed
- Use staff of proven trust to work on key systems

10.5.5 Outsourced software development

Where software development is outsourced, the following controls should be considered:

- Licensing arrangements, code ownership and intellectual property rights
- Certification of the quality and accuracy of the work carried out

- Escrow arrangement in case of failure of third party
- rights of access for audit of the quality and accuracy of work done
- contractual requirements for quality of code
- testing before installation to detect Trojan code

11 Network and Communications Controls

11.1 Introduction

The vast majority of systems encountered in organisations (whether small, medium or large) use networks to connect users, with the following benefits:

- the ability to share data;
- to use and share other peripherals, e.g. printer sharing;
- to leave system administration to a central team;
- allow users to send almost instantaneous messages, e.g. e-mail; and
- allow users to access the systems from remote locations.

Opening up systems and connecting them to networks is not without its risks. The network should be controlled such that only authorised users can gain access.

This chapter covers the following:

- a brief summary of the jargon and technical names used;
- network risks, security issues and controls; and
- Internet security.

11.2 Network revision

Networks and communications can be a very technical subject with many abbreviations, technical terms and phrases. In the next part of this chapter we cover some of the more commonly encountered communications phrases and terms. It may be noted that this section is merely a revision, and not a primer on communications and networking.

11.2.1 Types of Networks

Computer Networks can span either a few meters (e.g. Bluetooth) or thousands of kilometres (e.g. the Internet). They could be of various types:

- Personal Area Networks (PANs), which network computer devices (including telephones, and PDAs) close to a single person;

- Local Area Networks (LANs), which typically connect several computers within a small area – a home, an office or a group of buildings;
- Wireless Local Area Networks (WLANs), which allows computers to be connected without wires;
- Metropolitan Area Networks (MANs), which are large networks connecting computers within a city;
- Wide Area Networks (WANs), which connect computers within a large geographical area (typically crossing regional and/or national boundaries); and
- the Internet, which is the largest possible WAN

11.2.2 Network Switching

The three common techniques used to transmit or switch data:

- circuit or line switching : this involves setting up a dedicated channel (on a temporary basis) from end to end before communication takes place;
- message switching: complete messages are sent to a storage area until a communication path is available. The whole message is sent along that path; and
- packet switching: This technique, which is now the dominant communications technique, involves breaking up a message into smaller packets. Each packet is sent through the network independently. The route taken by the packet depends upon which route is best at the time. Any type of data can be sent in a packet. Costs are charged per packet, irrespective of distance or route;

11.2.3 Communications devices

Nodes : The originating or terminating point of information or signal flow across a computer/and or telecommunications network. Earlier, nodes only used to refer to computers. Nowadays, with the increasing convergence of data, voice and video, the devices which are connected (or are connectible) to other computers, include mobile phones, Personal Digital Assistants, and, in the not too far future, even household appliances like the washing machine or refrigerator !

Modems : convert digital signals into analogue and visa versa. They allow computers to connect to analogue telephone systems.

Multiplexor/concentrator : These combine signals from several computers into one signal. A Multiplexor at the other end separates the signals from each computer.

Front end processor : these connect all network communication links to a central computer. They control what goes in and out. Other features include network control, format conversion error correction and logging.

Buffer : devices which temporarily store data to compensate for different data flow rates. E.g. the auditor may need a buffer when connecting his/her laptop to a client's mainframe computer.

Repeaters : boost the signal to combat attenuation.

Gateways : these connect networks using different protocols.

Bridges : connect networks using the same technology or protocol

Routers: devices which connect networks using the same network protocol (unlike gateways). They also carry out network routing to ensure that transmitted data is sent on the right route to reach its destination

Network Cards: Hardware which allows computer devices to communicate to a wired or wireless network

Hubs: Connect multiple network segments into a single segment in "broadcast" mode

Switches: Connect different network segments, but, unlike hubs, split network traffic to different destinations

Proxy: computer network service, which allows clients to make indirect network connections to external network services

Firewall: Hardware or software which restricts or controls communication between an internal network and the outside world

11.2.4 Transmission media

Twisted pair: two insulated cables twisted around each other. Primary advantage is low cost. Disadvantages include susceptibility to electrical interference, relatively low capacity, and easy to tap. However, with Gigabit Ethernet in position and 100 Gigabit Ethernet under development, speeds have improved considerably in the last decade.

Coaxial cable: comprised of a central wire surrounded by an insulating sheath and an outer conductor. Advantages include higher capacity than twisted pair (up to 500Mb/s with broadband technology), less susceptible to interference. Disadvantage is increased cost over twisted pair and still relatively easy to tap.

Fibre optic: glass fibres carry data as flashes of light. Advantages include high capacity, low risk of tapping and immune to electrical interference. Main disadvantage is cost.

Wireless networking (Wi-fi): involves transmission of data through radio waves. Speeds of upto 54 Mbps are currently achievable. Security has been a major concern, but the introduction of the IEEE Standard 802.11i has resulted in improved security mechanisms for wireless networks/

Bluetooth: an industrial specification for wireless Personal Area Networks (PANs), which allows short-range radio frequency connectivity at relatively low speeds

between devices such as PCs, laptops, printers mobile phones, digital cameras, video game consoles etc. The earliest instance of Bluetooth connectivity was between mobile phones and handsfree head sets or car kits. Currently, data transmission speeds of upto 2.1 Mbps are achievable.

11.2.5 Protocols

Protocols are the rules of data transmission. They control the use of the transmission media so that network devices can communicate with each other. For example there are the IEEE standards which many manufacturers adopt. Protocols include CSMA/CD (Carrier Sense Multiple Access/ Collision Detect), Token bus using a passing token, and token ring using a passing token.

11.2.6 OSI Model

The Open Systems Interconnection Basic Reference Model (OSI Model) is a seven-layered model for communications and computer network protocol design. It is not in itself a set of specific protocols, although the development of the Internet Protocol (IP) has been influenced by this model.

The seven layers of the OSI model are described below.

Layer 1: Physical Layer	Defines the electrical and physical specifications for devices
Layer 2: Data Link Layer	Provides the functional and procedural means for transfer of data, and also to detect/ correct errors in the physical layer Example: Ethernet
Layer 3: Network Layer	Provides the means for transferring variable length data sequences from a source to a destination through one or more networks. Example: Internet Protocol (IP)
Layer 4: Transport Layer	Provides transparent transfer of data between end users, and is responsible for reliability of data transfer. Example: Transport Control Protocol (TCP)
Layer 5: Session Layer	Establishes, manages and terminates sessions (or connections) between local and remote applications.

Layer 6: Presentation Layer	Transforms data to provide a standard interface for the Application Layer. Examples: MIME encoding, converting ASCII to EBCDIC or vice versa
Layer 7: Application Layer	Enables users to access information through an application Examples: Telnet, applications using HTTP/FTP/SMTP etc.

11.3 New Threats and Risks

In addition to the traditional risks to confidentiality, integrity and availability, networks open up a client's computer systems to a wide, potentially anonymous user base, with a much greater set of risks, both as a result of intentional and unintentional activities and from within or outside the organisation. Some of the risks arising out of unintentional events include:

- data loss : data may be deleted or lost in transmission;
- data corruption : data errors can occur during transmission, e.g. a 1(in binary) is sent but due to interference, line noise etc, a 0 is received;
- system unavailability : network links may be easily damaged. A loss of a hub can affect the processing ability of many users. Communications lines often extend beyond the boundaries of control of the client, e.g. the client may rely on the local telephone company for ISDN lines;

However, it is in the area of activities specifically intended to disrupt IT security that networks have gained increasing attention. The advance of web service technologies has resulted in unprecedented levels of user friendliness, while evolutionary designs ensure that legacy applications and databases do not require major transformations. However, these very features often require paradigm changes to traditional security models and architectures. Some of the major issues and risks include:

- confidentiality and integrity of data transmitted via web services protocols, as well as establishment of trust between services for individual transactions;
- availability of services in the face of denial of services, which exploit vulnerabilities unique to web services.

Where the client's systems are connected to networks there is potentially a greater risk of Unauthorised access by outsiders (hackers) and non-authorised employees, leading to:

- fraud : from internal and external sources. Thieves no longer have to rely on robbing banks with guns and balaclavas. The clever ones can theoretically break into a banking system from the other side of the world and transfer money remotely;
- disclosure of confidential information : where confidential systems such as personnel, or research and development are connected to networks there is an increased risk of unauthorised disclosure, both accidentally and deliberate;
- virus and worm infections : Worm infections are specifically designed to spread over networks. Virus infections are more likely because traditional protective measures such as virus scanning are less effective. Users tend to scan disks they receive from external sources but are less likely to scan data received over a network; and
- contravention of copyright, data protection (privacy) legislation.

Traditional perimeter-based network security systems like firewalls are inadequate to protect such web services, since such applications are transmitted over HTTP, which is allowed to flow without restriction through most firewalls, and also due to the lack of granularity of such technologies.

