Proposed Draft Technical Report **ISO/IEC 1st PDTR 13335-1 (revision)**	
Date: **2001-11-28**	Reference number: ISO/IEC JTC 1/SC 27 **N 3009**
Supersedes document SC 27 N 2965rev1	

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2002-02-28** Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.

ISO/IEC 1st PDTR 13335-1 (revision)

Title: Information technology – Security techniques – Guidelines for the management of IT security - Part 1: Concepts and models for managing and planning IT security

Project: 1.27.14.01

INTRODUCTORY NOTE

Approval of Project

In accordance with resolution 17 (ref. document SC 27 N 2466) of the 11th SC 27 Plenary in Columbia, MD, USA, 1999-10-11/13 and resolution 14 (ref. document SC 27 N 2746) of the 12th SC 27 Plenary meeting in Tokyo, Japan, 2000-10-23/24, respectively, SC 27 approved revision of ISO/IEC TR 13335 Parts 1 and 2.

In accordance with document SC 27 N 2866 "Disposition of Comments Report on the revision of ISO/IEC TR 13335 Parts 1 & 2" (output document of the 22nd SC 27/WG 1 meeting, 2001-04-23/27) merging of Part 1 with Part 2 into TR 13335-1 was approved as consequence of the revision process.

PDTR Registration and PDTR Consideration

In accordance with resolution 5 (ref. document SC 27 N 3078) of the 13th SC 27 Plenary in Seoul, Republic of Korea, 2001-10-22/24, the attached document has been approved for registration as the 1st PDTR. Consequently, the attached document is hereby being submitted for a three-month PDTR letter ballot closing

2002-02-28

Medium: Server

No. of Pages:36

Address Reply to:
Secretariat, ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: krystyna.passia@din.de,
HTTP://www.din.de/ni/sc27

TABLE OF CONTENTS

FOREWORD ..... **IV**

EXECUTIVE SUMMARY ..... **V**

INTRODUCTION ..... **VI**

1 SCOPE **1**

2 NORMATIVE REFERENCES **1**

3 DEFINITIONS **1**

4 STRUCTURE **3**

5 AIM **3**

6 BACKGROUND **3**

7 SECURITY ELEMENTS **4**

7.1 ASSETS 4
7.2 THREATS 5
7.3 VULNERABILITIES 6
7.4 IMPACT 6
7.5 RISK 7
7.6 SAFEGUARDS 7
7.7 RESIDUAL RISK 8
7.8 CONSTRAINTS 8
7.9 MODELS 9
7.9.1 IT security management process model 9
7.9.2 Security Element Relationships 11
7.9.3 Risk Relationships 12

8 POLICY HIERARCHY **15**

8.1 OBJECTIVES, STRATEGIES AND POLICIES 15
8.2 POLICY RELATIONSHIPS 16
8.3 CORPORATE IT SECURITY POLICY ELEMENTS 18

9 ORGANIZATIONAL ASPECTS OF IT SECURITY **18**

9.1 ROLES AND RESPONSIBILITIES 18
9.1.1 Organizational Roles, Accountabilities and Responsibilities 18
9.1.2 IT Security Forum 20
9.1.3 Corporate IT Security Officer 21
9.1.4 IT Project Security Officer and IT System Security Officer 21
9.2 ORGANIZATIONAL PRINCIPLES 22
9.2.1 Commitment 22

9.2.2 Consistent Approach *22*
9.2.3 Integrating IT Security *23*

10 IT SECURITY MANAGEMENT FUNCTIONS 24

10.1 OVERVIEW 24
10.2 RISK MANAGEMENT 24
10.3 OTHER IT SECURITY MANAGEMENT FUNCTIONS 26
10.3.1 Safeguard Selection *26*
10.3.2 Security awareness *27*
10.3.3 Configuration management *27*
10.3.4 Change management *28*
10.3.5 Business continuity management *28*
10.3.6 Review and Monitoring *29*

11 SUMMARY 29

TABLE OF FIGURES

FIGURE 1: IT SECURITY MANAGEMENT FUNCTIONS: PROCESS MODEL 10
FIGURE 2: SECURITY ELEMENT RELATIONSHIPS 12
FIGURE 3: RISK RELATIONSHIPS MODEL 12
FIGURE 4: THREAT VIEW 14
FIGURE 5: VULNERABILITY VIEW 14
FIGURE 6: IMPACT VIEW 14
FIGURE 7: POLICY RELATIONSHIPS 17
FIGURE 8: SAMPLE IT SECURITY ORGANIZATION 20
FIGURE 9: RISK MANAGEMENT PROCESS OVERVIEW 25

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 representative 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, 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), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC TR 13335 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 13335 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

- *Part 1: Concepts and models for managing and planning IT Security,*
- *Part 3: Techniques for the management of IT Security,*
- *Part 4: Selection of safeguards, and*
- *Part 5: Management guidance on network security*

Executive Summary

ISO/IEC Technical Report 13335-1, Information Technology – Security techniques – Guidelines for the management of IT Security (GMITS) – Part 1: Concepts and Models for managing and planning IT Security, is the first in a series of guidelines that deal with the planning, management and implementation of information technology security. All organizations today, government and commercial, rely heavily on the use of information technology, and there is a consequent need to protect information and to manage the security of IT.

Part 1 of this series is intended for a senior management audience. It contains definitions applicable to all Parts, and introduces various concepts and models of information technology (IT) security that may be applicable to different organizations.
It also provides concepts and guidelines for managing and planning IT security. Principal amongst the concepts is risk management, which entails identification and analysis of threats, vulnerabilities, impact, and risk, and the treatment of risks through detailed IT security planning, including selection of safeguards and implementation processes. Risk management is key to in developing an effective IT security posture. Other important concepts include planning in terms of objectives, strategies and policies and other IT security management functions.

The further Parts of this Technical Report provide more in-depth discussion of the various aspects of IT security raised in Part 1.

