TECHNICAL REPORT

# ISO/IEC TR 13335-1

First edition
1996-12-15



# Information technology — Guidelines for the management of IT Security —

## Part 1:
Concepts and models for IT Security

*Technologies de l'information — Lignes directrices pour la gestion de la sécurité des technologies de l'information (TI) —*

*Partie 1: Concepts et modèles pour la sécurité des TI*

Reference number
ISO/IEC TR 13335-1:1996(E)

# Contents

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

– type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

– type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

– type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC TR 13335, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*.

ISO/IEC TR 13335 consists of the folowing parts, under the general title *Information technology – Guidelines for the management of IT Security*:

– *Part 1: Concepts and models for IT Security*
– *Part 2: Managing and planning IT Security*
– *Part 3: Techniques for the management of IT Security*

Additional parts may be added to this Technical Report in the future.

## Introduction

The purpose of this Technical Report (ISO/IEC TR 13335) is to provide guidance, not solutions, on management aspects of IT security. Those individuals within an organization that are responsible for IT security should be able to adapt the material in this report to meet their specific needs. The main objectives of this Technical Report are:

- to define and describe the concepts associated with the management of IT security,
- to identify the relationships between the management of IT security and management of IT in general,
- to present several models which can be used to explain IT security, and
- to provide general guidance on the management of IT security.

ISO/IEC TR 13335 is organized into multiple parts. Part 1 provides an overview of the fundamental concepts and models used to describe the management of IT security. This material is suitable for managers responsible for IT security and for those who are responsible for an organization's overall security programme.

Part 2 describes management and planning aspects. It is relevant to managers with responsibilities relating to an organization's IT systems. They may be:

- IT managers who are responsible for overseeing the design, implementation, testing, procurement, or operation of IT systems, or
- managers who are responsible for activities that make substantial use of IT systems.

Part 3 describes security techniques appropriate for use by those involved with management activities during a project life-cycle, such as planning, designing, implementing, testing, acquisition or operations.

Further parts may be added to address specific topics as required.

# Information technology — Guidelines for the management of IT Security —

## Part 1:
Concepts and models for IT Security

### 1. Scope
ISO/IEC TR 13335 contains guidance on the management of IT security. Part 1 of ISO/IEC TR 13335 presents the basic management concepts and models which are essential for an introduction into the management of IT security. These concepts and models are further discussed and developed in the remaining parts to provide more detailed guidance. Together these parts can be used to help identify and manage all aspects of IT security. Part 1 is necessary for a complete understanding of the subsequent parts of ISO/IEC TR 13335.

### 2. Reference
ISO 7498-2:1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

### 3. Definitions

The following definitions are used in the three parts of ISO/IEC TR 13335.

**3.1 accountability:** the property that ensures that the actions of an entity may be traced uniquely to the entity (ISO 7498-2: 1989).

**3.2 asset:** anything that has value to the organization.

**3.3 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.

**3.4 availability:** the property of being accessible and usable upon demand by an authorized entity (ISO 7498-2: 1989).

**3.5 baseline controls:** a minimum set of safeguards established for a system or organization.

**3.6 confidentiality:** the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO 7498-2: 1989).

**3.7 data integrity:** the property that data has not been altered or destroyed in an unauthorized manner (ISO 7498-2: 1989).

**3.8 impact:** the result of an unwanted incident.

**3.9 integrity:** see data integrity and system integrity.

**3.10 IT security:** all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

**3.11 IT security policy:** rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its IT systems.

**3.12 reliability:** the property of consistent intended behaviour and results.

**3.13 residual risk:** the risk that remains after safeguards have been implemented.

**3.14 risk:** the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

**3.15 risk analysis:** the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

**3.16 risk management:** the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources.

**3.17 safeguard:** a practice, procedure or mechanism that reduces risk.

**3.18 system integrity:** the property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system.

**3.19 threat:** a potential cause of an unwanted incident which may result in harm to a system or organization.

**3.20 vulnerability:** includes a weakness of an asset or group of assets which can be exploited by a threat.

## 4. Structure

This part of ISO/IEC TR 13335 is structured as follows: Clause 5 outlines the aim of this report and Clause 6 provides information on the background requirements for the management of IT security. Clause 7 presents a general overview of the concepts and models for IT security, and Clause 8 examines the elements of IT security. Clause 9 discusses the processes used for the management of IT security, and Clause 10 presents a general discussion of several models that are useful in understanding the concepts presented in this report. Finally, Part 1 is summarized in Clause 11.