A brief description of new risks includes the following:

11.3.1 Malware

Malware, also known as malicious code and malicious software, refers to programs inserted into a system, with a view to compromising the confidentiality, integrity and/or availability of the system, or otherwise annoying the victim. Malware falls into the following broad categories:

Virus	Designed to self-replicate and distribute copies to other files, programs or computers. Each virus has an infection mechanism, and the virus payload contains the code for the virus's objective (which can be either benign or malicious), Many viruses also have a trigger (for payload execution)
Worm	Self-replicating program that is completely self-contained (does not require a host program for infecting a victim). A worm is self-propagating (unlike a virus) and can create fully functional copies and execute itself without user intervention
Trojan Horse	Non-replicating program that appears benign but has a hidden malicious purpose

Logic Bomb	Malicious logic that performs an unwanted action when a specific criterion is met
Malicious Mobile Code	Software (typically in Java/ Active X/ JavaScript/ VBScript) that is transmitted from a remote system to be executed on a local system, which affects systems, often by taking advantage of default privileges granted to mobile code
Backdoor	Malicious program that listens for commands on a certain port. Most backdoors have a client component (residing on the intruder's remote computer) and a server component (residing on the infected computer). Once a connection between client and server is established, the remote intruder gains some degree of control over the infected computer e.g. for transferring files, acquiring passwords or executing arbitrary commands.
Zombie	Program installed on one system to attack other systems – typically to create DDOS attacks on a target
Keystroke Logger	Monitors and records keyboards uses, typically for recording account and financial information
Rootkit	A collection of files installed on a system to alter the standard functionality of the system in a malicious and stealthy way, also making it difficult to identify the presence of the rootkit and/ or changes made
Phishing[2]	Deception (usually by creating a fake website or sending fraudulent e-mails) to trick individuals into disclosing sensitive information (usernames, passwords, financial information etc.)
Virus Hoaxes	False warnings of viruses purportedly of devastating magnitude, which waste organisational resources, and occasionally direct users to alter settings or delete files, which could result in operational or security problems
Spyware	Software installed secretly or surreptitiously to gather

[2] Phishing and virus hoaxes are not really malware, but are commonly associated with malware

	information on individuals or organisations, without their knowledge, usually for commercial or other gains.

11.3.2 Attacker toolkits

Many attackers use toolkits with different types of utilities and scripts that can be used to probe systems and attack compromised/ vulnerable systems.

Packet Sniffer	Monitors network traffic on wired/ wireless networks and capture packets. Most packet sniffers are also protocol analysers, and can thus reassemble streams from individual packets and decode communications using different protocols
Port scanner	Program that attempts to determine remotely which ports or systems are open
Vulnerability Scanner	Looks for vulnerabilities on either the local or remote systems
Password Cracker	Program for cracking OS and application passwords either by attempting to guess passwords or performing brute force attempts by trying every possible password
Remote login programs	Programme for logging in remotely to compromised systems

11.3.3 Reconnaissance Attacks

These generally have the objective of collecting information about an application to better target other types of attacks:

Forceful browsing attack	Attempt to detect web services that are not explicitly publicised
Directory traversal attack	Attempts to access restricted files used by a web service
Privilege escalation attempts	Change the privilege level of a process, in order to bypass security controls

11.3.4 Attacks on Integrity

These attacks exploit the targeted application to make unauthorised changes; some examples are listed below:

Parameter tampering	Arbitrary data passed as parameters to Web service methods, which do not have sufficient verification mechanisms
Coercive parsing	Attempt to overload the XML parser, using large but legitimate XML files
Schema poisoning	Attempt to compromise XML schema in its stored location, by replacing it with a modified schema which could cause valid XML documents to be rejected and/or invalid or malicious XML documents to be accepted
Checksum spoofing	Attaches a recomputed hash (which is used as an integrity mechanism) tallying with an altered message
Principal spoofing	Sending a message appearing to be from a valid requested web service
Canonicalisation	Attempts to use different forms resolving to the same standard name (canonical name) e,g. URLs/ URIs, user names, files, pathnames etc. to attack web services, where the code makes security decisions based on the name of a resource passed on as input
Intelligent tampering and impersonation	Modify the web service program or data to allow the service to continue operating in a seemingly normal way, but which actually reflects a subverted or corrupted state/ data (e.g. overwriting program's data buffers with data in the correct format but different than expected values); establishing a rogue version of the legitimate Web service program

11.3.5 Denial of Service (DOS)Attacks

These are intended to ensure failure of web services through degradation of performance by ensuring requests for applications in volumes several times larger than expected volumes:

- Typically, such DOS attacks are Distributed Denial of Service (DDOS) attacks, where multiple hosts over the Internet are infected to ensure that they all send requests to the attacker's targeted web service to lead to its failure.
- Sophisticated DOS attacks target not only the first provider web service in a service, but also send additional requests to other services in the series/ collection via other conducts; this increases the load non the collection of services and reduces the risk of likelihood of detection.

Well-known DOS attacks are ping of death, teardrop and trinoo. Some examples of new XML-based DOS attacks are given below:

Flooding attack	Involves copying valid service requests and resending them to a provider Web service
Recursive / oversized payloads sent to XML parsers	Send XML documents which have thousands of elements, or documents which are very large in order to stress and break an XML parser
Buffer overflow exploits	Sending oversized data input to the web service components (typically in languages without mandatory input validation – C/ C++) , which causes a buffer overflow, and loads malicious code into the service's execution stack, with the objective of either causing DOS or to grant unauthorised permissions
Race Conditions	Attempt to use the web service to spawn multiple resources to access the same file; often combined with symlink attacks, which attempt to exploit symlink vulnerabilities on Unix/ Linux systems by making a symbolic link from a file to which the attacker has access to other files to which he/ she does not have access
Memory leak exploitation	Exploit memory leaks (where programs do not free up space after execution) to hog memory resources and cause DOS

11.4 Communication and Network Controls

Controls to safeguard communication and network C-I-A involve both policy and procedural controls, as well as operational controls

11.4.1 Network Policy and Procredures

The organisation should have a formally documented network and Internet policy (which may be a part of the overall IT security policy), along with associate procedures to ensure implementation.

11.4.2 Denial of Service (DOS) Protection

Sophisticated DOS attacks are often not detectable by firewalls or Intrusion Detection Systems (IDS), since these countermeasures do not provide the granularity to control DOS on a per-transaction/ operation basis. Measures are required to detect DOS attacks, continue operation as long as possible, and then gracefully recover and resume operations. These include:

- Replicating data and services to improve availability;
- Using logging of transactions to ensure accountability and non-repudiation;
- Using secure software design and development techniques to minimize vulnerabilities;
- Using performance analysis and simulating techniques for end-to-end quality of service and quality of protection; and
- Digitally signing UDDI[3] entries to verify the author of registered entries

11.4.3 Boundary Protection Devices

The organisation must ensure that all connections from the information system to the Internet or other external networks (or even other less secured internal networks from which separation/ protection is required) must be controlled or protected through boundary protection devices (e.g. proxies, gateways, routers, firewalls, encrypted tunnels etc.) arranged and operated in an effective manner. Typically,

- the number of access points is limited for better monitoring of both inbound and outbound network traffic;

[3] UDDI is a Universal Description, Discovery and Integration protocol to allow web services to easily located and subsequently invoked.

- External telecommunication links are suitably restricted and/or controlled e.g.:
  - Restricting the use of modems;
  - Use of call-back modems;
  - Use of private/ dedicated lines
- public access to the information system is allowed only in an appropriately mediated fashion;
- Publicly accessible information systems (e.g. public web services) are physically separate, with separate network interfaces
- Boundary protection devices are arranged in an effective architecture, e.g. routers protecting firewalls and application gateways residing on a DMZ (demilitarized zone)

Firewalls are the most common devices for controlling the flow of inbound and outbound network traffic. The different types of firewalls are described in this section.

11.4.3.1 Packet Filter Firewalls

These constitute the most basic type of firewall, operating mainly at Layer 3 (Network of the OSI model). Network access is controlled depending on the source and destination addresses of the packet, the specific network protocol used (e.g. Ethernet at Layer 2 and IP at Layer 3), source and destination ports of the sessions etc. Their main strengths are speed and flexibility, and they are ideally suited to working as "boundary routers" at the outermost boundary with an untrusted network, with a Demilitarised Zone (DMZ) to the inner firewall for the protected network.

However, packet filters have several limitations (primarily since they do not examine upper-layer data:

- They cannot prevent application-specific vulnerabilities.
- They do not support advanced user authentication, and are usually limited to network layer address-based authentication. Consequently, they are vulnerable to attacks like address spoofing.
- Their logging functionality is limited.
- They are susceptible to security breaches through improper configuration.

11.4.3.2 Stateful Inspection Firewalls

Stateful inspection firewalls are packet filter firewalls with added awareness at Layer 4 of the OSI model, e.g. by tracking client ports for TCP connections individually by creating a directory of outbound TCP connections with the session's corresponding

client port. The stateful inspection technology is relevant only to TCP/IP; with other network protocols, such firewalls behave identically to normal packet filters.

11.4.3.3 Application-Proxy Gateway Firewalls

Application-Proxy Gateway firewalls are advanced firewalls that combine lower layer access control with Layer 7 (Application) functionality. They do not require a Layer 3 (Network) route between the inside and outside interfaces, with the routing done by the firewall software. Individual proxy agents interact directly with the firewall access control ruleset to determine whether network traffic should be permitted or not, and also to require authentication of each individual network user. Such firewalls have several advantages over packet filter firewalls:

- They have more extensive logging capabilities.
- They allow advanced user authentication, and can be made less vulnerable to address spoofing.

However, application-proxy gateway firewalls are slower than packet filter firewalls, because of their "full packet awareness). Since an application-specific proxy agent is required for each type of network traffic, such firewalls tend to be limited in supporting newer network applications and protocols.

11.4.3.4 Dedicated Proxy Servers

These are separate servers which retain proxy control of traffic (e.g. an e-mail proxy or an HTTP proxy) but do not contain firewall capabilities, and are typically used to decrease the workload on firewalls and perform more specialised authentication, filtering and logging. In addition, they can be used for specialised web and email content scanning e.g. script/ applet filtering, virus/ worm scanning, or restricting specific types of content on an user-wise basis.

11.4.3.5 Host-based firewalls

These are firewall packages which can be used to secure the individual host only, and not the network as a whole. These are useful for internal network environments or regional offices, and end up protecting the server application better. However, these are not suitable for high-traffic and high-security environments, and have the disadvantage of needing to be administered individually.

11.4.3.6 Personal Firewalls/ Personal Firewall Appliances

These are typically used for securing personal computers at home or in remote locations. Personal firewalls are software packages installed on the system meant to be protected, while personal firewall appliances are more similar to traditional firewalls and run on specialised hardware, which often combine routing/ switching/ hub functions with network management (SNMP) and application-proxy agents.

