IS/ISO/IEC 13335-1 (2004): Information Technology - Security Techniques - Management of Information and Communications Technology Security, Part 1: Concepts and Models for Information and Communications Technology Security Management [LITD 17: Information Systems Security and Biometrics]

BLANK PAGE

IS/ISO/IEC 13335-1 : 2004

भारतीय मानक

सूचना प्रौद्योगिकी — सुरक्षा तकनीक सूचना एवं संचार प्रौद्योगिकी सुरक्षा का प्रबन्धन

भाग 1 सूचना एवं संचार प्रौद्योगिकी सुरक्षा प्रबन्धन की धारणा और प्रतिरुप

Indian Standard

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — MANAGEMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

PART 1 CONCEPTS AND MODELS FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY MANAGEMENT

ICS 35.040

BUREAU OF INDIAN STANDARDS
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI 110002

December 2009 **Price Group 10**

Information Systems Security and Biometrics Sectional Committee, LITD 17

NATIONAL FOREWORD

This Indian Standard (Part 1) which is identical with ISO/IEC 13335-1 : 2004 'Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management' issued by the Joint Technical Committee ISO/IEC JTC 1 of International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) jointly was adopted by the Bureau of Indian Standards on the recommendation of the Information Systems Security and Biometrics Sectional Committee and approval of the Electronics and Information Technology Division Council.

The text of ISO/IEC Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker in the International Standard while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

Indian Standard

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — MANAGEMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

PART 1 CONCEPTS AND MODELS FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY MANAGEMENT

1 Scope

ISO/IEC 13335 contains guidance on the management of ICT security. Part 1 of ISO/IEC 13335 presents the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security.

It is not the intent of this International Standard to suggest a particular management approach to ICT security. Instead ISO/IEC 13335-1 contains a general discussion of useful concepts and models for the management of ICT security. This material is general and applicable to many different styles of management and organizational environments. It is organized in a manner that allows the tailoring of the material to meet the needs of an organization and its specific management style.

2 Definitions

For the purpose of this document and the other Parts of 13335, the following terms and definitions apply. The following terms are derived from all parts of ISO/IEC 13335 and ISO/IEC 17799. Any deviation from the definitions found in these references derives from the specific usage in ISO/IEC 13335 concerning the IT security environment.

2.1
accountability
the property that ensures that the actions of an entity may be traced uniquely to the entity
[ISO/IEC 7498-2]

2.2
asset
anything that has value to the organization

2.3
authenticity
the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information

2.4
availability
the property of being accessible and usable upon demand by an authorized entity
[ISO/IEC 7498-2]

2.5
baseline controls
a minimum set of safeguards established for a system or organization

2.6
confidentiality
the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
[ISO/IEC 7498-2]

2.7
control
in the context of ICT security, the term “control” may be considered synonymous with “safeguard”. See 2.24, “safeguard”

2.8
guidelines
a description that clarifies what should be done and how, to achieve the objectives set out in policies

2.9
impact
the result of an information security incident

2.10
information security incident
any unexpected or unwanted event that might cause a compromise of business activities or information security. Examples of information security incidents are:
- loss of service, equipment or facilities,
- system malfunctions or overloads,
- human errors,
- non-compliances with policies or guidelines,
- breaches of physical security arrangements,
- uncontrolled system changes,
- malfunctions of software or hardware, and
- access violations.

2.11
ICT security
all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability, of ICT

2.12
ICT security policy
rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its ICT systems

2.13
information processing facility(ies)
any information processing system, service or infrastructure, or the physical locations housing them

2.14
information security
all aspects related to defining, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, of information or information processing facilities

2.15
integrity
the property of safeguarding the accuracy and completeness of assets

2.16
non-repudiation
the ability to prove an action or event has taken place, so that this event or action cannot be repudiated later
[ISO/IEC 13888-1; ISO IS 7498-2]

2.17
reliability
the property of consistent intended behaviour and results

2.18
residual risk
the risk that remains after risk treatment

2.19
risk
the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence

2.20
risk analysis
the systematic process of estimating the magnitude of risks

2.21
risk assessment
the process of combining risk identification, risk analysis and risk evaluation

2.22
risk management
the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect ICT system resources

2.23
risk treatment
the process of selection and implementation of controls to modify risk

2.24
safeguard
a practice, procedure or mechanism that treats risk. Note that the term “safeguard” may be considered synonymous with the term “control”. See 2.7, “control”

2.25
threat
a potential cause of an incident that may result in harm to a system or organization

2.26
vulnerability
a weakness of an asset or group of assets that can be exploited by one or more threats

3 Security concepts and relationships

3.1 Security principles

The following high-level security principles are fundamental to the establishment of an effective ICT security program.

Risk management: Assets should be protected through the adoption of appropriate safeguards. Safeguards should be selected and managed on the basis of a suitable risk management methodology, which assesses the organization's assets, threats, vulnerabilities and the impact of threats occurring, to arrive at attendant risks and taking constraints into consideration.

Commitment: Organizational commitment to ICT security and risk management is essential. To gain commitment, the benefits of deploying ICT security should be specified.

Roles and responsibilities: Organizational management is responsible for securing assets. Roles and responsibilities for ICT security should be clarified and communicated.

Objectives, strategies and policies: ICT security risk should be managed in consideration of the organization's objectives, strategies and policies.

Lifecycle management: ICT security management should be continuous throughout the lifecycle of an organizational ICT asset.

The following sub-clauses describe at a high level the major security elements and their relationships that are involved in security management, in view of the fundamental security principles. Each of the elements is introduced, and the major contributing factors are identified. Part 2 of this International Standard provides an in-depth discussion of elements of risk, including threats, vulnerabilities and safeguards.

3.2 Assets

The proper management of assets is vital to the success of the organization, and is a major responsibility of all management levels. The assets of an organization may be considered valuable enough to warrant some degree of protection. These may include, without being limited to:

- physical assets (e.g., computer hardware, communications facilities, buildings),
- information / data (e.g., documents, databases),
- software,
- the ability to provide a product or service,
- people, and
- intangibles (e.g., goodwill, image).

From a security perspective, it is not possible to implement and maintain a successful security program if the assets of the organization are not identified. In many situations, the process of identifying assets and assigning a value can be accomplished at a very high level and may not require a costly, detailed, and time consuming exercise. The level of detail for this exercise should be measured in terms of time and cost versus the value of the assets. In any case, the level of detail should be determined on the basis of the security objectives.

