TECHNICAL REPORT

ISO/IEC TR 13335-2

First edition
1997-12-15

Information technology — Guidelines for the management of IT Security —

Part 2:
Managing and planning IT Security

Technologies de l'information — Lignes directrices pour le management de sécurité IT —

Partie 2: Management et planning de sécurité IT

Reference number
ISO/IEC TR 13335-2:1997(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 Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.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 13335-2, which is a Technical Report of type 3, was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 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 IT Security*

— *Part 2: Managing and planning IT Security*

— *Part 3: Techniques for the management of IT Security*

— *Part 4: Selection of safeguards*

— *Part 5: Safeguards for external connections*

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,
- as well of course as managers responsible for IT security.

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.

Part 4 provides guidance on 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 provides guidance to an organization connecting its IT systems to external networks. This guidance includes the selection and use of safeguards to provide security for the connections and the services supported by those connections, and additional safeguards for the IT systems being connected.

Information technology — Guidelines for the management of IT Security —

Part 2:
Managing and planning IT Security

1 Scope

The guidelines in this part of ISO/IEC TR 13335 address subjects essential to the management of IT security, and the relationship between those subjects. These guidelines are useful for the identification and the management of all aspects of IT security.

Familiarity with the concepts and models introduced in Part 1 is essential for a complete understanding of this part.

2 Reference

ISO/IEC TR 13335-1:1996, *Information technology — Guidelines for the management of IT Security — Concepts and models for IT Security.*

3 Terms and definitions

For the purposes of this part of ISO/IEC TR 13335, the definitions given in ISO/IEC TR 13335-1 apply. The following terms are used: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, IT security, IT security policy, reliability, residual risk, risk, risk analysis, risk management, safeguard, system integrity, threat, vulnerability.

4 Structure

Part 2 is divided into 17 clauses. Clauses 5 and 6 provide information on the aim and background of this document. Clause 7 provides an overview of the various activities involved in successful IT security management. Clauses 8 through 16 elaborate on these activities. Clause 17 provides a summary.

5 Aim

The aim of this part is to present the different activities related to the management and the planning of IT security, as well as the associated roles and responsibilities within an organization. It is relevant to IT managers who typically have responsibility for procurement, design, implementation, or operation of IT systems. Apart from managers with responsibility for IT security, it is also relevant to managers who are responsible for activities that make substantial use of IT systems. Generally, this part is useful for anybody having managerial responsibilities relating to an organization's IT systems.

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 adverse impacts 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 the security threats to, and vulnerablilities of, the assets of IT systems within the organization,
- identifying and analyzing security 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 fulfill these management responsibilities for IT systems, security must be an integral part of an organization's overall management plan and be integrated into all functional processes of the organization. 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 Management of IT Security

7.1 Planning and Management Process Overview

IT security planning and management is the overall process of establishing and maintaining an IT security programme within an organization. Figure 1 shows the main activities within this process. Because management styles and organizational sizes and structures differ, this process should be tailored to the environment in which it is used. It is important that all of the activities and functions identified in Figure 1 are addressed within the style, size and structure of the organization, and its manner of doing business. It is implicit that management reviews are conducted as part of all these activities and functions.

The starting point is to establish a clear view of the organization's IT security objectives. These objectives follow from higher level objectives (e.g. the business objectives) and, in turn, lead to the IT security strategy for the organization and the corporate IT security policy, as detailed in Clause 8. Therefore, a part of the corporate IT security policy is the creation of an appropriate organizational structure that will ensure that the defined objectives can be reached.