11.4.3.7 General Considerations for Firewalls

- The type of firewall to use would depend on the size of the site, the amount of traffic, the sensitivity of data, the applications run by the organisation, and other factors.
- A typical firewall configuration would involve a packet filter router at the boundary, with a more powerful firewall in the Demilitarized Zone protecting the internal network.
- To secure remote access, the firewall may have a Virtual Private Network (VPN) to encrypt traffic between the firewall and either remote users or remote users on the Internet.
- Firewalls are vulnerable to misconfigurations and their configuration and administration should be performed carefully.
- Firewalls should be treated as the first (and not the only) line of defence in a comprehensive security architecture.

11.4.3.8 Other forms of remote access

Many organisations permit remote access for selected employees and third parties through dial-up or other connections. The following must be considered:

- The security of a network is equal to the security of its weakest link. There is no point in having a strong firewall to the Internet, when selected employees have modem-based access which does not go through a firewall. Also, the value of encrypting traffic to/ from the Internet is diminished, if other forms of remote access do not use encryption.
- Remote access rights should be restricted on the basis of need.
- Remote access should be monitored and logged.

11.4.4 General security considerations for Telecommuting and broadband communications

The recent trend of common-place availability of broadband connectivity at reasonable costs has increased the security risks for remote/ home access to corporate networks. The relatively short duration and slow speeds (as well as lack of fixed IP addresses) of dial-up connectivity made it more difficult for attackers, as compared to broadband connectivity. Some of the measures to control the security risks from such communication are:

- Installing firewall software or firewall appliances on home networks/ remote PCs
- Configuring web browsers and OS options to limit vulnerability to intrusion

- Select appropriately secure wireless and home networking technologies
- Using a VPN (Virtual Private Network) for providing secured end-to-end connections

11.4.5 Virtual Private Networks (VPNs)

A Virtual Private Network (VON) is a virtual network built on top of existing physical networks for ensuring a secure communications mechanism for data transmitted between networks, typically for information carried over the Internet. IPsec (Internet Protocol Security) is the commonly accepted framework of open standards for ensuring private communications over IP networks, for providing the following types of protection:

- Confidentiality – by encrypting data
- Integrity – by generating a Message Authentication Code (MAC), a cryptographic checksum of data
- Peer Authentication – for confirming the identity of the IPsec endpoints
- Replay protection – to prevent multiple delivery and ensure that data is not delivered grossly out of order
- Traffic analysis protection – to prevent persons monitoring network traffic for knowing the details of the parties, or how much data is exchanged.
- Access control – by ensuring access to only authorized users for specified types of network traffic

The three major models for VPN architectures are:

- Gateway-to-gateway – for communication between two specific networks;
- Host-to-gateway – for communication between individual hosts and a specific network;
- Host-to-host – for communication between two specific computers.

IPSec has the following components:

- Encapsulating Security Payload (ESP) and Authentication Header (AH) – these are two security protocols, of which ESP is preferred because of its encryption capabilities
- Internet Key Exchange (IKE) protocol, which negotiates the cryptographic algorithms and related settings for AH and ESP
- IP Payload Compression (IPComp) protocol, which is optionally used to compress packet payloads before encrypting them.

VPNs generally use a combination of both symmetric and asymmetric cryptography algorithms:

- Asymmetric encryption should be used to provide peer authentication.
- Data communication should be encrypted with a strong symmetric algorithm e.g. Advanced Encryption Standard (AES) or Triple Data Encryption Algorithm (TDEA or 3DES) and integrity protection should be ensured with a strong symmetric algorithm e.g. the Hash Message Authentication Code (HMAC) versions of Secure Hash Algorithm (SHA-1) or Message Digest 5 (MD-5)

11.4.6 Malware Prevention and Handling

- A systematic and structured approach for malware prevention and handling should be developed and implemented. Without such an approach, using malware detection and prevention tools in an ad hoc manner will not ensure consistent network/ system-wide barriers to malware.
- Malware policies and procedures should also cover remote workers, as well as third-party users
- Awareness programmes on malware incident prevention and detection should be conducted.
- Operating system and application vulnerabilities should be mitigated through systematic procedures involving patch/ hotfix management, applicaction of security configuration guides and additional “host hardening measures.
- Malware threat mitigation efforts primarily involve deployment of anti-virus software and spyware detection and removal utilities on various types of hosts, supplemented by other controls like intrusion prevention systems, firewalls and certain application configuration settings.
- There must be systematic procedures to ensure that (a) antivirus and anti-spyware software are kept upto date; and (b) that they are installed and administered on a network-wide basis rather than in an ad hoc manner.
- There should be a robust incident response mechanism for handling malware incidents, covering preparatory activities, detection and analysis, containment, eradication, recovery and post-incident learning.

11.4.7 Using Intrusion Detection and Prevention (IDP) systems

Intrusion Detection and Prevention (IDP) systems identify potential incidents by monitoring events in a computer system and analysing them for signs of potential incidents, log and report such incidents, and attempt to stop them. Major types of IDP technologies include:

- Network-based IDP systems, which monitor network traffic for particular segments or devices and analyse the network and application protocol activity to identify activity;
- Wireless IDP systems, which monitor wireless network traffic and identify suspicious activity involving wireless networking protocols;
- Network behaviour anomaly detection (NBAD) systems, which examine network traffic to identify threats that generate unusual traffic flows like DDoS attacks
- Host-based systems, which monitor a single host for suspicious activity.

The following need to be kept in mind, while planning and implementing IDP systems:

- While IDP systems are useful tools, they constitute only one component of the security management process.
- A robust IDP system may require a combination of IDP technologies for more comprehensive and accurate detection capabilities. In such a situation, the extent of integration between the IDP technologies and tools also needs to be considered.
- IDP components themselves need to be secured appropriately, since attackers often target IDPs to prevent them from detecting attacks or for gaining information about host configurations etc.

11.4.8 Security of Wireless Networks (WLANs)

11.4.8.1 Wireless Networks – An Introduction

The most commonly used family of standards for WLANs is the IEEE 802.11 Standard, also known as WiFi. These comprise of several individual standards:

- The original 802.11 Standard ratified in 1997 had a maximum data rate of 2 Mbps.
- 802.11a and 802.11b, which were ratified in 1999, supported maximum data rates of 54 Mbps and 11 Mbps in the 5 GHz and 2.4 GHz bands respectively. However, because of cost and performance considerations, 802.11b quickly became the dominant standard.
- 802.11g, which was ratified in 2003, supported maximum data rates of 54 Mbps in both the 5 GHz and 2.4 GHz bands.

802.l1 has two fundamental components:

- Station (STA), which is the wireless endpoint device e.g. laptop, PDA etc.
- Access Point (AP), which connects stations with a wired LAN or with each other.

There are two WLAN design structures:

- Ad hoc mode, which involves peer-to-peer station communication, without access points (the set of stations configured in this mode is termed as an Independent Basic Service Set)
- Infrastructure mode, where APs are used for connecting stations; one AP and one or more STAs in infrastructure mode constitute a Basic Service Set (BSS), while an Extended Service Set (ESS) comprises more than one BS connected by a distribution system (typically a wired LAN)

11.4.8.2 Security Considerations of 802.11

The above 802.11 variants include security features known collectively as Wired Equivalent Privacy (WEP), that are supposed to provide a level of security comparable to that of wired LANs. However, these have a number of weaknesses:

- The mandatory authentication mechanism is open system authentication, which does not provide true verification of identities of either the AP or STAs.
- Even the optional shared key authentication mechanism is still weak since
  - the AP is not authenticated to the STA
  - The simple challenge response mechanisms are weak, and subject to man-in-the-middle and brute force attacks, as well as eaversdropping
  - All devices use the same WEP key or small set of keys, which reduces accountability and complicates troubleshooting and incident response
- The standard encryption for WEP specifies support for only a 40-bit WEP key; in addition, the cryptographic technique has known flaws that cannot be mitigated by longer keys
- Data integrity under WEP is ensured through a simple 32-bit CRC, which does not provide adequate protection against intentional forgeries
- There is no replay protection
- No defense is provided against DOS attacks like jamming or flooding.

11.4.8.3 802.11i Amendment

IEEE 802.11i, which was introduced in 2004, addressed the security problems of WEP-based 802.11. This introduces the concept of a Robust Security Network (RSN), a wireless network allowing the creation of only RSN associations (RSNAs). The main features of 802.11i are as follows:

- Enhanced user and message authentication mechanisms are in place, based on the Extensible Authentication Protocol (EAP). To accomplish mutual authentication between an AP and STA, an additional entity (AS – Authentication Server) is introduced.

- RSNAs involving logical connections between communicating 802.11 entities are established through a 4-way handshake, which validates that both entities share a pair-wise master key (PMK), and confirms the selection and configuration of data confidentiality and integrity protocols. PMKs are obtained either as Pre-Shared Keys (which are less desirable, since they are more difficult to manage) or as a side effect of successful EAP authentication.
- Better enciphering and data integrity mechanism are in place, with two additional protocols for RSNAs: Temporary Key Integrity Protocol (TKIP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP, which is considered superior since it uses the strong AES standard)
- Flooding and jamming attacks are prevented through a port-based access control, which distinguishes between authenticated and unauthenticated data and blocks user access unless authentication is successful.

802.11 is fully supported through WLAN products which are WPA2 (WiFi Protected Access -2) certified, while WPA (WiFi Protected Access) includes a subset of 802.11i specifications that address the weaknesses of WEP.

11.4.8.4 Overall Security Considerations

- When a new WLAN is being planned, it should conform to 802.11i. Further, for a corporate network, EAP based authentication methods should be selected, with a strong protocol, preferably CCMP. Also, products should be WPA2 certified.
- Where existing 802.11 WLANs are in place, additional security measures should be put in place, e.g. by putting in place an IPSec VPN.
- Communication between the APs and ASs are not covered by 802.11i, and should be protected sufficiently through cryptography. A dedicated VLAN to support AP connections to the distribution system could also be considered.
- A clear WLAN usage policy specifying the user groups/ communities authorized to use WLAN technology should be established.