Introduction

The purpose of this Technical Report (ISO/IEC TR 13335) is to provide guidance, not solutions, on management aspects of information technology (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 that 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. Part 1 also describes management and planning aspects. This material is suitable for senior managers and those responsible for IT security and for those who are responsible for an organization's overall security program and those with responsibilities relating to an organization's IT systems.

Part 3 (ISO/IEC TR 13335-3 Guidelines for the management of IT Security Part 3: Techniques for the Management of IT Security) 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.

Part 4 (ISO/IEC TR 13335-4 Guidelines for the management of IT Security Part 4: Selection of Safeguards) provides guidance for the selection of safeguards, and how this can be supported by the use of baseline models and controls. It also describes how this complements the security techniques described in Part 3, and how additional assessment methods can be used for the selection of safeguards.

Part 5 ISO/IEC TR 13335-5 Guidelines for the management of IT Security Part 5: Management guidance on network security) provides guidance with respect to networks and communications to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements. It also contains a brief introduction to the possible safeguard areas.

Information technology – Guidelines for the management of IT Security –

Part 1:
Concepts and models for management and planning 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 concepts and models fundamental to a basic understanding of IT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of IT security. The other three parts provide operational guidance for IT security managers. Together these parts can be used to help identify and manage all aspects of IT security.

2 Normative References

- ISO 7498-2:1988 Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture
- ISO/IEC 13888-1: 1997, Information technology - Security techniques - Non-repudiation - Part 1: General

Other standards or technical reports related to topics within this broad subject area may be developed in future.

3 Definitions

The following definitions are used in the five parts of ISO/IEC TR 13335. These definitions are also found in SC 27 Standing Document no 6 Glossary of IT Security Terminology SD 6, March 1998.

3.1	accountability:	the property that ensures that the actions of an entity may be traced uniquely to the entity (ISO 7498-2: 1988).
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: 1988).
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: 1988).

3.7 control: in the context of information technology security, the term "control" is normally considered to be synonymous with "safeguard". See 3.22. Reference as well IS 17799:2000.

3.8 impact: the result of an unwanted incident.

3.9 integrity: the property of safeguarding the accuracy and completeness of assets.

3.10 IT security: all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, 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 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: 1997; ISO IS 7498-2)

3.13 reliability: the property of consistent intended behaviour and results.

3.14 residual risk: the risk that remains after implementation of the IT security plan.

3.15 risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

3.16 risk analysis: the systematic process of estimating the magnitude of risks.

3.17 risk assessment: the process of combining risk identification, risk analysis and risk evaluation.

3.18 risk evaluation: the process of comparing analyzed levels of risk against pre-established criteria and identifying areas needing risk treatment.

3.19 risk identification: the process of identifying risks considering business objectives, threats and vulnerabilities as the basis for further analysis.

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

3.21	risk treatment:	the process of defining an IT security management plan based on risk evaluation.
3.22	safeguard:	a practice, procedure or mechanism that reduces risk. Note that the term “safeguard” is normally considered to be synonymous with the term “control”.
3.23	threat:	a potential cause of an unwanted incident that may result in harm to a system or organization.
3.24	vulnerability:	a weakness of an asset or group of assets that can be exploited by one or more threats.

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 examines the elements and relationships of IT security both conceptually and through models. Clause 8 discusses the policy and documentation hierarchy for managing and planning IT security, from business objectives and corporate policy to detailed specifications on topics such as network security. Clause 9 discusses IT security organization. Clause 10 presents an overview of IT security management functions, including risk management. 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 provide a high-level management overview. This should be suitable for senior managers within an organization who are responsible for security and those who have responsibility for procurement, design, implementation, or operation of IT systems.

It is not the intent of this report to suggest a particular management approach to IT security. Instead the report contains a general discussion of useful concepts and models for the management and planning 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 that 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, non-repudiation, 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 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.

In order to fulfill 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 Security Elements

The following sub-clauses describe at a high level the major elements that are involved in security management and planning. 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.

7.1 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 to determine whether the assets are adequately protected.

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 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. Vulnerabilities in the presence of particular threats influence protection requirements for assets. If these aspects are apparent to the asset owner, they should be captured at this stage. The

environments, cultures and legal systems 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, cultural and legal variations can be significant for international organizations and their use of IT systems across international boundaries.

7.2 Threats

Assets are subject to many kinds of threats. A threat has the potential to cause an unwanted incident that may result in harm to a system or organization and its assets. This harm can occur from a direct or 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	Earthquake Lightning Floods Fire
Eavesdropping Information modification System hacking Malicious code Theft	Errors and omissions File deletion Incorrect routing Physical accidents	

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 amount of harm caused by a threat can vary widely for each occurrence. 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.

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.

Threats have characteristics that 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.

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

7.3 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.

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 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 that may be exploited by identified threats. This analysis 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.

7.4 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, non-repudiation, 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.

7.5 Risk

Risk is the potential that a given threat will exploit vulnerabilities of an asset and thereby cause loss or damage to an 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.

Risk management is discussed more fully in Clause 10 and in greater depth in the risk management Part of this report.

7.6 Safeguards

Safeguards are practices, procedures or mechanisms that 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:

- prevention,
- deterrence,
- detection,
- limitation,
- correction,
- recovery,
- monitoring, and
- awareness.

An appropriate selection of safeguards is essential for a properly implemented security program. 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.

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
- back-up copies of information.

7.7 Residual risk

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 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.

7.8 Constraints

Constraints are normally set or recognized by the organization's management and influenced by the environments 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 must 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.

7.9 Models

It is recognized that many models exist for the management of IT security. The following models provide those concepts that are necessary for an understanding of the IT security management issues. The following models are described:

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

7.9.1 IT security management process model

IT security management is a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. 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. See Clause 10.1 for additional guidance.

Figure 1 depicts a process flow model of IT security management functions.