Asset attributes to be considered include their value and/or sensitivity, and any safeguards present. Vulnerabilities in the presence of particular threats influence protection requirements for assets. The environments, cultures and legal systems in which the organization operates may affect assets and their attributes. For example, some cultures consider the protection of personal information as very important while others give a lower significance to this issue. These environmental, cultural and legal variations can be significant for international organizations and their use of ICT systems across international boundaries.

Based on an assessment of threats and vulnerabilities, and their combined impact, risk can be assessed and then safeguards applied to protect the assets as appropriate. An assessment of residual risk is then necessary to determine whether the assets are adequately protected.

3.3 Threats

Assets are subject to many kinds of threats. A threat has the potential to cause harm to an asset and therefore an organization. This harm can occur from an attack on the information being handled by an ICT system or service, on the system itself, or on other resources, e.g., by causing unauthorized destruction, disclosure, modification, corruption, and unavailability or loss. A threat needs to exploit an existing vulnerability of the asset in order to harm the asset. Threats may be of environmental or human origin and, in the latter case, may be either accidental or deliberate. Both accidental and deliberate threats should be identified and their level and probability of occurrence assessed. Statistical data are available concerning many types of environmental threats. Such data may be obtained and used by an organization while assessing threats.

Examples of threats are:

Human		Environmental
Deliberate	Accidental	Earthquake Lightning Floods Fire
Eavesdropping Information modification System hacking Malicious code Theft	Errors and omissions File deletion Incorrect routing Physical accidents	

Table 1 – Examples of threats

Threats may impact specific parts of an organization, for example disruption to computers. Some threats may be general to the surrounding environment in a particular location in which a system or organization exists, for example, damage to buildings from hurricanes or lightning. A threat may arise from within the organization, for example, sabotage by an employee, or from outside, for example, malicious hacking or industrial espionage. The amount of harm can vary widely for each occurrence of a threat. The harm may be of a temporary nature or may be permanent as in the case of the destruction of an asset.

Threats have characteristics that define their relationships with other security elements. These characteristics may include the following:

- source, i.e., insider vs. outsider,
- motivation, e.g. financial gain, competitive advantage,
- frequency of occurrence,
- likelihood, and
- impact.

Some threats may affect more than one asset. In such cases they may cause different impacts depending on which assets are affected. For example, a software virus on a stand-alone personal computer may have a limited or localized impact. However, the same software virus on a network based file server may have widespread impact.

The environments and cultures in which the organization is situated can have a significant bearing and influence on how the threats to the organization and to its assets are addressed. Some threats may not be considered harmful in some cultures. Aspects of environment and culture must be considered when addressing threats.

Threats may be qualified in terms such as High, Medium, and Low, depending on the outcome of threat assessment.

3.4 Vulnerabilities

A weakness of an asset, or group of assets, that can be exploited by one or more threats is known as a vulnerability. Vulnerabilities associated with assets include weaknesses in physical layout, organization, procedures, personnel, management, administration, hardware, software or information. Threats may exploit vulnerabilities to cause harm to the ICT system or business objectives. A vulnerability can exist in the absence of corresponding threats. A vulnerability in itself does not cause harm; a vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset. Vulnerabilities arising from different sources need to be considered, for example, those intrinsic or extrinsic to the asset. Vulnerabilities may remain unless the asset itself changes such that the vulnerability no longer applies. Vulnerabilities should be assessed both individually and in aggregate to consider the full operational context.

An example of a vulnerability is lack of access control, which could allow the threat of an intrusion to occur and assets to be lost.

Within a specific system or organization not all vulnerabilities will be susceptible to a threat. Vulnerabilities that have a corresponding threat are of immediate concern. However, as the environment can change unpredictably, all vulnerabilities should be monitored to identify those that have become exposed to new or re-emerging threats.

Vulnerability assessment is the examination of weaknesses that may be exploited by identified threats. This assessment must take into account the environment and existing safeguards. The measure of a vulnerability of a particular system or asset to a threat is a statement of the ease with which the system or asset may be harmed.

Vulnerabilities may be qualified in terms such as High, Medium, and Low, depending on the outcome of the vulnerability assessment.

3.5 Impact

Impact is the result of an information security incident, caused by a threat, which affects assets. The impact could be the destruction of certain assets, damage to the ICT system, and compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Possible indirect impact includes financial losses, and the loss of market share or company image. The measurement of impact permits a balance to be made between the anticipated results of an incident and the cost of the safeguards to protect against the incident. The probability of occurrence of an incident needs to be taken into account. This is particularly important when the amount of harm caused by each occurrence is low but where the aggregate effect of many incidents over time may be harmful. The assessment of impacts is an important element in the assessment of risks and the selection of safeguards.

Quantitative and qualitative measurements of impact can be achieved in a number of ways, such as:

- establishing the financial cost,
- assigning an empirical scale of severity, e.g., 1 through 10, and
- using adjectives selected from a predefined list, e.g., High, Medium, and Low.

3.6 Risk

Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. Single or multiple threats may exploit single or multiple vulnerabilities.

A risk scenario describes how a particular threat or group of threats may exploit a particular vulnerability or group of vulnerabilities that exposes assets to harm. The risk is characterized by a combination of two factors, the probability of the incident occurring and its impact. Any change to assets, threats, vulnerabilities and safeguards may have significant effects on risks. Early detection or knowledge of any changes increases the opportunity for appropriate actions to be taken to treat risk. Options for risk treatment include risk avoidance, risk reduction, risk transfer and risk acceptance.

Risk is never completely eliminated. Part of judging whether the security is appropriate to the needs of the organization is the acceptance of the residual risk. Management should be made aware of all residual risks in terms of impact and the probability of an incident occurring. The decision to accept residual risks must be taken by those who are in a position to accept the impact of incidents occurring and who can authorize the implementation of additional safeguards if the level of residual risk is not acceptable.

3.7 Safeguards

Safeguards are practices, procedures or mechanisms that may protect against a threat, reduce a vulnerability, limit the impact of an information security incident, detect incidents and facilitate recovery. Effective security usually requires a combination of different safeguards to provide layers of security to protect assets. For example, access control mechanisms applied to computers should be supported by audit controls, personnel procedures, training and physical security. Some safeguards may exist already as part of the environment, or as an inherent aspect of assets, or may be already in place in the system or organization.

An appropriate selection of safeguards is essential for a properly implemented security program. A safeguard can serve multiple purposes; conversely, one function may require several safeguards. Safeguards may be considered to perform one or more of the following functions:

- prevention,
- deterrence,
- detection,
- limitation,
- correction,

- recovery,
- monitoring, and
- awareness.

Some examples of areas where safeguards can be used include:

- physical environment,
- technical environment (hardware, software and communications),
- personnel, and
- administration.