11.4.9 Voice over IP (VOIP) security

Voice over IP – the transmission of voice over packet-switched IP networks, instead of on separate analogue networks – is gaining importance for telecommunications within organisations. Greater flexibility, ease of management and lower cost are benefits arising from the “convergence” of data, voice and video onto a single network, instead of separate networks. Some of the security issues to be considered are as follows:

- It must be recognized that with current technologies, VOIP systems will be more vulnerable and less reliable than conventional telephone systems. Further, there is likely to a tradeoff between security and Quality of Service (QOS).
- An appropriate network architecture should be developed:
  - If feasible, voice and data should be separated into logically different networks.
  - At the voice gateway, which interfaces to the PSTN, VOIP protocols from the data network should be disallowed.
  - Firewalls designed for VOIP protocols should be deployed.
  - If practical, remote management of IP PBXs may be avoided.
  - If performance at VOIP endpoints is an issue, encryption may be used at the router or other gateway to provide for IPSec tunnelling.
- Physical controls over access to VOIP network components are of importance.
- If practical, "softphone" systems, which implement VOIP on ordinary PCs, should be avoided where security and privacy are concerns, since malware vulnerabilities are high; further, this conflicts with the need to separate data and voice networks to the extent possible.

11.4.10 E-Mail Security

E-mail is probably the most frequently used network application in most organisations. The need for exchanging e-mail with the outside world (including untrusted third parties) also results in major security risks e.g.:

- E-mails used as vectors for propagating worms and viruses;
- Users sending confidential or inappropriate information via e-mail, exposing the organization to legal action and loss of business;
- Receipt of spam (e-mail based advertisements), as also malicious misuse of the e-mail server for sending spam;
- DoS and other attacks on the organisation's IT system through or on the mail server.

Some important controls needed to secure the mail server and mail clients are indicated below:

- The security aspects of deployment of a mail server should be carefully planned, and appropriate security management practices (e.g. IS security policy, risk management, configuration management, security awareness and training, contingency planning etc.) should be implemented.

- Both the mail server OS as well as the mail server application should be appropriately deployed, configured and managed:
  - Patch/ hotfix/ update/ upgrade management
  - Remove or disable unnecessary services and applications
  - Careful configuration of system and mail server user authentication
  - Using security configuration guides and checklists
- Most standard mail protocols default to unencrypted user authentication as well as clear text e-mail data transmission. The implementation of encryption technologies should be considered; at the very least, the user authentication session should be encrypted.
- Network infrastructure (firewalls, routers, intrusion detection systems) etc. should be employed as the first line of defence to protect the mail servers
- Specific protection for e-mail servers against malware should be adopted, and such protection should be kept upto date
- Data should be backed up regularly, and such backups should be regularly tested
- Detailed procedures should be established and followed for recovering from security breaches.

11.4.11 Transmission Integrity

Mistakes and errors are inevitable in any form of communication. The communication of computerised data is no exception. Errors can arise in each step in the communication cycle, from data input by a user, to failures in mechanical parts (keyboards, MICRs), to errors when data is in transit (in the cables).

Controls can be designed into each stage of the communication cycle. In this chapter we examine controls within the data transmission stage and look at the controls which are designed to reduce the risk of errors during data transmission.

Errors arise when digital signals, binary numbers, are sent from one place to another, for example a 1 is transmitted and a 0 is received at the other end. Errors can also arise when whole bits are lost, so a 1 is transmitted but not received. Missing bits normally have a significant effect on the data received (all the following data will probably be incomprehensible).

Error rates are used to provide an indication of the frequency of bit errors. Error rates are quoted as one error in so many bits ,for example 1 in 10^4 means that on average there will be one bit error per 10,000 transmitted bits.

The importance of errors in data transmission will depend on the application. Where even a few errors are deemed to be unacceptable, the system designers should build in error control techniques and routines to reduce the errors to an acceptable level.

Error detection and correction controls include:

- loop/echo checks: these controls detect when there is a problem with the communication link. The control involves the receiver sending back a copy of the received message to the sender. The sender compares the echoed message to the original and any errors are picked up. Loop checks are a form of information feedback control;
- redundancy checks : the messages are transmitted with in-built redundancy. Data transmission errors are detected by adding a calculated bit to the end of each segment of data. If errors arise the calculated bit will change and the error detected; and
- parity checks : these are hardware checks which are built into the components by the manufacturer. Parity checks detect errors by determining if the value of digits in a data group are odd or even. A bit is then added to the end of the transmitted data. At the receiving end the bits are added and summed to an odd or even number which should be the same as the transmitted bit. If the data has changed there is a 50/50 chance that the parity check detects an error. The extra parity bits are checked as data moves around the system.

12 Compliance Controls

More and more countries are increasing passing legislations regarding the use of information technology. Such law places a specific responsibility on the managers of the IT systems to ensure compliance with the legislation. Besides, organisations have started prescribing their own security policies and standards. There is a need to check whether such policies and standards are being complied with. This session will focus on the compliance of laws and regulations as well as with the organisational security policies and standards. Besides, the session will also focus on procedures necessary to ensure an effective systems audit. The important issues to be discussed in the session are:

Compliance with legal requirements:

- The objective is to avoid breaches of criminal and civil law, statutory and contractual obligations

Reviews of security policy and compliance:

- The objective of this control is to ensure compliance of systems with organisational security policies

System audit considerations:

- The objective is to maximise effectiveness of and to minimise interference to/from system audit process.

12.1 Compliance with legal requirements

To ensure compliance with legal requirements the following controls may be necessary:

12.1.1 Identification of applicable legislation

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system. The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

12.1.2 Intellectual property rights

Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, trade marks. Copyright infringement can lead to legal action which may involve criminal proceedings.

Legislative, regulatory and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organisation, or that is licensed or provided by the developer to the organisation can be used.

Proprietary software products are usually supplied under a licence agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. The following controls should be considered:

- Publishing a software copyright compliance policy which defines the legal use of software and information products
- Issuing standards for the procedures for acquisition of software products
- Maintaining awareness of software copyright and acquisition policies, and giving notice of the intent to take disciplinary action against staff who breach them
- Maintaining appropriate asset registers
- Maintaining proof and evidence of ownership of licenses, master disks, manuals etc.
- Implementing controls to ensure that maximum number of permitted users is not exceeded

- Carrying out checks that only authorized software and licensed products are installed
- Providing a policy for maintaining appropriate licence conditions
- Providing a policy for disposing or transferring software to others
- Using appropriate audit tools
- Complying with terms and conditions for software and information obtained from public networks

12.1.3 Safeguarding of records

Important records of am organisation should be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples of this are records that may be required as evidence that an organisation operates within the statutory rules, or to ensure adequate defence against potential civil or criminal action, or to confirm the financial status of an organisation with respect to the shareholders, partners and auditors. The following controls may be necessary to ensure safeguarding of records:

- Categorisation of records: Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedure
- Retention period and storage type: For each record the period of retention as well as the type of storage e.g. paper, microfiche, magnetic, optical should be prescribed.
- Manufacturers' recommendation: Storage and handling should be implemented in accordance with the manufacturer's recommendation.
- Access of electronic records: Where electronic storage media are chosen, procedures to ensure the ability to access data throughout the retention period should be included, to safeguard against loss due to future technology change.
- Acceptable to a Court of law: Data storage systems should be chosen such that required data can be retrieved in a manner acceptable to a court of law; e.g. all records required can be retrieved in an acceptable timeframe and in an acceptable format.
- Destruction of records: The system of storage and handling should ensure clear identification of records. It should permit appropriate destruction of records after the retention period if they are not needed by the organisation.
- Guidelines: Guidelines should be issued on the retention, storage, handling and disposal of records and information.

- Cryptographic keys: Any related cryptographic keys associated with encrypted archives or digital signatures should be kept securely and made available to authorised persons when needed.
- Inventory of key information: An inventory of sources of key information should be maintained.

12.1.4 Data protection and privacy of personal information

A number of countries have introduced legislation placing controls on the processing and transmission of personal data (generally information on living individuals who can be identified with that information). Such controls may impose duties on those collecting, processing and disseminating personnel information, and may restrict the ability to transfer the data to other countries.

Compliance with data protection legislation requires the following controls:

- Often control is best achieved by the appointment of a data protection officer who should guide managers, users and service providers on their individual responsibilities and the procedures that should be followed.
- It should be the responsibility of the owner of the data to inform the data protection officer about any proposals to keep personal information in a structured file, and to ensure awareness of the data protection principles defined in the relevant legislation.

12.1.5 Prevention of misuse of processing facilities

The information processing facilities of an organisation are provided for business purposes. Management should authorise their use. Any use of these facilities for non-business or unauthorised purposes, without management approval, should be regarded as improper use of the processing facilities. Following controls are suggested to prevent such misuse:

Disciplinary action:

- If misuse of facility is identified by monitoring or other means, it should be brought to the attention of the individual manager for appropriate disciplinary action.

Monitoring:

- The legality of monitoring the usage varies from country to country and may require employees to be advised of such monitoring or to obtain their consent.
- Legal advice should be sought before implementing monitoring procedures.

Awareness of scope of access:

- It may be a criminal offence to use a computer for an unauthorised purpose. It is therefore, essential that all user are aware of the precise scope of their permitted access.

- This can be achieved by giving users written authorisation, a copy of which should be signed by the user and securely retained by the organisation.

Warning message:

- At log-on a warning message should be presented on the computer screen indicating that the system being entered is private and that unauthorised access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.

12.1.6 Regulation of cryptography

Some countries have implemented agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls. Such control may include:

- Import and/or export of computer hardware and software for performing cryptographic functions;
- Import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;
- Mandatory or discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with national law. Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

12.1.7 Collection of evidence

It is necessary to have adequate evidence to support an action against a person or organisation. Wherever this action is an internal disciplinary matter the evidence necessary will be described by internal procedure. Where the action involves the law, either civil or criminal, the evidence presented should conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. The following controls will be necessary to ensure the quality of evidence:

Admissibility of evidence:

- To achieve admissibility of evidence, organisations should ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.