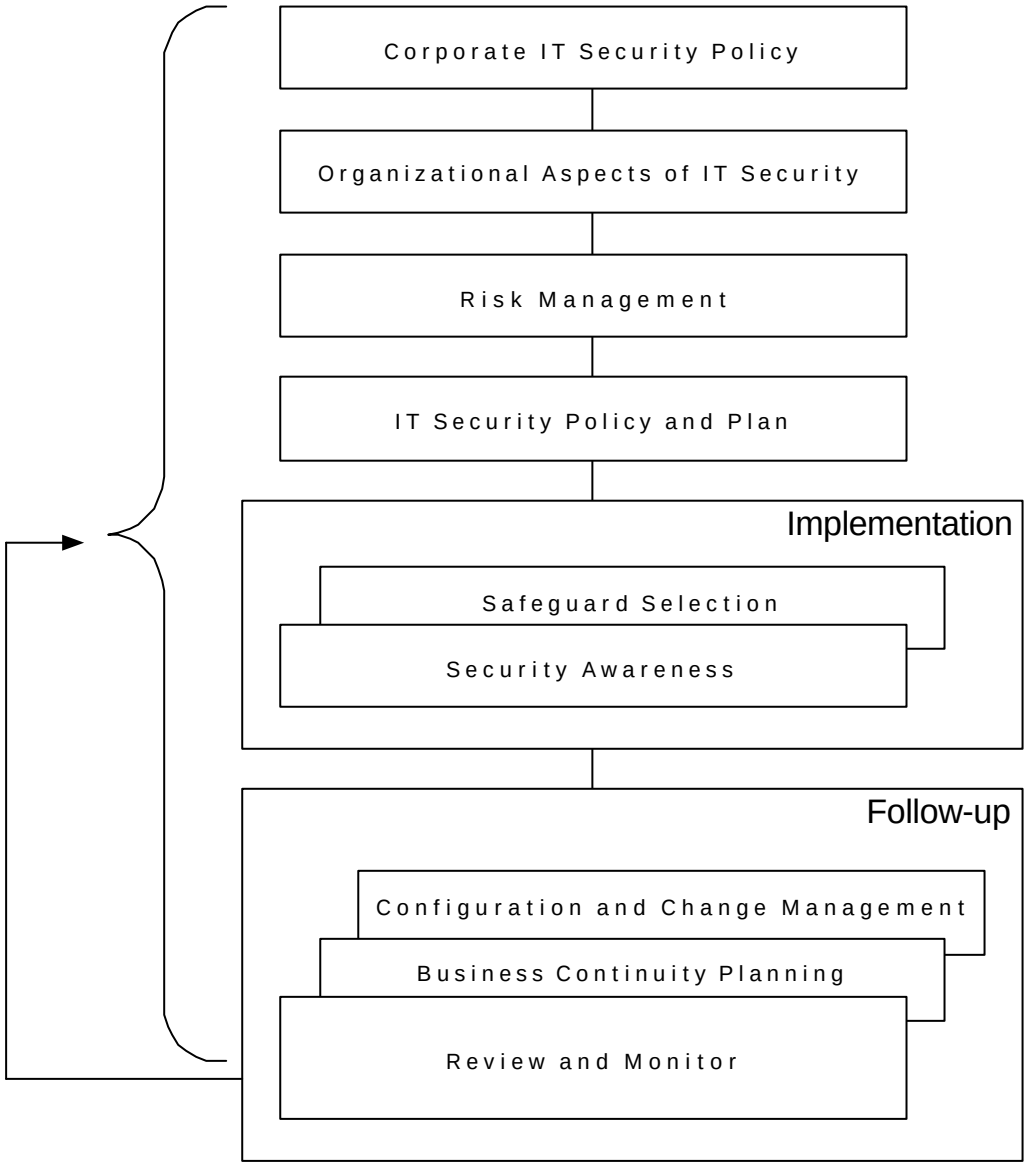

Figure 1: IT Security Management Functions: Process Model

7.9.2 Security Element Relationships

Security of IT systems is a multi-dimensional discipline that can be viewed from different aspects. 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.

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.

As illustrated in Figure 2, some safeguards (S) may be effective in reducing the risks (R) associated with multiple threats (T) and/or multiple vulnerabilities (V). A threat can only become effective if the asset is vulnerable to it. Sometimes several safeguards are required to reduce the residual risks (RR) 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 (C) affect the selection of safeguards.