Certain safeguards send a strong and clear message with regard to the organization's attitude towards security. In this regard, it is important to select safeguards that are not offensive to the culture and/or the society in which the organization operates.

Examples of specific safeguards are:

- policies and procedures,
- access control mechanisms,
- anti-virus software,
- encryption,
- digital signatures,
- monitoring and analysis tools,
- redundant power supplies, and
- backup copies of information.

3.8 Constraints

Constraints are normally set or recognized by the organization's management and influenced by the environment within which the organization operates. Some examples of constraints to be considered are:

- organizational,
- business,
- financial,
- environmental,
- personnel,
- time,
- legal,
- technical, and
- cultural/social.

These factors should be considered when selecting and implementing safeguards. Periodically, existing and new constraints should be reviewed and any changes identified. It should also be noted that constraints might change with time, geography, and social evolution, as well as organizational culture. The environment and culture in which the organization operates can have a bearing on several security elements, especially threats, risks, and safeguards.

3.9 Security element relationships

Security of ICT systems is a multi-dimensional discipline that can be viewed from different perspectives. Figure 1 presents a model that shows how assets are potentially subject to a number of threats. This collection of threats changes constantly over time and is only partially known. As well, the environment changes over time and this change may impact the nature of threats and the probability of their occurrence.

The model represents:

- an environment containing constraints and threats that change constantly and are only partially known,
- the assets of an organization,
- the vulnerabilities associated with those assets,
- safeguards selected to protect assets, and
- residual risks acceptable to the organization.

At least five scenarios are feasible and are illustrated in Figure 1. These scenarios include:

Scenario 1 – A safeguard (S) may be effective in reducing the risks (R) associated with a threat (T) capable of exploiting a vulnerability (V). A threat can only become effective if the asset is vulnerable to it.

Scenario 2 – A safeguard may be effective in reducing the risks associated with a threat exploiting multiple vulnerabilities.

Scenario 3 – Multiple safeguards may be effective in reducing the risks associated with multiple threats exploiting a vulnerability. Sometimes several safeguards are required to reduce risk to an acceptable level so that the residual risk (RR) is acceptable.

Scenario 4 – The risk is considered acceptable and no safeguards are implemented even if threats are present and a vulnerability exists.

Scenario 5 – A vulnerability exists but there are no known threats to exploit it.

Safeguards may be implemented to monitor the threat environment to ensure that no threats develop which can exploit the vulnerability. Constraints affect the selection of safeguards.

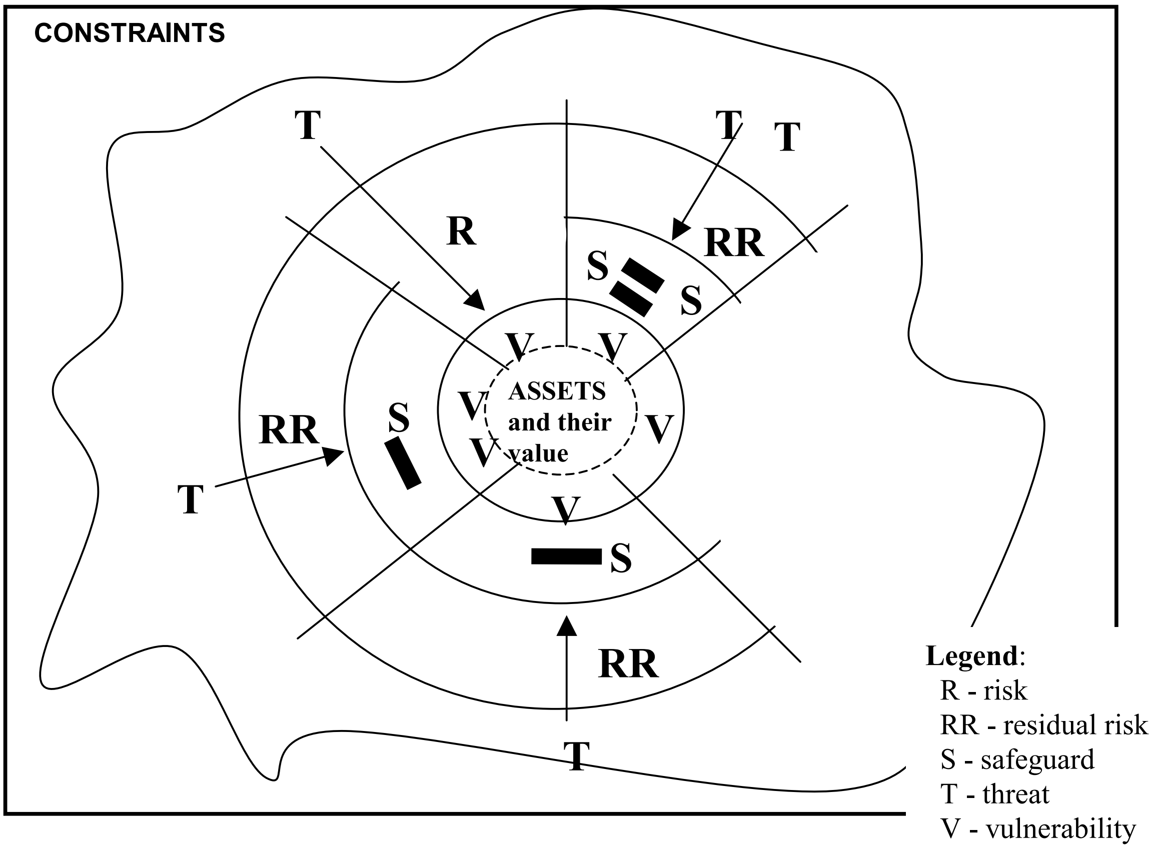


Figure 1 – Security element relationships

Any ICT system comprises assets (particularly information, but also hardware, software, communications services, etc.) that are important to the success of an organization's business. These assets have value to the organization, which is normally expressed in terms of the impact on business operations from unauthorized disclosure, modification or repudiation of information, or unavailability or destruction of information or service. The impact is first determined regardless of which threats might occur to cause the impact, to be sure of identifying the real values. Then the question of what threats might occur to cause such impact, and the probability of their occurrence, is addressed, i.e. assets could be subject to a number of threats. Then the question of what vulnerabilities (or weaknesses) might be exploited by the threats to cause the impact is addressed, i.e. threats could exploit vulnerabilities to expose assets. Each of these components, i.e. values, threats and vulnerabilities, can increase risk. Measures of risk will then indicate the overall protection requirement, which in real terms is effected or met by the implementation of safeguards. The implemented safeguards then reduce the risk, protect against threats and indeed can reduce vulnerabilities.