Quality and completeness of evidence:

- To ensure quality and completeness of evidence a strong evidence trail is needed, which can be established in the following conditions:
  - ❖ For paper documents: the original is kept securely and it is recorded who found it, where it was found, when it was found and who witnessed the

discovery. Any investigation should ensure that originals are not tampered with

- ❖ For information on computer: copies of any removable media, information on hard disks or in memory should be taken to ensure availability. The log of all actions during the copying process should be kept and the process should be witnessed.

12.2 Reviews of security policy and technical compliance

We had discussed earlier about the controls necessary to ensure compliance with laws, rules and contractual obligations. Similarly, there is a need to put in controls to review the security policy and its compliance. This could be achieved with the following controls:

12.2.1 Compliance with security policy

Managers should ensure that all security procedures within their area of responsibility are carried out correctly. In addition, all areas within the organisation should be considered for regular review to ensure compliance with security policies and standards. These should include the following:

- Information systems
- Systems providers
- Owners of information and information assets
- Users
- management

Owners of information systems should support regular reviews of the compliance of their systems with the appropriate security policies, standards and any other security requirements.

12.2.2 Technical compliance checking

Information systems should be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operating systems to ensure that hardware and software controls have been correctly implemented. The following points should be considered to perform such checking:

- This type of checking requires specialist technical advice.
- It should be performed manually by an experienced system engineer, or by an automated software package, which generates a technical report for subsequent interpretation by a technical specialist.

- It also covers penetration testing, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorised access due to these vulnerabilities.

12.3 System audit considerations

The objective of this control is to maximise the effectiveness of and to minimise interference to/from the system audit process. There should be controls to safeguard operational systems and audit tools during system audits. This can be achieved through:

12.3.1 System audit controls:

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business process. The following should be observed:

- Audit requirements should be agreed with appropriate management
- The scope of the checks should be agreed and controlled
- The scope should be limited to read-only access to software and data
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased when audit is completed.
- IT requirements for performing the checks should be explicitly identified and made available.
- Requirements for special or additional processing should be identified and agreed
- All access should be monitored and logged to produce a reference trail.
- All procedures, requirements and responsibilities should be documented.

12.3.2 Protection of system audit tools:

Access to system audit tools, i.e. software or data files, should be protected to prevent any possible misuse or compromise. Such tools should be separated from development and operational systems and not held in tape libraries or user areas.

12.4 Digital Signatures and Cryptography

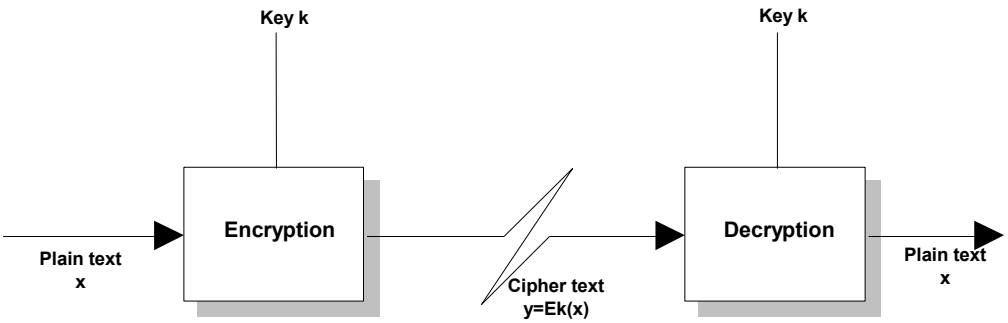
12.4.1 Overview

Cryptography offers solutions to problems with regard to confidentiality and integrity of information, authentication of communication partners and non-repudiation of

messages. Confidentiality of information is accomplished by encrypting data and making it unintelligible to an outsider Encryption can be applied to data in storage or physical transit, and during transmission over telecommunication links (see figure 5 below).

One problem with the use of encryption is that various countries have laws that prohibit the export of encryption hardware and software and some countries have laws about the use of encryption without a license.

Figure 5 : encryption during transmission



12.4.2 Encryption

12.4.2.1 The components

The two basic components of classical cryptographic techniques are SUBSTITUTION and TRANSPOSITION.

Substitution is simple the replacement of each character in a message by another form of chosen character set. The CAESAR code is the simplest form of substitution cipher, e.g.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Plain text.....this is a CAESAR code example

Cipher text.....NBCMCMUWUYMULWIXYYRUGJFY

A more complex substitution can be obtained by scrambling the alphabet.

Transposition is a process that is familiar to crossword and word-game puzzlers in the form of anagrams. It involves the re-sequencing of characters in the original message according to a defined pattern to produce a cipher text, for example:

Plain text.....NOW IS THE TIME FOR ALL GOOD MEN

Transposition scheme.....213654

Cipher text.....ONWSI HTEIT EMFRO LALOG DOMNE

These simple cipher techniques demonstrate the elements and processes of encipherment:-

- encryption : the process which transforms plain text into cipher text;
- decryption : the reverse process which restores the original plain text;
- key : a parameter which controls the encryption/decryption processes.

Two forms of encryption are widely used:

- **symmetric** encryption uses the same key for encryption and decryption. Two people who wish to share symmetrically encrypted information must share the same key. This gives rise to a key distribution problem since it is clearly undesirable for anyone else to find out the shared secret key. The Data Encryption Standard (DES) and IDEA are the best known symmetric encryption algorithms.
- **asymmetric** encryption involves generating a pair of keys which are known as the public and private keys. Information encrypted with one of the keys can only be decrypted using the other key of the pair. The public key can be published which gets around the key distribution problems associated with symmetric encryption. RSA is the best known asymmetric encryption algorithm.

12.4.2.2 The Data Encryption Standard ("DES")

When used individually, substitution and transposition are very weak methods of encipherment. Used in repeated combination, however, they are more effective. This is the basis of the U.S. Data Encryption Standard.

DES is based on an algorithm that takes data in blocks of 64 bits and enciphers according to a 64 bit key. The algorithm is published so that all the security of the method is vested in the participants keeping their shared keys secret. The algorithm was originally made sufficiently complex to make it technically infeasible for an attacker possessing corresponding plain and enciphered text to ascertain the key other than by exhaustive incremental key trials. Since new computers have greater processing power, attackers may succeed in breaking the code quicker.

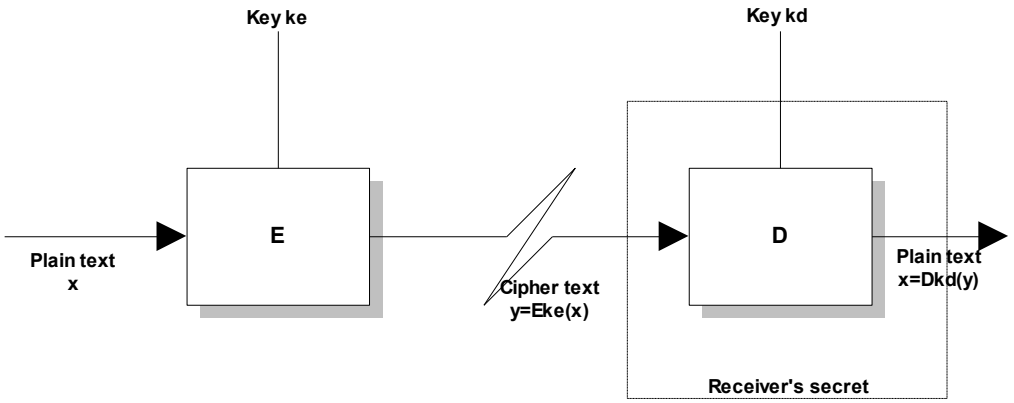
In view of current computing power, DES is no longer considered an acceptable encryption standard by the US Federal Government. Increasingly, organisations are turning to adopt more complex encryption schemes, such as Triple DES – 192 bit security, and AES (Advanced Encryption Standard) – 256 bit security.

12.4.2.3 Public key systems

In secret key systems, security lies with the generation, distribution, storage and destruction of cryptographic keys. Public key systems were first proposed in 1976, mainly to provide a solution to the problem of secure transmission of secret keys using the communications medium itself. The basic principles are:-

- the process is asymmetric, i.e. a different process is required from A to B, as from B to A;
- two keys are used, one to encrypt which is known to the world, and a secret key for decryption which is known only to the receiver.

Figure 6 : public key encryption



In practice there needs to be a relationship between *kd* and *ke*. The security of the process depends on the technical unfeasibility of determining *kd* from a knowledge of *ke.*

12.4.2.4 Key management

The keys shared between transmitter and receiver provide the means of authorised decipherment and of exclusion of unauthorised persons. The practice of key management is therefore fundamental to the integrity of the system. Key management involves:

- **key generation** : it should be impossible to predict future key selections from a historical sequence. Known "weak keys" should be avoided;
- **key distribution** : transporting the keys to the participants should be performed in a secure way. Synchronisation of the use of new keys should be guaranteed;
- **key storage** : it should be impossible for an attacker to extract encryption keys from solid state or magnetic storage. The means of injecting the keys to storage should also be secure;

- **key destruction** : to reduce the possibility of an attacker deciphering recorded historical information, expired keys should be treated securely.

12.4.2.5 Combining symmetric and asymmetric encryption

Symmetric encryption is fast but makes key distribution hard. Public key methods, on the other hand, require enormous key values and a great deal of processing power. For this reason, they are better suited to protecting small volumes of data. A combination of the two approaches may provide the best overall solution to encryption and key management.

Say, for example, that Bob and Alice want to share some private information. Using a symmetric method and a secret key known only to him:-

- Bob encrypts the information and places the resulting *encrypted information* in file-1;
- Bob then transmits file-1 to Alice;
- using an asymmetric method and Alice's public key, Bob then encrypts the secret key and places the resulting *encrypted key* in file-2;
- Bob then transmits file-2 to Alice. Only Alice's private key can now decrypt the secret key sent to her by Bob in file-2;
- Alice decrypts the secret key held in file-2 using her secret key;
- once file-2 is decrypted Alice will know the secret key used by Bob and will be able to decrypt the information he sent her in file-1.