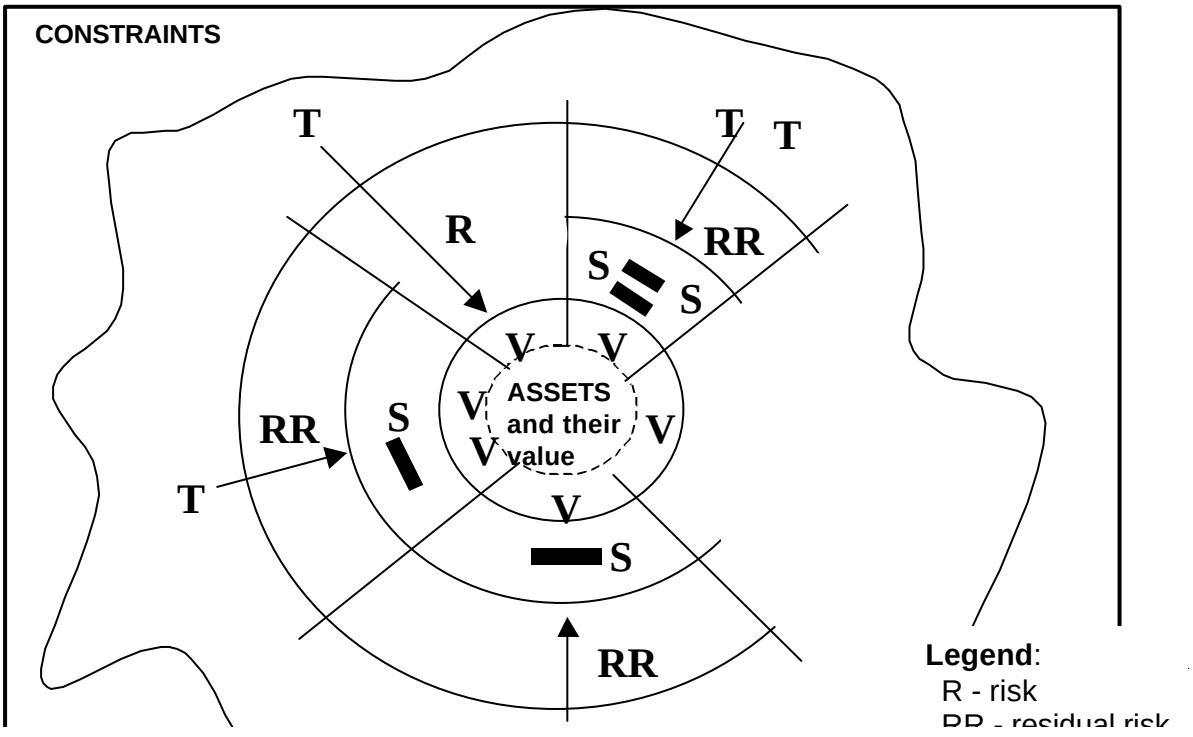

Figure 2: Security Element Relationships

7.9.3 Risk Relationships

Figure 3 illustrates the relationships between security elements often associated with risk. For clarity only the major relationships are shown.

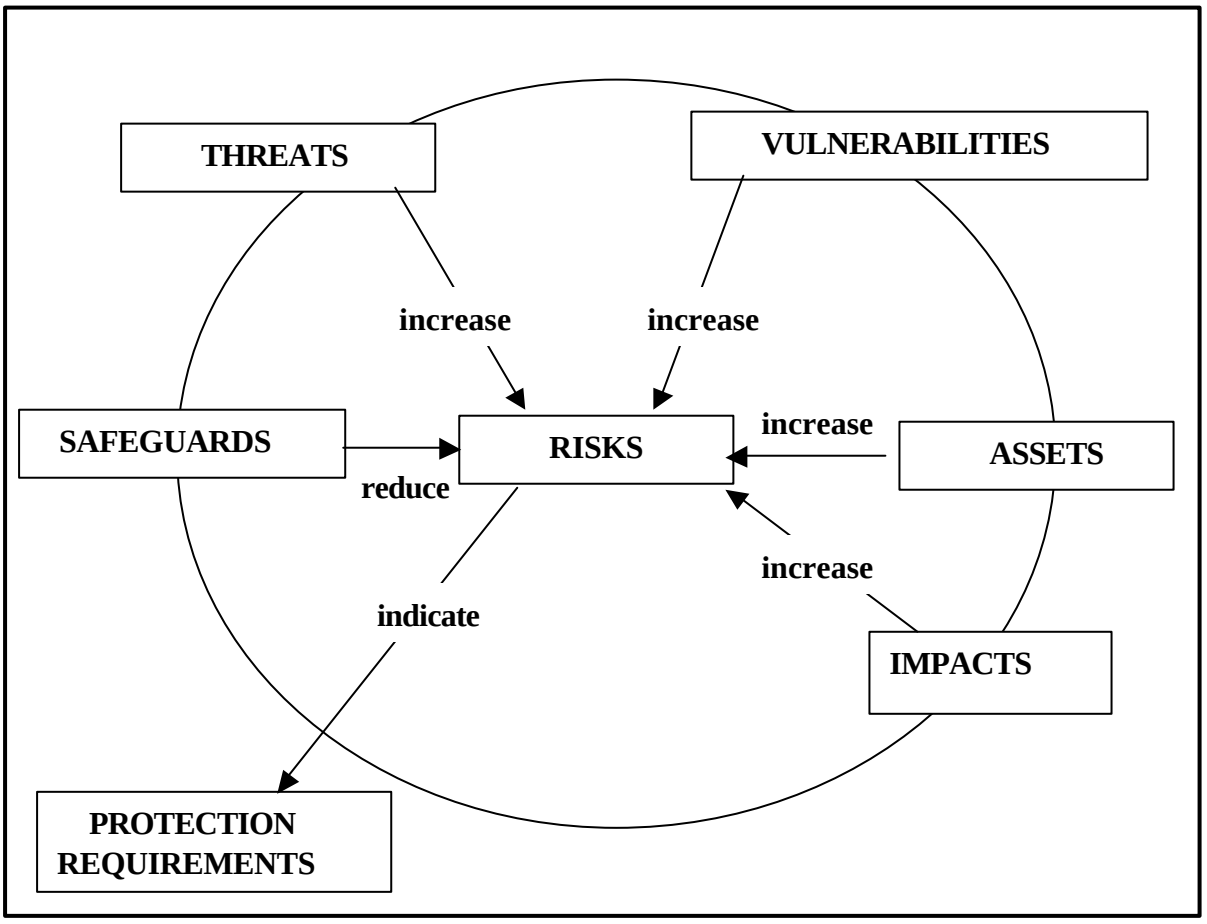

Figure 3: Risk Relationships Model

There are a number of relationships between the components shown in Figure 3. The following paragraph provides an introduction to these. For clarity, the italicized text directly references one or more of the components of Figure 3.