## 5. Aim

ISO/IEC TR 13335 is intended for a variety of audiences. The aim of Part 1 is to describe the various topics within the management of IT security and to provide a brief introduction to basic IT security concepts and models. The material is kept brief in order to provide a high level management overview. This should be suitable for senior managers within an organization who are responsible for security and give an introduction to IT security for others interested in the remaining parts of the report. Parts 2 and 3 provide more comprehensive information and material suitable for individuals who are directly responsible for the implementation and monitoring of IT security. This is based on the concepts and models presented in Part 1.

It is not the intent of this report to suggest a particular management approach to IT security. Instead the report begins with a general discussion of useful concepts and models and ends with a discussion of specific techniques and tools that are available for the management of IT security. This material is general and applicable to many different styles of management and organizational environments. This report is organized

in a manner which allows the tailoring of the material to meet the needs of an organization and its specific management style.

## 6. Background

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

IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:

- determining organizational IT security objectives, strategies and policies,
- determining organizational IT security requirements,
- identifying and analyzing security threats to IT assets within the organization,
- identifying and analyzing risks,
- specifying appropriate safeguards,
- monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization,
- developing and implementing a security awareness programme, and
- detecting and reacting to incidents.

In order to fulfil these management responsibilities for IT systems, security must be an integral part of an organization's overall management plan. As a result, several of the security topics addressed in this report have broader management implications. This report will not attempt to focus on the broad management issues, but rather on the security aspects of the topics and how they are related to management in general.

## 7. Concepts for the Management of IT Security

The adoption of the concepts that follow needs 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, they 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.

### 7.1 Approach

A systematic approach is necessary for the identification of requirements for IT security within an organization. This also is true for the implementation of IT security, and its ongoing administration. This process is referred to as the management of IT security and includes the following activities:

- development of an IT security policy,
- identifying roles and responsibilities within the organization,
- risk management, involving the identification and assessment of:
  - assets to be protected,

  - threats,
  - vulnerabilities,
  - impacts,
  - risks,
  - safeguards,
  - residual risks, and
  - constraints,
- configuration management,
- change management,
- contingency planning and disaster recovery planning,
- safeguard selection and implementation,
- security awareness, and
- follow up, including:
  - maintenance,
  - security audit,
  - monitoring,
  - review, and
  - incident handling.

### 7.2 Objectives, Strategies and Policies

Corporate security objectives, strategies and policies (see Figure 1) need to be formulated as a basis for effective IT security in an organization. They support the business of the organization and together they ensure consistency between all safeguards. The objectives identify what shall be achieved, strategies identify how to achieve these objectives, and the policies identify what needs to be done.

Objectives, strategies and policies may be developed hierarchically from the corporate to the operational level of the organization. They should reflect organizational requirements and take into account any organizational constraints, and they should ensure that consistency is maintained at each level and throughout all levels. Security is the responsibility of all levels of management within the organization and occurs in all phases of a systems life cycle. The objectives, strategies and policies should be maintained and updated based on the results of periodic security reviews (e.g., risk analysis, security audits) and changes in business objectives.

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

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

An **IT system security policy** must reflect the security principles and directives contained within the corporate IT security policy. It should also contain details of the particular security requirements and safeguards to be implemented and how to use them 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.