12.4.3 Authentication

If it is decided that confidentiality of a message is not a prime concern but that its integrity is (e.g. transferring a sum of money), it may be appropriate to transmit the message in plain text and to provide some means of detecting any change in the text. Authentication techniques provide this capability.

Authentication normally works by providing some form of algorithm to compress the message into a manageable parameter (the "Message Authentication Code" or MAC); the MAC can then be protected by encrypting it before appending it to the message. If the receiver can subsequently perform the same compression and compare the resulting MAC with that attached to the message, he can obtain assurance that the message has not been altered since it left its point of origin. He can also obtain assurance that it originated from a valid person based on the secrecy of the key that the sender used to encrypt the MAC. This is the principle of the *digital signature*.

The security services that are required to be provided by a digital signature are thus :-

- proof of origin - the recipient of a message must be sure of the origin of the message;

- message integrity - the recipient of the message must be sure that the message has not been accidentally or deliberately modified since it left its point of origin;
- non-repudiation - that one of the parties involved in a transaction should not, at some later date, be able to deny their involvement.

Essentially the non-repudiation requirement means that in the event of a dispute between communicating parties a trusted third party (an "Arbiter") can determine their respective involvements. For instance, an organisation who send an order to their supplier by EDI should not subsequently be able to claim that they did not send it; while if the supplier failed to process the order claiming that it had not been received, it may be equally important to the sender to be able to prove that the order was in fact received. In communications security these particular problems are referred to as "non-repudiation of origin" and "non-repudiation of receipt".

Proof of origin and message integrity can be provided by digital signature. However use of a symmetric encryption algorithm gives rise to the problem that, as both sender and recipient share the same secret key, an arbiter cannot subsequently decide which of them actually computed the MAC as both have equal capability. This opens the possibility of claims of forgery by the recipient.

Thus the essential characteristic of a digital signature must be that it can only be produced by the sender; if the signature subsequently needs to be verified, it can be proved to an arbiter that only the sender could have produced it. This requirement can be satisfied using asymmetric encryption in which the sender encrypts the MAC using their secret key, while the recipient decrypts the MAC using the sender's public key.

Proving that the sender did in fact receive the message is more problematic and involves the intervention of an arbiter in the transaction. If the arbiter is placed between the communicating parties he can intercept, and digitally sign (or "certify"), messages from the sender before relaying them to the recipient.

Although this level of formality is not normally used in EDI transactions, in systems that use a network supplier to provide a store and forward facility (i.e. an electronic mailbox) the supplier should be able to fulfil the role of arbiter and prove, if required, exactly when traffic was received into a recipient's mailbox, and when the recipient collected it, thus providing assurance on message delivery.

12.4.4 Trusted third parties

As already mentioned, the implementation of some IT security measures requires an independent third party to play a role. In addition to confirming that messages were sent or received at a given time, other functions that a trusted third party might perform include providing certified copies of public keys and confirming ownership.

12.4.4.1 Certification authorities

The widespread use of asymmetric encryption requires a "Public Key Infrastructure" which can provide reliable copies of a given user's public key. There is always a risk that someone wishing to forge messages from a particular user will arrange for recipients to receive a false public key for that user. . In that case the malefactor will have generated a public/private key pair and kept the private key to himself, so that he will be able to decipher any messages that are encrypted with the false public key. If users are going to rely upon digital signatures then they require a means of gaining an assurance that the public keys they receive are valid; an independent third party is needed to gain this assurance.

The body that provides reliable copies of public keys is known as a "Certification Authority" or CA. The role of the CA is defined in the ISO standard for directory services (X.500). The idea is that each CA will have its own public / private key pair and that the public key will be distributed to users securely (perhaps by courier). The following process can then provide a user with a "guaranteed" copy of someone else's public key:

- a user sends a request for the public key associated with a user identifier to the CA;
- the CA looks up the user identifier and extracts the public key;
- the CA encrypts the public key using the CA's private key to produce a certificate which is returned to the user; and
- the user decrypts the certificate using the CA's public key and extracts the public key that was requested.

The standards provide for CAs to be organised in a hierarchy so that the database of user details can be distributed and one CA can provide another with information.

12.4.4.2 Recorded delivery

If a message is important, then both sender and recipient may have an interest in establishing evidence of the time that it is sent and the time that it is received. Where messages are routed through a trusted third party this can assist in establishing the necessary evidence as the third party can keep a log messages.

This kind of service is commonly provided by Value Added Networks (VANs) that support Electronic Data Interchange (EDI).

13 Audit considerations

It is impossible to write a detailed audit programme without a comprehensive knowledge of the client's business and of both the geographical distribution and the technical aspects of their IT systems. However, the following guidelines on the

overall management of IT security should apply to most organisations that make use of IT.

The following requirements should be met:-

a) **A fully documented IT security policy**: IT security starts with a comprehensive and clearly written (i.e. it must be understood to all) directive issued by the Board. It should demonstrate their support and commitment to IT security, and should be available to all employees.

b) **There should be a security organisation**: there should be a framework to management IT security within the organisation. This management forum should approve and review IT security policies, assign security roles (these need not be full time jobs) and co-ordinate the implementation of IT security. Ideally, specialist security advice should be sought, and contacts with external security specialists - particularly on the more technical aspects of IT security - developed.

c) **A risk assessment should be performed and reported in a form that general management can readily understand** : It should be encompassing in the sense that it covers the use of IT within all organisational units

d) **IT assets should be controlled and, where applicable, classified**: in order to maintain appropriate protection, all IT assets (hardware, software, data communications equipment, system and user documentation and data) should be accounted for and have a nominated "owner". An inventory of each asset should be maintained and, where applicable, provide each with a security classification to indicate its status for IT security purposes.

e) **Personnel security procedures should be defined**: in order to reduce human error, theft, fraud and misuse of IT facilities, an effective recruitment process, which includes a rigorous screening process, is essential. Prospective employees should be made aware of the organisation's IT security policy and should sign a confidential ("non-disclosure") agreement.

f) **All employees should be aware of IT security risks and what is expected of them**: IT security is, to a greater or lesser extent, everyone's responsibility. The organisation should have an on-going IT awareness training programme in operation that is designed to alert all employees to the risks that failure to maintain adequate standards of IT security can bring about. The programme should teach good security practice and contribute

to the maintenance of a "security culture" within the organisation.

g) **There should be adequate standards of physical security:** prevention of unauthorised access, damage and interference to critical and sensitive activities should be supported by defined perimeters within which there are secure areas guarded by entry controls. All IT equipment, power and telecommunications cabling should be protected from interception, damage, power failure and other electrical problems (e.g. spikes, electrical noise, low voltages, lightening strikes).

h) **Computers and networks should be securely managed**: correct and secure operations of computers and network facilities should be established with, among other things, clearly documented operating procedures. Job rotation coupled with a segregation of duties (both around and within IT systems) should be established in order to minimise the risk of both negligent and deliberate system misuse.

i) **There should be procedures for backing up and restoring computer systems**: it is essential that advanced planning and preparation insure against risks of system failure, and that the integrity of and availability of data and software are adequately safeguarded. Computer systems must be backed up at a frequency that is appropriate to business needs, and at least one complete copy of the backup including key documentation held in a secure remote store. The organisation should prove, periodically, that systems can be restored from backup copies.

j) **Logical access to business systems should be controlled**: unauthorised access to business systems must be prevented. Methods of achieving this include formal registration and de-registration procedures for access to all multi-user IT services; a secure logon process; an effective password system and, if necessary, a duress alarm system for users who may be the target of coercion. Unauthorised activities should be detected, prevented and also monitored via audit trails.

k) **IT security should be "built in" to new systems and included in systems that are bought**: prior to the development or purchase of IT systems, an analysis of IT security requirements should be carried out to ensure that they provide an appropriate level of security. Means of preventing loss, modification or misuse of data should be designed into applications via audit trails and data encryption for highly sensitive information. Such countermeasures ensure that

applications are substantially cheaper and more effective in operation.

1. Proper software development procedures should be in place. These include test, acceptance, and installation procedures. These procedures should ensure that only authorised software is installed and that all installed software complies with the corresponding requirements.

   l) **Business continuity planning**: (this subject is covered in greater detail in the INTOSAI module on business continuity planning) to counteract interruptions to business activities stemming from prolonged system failure or environmental problems such as fire or severe weather, a Business Continuity Plan should be available to protect key business processes. Such a plan should include measures to identify and reduce risks, limit the consequences should a threat be realised, and ensure the speedy resumption of essential business operations. To ensure that it is workable (a plan that isn't workable is of no value), the Plan should be tested periodically. It must also be maintained to take account of changes in business systems. In fact, these tests should prove that the most critical business processes can indeed be resumed.

   m) **Incident reporting and investigation**: the IT security policy should mandate that all incidents which contravene its requirements are promptly reported to a central point and, where necessary, are investigated by a competent person who is managerially independent of the System Owner involved (e.g. the IT Security Manager or Internal Audit). Suitably categorised records of security incidents should be maintained and periodically analysed to detect weaknesses in policy implementation and any emerging trends.

   n) **Compliance**: to help ensure that the Board do not have a false sense of security based on policy that has not been adequately implemented, the above requirements should be subject to an annual audit carried out by a competent person(s) who is managerially independent of system owners or others who are tasked with implementing IT security policy. The resulting report should be presented directly to the Board.