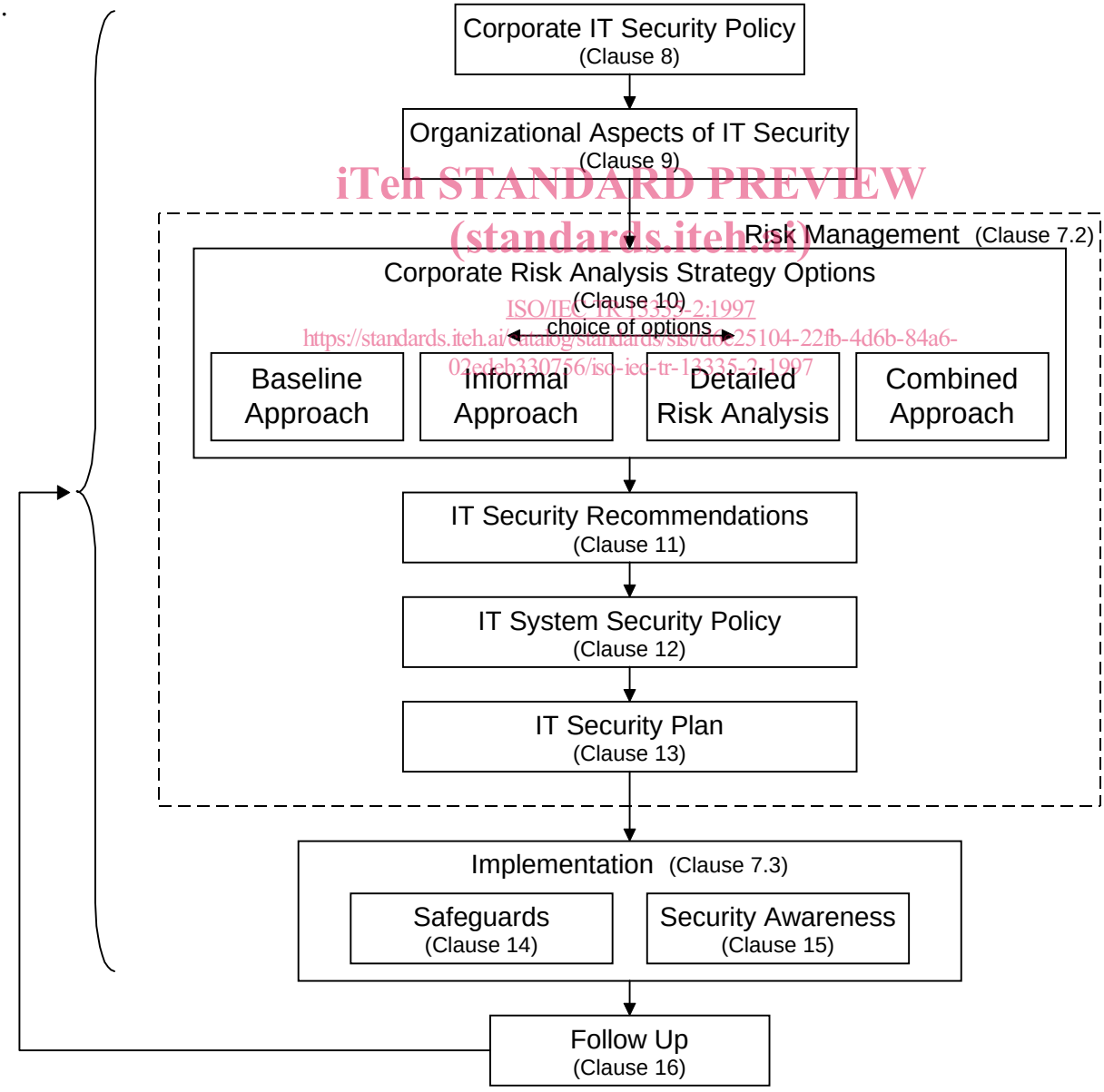

Figure 1 — Overview of the Planning and Management of IT Security

7.2 Risk Management Overview

Risk Management includes four distinct activities:

- determination of the overall risk management strategy appropriate to the organization within the context of the corporate IT security policy,
- selection of safeguards for individual IT systems as a result of risk analysis activities or according to baseline controls,
- formulation of IT system security policies from the security recommendations, and as necessary the update of the corporate IT security policy (and where appropriate the departmental IT security policy), and
- construction of IT security plans to implement the safeguards, based on the approved IT system security policies.

7.3 Implementation Overview

The implementation of the necessary safeguards for each IT system should be done according to the IT security plan. The improvement of general IT security awareness, although very often neglected, is an important aspect for the effectiveness of safeguards. Figure 1 makes clear that these two tasks, i.e., safeguard implementation and a security awareness programme, should run in parallel, as user behaviour cannot be changed overnight, and awareness needs to be enhanced continuously over a longer period of time.

7.4 Follow-up Overview

The activities addressed in clause 16, 'Follow-up', include:

- maintenance of safeguards, to ensure their continued and effective operation,
- checking to ensure that safeguards comply with approved policies and plans,
- monitoring of assets, threats, vulnerabilities and safeguards for differences, to detect changes which may affect risks, and
- incident handling to ensure the appropriate reaction to unwanted events.