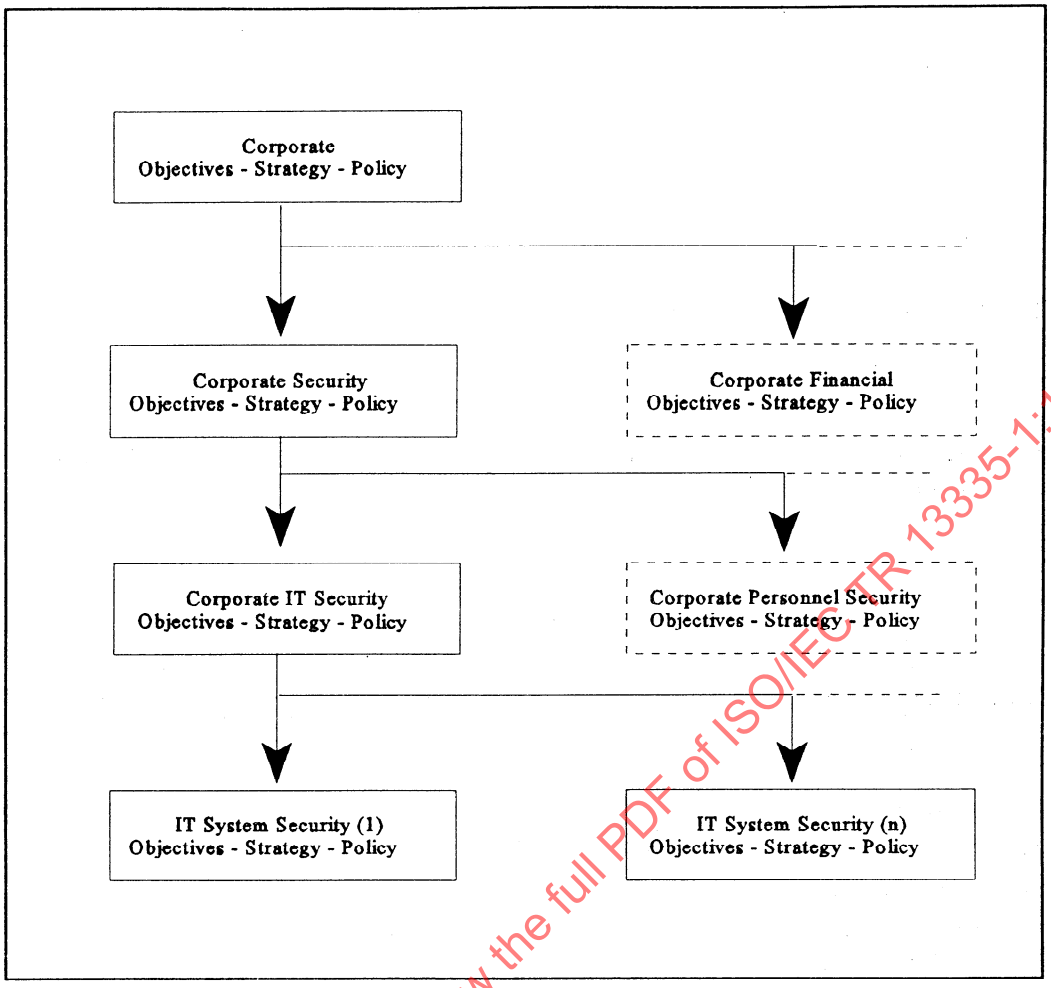


**Figure 1: Hierarchy of Objectives, Strategies and Policies**

IT system security objectives, strategies and policies represent what is expected from the IT 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 mathematical language. They should address IT security concerns, such as:

- confidentiality,
- integrity,
- availability,
- accountability,
- authenticity, and
- reliability.

The objectives, strategies and policies will establish the level of security for the organization, the threshold for risk acceptance, and the organization's contingency requirements.

## 8. Security Elements

The following sub-clauses describe at a high level the major elements that are involved in the security management process. Each of the elements is introduced, and the major contributing factors identified. More detailed descriptions and discussions of these elements and their relationships are contained in other parts of this report.

## 8.1 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 include:

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

Most or all of these assets may be considered valuable enough to warrant some degree of protection. An assessment of the risks being accepted is necessary if the assets are not protected.

From a security perspective, it is not possible to implement and maintain a successful security programme 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 analysis. The level of detail for this analysis must 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. In many cases, it is helpful to group assets.

Asset attributes to be considered include their value and/or sensitivity, and any inherent safeguards. The protection requirements of assets are influenced by their vulnerabilities in the presence of particular threats. If these aspects are apparent to the asset owner, they should be captured at this stage. The environments and cultures the organization operates in 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 and cultural variations can be significant for international organizations and their use of IT systems across international boundaries.