Figure 2 illustrates in a simpler model how some safeguards may be effective in reducing risks. Often, several safeguards are required to reduce the residual risks to an acceptable level. It is possible that no safeguards are implemented if the risk is considered acceptable.

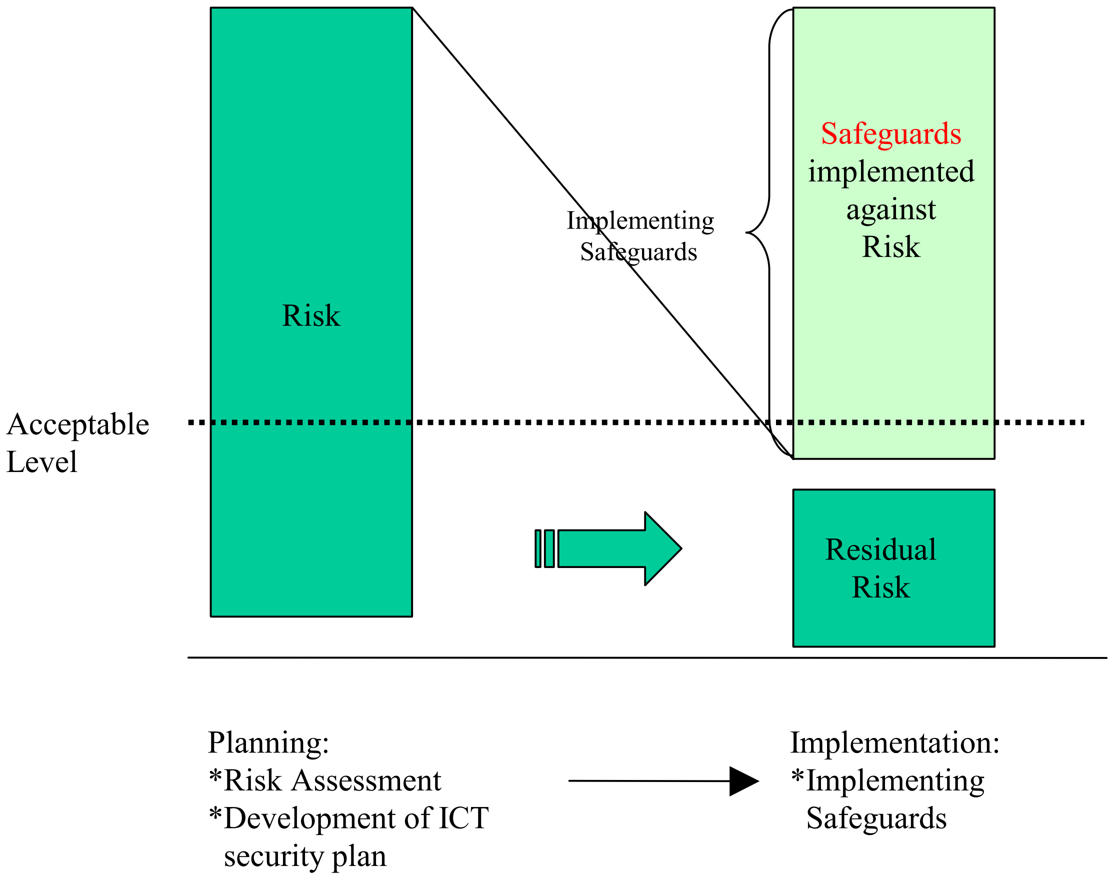


Figure 2 – Safeguard and risk relationships

4 Objectives, strategies and policies

Corporate security objectives, strategies and policies need to be formulated as the basis for effective ICT security in an organization. They support the business of the organization and together they ensure consistency between all safeguards. It is particularly important, to ensure such consistency, that objectives, strategies and policies be included as an integral part of security training and awareness programmes.

Objectives (what is to be achieved), strategies (how to achieve these objectives), policies (the rules to be observed in implementing the strategies), and procedures (the methods for implementing the policies) may be defined and developed hierarchically from the corporate to the operational levels of the organization and for each division, business unit or department. The directing documentation should reflect organizational requirements and take into account any organizational constraints. Consistency amongst the corresponding documents, although influenced by different points of view, and amongst the various levels of the organization, is important, since many threats (such as system hacking, file deletion and fire) are common business problems.

Furthermore, general corporate objectives, strategies and policies should be reflected and refined in detailed and specific objectives, policies and procedures in all areas of interest to the organization, such as financial management, personnel management – and security management. Security should then be further broken into its constituent parts (personnel, physical, information, ICT, etc.). The hierarchy of documentation should be maintained and updated based on the results of periodic security reviews (e.g., risk assessment, internal and/or external security audits) and changes in business objectives.

ICT system security objectives, strategies, policies and procedures should represent what is expected from the ICT system in terms of security. They are normally expressed using a natural language, but there may be a requirement to express them in a more formal way using some established language. The objectives, strategies, policies and procedures will establish the level of security for the organization and the threshold for risk acceptance.

4.1 ICT security objectives and strategy

After establishing the organization's ICT security objectives, an ICT security strategy should be developed to form a basis for the development of a corporate ICT security policy. The development of a corporate ICT security policy is essential to ensure that the results of the risk management process are appropriate and effective. Management support across the organization is required for the development and effective implementation of the policy. It is essential that a corporate ICT security policy takes into account the corporate objectives and particular aspects of the organization. It must be in alignment with the corporate security policy and the corporate business policy. With this alignment, the corporate ICT security policy will help to achieve the most effective use of resources, and will ensure a consistent approach to security across a range of different system environments.

It may be necessary to develop a separate and specific security policy for each or some of the ICT systems. These policies should be based on risk assessment and be consistent with the corporate ICT security policy, thus taking into account the security recommendations for the systems to which they relate.

As a first step in the process of managing ICT security, one should consider the question 'what broad level of risk is acceptable to the organization?' Accurate definition of acceptable risks, and thence the appropriate level of security, is the key to successful security management. The necessary broad level of security is determined by the ICT security objectives an organization needs to meet. In order to assess these security objectives, the organization's assets and their value should be considered. This should be determined by the importance that ICT has for supporting the conduct of the organization's business; the cost of ICT itself is only a small part of its value.

Possible questions for assessing how much an organization's business depends on ICT are:

- What are the important components of the business that cannot be carried out without ICT support?
- What are the tasks that can only be done with the help of ICT?
- What essential decisions depend on the confidentiality, integrity, availability, non-repudiation, accountability and authenticity of information stored or processed by ICT, or on how up-to-date this information is?
- What confidential information stored or processed needs to be protected?
- What are the implications of an information security incident for the organization?