Follow-up is a continuous task, which should include the reassessment of earlier decisions.

7.5 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 which includes 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 which 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. Only the overall feedback path is shown in Figure 1. In most situations, feedback will also 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.

8 Corporate IT Security Policy

8.1 Objectives

Objectives (what is to be achieved), strategies (how to achieve these objectives), and policies (the rules for achieving the objectives) may be defined for each level of an organization and for each business unit or department. In order to achieve

effective IT security it is necessary to align the various objectives, strategies and policies for each organizational level and business unit. Consistency between the corresponding documents, although influenced by different points of view, is important, since many threats (such as system hacking, file deletion and fire) are common business problems.

8.2 Management Commitment

The commitment of top management to IT security is important and should result in a formally agreed and documented corporate IT security policy. The corporate IT security policy should be derived from the corporate security policy.

8.3 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 2 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.

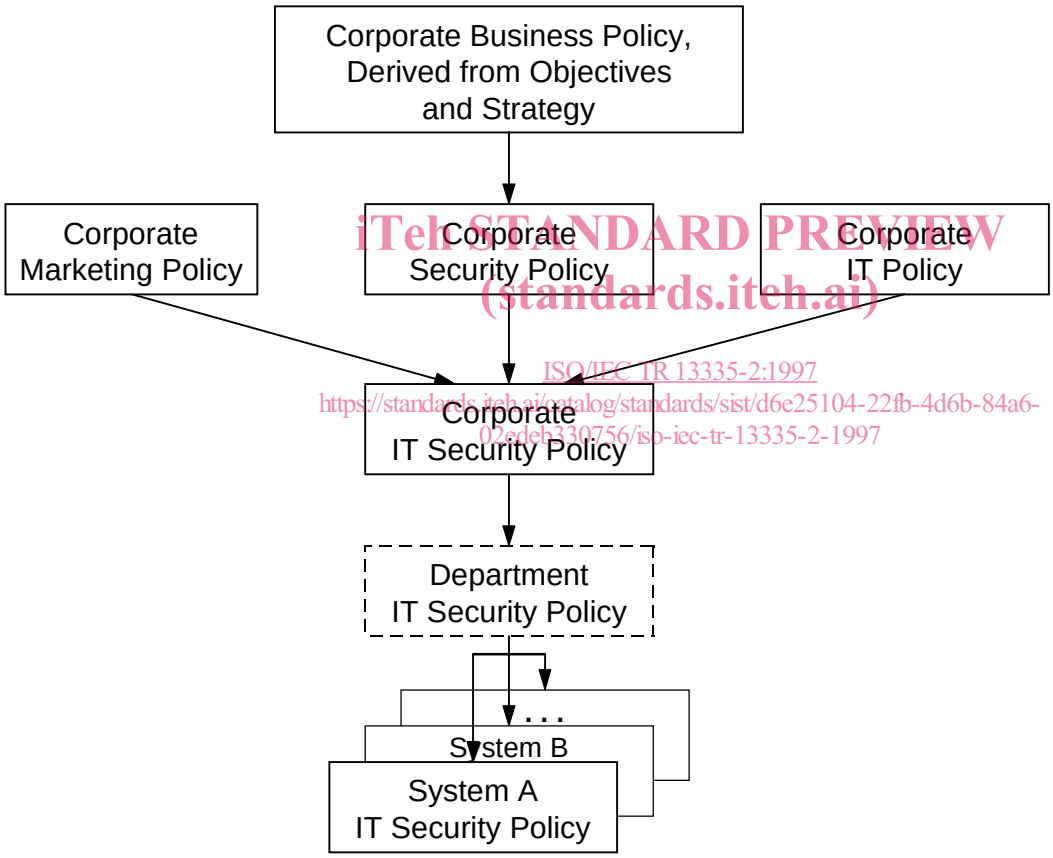

Figure 2 — Policy Relationships

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 business and technical reasons.

8.4 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,
- directives and procedures,
- definition of classes for information classification,
- risk management strategies,
- contingency 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

IT security is an interdisciplinary topic and relevant to every IT project and system and all IT users within an organization. Appropriate assignment and demarcation of 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 directives and standards, 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 3 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 3 uses three organizational levels. This 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.