Any IT 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 *potential adverse impacts* on the business operations of the organization were unauthorized disclosure, modification or repudiation of information, or unavailability or destruction of information or service, to occur. These impacts are first determined regardless of which threats might occur to cause the impacts, to be sure of identifying the real values. Then the question of what threats might occur to cause such impacts, and is the likelihood of their occurrence, is addressed, i.e. *assets could be the subject to a number of threats.* Then the question of what vulnerabilities (or weaknesses) might be exploited by the threats to cause the impacts is addressed, i.e. *threats could exploit vulnerabilities to expose assets.* Next the asset values (potential adverse business impacts), and the likelihood of threats, and the seriousness of vulnerabilities, are brought together to determine *risks. Each of these components, i.e. values, threats and vulnerabilities, can increase risks.* Measures of risks 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 risks, protect against threats and indeed can reduce vulnerabilities.*

Figures 4, 5 and 6 illustrate the relationships between protection requirements and threats, vulnerabilities, and assets, respectively. Some IT security management approaches may emphasize one of the perspectives illustrated by these figures. Such approaches may, however, overlook some important aspects. Consequently, Figure 3 provides the more general approach and is used as the basis for Part 3 of ISO/IEC TR 13335.

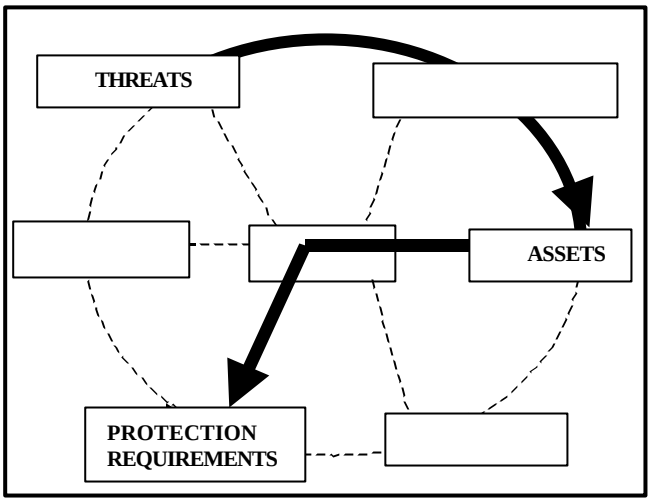

Figure 4: Threat View

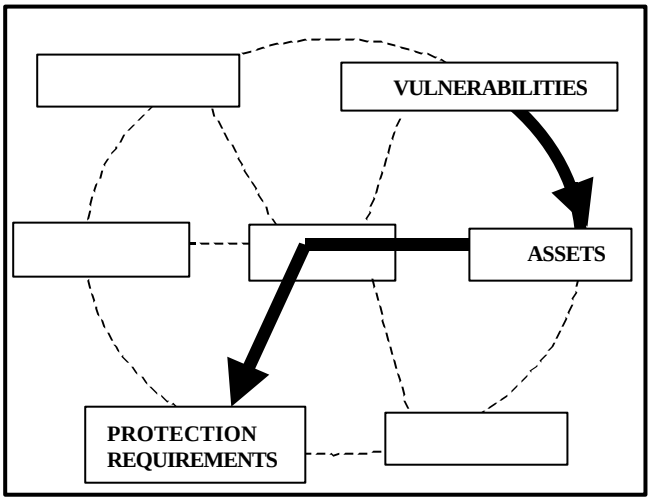

Figure 5: Vulnerability View

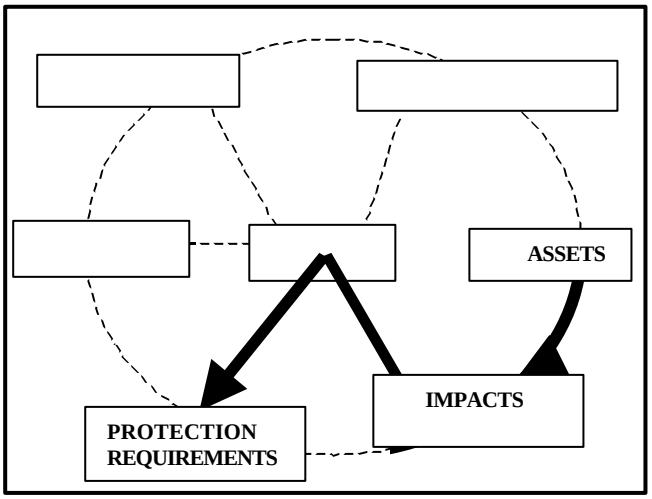

Figure 6: Impact View

8 Policy Hierarchy

8.1 Objectives, Strategies and Policies

Corporate security objectives, strategies and policies need to be formulated as the basis for effective IT security in an organization. They support the business of the organization and together they ensure consistency between all safeguards.

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, and taking into account business objectives, 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, IT, etc.). The hierarchy of documentation 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 should reflect the broader corporate policies, including those that address individual rights, legal requirements and standards.

The **corporate IT security policy** should reflect the essential IT 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** should 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 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.

IT system security objectives, strategies, policies and procedures 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,
- non-repudiation,
- accountability,
- authenticity, and
- reliability.

The objectives, strategies, policies and procedures will establish the level of security for the organization and the threshold for risk acceptance.

8.2 Policy Relationships

Where appropriate, the corporate IT security policy may be included in the range of corporate technical and management policies, that together build a basis for a corporate IT strategy statement. This statement should include some persuasive words on the importance of security, particularly if security is necessary for the compliance with that strategy. Figure 7 shows the relationships between the various 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.