## 8.2 Threats

Assets are subject to many kinds of threats. A threat has the potential to cause an unwanted incident which may result in harm to a system or organization and its assets. This harm can occur from a direct or indirect attack on the information being handled by an IT system or service, e.g., its unauthorized destruction, disclosure, modification, corruption, and unavailability or loss. A threat needs to exploit an existing vulnerability of the asset in order to successfully cause harm to the asset. Threats may be of natural or human origin and can be accidental or deliberate. Both accidental and deliberate threats should be identified and their level and likelihood assessed.

Examples of threats are:

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

Statistical data is available concerning many types of environmental threats. This data should be obtained and used by an organization during the threat assessment process. Threats may impact specific parts of an organization, for example the disruption to personal 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 harm caused by the unwanted incident may be of a temporary nature or may be permanent as in the case of the destruction of an asset.

The amount of harm caused by a threat can vary widely for each occurrence. For example:

- a software virus may cause different amounts of harm depending on its actions, and
- earthquakes in a particular location may have different strengths on each occasion.

Such threats frequently have a measure of severity associated with them. For example:

- a virus may be described as destructive or non destructive, and
- the strength of an earthquake may be described in terms of the Richter Scale.

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 single personal computer may have a limited or localized impact. However, the same software virus on a network based file server may have widespread impact. Other threats, or the same threat in a different location, may be consistent in the amount of harm they cause. If the harm caused by the threat is consistent, a generic approach can be taken. However, if the harm varies widely, a more specific approach for each threat occurrence is appropriate.

Threats have characteristics which provide useful information about the threat itself. Examples of such information include:

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

The environments and cultures in which the organization is situated can have a significant bearing and influence on how the threats to the organization are dealt with. In extreme cases, some threats may not be

considered harmful in some cultures. Aspects of environment and culture must be considered when addressing threats.

### 8.3 Vulnerabilities

Vulnerabilities associated with assets include weaknesses in physical layout, organization, procedures, personnel, management, administration, hardware, software or information. They may be exploited by a threat that may cause harm to the IT system or business objectives. 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 to the asset. Vulnerabilities may remain unless the asset itself changes such that the vulnerability no longer applies.

Vulnerabilities include weaknesses in a system that can be exploited and may lead to undesirable consequences. They are opportunities which may allow a threat to cause harm. For example, the lack of an access control mechanism is a vulnerability 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 which have a corresponding threat are of immediate concern. However, as the environment can change dynamically, all vulnerabilities should be monitored to identify those that have become exposed to old or new threats.

Vulnerability analysis is the examination of weaknesses which may be exploited by identified threats. This analysis must take into account the environment and existing safeguards. The 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.

### 8.4 Impact

Impact is the consequence of an unwanted incident, caused either deliberately or accidentally, which affects the assets. The consequences could be the destruction of certain assets, damage to the IT system, and loss of confidentiality, integrity, availability, accountability, authenticity or reliability. Possible indirect consequences include financial losses, and the loss of market share or company image. The measurement of impacts permits a balance to be made between the results of an unwanted incident and the cost of the safeguards to protect against the unwanted incident. The frequency of occurrence of an unwanted 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
- the use of adjectives selected from a predefined list, e.g., low, medium, high.

### 8.5 Risk

Risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organization. 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 exposing assets to harm. The risk is characterized by a combination of two factors, the probability of the unwanted incident occurring and its impact. Any change to assets, threats,

vulnerabilities and safeguards may have significant effects on risks. Early detection or knowledge of changes in the environment or system increases the opportunity for appropriate actions to be taken to reduce the risk.

### 8.6 Safeguards

Safeguards are practices, procedures or mechanisms which may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recovery. Effective security usually requires a combination of different safeguards to provide layers of security for 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.

Safeguards may be considered to perform one or more of the following functions: detection, deterrence, prevention, limitation, correction, recovery, monitoring, and awareness. An appropriate selection of safeguards is essential for a properly implemented security programme. Many safeguards can serve multiple functions. It is often more cost effective to select safeguards that will satisfy multiple functions. Some examples of areas where safeguards can be used include:

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

Security awareness is a safeguard and is relevant to the personnel area. However, due to its importance it will be discussed in Clause 9.6. The environments and cultures the organization operates in may have a bearing on the safeguards selected and on the security awareness of the organization. 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 which are not offensive to the culture and/or the society the organization operates in.