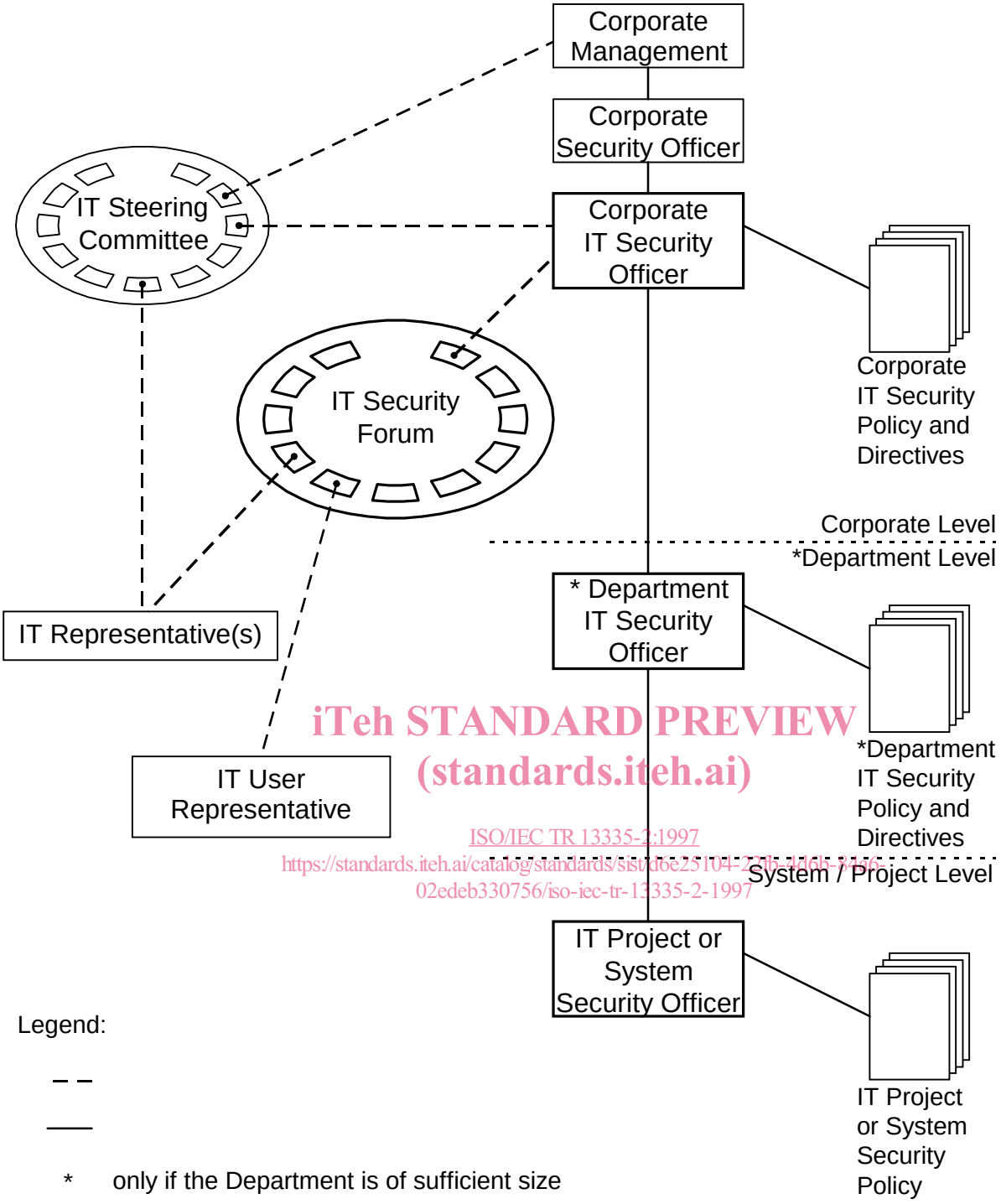

Figure 3 — Example IT Security Organization

9.1.1 IT Security Forum

Such a forum should involve people with the necessary skills to identify requirements, formulate policies, draw up the security programme, 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 programme,
- monitor the implementation of the IT security programme,
- 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 programme 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.

9.1.2 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 is 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 programme,
- liaison with and reporting to the IT security forum and the corporate security officer,
- maintaining the corporate IT security policy and directives,
- co-ordinating incident investigations,
- managing the corporate-wide security awareness programme, and
- determining the terms of reference for IT project and system security officers (and where relevant department IT security officers).

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

9.2 Commitment

It is vital for effective IT security that the management at all levels supports the efforts made by individuals. 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.

9.3 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 3, 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.