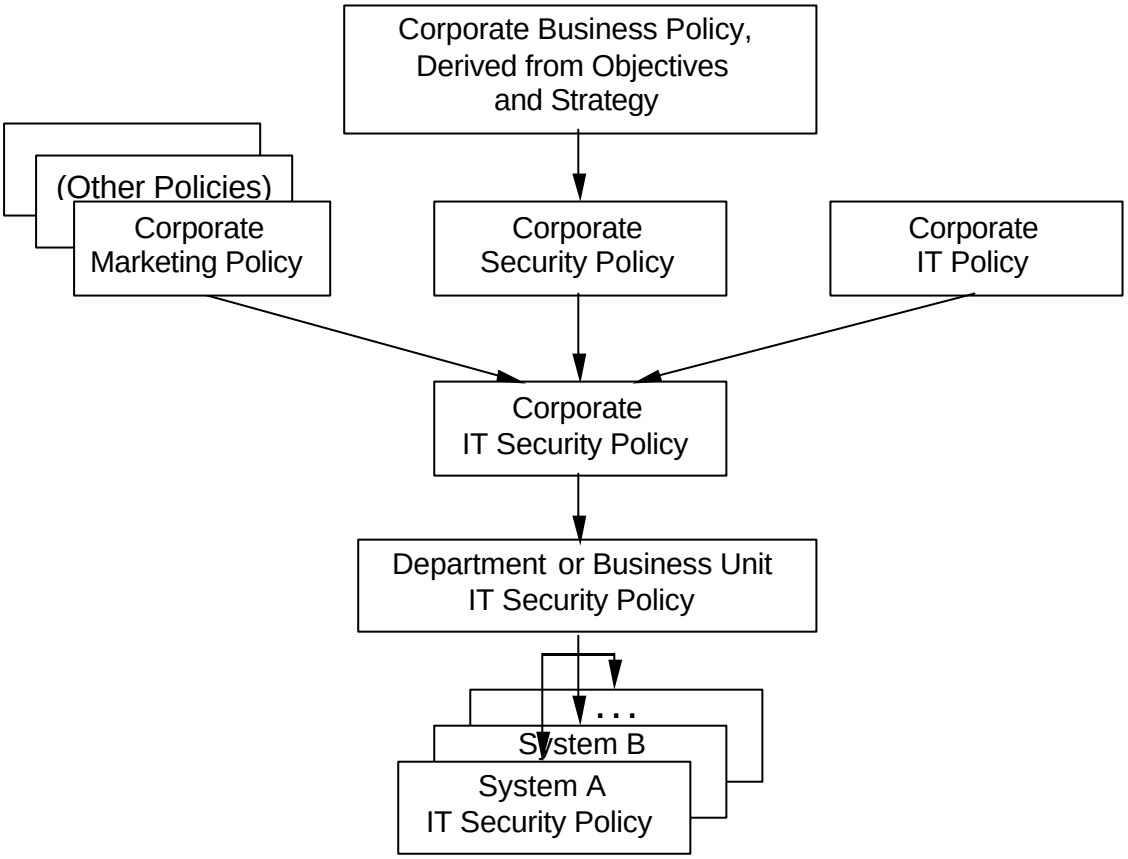

Figure 7: Policy Relationships

Other, more detailed, IT security policies are required for specific systems and services, or for a group of IT systems and services. These are normally known as IT 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.

8.3 Corporate IT Security Policy Elements

The corporate IT security policy should at least cover the following topics:

- IT security requirements, e.g., in terms of confidentiality, integrity, availability, authenticity, accountability 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 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
- incident handling.

9 Organizational Aspects of IT Security

9.1 Roles and Responsibilities

9.1.1 Organizational Roles, Accountabilities and Responsibilities

Effective security requires accountability and the explicit assignment and acknowledgement of security responsibilities. Senior management is responsible for all aspects of security management including risk-management decision-making. IT security is an interdisciplinary topic and relevant to every IT project and system and to all IT users within an organization. Appropriate assignment and demarcation of accountability and specific responsibilities should ensure that all important tasks are accomplished and that they are performed in an efficient way.

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 IT security forum, which typically resolves the interdisciplinary issues and approves policies and procedures, and
- the corporate IT security officer, who acts as the focus for all IT security aspects within

an organization.

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

Figure 8 shows a typical example of the relationships between the corporate IT security officer, the IT security forum and the representatives from other areas within the organization, such as other security functions, the user community, and IT personnel. These relationships may be line management or functional. The example for the organization of IT security described in Figure 8 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 IT 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 power in one person's hands without having the possibility of influence or control.