Annex 1: Glossary of terms

Some of the terms used in relation to risk analysis may require clarification:

Accountability	A system supports accountability if records are kept of who did what and when. In a computer system this will only be possible if every user has a unique identifier, it is hard for someone else to pretend to be someone else, actions are logged and logs are protected from unauthorised amendment.
Asset	An asset is anything that is of value; this includes people, information, computers, buildings, communications links and computer software.
Accountability	Accountability is the ability to hold an individual responsible for an action. It is only possible if a system supports a strong means of uniquely identifying individuals, authenticating a claimed identity, logging significant actions, protecting logs, retaining logs and providing a means for authorised personnel to interrogate the logs.
Authenticity	Authentication involves gaining assurance that something is genuine. The purpose of a password, for example, is to help to ensure that someone is who they claim to be. Paper money usually has a number of authentication mechanisms built into it such as watermarks, metal strips and special printing. The equivalent for an electronic document might be a digital signature.
Availability	The property of being accessible to authorised users when and where required. Availability involves planning for the delivery of an acceptable level of service in the event of a system failing or being destroyed.
B2B	Communication and transactions between two business partners, mainly over the Internet
B2C	Communication and transactions between businesses and customers, mainly over the Internet.
BSI	British Standards Institute - the national body that issues British Standards and contributes to the International Standards Organisation.
Conditions of connection	Conditions of connection set out the responsibilities of a user of a networked service.
Confidentiality	The property of being accessible only to those who are authorised. Confidentiality involves keeping information secret.
Countermeasure	A control which helps to reduce the level of a threat, reduce vulnerability to a threat, reduce the impact of a threat affecting

	the system. Countermeasures may be preventive, detective or remedial.
Denial of Service Attack (DoS)	An attempt to flood a communications connection with bogus requests for services, thus preventing or limiting real users from using the service connection.
Digital signature	The result of producing a message digest and then encrypting it with a key known only to the signatory. Recipients can check the signature by producing their own message digest, decrypting the signature and then comparing the two digests. If the comparison succeeds then the recipient gains an assurance that the document did indeed come from the signatory and that it has not been altered since it was signed.
EDI	Electronic Data Interchange is the exchange of structured electronic information between organisations; a wide range of formats have been defined by ANSI X.12 and EDIFACT but a typical example is the exchange of orders and invoices.
Impact	The result of a security incident. The immediate impact of the theft of a computer might be the cost of replacement and unavailability of the data stored on it but there may be more serious consequences in terms of disruption to the business or the disclosure of sensitive information.
Incident	A security incident is any event which causes a negative impact on the business.
Information system (IS)	An information system includes any computer system that may be involved in delivery of a service but also extends to voice communications and paper records.
Integrity	The property that information or systems have not been altered or destroyed in an unauthorised manner.
Interchange agreement	Interchange Agreements (often abbreviated to ICA) set out preconditions for the exchange of electronic information between two organisations. EDI relationships are often based on an ICA.
ISO	International Standards Organisation - a body that sets world-wide standards on, amongst other things, information system security. The security related committees are called SC27 and SC21.
IT	Information Technology includes computers, software and telecommunications systems.
IS security	All aspects of defining, achieving and maintaining confidentiality, integrity and availability of information systems
Load testing	Load testing involves subjecting a system or system component

	to stress by placing it in a test environment that simulates the demands that will be placed upon it in the live system. This may extend to deliberately overloading the system (stress testing) until it fails to demonstrate the degree to which capacity exceeds the expected level of demand.
Message digest	A number derived by applying a mathematical process to a document in such a way that a different number would be produced if the document were altered. Keeping an independent record of a message digest and later comparing it to one that has been newly computed provides an assurance that a document has not been changed in the intervening period.
Penetration testing	Penetration testing involves employing a team of independent experts to attempt to deliberately breach the confidentiality, integrity or availability of a system by attacking it.
Risk	Risk is derived from a consideration of the types and magnitudes of threats facing a business and the likelihood and magnitude of adverse consequences arising if a threat occurred. Risk is thus related to threats, vulnerabilities and business impacts resulting from unauthorised modification, destruction or disclosure.
Residual risk	The risk that remains after safeguards (countermeasures) have been implemented.
Signing	See digital signature.
SLA	A Service Level Agreement is a contract between a service supplier and customer that specifies the quality of the service to be provided and the rights and duties of both supplier and customer.
Stress testing	Deliberately overloading a system until it fails.
Threat	Threats are events which, if they occur, will adversely affect the business by causing impacts such as disruption, loss of revenue, personal injury, embarrassment or legal liability.
Vulnerability	Vulnerabilities are features of a particular class of entities or services which make it more likely that adverse impacts will result if a threat occurs. Radio broadcasts are, for example, vulnerable to the threat of unauthorised interception.

Annex 2: Examples of risk analysis methodologies

(a) Examples of automated methodologies

The following is a brief description of two examples of computer-assisted risk analysis methods.

CRAMM

CRAMM was originally developed by the central Computer and Telecommunications Agency (the CCTA) during the 1980s for use in UK government departments. It has been updated and refined on several occasions - version 3 was released at the end of 1995 - and is now available world wide on the open market.

CRAMM adopts a staged approach to risk assessment and risk management.

Stage 1 in a CRAMM review involves identifying and valuing the information system (IS) assets within the review boundary. The package records all the physical and data assets within the boundary of the review. Physical assets are valued at replacement cost. Data assets are valued by asking the key users of the data to consider the worst scenario that could result from loss, modification or disclosure of the information that they use. Their conclusions are converted to a score within the range 1 to 10 using ten separate scales covering :-

- political or corporate embarrassment
- loss of commercial confidentiality
- infringement of personal privacy
- personal safety hazards
- failure to meet legal obligations
- financial loss
- disruption of user activities.

Stage 2 begins be establishing the chain of IS assets that have to be in place for each user to get the information that they require. The CRAMM software support tool prints out the appropriate threat and vulnerability questionnaires for each asset to be examined. The questionnaires contain weighted multiple choice questions the answers to which are input to the package to enable it to arrive at an assessment of the threats facing the assets under review and the degree to which the asset is vulnerable to the threats.

Stage 3 deals with risk management. The expert system within CRAMM prints out a list of the countermeasures which are appropriate to the results of the data valuation, and threat and vulnerability analysis. The security reviewer then determines which countermeasures have already been installed and feeds the results back to the package. From this information CRAMM can generate management reports including a prioritised list of countermeasures which need to be installed.

The CRAMM software supports ‘what if’ calculations. The reviewer can alter the assets in the system to see what effect this has on the recommended countermeasures, a feature that is particularly useful in helping to decide whether it is worth removing a sensitive application from a system which in other respects supports non-sensitive applications. CRAMM can also backtrack through each stage to enable the reviewer to examine the basis for recommended countermeasures.

MARION

MARION is a French package (also available in English) that is widely used in Europe and is supported world-wide by consultancy firms.

The method, which is software supported, takes a staged approach to risk analysis and risk management.

Stage 1 identifies major risks to the business and quantifies the potential loss. The reviewer uses structured interviews to provide MARION with a risk profile.

Stage 2 involves examining the business profile to determine maximum acceptable loss. This is used to identify major incidents from which the business must be protected.

Stage 3 gathers information on the current level of security. The software presents the results of stages one to three in both graphical and tabular form showing key areas of vulnerability.

Stage 4 involves the identification of factors which impede improvements to security and helps to build a portfolio of countermeasures balanced between those which seek to prevent disasters occurring and those which aid recovery from disasters that have occurred.

Stages 5 and 6 produce a prioritised list of the security measures that should be introduced and an action programme. The effect of introducing one or more of the proposed measures can be displayed graphically.

(b) Examples of manual methodologies

The following two methods are primarily manual, in that they do not comprise purpose built software to assist in the production and processing of interview questionnaires, management reports, or recommended countermeasures. However, spreadsheets can easily be adapted to improve presentation and provide limited document control.

INTOSAI : Information System Review Method

This methodology was issued by the EDP Audit Committee in October 1995.

The methodology comprises general guidance on IT security, a risk analysis method (together with pro-formas) and guidance on countermeasure selection.

The INTOSAI methodology adopts a five stage approach to risk analysis :-

1. **Sensitivity statement and security classification :** assess the sensitivity of program administrative information systems used in the organisation, and determine their security classification. The methodology contains a pro-forma questionnaire to assist the documentation process. Based on the information gathered, the review team are required to estimate the criticality of each system reviewed on a 1 to 5 scale (5 = very critical), and in respect of each of its confidentiality, integrity and availability requirements. The team are also required to assess the percentage of system data that falls into the categories “basic security standards”, “protected” and “classified”.

2. **Business impact assessment :** involves determining possible business impacts to the organisation if the system’s information were to be disclosed, integrity compromised, or service disrupted. Impact is measured in terms of being “very serious”, “serious” or “less serious”.

3. **Threat and probability assessment :** involves determining the probability that identified threats could succeed in attacking the system. Assessments are measured as being “high”, “medium” or “low”.

4. **Security exposure rating :** business impacts and probability are brought together on an “exposure rating chart” (see below) to determine the overall exposure rating (of the system under review) to the organisation.

5. **Security decision and recommended action :** the final step is to bring all the summarised information together on a “summary of assessments form” (provided by the method). This information forms the basis for taking decisions on countermeasure implementation.

Exposure rating chart

Business impact / Probability	Very Serious	Serious	Less Serious
High	**9**	**8**	**4**
Medium	**7**	**6**	**3**
Low	**5**	**2**	**1**

CRISP (Computer Risk Identification Security Planner)

The **Further Education Funding Council for Wales** have developed a Good Practice Guide to Computer Security. The Computer Security Guide (which is one of a set of guides on financial management) is designed to enable the educational institutions that come within the Council's control to implement cost effective computer security within their organisations. In common with the automated methodologies described above, the Guide takes a staged approach to the task of identifying and managing risks in computer systems. Each of the four stages comprises a number of distinct steps, which address the following broad questions :-

Stage 1 - *where are we now?* The review team complete a systematic review of the organisation's present computer security arrangements. *A CRISP review is carried out during stage 1.*

Stage 2 - *where do we want to be?* The review team identify the different computer security controls relevant to meeting the organisation's requirements. This will include a need to introduce staff awareness, contingency planning and disaster recovery arrangements.

Stage 3 - *how do we get there?* During this stage, effective computer security arrangements covering hardware, communications, software and data are implemented.

Stage 4 - *how do we stay there?* Management controls are implemented to support the availability, security and integrity of the organisation's IS facilities.