Examples of safeguards are:

- network firewalls,
- network monitoring and analysis,
- encryption for confidentiality,
- digital signatures,
- anti virus software,
- back-up copies of information,
- reserve power supplies, and
- access control mechanisms.

### 8.7 Residual Risk

Risks are usually only mitigated partially by safeguards. A partial mitigation is all that is usually possible to achieve, and the more that is to be achieved the greater the cost. This implies that there are usually residual risks. Part of judging whether the security is appropriate to the needs of the organization is the acceptance of the residual risk. This process is known as risk acceptance.

Management should be made aware of all residual risks in terms of impact and the likelihood of an event occurring. The decision to accept residual risks must be taken by those who are in a position to accept the

consequences of the impact of unwanted incidents occurring and who can authorize the implementation of additional safeguards if the residual risk levels are not acceptable.

### 8.8 Constraints

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

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

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

## 9. Processes for the Management of IT Security

The management of IT security is an ongoing process consisting of a number of other processes. Some processes such as configuration management and change management have applicability to disciplines other than security. One process that experience has shown to be very useful in the management of IT security is risk management and its sub-process of risk analysis. Several aspects of the management of IT security, including risk management, risk analysis, change management, and configuration management, are shown in Figure 2.

### 9.1 Configuration Management

Configuration management is the process of keeping track of changes to the system and can be done formally or informally. The primary security goal of configuration management is to ensure that changes to the system do not reduce the effectiveness of safeguards and the overall security of the organization.

The security goal of configuration management is to know what changes have occurred, not to use security as a means of preventing changes to IT systems. In some cases, there may be reasons for making changes which will reduce security. In these situations, the decrease in security should be assessed and a management decision made which is based on all relevant factors. In other words, changes to a system must adequately address security concerns. Another goal of configuration management is to ensure that changes to the system are reflected in other documents, such as disaster recovery and contingency plans. If the change is a major one it may be necessary to analyse some or all of the system safeguards again.