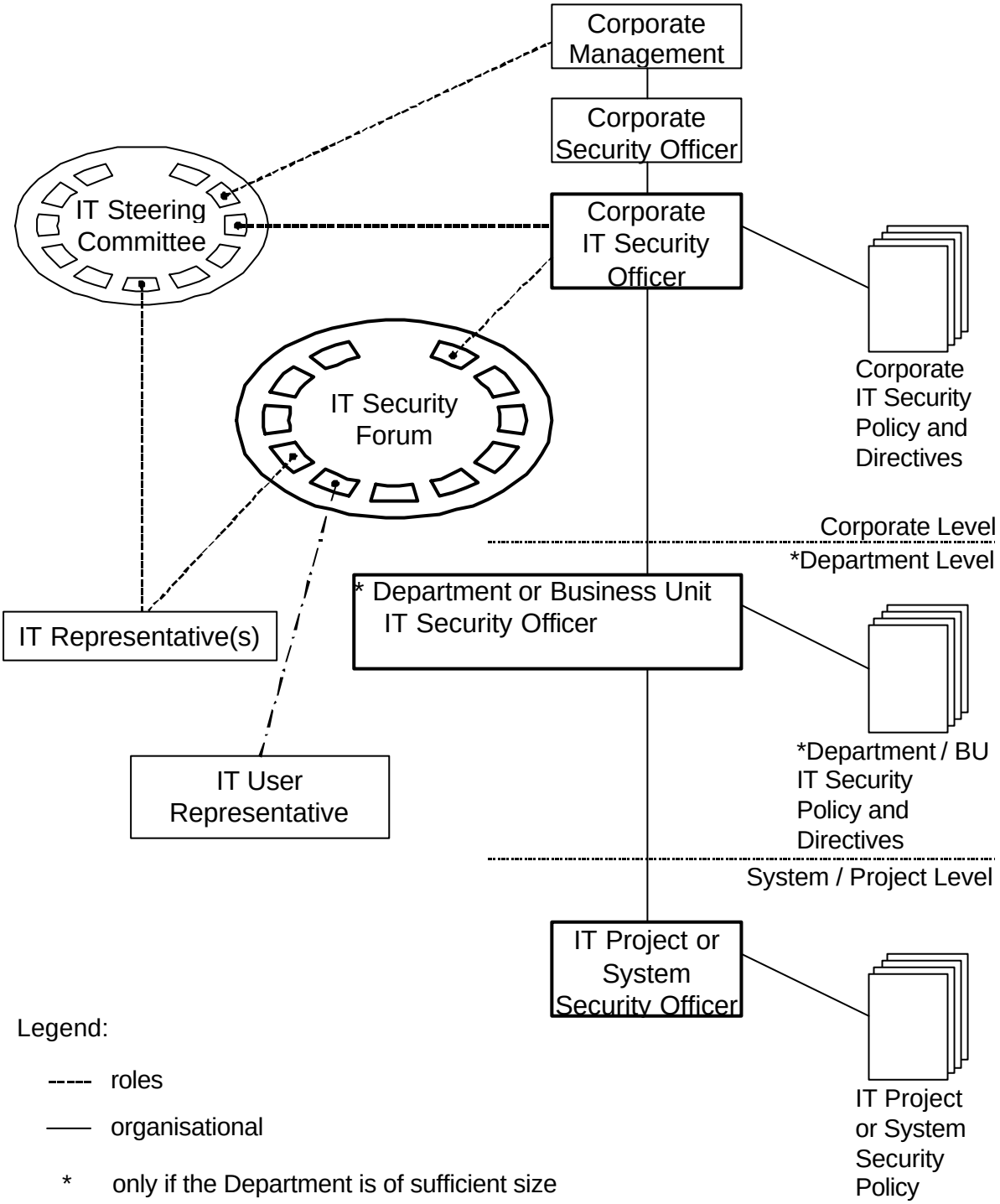

Figure 8: Sample IT Security Organization

9.1.2 IT Security Forum

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

- advise the IT steering committee regarding strategic security planning,

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

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

9.1.3 Corporate IT Security Officer

Because the responsibility for IT security is shared, there is a risk that, in the end, nobody will feel responsible at all. To avoid this, responsibility should be assigned to a specific individual. The corporate IT security officer should act as the focus for all IT security aspects within the organization. There may already be a suitable person who can take on the additional responsibilities, although it is recommended that a dedicated post be established. It is preferable to select a person with background in security and IT as corporate IT security officer. The chief responsibilities are:

- oversight of the implementation of the IT security program,
- liaison with and reporting to the IT security forum and the corporate security officer,
- maintaining the corporate IT security policy and directives,
- coordinating incident investigations,
- managing the corporate-wide security awareness program, and
- determining the terms of reference for IT project and system security officers (and where relevant departmental IT security officers).

9.1.4 IT Project Security Officer and IT System Security Officer

Individual projects or systems should have someone responsible for security, usually called the IT security officer. In some cases, this may not be a full time role. The functional management of these officers will be the responsibility of the corporate IT security officer (or, where applicable, the department IT security officer). The security officer acts as the focal point for all security aspects of a project, a system, or a group of systems. The chief responsibilities of the post are:

- liaison with and reporting to the corporate IT security officer (or, where applicable, the

departmental IT security officer),

- issuing and maintaining the IT project or system security policy,
- developing and implementing the security plan,
- day-to-day monitoring of implementation and use of the IT safeguards, and
- initiating and assisting in incident investigations.

9.2 Organizational Principles

9.2.1 Commitment

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

A business wide commitment to the goals of IT security includes:

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

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

9.2.2 Consistent Approach

A consistent approach to IT security should be applied to all development, maintenance and operational activities. Protection should be ensured throughout the life cycle of information and IT systems, from planning to disposal.

An organizational structure, such as the one illustrated in Figure 8, can support a harmonized approach to IT 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 IT security needs of the organization. Technical standards need to be complemented by rules and guidelines on their implementation, use

and management.

The benefits of using standards include:

- integrated security,
- interoperability,
- consistency,
- portability,
- economies of scale, and
- interworking between organizations.

9.2.3 Integrating IT Security

All IT security activities are most effective if they occur uniformly throughout the organization and from the beginning of any IT system's life cycle. The IT security process is itself a major cycle of activities and should be integrated into all phases of the IT system life cycle. 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 IT system life cycle can be subdivided into three basic phases. Each of these phases relates to IT security in the following way:

- Planning: IT security needs should be addressed during all planning and decision making activities.

- Acquisition: IT 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 that cost effective security features are included in systems at the appropriate time and not afterwards.

- Operations: IT security should be integrated into the operational environment. As an IT system is used to perform its intended mission, it typically undergoes 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.

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

It is also worth noting that each of an organization's business areas may identify IT security

requirements that are unique. These areas should mutually support each other and the overall IT security process by sharing information on security aspects which can be used to support the management decision making process.

10 IT Security Management Functions

10.1 Overview

The adoption of the concepts discussed in Part 1 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.

IT security management activities include:

- determining organizational IT security objectives, strategies and policies,
- determining organizational IT security requirements,
- development of an IT security policy (Clause 8),
- identifying roles and responsibilities within the organization (Clause 9),
- risk management (Clause 10.2)
- reviewing and monitoring the implementation and operation of safeguards,
- developing and implementing a security awareness program,
- configuration management,
- change management,
- business continuity management,
- security audit, and
- incident handling.

Security is the responsibility of all levels of management within the organization and occurs in all phases of a systems life cycle.

10.2 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 main elements of the risk management process are shown in Figure 9. Each of the boxes in the Figure are briefly described below, and more fully explained in Part 3 of this report. Note that this

graphic representation is intended as illustrative of one methodology. Implementing this methodology may involve combining some of the steps that are shown as separate boxes. As noted in Clause 3.17, the activity of identifying risks is considered an integral part of the risk assessment process, although it may occur as a separate step.