CRISP has been designed to provide a systematic identification and ranking of the computer security risks facing the delivery of IS services. The information provided by CRISP (together with countermeasure guidelines contained in the Guide) assists the review team to determine what additional countermeasures are required to provide an adequate level of security. CRISP takes an empirical approach to assessing overall risk which is partly based on the organisation's previous experience.

The following table illustrates how security information is presented in a CRISP report. In this example the risk of *'disruption through static electricity'* is considered.

Risk to Computer Equipment, Software and Communications	Control Element	Current Safeguards in Place	Risk Matrix A	B	C	D	Total Risk Rating (A+B+C+D)	Proposed Future Actions and Solutions	Cost of Solut-ion
Disruption through static electricity	Environmental	Anti-static carpets in all offices	1 1		1	1	4	Anti-static precautions to be considered on any new IT acquisitions	N/A
etc. etc.									

Notes

Risk to Computer Equipment, Software and Communications : *a brief indication of the nature of the computer security risk and disruption identified. All potential risks should be assessed. A record/log of all matters relating to breaches in computer security should be kept in order to assist future assessments/reviews.*

Control Element : *CRISP recognises three security elements; environmental controls (including physical access), logical access control and application controls. The grouping of all similar risks under the appropriate control element will enable a comprehensive range of controls and procedures to be put in place.*

Current Safeguards in Place : *a brief statement of any existing countermeasures. An assessment of the effectiveness of the existing countermeasures needs to be undertaken to assist the subsequent risk management exercise.*

Risk Matrix : *the actual measures are for each organisation to determine in the light of their experience. A suggested matrix could include the following elements :-*

Category	Element	Scale	Key
A	Past occurrence - has this risk occurred before?	1 or 3	1 = not occurred 3 = has occurred
B	Adequacy of existing countermeasures against this particular risk	1 to 5	1 = very adequate 5 = very inadequate
C	Future occurrence - an assessment of the likelihood/frequency of the risk re-occurring	1 to 5	1 = very unlikely 5 = very likely
D	Potential disruptive impact - an assessment of the operational impact should the risk re-occur	1 to 5	1 = no long term impact 5 = immediate operational impact

Total Risk Rating : *the totals (A, B, C and D) for each identified computer security risk are summed to provide an overall risk rating. The review team can use this information to prioritise the need for, and expenditure on, countermeasures.*

Proposed Future Actions and Solutions : *the most cost-effective and appropriate safeguards should be identified by the review team - the Guide gives some assistance by describing a range of baseline countermeasures.*

Cost of Solution : *finally, in recognition of the fact that the security budget is finite, the cost of remedial action is estimated.*

"Computer Security" is available (cost £6-00) from :-

The Further Education Development Agency (Publications), Coombe Lodge, Blagdon, BRISTOL BS18 6RG, U.K.

Annexe 1 – Summary of Controls for Low, Moderate and High Baselines as per NIST' SP 800 53 Publication

CNTL NO.	CONTROL NAME	LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)

Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4 (1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5

CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2)
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1

IA-2	User Identification and Authentication	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6

Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	Not Selected	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1) (2)	MP-5 (1) (2) (3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	Not Selected	PE-4
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12

PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7

PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8

SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
System and Communications Protection				
SC-1	System and Communications Protection Policy	SC-1	SC-1	SC-1

	and Procedures			
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information Remnance	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-	Voice Over Internet Protocol	Not	SC-19	SC-19

19		Selected		
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6

SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1) (2)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

Annex 3: Sample IT security standards

THE AUSTRALIAN NATIONAL UNIVERSITY

STATEMENT ON UNIVERSITY INFORMATION TECHNOLOGY SECURITY

[This section is from The Australian National University document ITS 2194/1999 'University IT Security Policy' of November 1999]

INTRODUCTION

1. This Statement sets out University policy on Information Technology (IT) Security and procedures for implementation of that policy including monitoring and reporting of security incidents. IT Security is the process that ensures the availability, integrity and confidentiality of IT systems. [See Appendix for definitions.]

2. University IT systems and the services they support are provided to further the objectives of the University and are integral to the ability of the University to effectively carry out its operations.

3. IT security is essential to ensuring that IT services are delivered to all users in an environment in which the University's obligations for security, privacy and intellectual property rights are met.

4. The University's policy on IT security applies to all members of the University community in their interactions with any IT system, operated either by the University or any other agency, while acting in their capacity as a member of the University community or while using University IT services. Members of the University community who use Public Access IT services are also obliged to respect University IT security policy.

5. The University recognises that successful implementation of IT security measures relies on having a well-informed user [see Appendix] community combined with effective management procedures.

POLICY

6. The University's Policy on IT Security is as follows:

6.1 **Management**

University IT systems, and the services they deliver, will be protected by effective management of IT security risks at all levels of the University.

University IT systems will be provided, managed and operated in such a way that:

a) specific objectives and security requirements regarding availability, confidentiality and integrity of each IT system are met;

b) the legal obligations of the University are met;

c) every effort is made to protect copyright, licensing conditions and intellectual property rights of the University and third parties.

6.2 **Access**

In accordance with the University's policy on access to University-provided IT systems, users may access and use only those University IT systems:

a) for which they have been individually authorised by the manager of that system;

b) for which they have been granted access by virtue of their affiliation with the University; or

c) that operate as a Public Access IT service.

6.3 **User Responsibilities**

Users of IT systems are accountable for their own behaviour and are personally responsible for:

a) understanding and adhering to University IT security policy;

b) complying with all official notices regarding the terms and conditions applying to use ~~of~~ IT services provided by the University;

c) complying with relevant University policies, Statutes, Rules and Orders;

d) notifying any breach of local or University IT security to the manager of the IT system or the Director IT Services..

6.4 **Information and Training**

Information about the existence and general extent of policies, requirements, measures and procedures for the security of University IT systems will be readily available to all users. The University will provide IT security awareness, training and support services to allow users to acquire the information and develop the skills needed to carry out their obligations under paragraph 6.3.

6.5 **Breaches**

Breaches of this Policy may be dealt with under the relevant Statutes, Rules and Orders of the University. In addition, the University may advise law enforcement agencies when it considers that a criminal offence may have been committed. The Australian National University Information Technology Services Rules, Discipline Rules and relevant industrial awards contain provisions which will be used to deal with users in breach of this policy.

Deans, directors and other heads of areas, through their nominated IT system managers, are responsible for addressing breaches of IT security. Failure to address security breaches may result in disconnection of relevant IT systems from the Campus Network [see Appendix]

6.6 **Monitoring**

Where monitoring of IT security involves the activities of an individual user or access to information stored on IT systems by users, it will be carried out in accordance with the University's Privacy Policy and in a manner which respects the rights and legitimate interests of those concerned, including the University.

IMPLEMENTATION OF UNIVERSITY IT SECURITY POLICY

7. Responsibity for Implementation of IT Security

The **Director, IT Services** is responsible for:

a) carriage of University IT security policy;

b) providing campus-wide support services;

c) assisting managers of IT systems in the development and provision of IT security awareness and training programs;

d) issuing guidelines, with the approval of the IT Strategy Committee, for the secure operation of specific aspects of University IT systems;

e) authorising the disconnection from or restricted access to the Campus Network of any IT system or area in which it operates that fails to comply with IT security policy or relevant guidelines;

f) determining the effectiveness of IT security measures through regular monitoring programs;

g) reporting annually to the IT Strategy Committee on security incidents and implementation of University IT Security Policy.

Deans of Faculties, Heads of Research Schools, the University Librarian, Heads of Centres, Divisions and Units and Heads of IT Services Agencies.

Each of the above officers is responsible for:

a) appointing a manager for each IT system connected to the Campus Network and for advising the Director, IT Services of the name of this officer. Areas which wish to appoint a systems administrator or manager who is not a member of the University staff must seek the approval of the Director, IT Services;

b) developing an IT security program for each Faculty, School, Centre, Division or Unit and providing the Director, IT Services with a copy of the program;

c) ensuring security incidents and breaches of security are dealt with in a co-ordinated and timely manner and reported to the Director, IT Services.

Managers of University IT Systems are responsible for:

a) developing, operating and managing those IT systems in accordance with University IT security policy and relevant guidelines, and the requirements of deans, directors and heads of other areas;

b) maintaining and operating IT systems in a manner which effectively balances IT security with users need to use them free from undue intervention;

c) maintaining IT security awareness by provision of information and training on IT security to users of those IT systems which they manage;

d) periodically monitoring and reassessing their IT security measures to ensure their effectiveness and to respond to changes in requirements;

e) reporting all security incidents to the Director, IT Services, immediately it is known that a breach has occurred.

The Audit Coordinator, in consultation with the Director, IT Services, will undertake audits to gauge the effectiveness of IT security measures.

Appendix: DEFINITIONS

Campus Network

The Campus Network comprises:

- the inter-building and off campus network links comprising the Campus Backbone Network;
- network cabling and other transmission media up to and including wall outlets and other access points that are connected to the Campus Backbone Network;
- equipment associated with the low level data transfer on the above;
- low level services associated with the operation of the network infrastructure. The above definitions apply independently of how any item is funded, installed or operated.

IT system

An IT system is:

- a related set of hardware, software used for the communication, processing and storage of information;
- the electronic form (not content) of information that they hold or process. University IT systems connect to and in some cases deliver services across the Campus Network, but are not part of the Campus Network. This definition includes, but is not limited to, computers and their peripherals and other communication equipment, communication networks and other telecommunication facilities used to link such equipment together, the operating software used on all such equipment, and the people involved in the maintenance and administration of the equipment.

User

means a person who accesses University IT services and systems whether that access is from within the University or from outside of the University.



Please direct enquiries regarding this page to the Webmaster.
The information on this page was updated on Tue, 16 Nov 1999. The page has been authorised by the Director, Information Infrastructure Services as relevant officer.
© 2000 The Australian National University

Author: Executive Assistant, IT Services

Date Last Modified: Thu, 6 Jun 1996

Feedback: please direct comments about this page to

URL: http://cais.anu.edu.au/Admin/ITServices/Policies/security.html