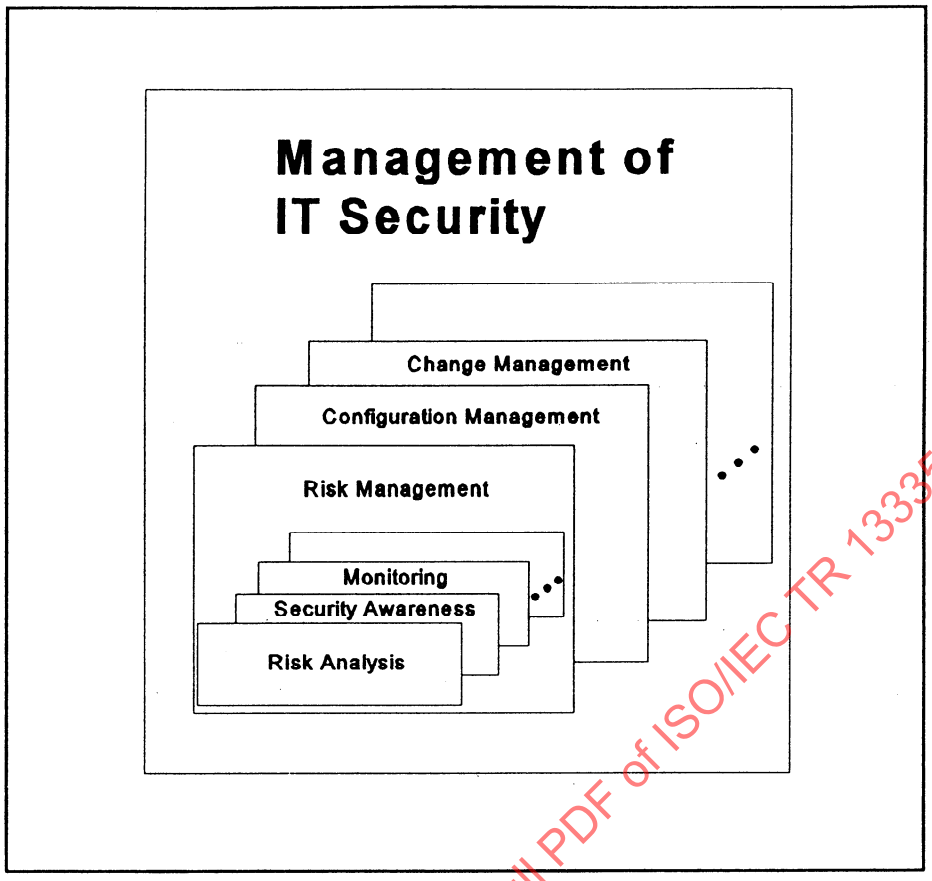


**Figure 2: Aspects of the Management of IT Security**



## 9.2 Change Management

Change management is the process used to help identify new security requirements when IT systems changes occur.

IT systems and the environment in which they operate are constantly changing. These changes are a result of the availability of new IT features and services, or the discovery of new threats and vulnerabilities. Changes to IT systems include:

- new procedures,
- new features,
- software updates,
- hardware revisions,
- new users to include external groups or anonymous groups, and
- additional networking and interconnection.

When a change to an IT system occurs or is planned, it is important to determine what, if any, impact the change will have on the security of the system. If the system has a configuration control board or other organizational structure to manage technical system changes, the IT security officer should be assigned to the board and be given the responsibility to make decisions about whether the change will impact security, and if so how. For major changes that involve the purchase of new hardware, software or services an analysis will be required to determine the new security requirements. On the other hand, many changes made to systems are minor in nature and do not require the extensive analysis that is needed for major changes. For both types of changes, a risk assessment that considers the benefits and costs should be made. For minor changes, this

can be performed informally at meetings, but the results and the management decisions should be documented.

### 9.3 Risk Management

Risk management activities are most effective if they occur throughout the system's life cycle. The risk management process is itself a major cycle of activities. While the entire cycle can be followed for new systems, in the case of legacy systems it can be initiated at any point in the system's life cycle. The strategy may dictate that a review is carried out at certain points in a system's life cycle, or at predefined times. There may be follow up actions from a previous review, with the aim of checking on the progress of implementation of safeguards. There may be a requirement to carry out risk management during the design and development of systems, thus ensuring that security is designed and implemented at the most cost effective time. When significant changes in the system are planned, risk management should also be initiated. Clause 10, Figure 4, shows the elements involved in risk management.

Whatever risk management method or technique is used, it is important to provide a good balance between minimizing the time and resources spent in identifying and implementing safeguards while still ensuring that all systems are appropriately protected.

Risk management is the process of comparing assessed risks with the benefits and/or costs of safeguards, and deriving an implementation strategy and system security policy consistent with the corporate IT security policy and business objectives. Different types of safeguards should be considered and a cost and/or benefit analysis performed. The safeguards are selected in relation to risks and the potential impacts. The level of acceptable residual risk must also be taken into account.

It should also be noted that safeguards themselves may contain vulnerabilities and thus result in new risks. Thus care must be taken in selecting the appropriate safeguards not only to reduce the risks but also not to introduce potential new risks.

The following clauses provide additional details about the risk management process.

### 9.4 Risk Analysis

Risk analysis identifies risks that need to be controlled or accepted. In the context of IT security, risk analysis for IT systems involves the analysis of asset values, threats and vulnerabilities. Risks are assessed in terms of potential impact that would be caused by a breach of confidentiality, integrity, availability, accountability, authenticity or reliability. The result of a risk analysis review is a statement of the likely risks to assets.

Risk analysis is part of risk management and can be accomplished without an unnecessary investment in time and resources by conducting an initial brief analysis on all systems. This will determine which systems can be adequately protected by a code of practice or baseline controls, and those systems which will benefit from a detailed risk analysis review. A code of practice comprises a set of guidance and baseline controls which can be used as a common basis of agreement and best practice to meet baseline protection requirements.