Answering these questions can help to assess the ICT security objectives of an organization. If, for example, some important or very important components of the business are dependent on accurate or up-to-date information, then one of the ICT security objectives of this organization may be to ensure the integrity and timeliness of the information as it is stored and processed in the ICT systems. Also, important business objectives and their relation to security should be considered when assessing ICT security objectives.

Dependent on the ICT security objectives, a strategy for achieving these objectives should be agreed upon. The strategy chosen should be appropriate to the value of the assets to be protected. If, for example, the answers to one or more of the questions above indicates a strong reliance on ICT, then it is likely that the organization has high ICT security requirements, and it is advisable to choose a strategy that is sufficient to fulfill these requirements.

An ICT security strategy outlines in general terms how an organization will achieve its ICT security objectives. The topics such a strategy should address will depend on the number, type and importance of those objectives, and will normally be those that the organization considers important to address uniformly. The topics could be quite specific, or very broad, in nature.

As an example of a specific topic, an organization could have a primary ICT security objective that, because of the nature of its business, all of its systems should be continuously available. In this case, one strategy topic could be directed at minimizing virus infestation through organization-wide installation of anti-virus software.

As an example of a broader topic, an organization could have an ICT security objective, because its business is selling its ICT services, that the security of its own systems be proven to potential customers. In this case, a strategy topic could be security validation by a recognized third party.

Other possible topics for an ICT security strategy, because of specific objectives or combinations thereof, could include:

- risk assessment strategy and methods to be adopted organization-wide,
- ICT system security policy for each system,
- security operating procedures for each system,
- organization-wide information sensitivity categorization scheme,
- security awareness and training,
- security conditions of connections to be met, and checked, before other organizations are connected, and
- standard information security incident management scheme across the organization.

Once determined, the security strategy and its constituent topics should be encompassed in the corporate ICT security policy.

4.2 Policy hierarchy

The **corporate security policy** may comprise the security principles and directives for the organization as a whole. Corporate security policies should reflect the broader corporate policies, including those that address individual rights, legal requirements and standards.

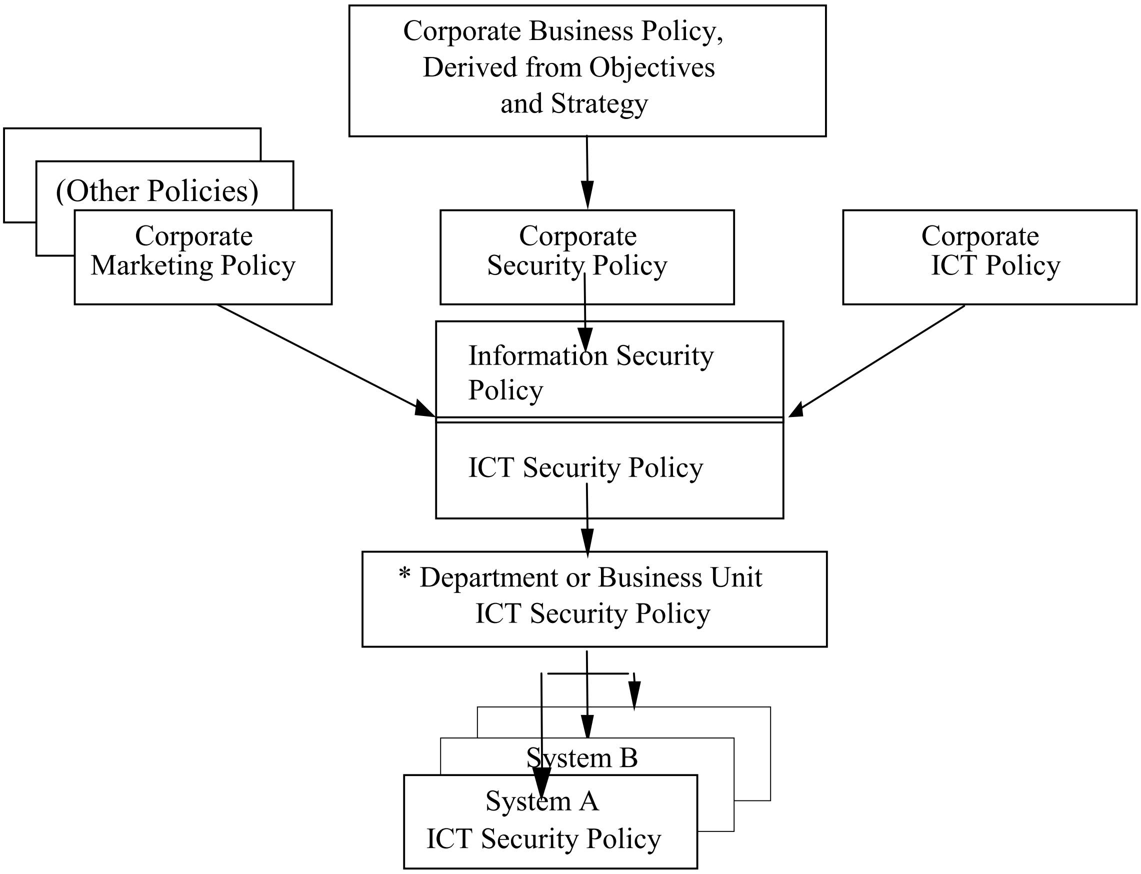
The **information security policy** may contain the principles and directives specific to the protection of information that is sensitive or valuable, or otherwise of importance, to the organization. Principles contained therein will be derived from, and thus consistent with, the principles of the corporate security policy.

The **corporate ICT security policy** should reflect the essential ICT security principles and directives applicable to the corporate security policy and information security policy, and the general use of ICT systems within the organization.

An **ICT system security policy** should reflect the security principles and directives contained within the corporate ICT security policy. It should also contain details of the particular security requirements and safeguards to be implemented and procedures on how to use safeguards correctly to ensure adequate security. In all cases, it is important that the approach taken is effective in relation to the business needs of the organization.

Where appropriate, the corporate ICT security policy may be included in the range of corporate technical and management policies, which together build a basis for a corporate ICT policy. This policy should include some persuasive words on the importance of security, particularly if security is necessary for compliance with that policy. Figure 3 shows a sample of a possible hierarchical relationship of policies. Regardless of the documentation and organizational structure in use by the organization, it is important that the different messages of the policies described are addressed, and that consistency is maintained.

Other, more detailed, ICT security policies are required for specific systems and services, or for a group of ICT systems and services. These are normally known as ICT system security policies. It is an important management aspect that their scope and boundaries are clearly defined, and based on both business and technical requirements.



* The depth of the hierarchy (number of layers) is dependent on several factors, such as the size of the organization.