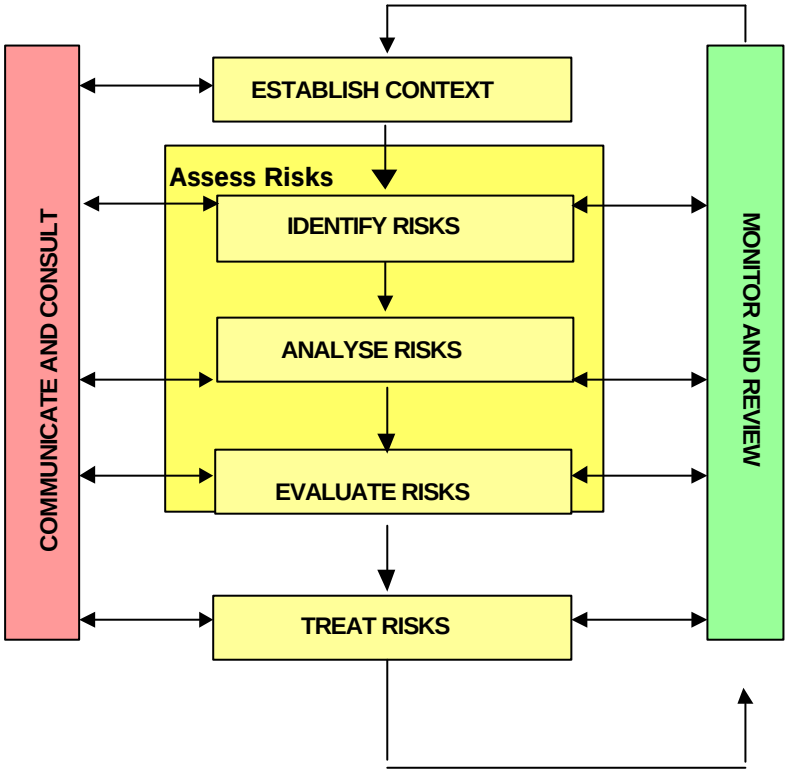

Figure 9: Risk Management Process Overview

Establish the context

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

Identify risks

Identify what, why and how things can arise as the basis for further analysis.

Analyze Risks

Determine the existing safeguards and analyze risks in terms of consequence and likelihood in the context of these safeguards. The analysis should consider the range of potential consequences and

how likely these consequences are to occur. Consequence and likelihood may be combined to produce an estimated level of risk.
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, non-repudiation, 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 that will benefit from a detailed risk analysis review.

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

Treat Risks
Develop and implement a specific management plan that includes consideration of funding. Options include risk avoidance, risk reduction and risk transference. Accept and monitor low priority risks.

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

Monitor and review
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. More in-depth information can be found in the risk management Part of this Technical Report.

10.3 Other IT Security management functions

10.3.1 Safeguard Selection

There are several types of safeguards: those that prevent, reduce, monitor, detect, or correct unwanted incidents, and those that recover from them. Prevention can include the deterrence of unwanted actions and activities that enhance security awareness. Management responsibilities include assessing the costs of individual safeguards relative to the benefits they will provide, and relative to the level of residual risk deemed acceptable. ISO/IEC TR 13335 Part 4 provides detailed guidelines on selection of safeguards

10.3.2 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 program. The aim of a security awareness program 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 program should be designed to motivate employees, partners, contractors, and suppliers, and ensure acceptance of their responsibilities for security.

A security awareness program 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 program 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 programs within an organization may include a variety of activities. One such activity is the development and distribution of security awareness material (e.g., posters, bulletins, pamphlets, or briefings). Another activity is the presentation of courses that train specific employees on the proper security practices. In some circumstances, it may be effective to integrate appropriate security requirements within other training courses or materials required by an organization. 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 programs. This approach should be considered in addition to, or as an alternative to, stand alone security awareness programs. To develop a security awareness program that blends with cultural and administrative requirements of a given organization, the following aspects need to be considered:

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

10.3.3 Configuration management

Configuration management or control is the process of maintaining system configuration and can be done formally or informally. The primary security goal of configuration management is to ensure that up-to-date system configuration documentation is maintained, and that approved changes to the system are managed in such a manner that such changes do not reduce the effectiveness of safeguards and the overall security of the organization.

Configuration management is intended to manage approved changes. It is not intended to prevent changes to IT systems on the basis of security. A related goal of configuration management is to ensure that changes to the system are reflected in other documents, such as disaster recovery and business continuity plans. If the change is a major one it may be necessary to analyze some or all of the system safeguards again.

10.3.4 Change management

Change management is the process used to help identify whether different security safeguards are required when changes to IT systems 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. In some cases, there may be reasons for making changes that 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. 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 analysis 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.

10.3.5 Business continuity management

There should be a managed process in place for developing and maintaining business continuity throughout an organization. Business continuity management provides for the availability of processes and resources in order to ensure the continued achievement of critical business objectives. It includes planning for contingencies and recovery from disasters.

Before being able to produce business continuity plans, an organization should ensure that a strategy is developed for the overall approach to business continuity. This strategy should be based on

business impact analysis results and related agreed minimum resource, accommodation, IT infrastructure and communications requirements, and agreed recovery time periods.

Continuity 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,
- descriptions of recovery activities, and
- responsibility for testing that the recovery plan is effective.

10.3.6 Review and Monitoring

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 that 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. 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.

11 Summary

The concepts and models discussed in this part of ISO/IEC TR 13335 can be used to manage and develop plans for protecting an organization's IT assets. This information is intended to give managers familiarity with the major processes and functions that play a role in IT security management. The information provided in this part may not be directly applicable to all organizations. In particular, small organizations are not likely to have all the resources available to completely perform some of the functions described. In these situations, it is important that the basic concepts and functions are addressed in an appropriate manner for the organization. Even in some large organizations, some of the functions discussed in this part may not be accomplished exactly as described.

The other Parts of ISO/IEC TR 13335 will provide more in-depth information on these subjects, and in particular on the risk management process.