### 9.5 Accountability

Effective security requires accountability and the explicit assignment and acknowledgement of security responsibilities. Responsibilities and accountabilities need to be assigned to asset owners, providers and users of IT systems. Consequently, asset ownership and the associated security responsibilities, along with auditing of security performance, is important to effective security.

### 9.6 Security Awareness

Security awareness is an essential element for effective security. The lack of security awareness and poor security practices by personnel within an organization can significantly reduce the effectiveness of safeguards. Individuals within an organization are generally considered to be one of the weakest security links. In order to ensure that an adequate level of security awareness exists within an organization it is important to establish and maintain an effective security awareness programme. The aim of a security awareness programme is to explain to the employees, partners and suppliers:

- the security objectives, strategies and policies, and
- the need for security and their associated roles and responsibilities.

In addition the programme should be designed to motivate employees, partners, and suppliers, and ensure acceptance of their responsibilities for security.

A security awareness programme should be implemented at all levels in the organization from top management to the individuals responsible for day to day activities. It will often be necessary to develop and deliver different awareness material to people in different parts of an organization, and with different roles and responsibilities. A comprehensive security awareness programme is developed and delivered in stages. Each stage builds upon the lessons of the previous, beginning with the concept of security and working through to responsibilities for implementing and monitoring security.

Security awareness programmes within an organization include a variety of activities. One such activity is the development and distribution of security awareness material (e.g., posters, bulletins, pamphlets, or briefings). The purpose of the material is to increase the general awareness of employees and contractors. Another activity is the presentation of courses which train specific employees on the proper security practices. Finally courses are required which provide education at a professional level in very specific security topics.

In some cases it is effective to incorporate security messages into other training programmes. This approach should be considered in addition to, or as an alternative to, stand alone security awareness programmes. To develop a security awareness programme which blends with cultural and administrative requirements of a given organization, the following aspects need to be considered:

- needs analysis,
- programme delivery,
- monitoring, and
- awareness programme content.

### 9.7 Monitoring

The use of safeguards should be monitored to ensure they function appropriately, that changes in the environment have not rendered them ineffective and that accountability is enforced. Automated review and analysis of system logs is an effective tool for helping to ensure the intended performance. These tools can also be used to detect unwanted events, and their use may have a deterrent effect.

The effectiveness of security safeguards should be verified periodically. This is achieved by monitoring and compliance checking to ensure that the safeguards are functioning, and being used, in the manner expected. Many safeguards produce an output which should be checked for security significant events e.g., logs, alarm reports. General system audit functions can provide useful information from a security perspective and can be used in this regard.

### 9.8 Contingency Plans and Disaster Recovery

Contingency plans contain information about how to operate a business when the support processes, including IT systems, are degraded or unavailable. These plans should address the possible compounding of a number of scenarios including:

- various lengths of interruption,
- loss of different types of facilities,
- total loss of physical access to premises, and
- the need to return to the state that would have existed if the disruption had not occurred.

Disaster recovery plans describe how to restore to operation IT systems affected by an unwanted incident. Disaster recovery plans include:

- criteria that constitute a disaster,
- responsibility for activating the recovery plans,
- responsibilities for various recovery activities, and
- descriptions of recovery activities.

## 10. Models

It is recognized that many models exist for the management of IT security. However, the models presented in this part of ISO/IEC TR 13335 provide those concepts which are necessary for an understanding of the IT security management issues. The following models are described:

- security element relationships,
- risk management relationships, and
- the management of IT security process.

The concepts introduced previously and the business objectives of the organization come together to form plans, strategies and policies for the IT security of the organization. The overriding aim is to ensure that an organization retains the ability to carry out its business with risks limited to an acceptable level. No security can be totally effective and it is important to plan for recovery from an unwanted incident and to structure the security to limit the extent of the damage.

Security of IT systems is a multi-dimensional problem which can be viewed from different aspects. Therefore, in order to determine and implement a global and consistent IT security strategy and policy an organization should take into account all relevant aspects. Figure 3 shows how assets are potentially subject to a number of threats. This collection of threats changes constantly over time and is only partially known.