Figure 3 – Policy hierarchy

4.3 Corporate ICT security policy elements

A corporate ICT security policy should be produced based on the agreed corporate ICT security objectives and strategy. It is necessary to establish and maintain a corporate ICT security policy, consistent with the legislation, regulation, corporate business, security, and ICT policies.

The more an organization relies on ICT, the more important ICT security is, to help ensure that the business objectives are met. When writing the corporate ICT security policy, the cultural, environmental and organizational characteristics should be borne in mind, since they can influence the approach towards security, e.g. some safeguards, which might be easily accepted in one environment, may be totally unacceptable in another.

The security activities described in the corporate ICT security policy can be based on the organizational objectives and strategy, the results of previous security risk assessment and management reviews, the results of follow-up actions such as security compliance checking of implemented safeguards, of monitoring, auditing and reviewing ICT security in day-to-day use, and of reports of security incidents. Any serious threat or vulnerability detected during these activities needs to be addressed, with the corporate ICT security policy describing the organization’s overall approach to deal with these security problems. The detailed actions are described in the various ICT system security policies, or in other supporting documents, for example, security operating procedures.

When developing the corporate ICT security policy, representatives from the following functions should participate:

- audit,
- legal,
- finance,
- information systems (technicians and users),
- utilities/infrastructure (i.e. persons responsible for building structure and accommodation, power, air-conditioning),
- personnel,
- security, and
- business management.

According to the security objectives, and the strategy an organization has adopted to achieve these objectives, the appropriate level of detail for the corporate ICT security policy is determined. The corporate ICT security policy should address the following general areas:

- its scope and purpose,
- the security objectives with respect to legal and regulatory obligations, and business objectives,

- ICT security requirements, in terms of confidentiality, integrity, availability, non-repudiation, accountability and authenticity of information,
- references to standards on which the policy is based,
- the administration of information security, covering organization and individual responsibilities and authorities,
- the risk management approach adopted by the organization,
- the means by which priorities for the implementation of safeguards can be determined,
- the broad level of security and residual risk sought by management,
- any general rules for access control (logical access control as well as the control of physical access to buildings, rooms, systems, and information),
- the approach to security awareness and training within the organization,
- broad procedures to check and maintain security,
- general personnel security issues,
- the means by which the policy will be communicated to all persons involved,
- the circumstances under which the policy should be reviewed or audited, and
- the method of controlling changes to the policy.

Organizations should assess their requirements, environment and culture, to determine the specific topics that best suit their circumstances. Topics might include:

- ICT security requirements, e.g., in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, particularly with regard to the views of the asset owners,
- organizational infrastructure and assignment of responsibilities,
- integration of security into system development and procurement,
- definition of methods and classes for information classification,
- risk management strategies,
- business continuity planning,
- personnel issues (special attention should be paid to personnel in positions requiring trust, such as maintenance personnel and system administrators),
- awareness and training,
- legal and regulatory obligations,
- outsourcing management, and
- information security incident management.

As discussed earlier in this clause, the results of previous risk assessment reviews, security compliance checking and information security incidents may have an effect on the corporate ICT security policy. This, in turn, may require that a previously defined strategy or policy be reviewed or refined.

To ensure adequate support for all security related measures, the corporate ICT security policy should be approved by management.

Based on the corporate ICT security policy, a directive should be written that is binding for all managers and employees. This may require the signature of each employee on a document, which acknowledges his/her responsibility for security within the organization. Furthermore, a programme for security awareness and training should be developed and implemented to communicate these responsibilities.

An individual should be designated to be responsible for the corporate ICT security policy, and for ensuring that this policy reflects the requirements and the actual status of the organization. This person would typically be the corporate ICT security officer, who amongst other things should be responsible for the follow-up activities. This includes security compliance checking, reviews and audits, the handling of incidents and security weaknesses, and any changes to the corporate ICT security policy that might become necessary according to the results of those actions.

5 Organizational aspects of ICT security

5.1 Roles and responsibilities

5.1.1 Organizational roles, accountabilities and responsibilities

Effective security requires accountability and the explicit assignment and acknowledgement of security responsibilities. Management should be responsible for all aspects of security management including risk-management decision-making. Several factors, such as the nature, form of incorporation, size and structure of an organization, will determine the level at which the responsibilities will be assigned. ICT security is an interdisciplinary topic and relevant to every ICT project and system and to all ICT users within an organization. Appropriate assignment and demarcation of accountability and specific roles and responsibilities should ensure that all important tasks are accomplished and that they are performed in an effective and efficient way. For small organizations, management may fill security roles, or other staff may carry out two or more security roles. In such cases, independent review is important to avoid conflict of interest and to ensure appropriate separation of roles.

Although this goal may be achieved through various organizational schemes, dependent upon the size and structure of an organization, the following roles need to be covered in every organization:

- an ICT security forum, which typically resolves the interdisciplinary issues, advises on and recommends strategy, and approves policies and procedures, and
- the corporate ICT security officer, who acts as the focus for all ICT security aspects within an organization.

Both the ICT security forum and the corporate ICT security officer should have well defined and unambiguous duties, and be sufficiently senior to ensure commitment to the corporate ICT security policy. The organization should provide clear lines of communication, responsibility, and authority for the corporate ICT security officer, and the duties should be approved by the ICT security forum. The conduct of these duties may be supplemented by the use of external consultants.

Figure 4 shows an example of the relationships between the corporate ICT security officer, the ICT security forum and the representatives from other areas within the organization, such as other security functions, the user community, and ICT personnel. These relationships may be line management or functional. The example of the ICT security organization described in Figure 4 uses three organizational levels. These are broadly based upon classical organizational structures such as corporate / department or corporate centre / business unit, but can easily be adapted to any organization by adding or omitting levels according to the organization's need. Small to medium organizations may choose to have a corporate ICT security officer whose responsibilities cover all security roles. When functions are combined it is important to ensure that the appropriate checks and balances are maintained to avoid concentrating too much responsibility in one person's hands without having the possibility of influence or control.

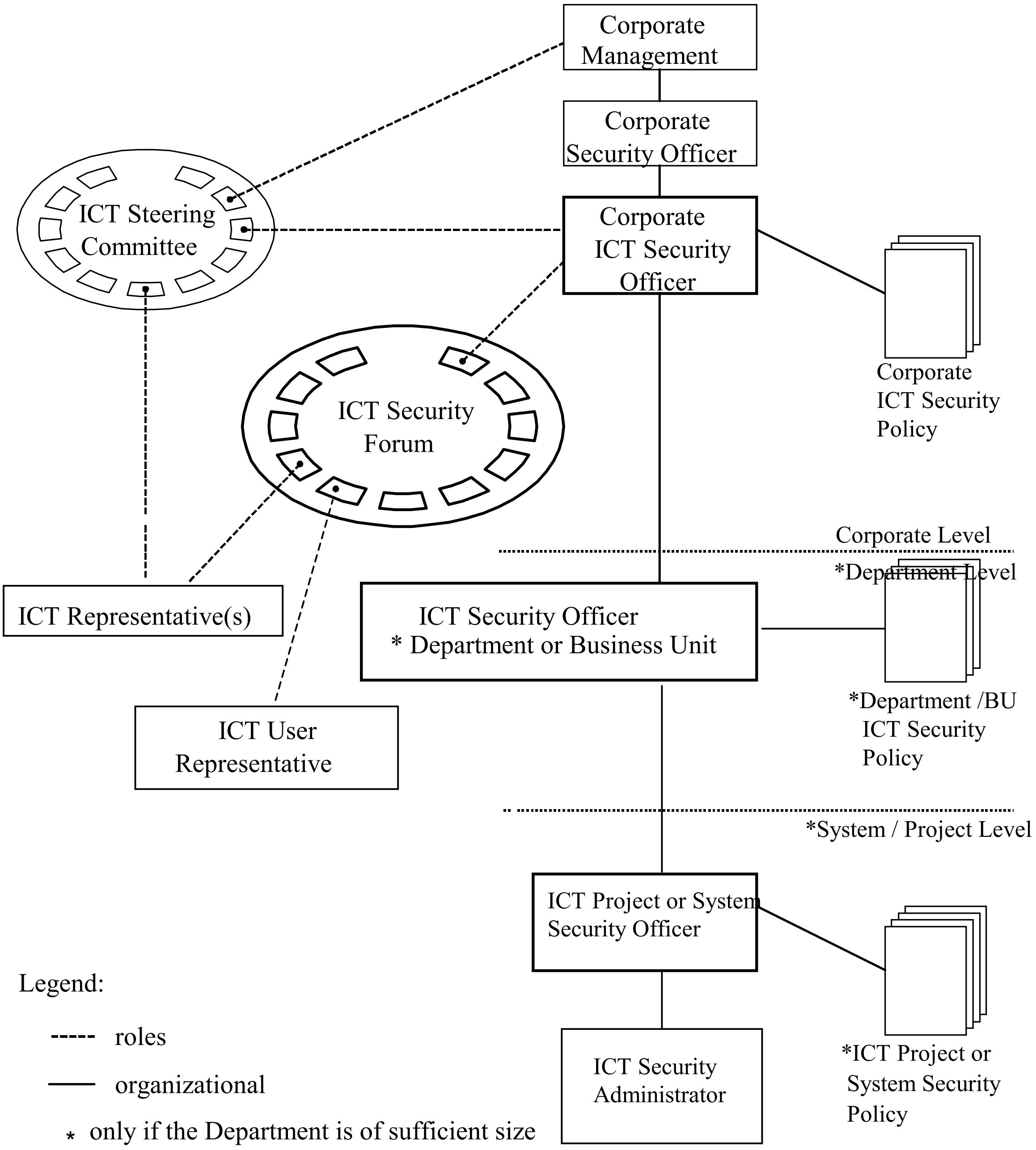

Corporate Management
Corporate Security Officer
Corporate ICT Security Officer
ICT Steering Committee
ICT Security Forum
Corporate ICT Security Policy
Corporate Level
*Department Level
ICT Representative(s)
ICT Security Officer
* Department or Business Unit
*Department /BU ICT Security Policy
ICT User Representative
*System / Project Level
ICT Project or System Security Officer
*ICT Project or System Security Policy
ICT Security Administrator
Legend:
----- roles
—— organizational
* only if the Department is of sufficient size

Figure 4 – Sample ICT security organization

5.1.2 ICT security forum

Such a forum should involve people with the necessary skills to advise on and recommend strategies, identify requirements, formulate policies, draw up the security program, review achievements and direct the corporate ICT security officer. There may already be a suitable forum, or a separate ICT security forum may be preferred. The role of such a forum or committee is to:

- advise the ICT steering committee regarding strategic security planning,
- formulate a corporate ICT security policy in support of the ICT strategy and obtain approval from the ICT steering committee, if one exists,
- translate the corporate ICT security policy into an ICT security program,
- monitor the implementation of the ICT security program,
- review the effectiveness of the corporate ICT security policy,
- promote awareness of ICT security issues,
- advise on resources (people, money, knowledge, etc.) needed to support the planning process and the ICT security program implementation, and
- resolve interdisciplinary issues.

To be effective, the forum should include members with a background in security and the technical aspects of ICT systems, as well as representatives of the providers and users of ICT systems. Knowledge and skills from all these areas are needed to develop a practical corporate ICT security policy.

5.1.3 Corporate ICT security officer

Responsibility for ICT security should be assigned to a specific individual. The corporate ICT security officer should act as the focus for all ICT security aspects within the organization; however, the corporate ICT security officer may delegate some aspects of the role. There may be a suitable person who can take on the additional responsibilities of the corporate ICT security officer, although, in medium and large organizations, it is recommended that a dedicated post be established. In large organizations, there may be a network of ICT security officers for business units, departments, etc. It is preferable to select people with background in security and ICT as corporate ICT security officer and departmental/business unit ICT security officers. The role of a corporate ICT security officer includes:

- oversight of the implementation of the ICT security program,
- liaison with and reporting to the ICT security forum and the corporate security officer,
- issuing and maintaining the corporate ICT security policy and directives,
- coordinating incident investigations,
- managing the corporate-wide security awareness program,
- setting ICT security objectives and criteria derived from policies,
- reviewing, auditing and monitoring the effectiveness of security controls, and

- reviewing, auditing or monitoring adherence to ICT security procedures throughout the organization.

As noted in 5.1.1, above, roles can be segregated, given the organization's size, complexity of security systems, and other relevant variables.

Examples of possible delegated functions are as follows:

ICT security project officer
Individual projects or systems should have someone responsible for security, sometimes called the ICT security project officer. In some cases, this may not be a full time role. The functional management of these officers should be the responsibility of the corporate ICT security officer. The ICT security project officer acts as the focal point for all security aspects of a project, a system, or a group of systems. The role of an ICT security project officer includes:

- liaison with and reporting to the corporate ICT security officer,
- developing and implementing the security plan for the project,
- day-to-day monitoring of implementation and use of the ICT safeguards, and
- initiating and assisting in incident investigations.