The model represents:

- an environment containing threats that change constantly and are only partially known,
- the assets of an organization,

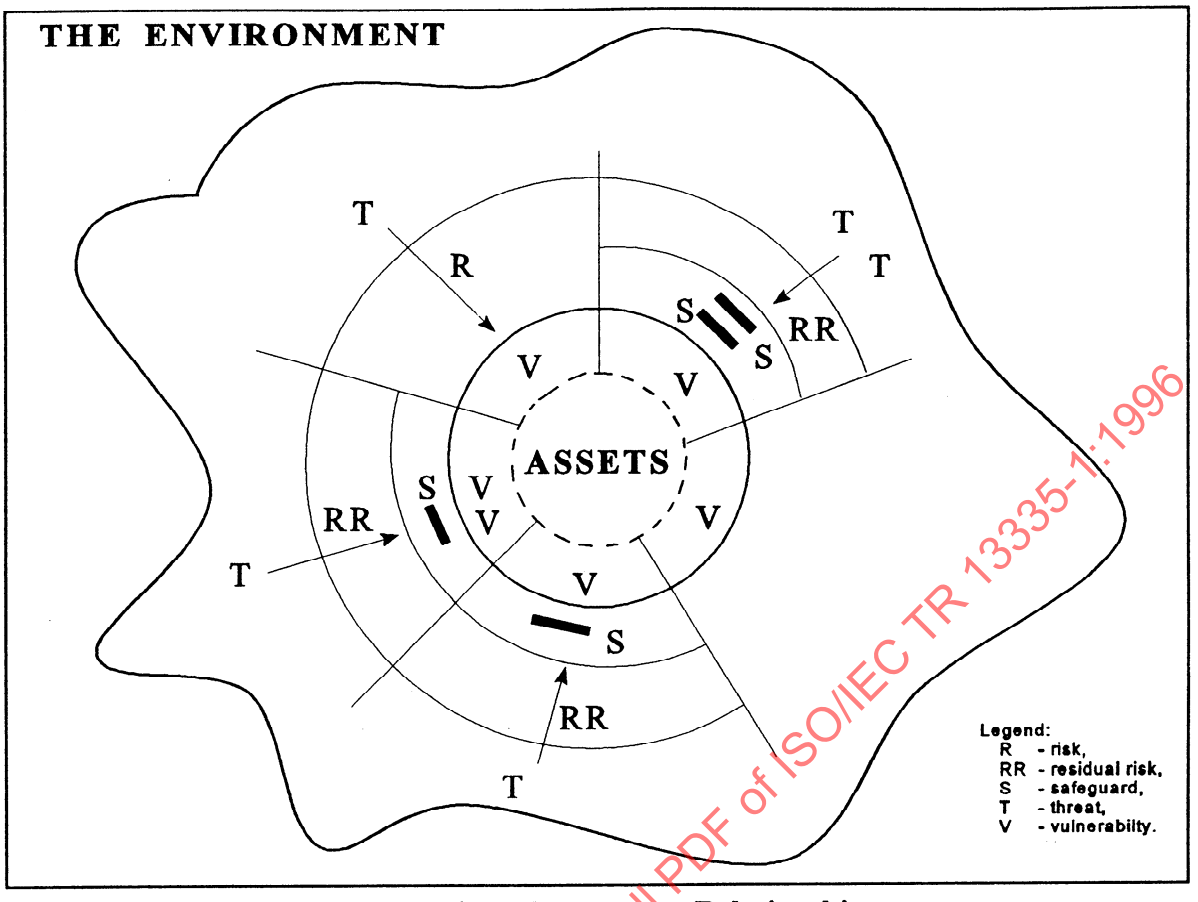


**Figure 3: Security Element Relationships**

- the vulnerabilities of those assets,
- safeguards selected to protect assets and to reduce the consequences of the threats,
- safeguards which modify risks, and
- residual risks acceptable to the organization.

As shown in Figure 3, some safeguards may be effective in reducing the risks associated with multiple threats and/or multiple vulnerabilities. Sometimes several safeguards are required to reduce the residual risks to an acceptable level. In some cases, when the risk is considered acceptable, no safeguards are implemented even if threats are present. In other cases, a vulnerability may exist, 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, which are not shown in Figure 3, affect the selection of safeguards.

Figure 4 illustrates the relationship between security elements often associated with risk management. For clarity only the major relationships are shown.