ICT security administrator
In medium and large organizations there is a role for delegated administration. This would include the following :

- executing and applying ICT security procedures;
- administering systems and network security;
- upgrading specific security programs, e.g., virus tools, software versions, software patches and fixes;
- administering specific security controls, e.g., backups, access control lists, etc.

Security administrators must have the appropriate training to administer the specific activities and tools.

5.1.4 ICT users

Users have responsibility for:

- using ICT resources in conformance with ICT policy, directives and procedures; and
- protecting ICT business assets in conformance with ICT security policy, directives and procedures.

5.2 Organizational principles

5.2.1 Commitment

The commitment of management to ICT security is essential if appropriate protection of corporate assets is to be realized. Any actual or perceived lack of such commitment will undermine the position of corporate ICT security officer and considerably weaken corporate defences to threats. Visible support from the top should result in a formally agreed and documented corporate ICT security policy, derived from the corporate security policy. The existence of these policies and their key elements should be regularly communicated to all employees and contractors, as appropriate, underlining management interest and support.

A business-wide commitment to the goals of ICT security includes:

- an understanding of the organization's global needs,
- an understanding of the needs for ICT security within the organization,
- a demonstration of the commitment to ICT security,
- a willingness to address the ICT security needs,
- a willingness to allocate resources to ICT security, and
- an awareness, at the highest level, of what ICT security means, or consists of (scope, extent).

The goals of ICT security should be promulgated throughout the organization. Each employee and contractor should know his or her role and responsibility, contribution to ICT security and should be entrusted to achieving such goals.

5.2.2 Consistent approach

A consistent approach to ICT security should be applied to all planning, implementation and operational activities. Protection should be ensured throughout the life cycle of information and ICT systems, from planning to acquisition, testing and operation.

An organizational structure, such as the one illustrated in Figure 4, can support a harmonized approach to ICT security throughout the organization. This needs to be supported by a commitment to standards. Standards may include international, national, regional, industry sector, and corporate standards or rules, selected and applied according to the ICT security needs of the organization. Technical standards need to be complemented by rules and guidelines on their implementation and use.

The benefits of using standards include:

- integrated security,
- interoperability,
- consistency,

- portability,
- economies of scale, and
- interworking between organizations.

5.2.3 Integrating ICT security

All ICT security activities are most effective if they occur uniformly throughout the organization and from the beginning of any ICT system's lifecycle. The ICT security process is itself a major cycle of activities and should be integrated into all phases of the ICT system lifecycle. Whilst security is most effective if it is integrated into new systems from the beginning, legacy systems and business activities benefit from the integration of security at any point in time.

An ICT system lifecycle can be subdivided into four basic phases. Each of these phases relates to ICT security in the following way:

- Planning: ICT security needs should be addressed during all planning and decision making activities.
- Acquisition: ICT security requirements should be integrated into the processes by which systems are designed, developed, purchased, upgraded or otherwise constructed. Integration of the security requirements into these activities ensures cost-effective security features are included in systems at the appropriate time and not afterwards.
- Testing: ICT system testing should include testing of ICT security components, features and services. New or changed security components should be tested separately to ensure that they operate as intended, and then tested in the operational environment, to ensure that the integration into the ICT system does not impact the security properties or features. Testing should be regularly scheduled during the operational lifetime of the system.
- Operations: ICT security should be integrated into the operational environment. As an ICT system is used to perform its intended mission, it must be maintained, and it typically will also undergo a series of upgrades that include the purchase of new hardware components or the modification or addition of software. In addition, the operational environment frequently changes. These changes in the environment could create new system vulnerabilities that should be analyzed and assessed, and either mitigated or accepted. Equally important is the secure disposal or reassignment of the systems.

ICT security should be a continuous process with many feedbacks within and between an ICT system's lifecycle phases. In most situations, feedback will occur between and within all major activities of the ICT security process. This provides a continual flow of information about ICT system vulnerabilities, threats and safeguards throughout the phases of an ICT system's lifecycle.

It is also worth noting that each of an organization's business areas may identify ICT security requirements that are unique. These areas should mutually support each other and the overall ICT security process by sharing information on security aspects, which can be used to support the management decision-making process.

6 ICT security management functions

6.1 Overview

Successful ICT security management requires that a number of activities be carried out. These activities include the following, to be carried out as a cyclical process:

- Planning:
  - determining organizational ICT security requirements,
  - determining organizational ICT security objectives, strategies and policies,
  - identifying roles and responsibilities within the organization,
  - development of the ICT security plan,
  - risk assessment.
  - risk treatment decisions and safeguard selection, and
  - business continuity planning
- Implementation:
  - implementing safeguards,
  - approval of ICT systems,
  - developing and implementing a security awareness program, and
  - reviewing and monitoring the implementation and operation of safeguards,
- Operations and maintenance:
  - configuration control and change management,
  - business continuity management,
  - review, audit and monitoring, and security compliance checking, and
  - information security incident management.

6.2 Cultural and environmental conditions

Information security management functional activities need to take into account the culture and the environment in which the organization operates, as these may have a significant effect on the overall approach to security. In addition, the culture and environment can have an impact on those that are responsible for the protection of specific parts of the organization. In some instances the government is considered to be responsible and discharges this responsibility by the enactment and enforcement of laws. In other instances it is the owner or manager who is considered responsible. This issue may have a considerable influence on the approach adopted.

6.3 Risk management

Risk management is an on-going activity. For new systems and systems at the planning stage, it should be part of the design and development process. For existing systems, risk management should be introduced at any appropriate point. When significant changes to systems are planned, risk management should be part of this planning process. It should take into account all systems within the organization and not be applied to one system in isolation. The risk management process is more fully explained in Part 2 of this International Standard.

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 1986 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard alongwith amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 17 (2058).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.org.in

Regional Offices: *Telephones*

Central : Manak Bhavan, 9 Bahadur Shah Zafar Marg
NEW DELHI 110002
{ 2323 7617
2323 3841

Eastern : 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi
KOLKATA 700054
{ 2337 8499, 2337 8561
2337 8626, 2337 9120

Northern : SCO 335-336, Sector 34-A, CHANDIGARH 160022
{ 260 3843
260 9285

Southern : C.I.T. Campus, IV Cross Road, CHENNAI 600113
{ 2254 1216, 2254 1442
2254 2519, 2254 2315

Western : Manakalaya, E9 MIDC, Marol, Andheri (East)
MUMBAI 400093
{ 2832 9295, 2832 7858
2832 7891, 2832 7892

Branches : AHMEDABAD. BANGALORE. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. KANPUR. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAJKOT. THIRUVANANTHAPURAM. VISAKHAPATNAM.

Published by BIS, New Delhi