

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)

AVA Documents
Document Sharing Hub

Contents

Foreword	iii
Introduction	iv
1. Scope	1
2. Reference	1
3. Definitions	1
4. Structure	2
5. Aim	2
6. Background	3
7. Concepts for the Management of IT Security	3
7.1 Approach	3
7.2 Objectives, Strategies and Policies	4
8. Security Elements	5
8.1 Assets	6
8.2 Threats	6
8.3 Vulnerabilities	8
8.4 Impact	8
8.5 Risk	8
8.6 Safeguards	9
8.7 Residual Risk	9
8.8 Constraints	10
9. Processes for the Management of IT Security	10
9.1 Configuration Management	10
9.2 Change Management	11
9.3 Risk Management	12
9.4 Risk Analysis	12
9.5 Accountability	12
9.6 Security Awareness	13
9.7 Monitoring	13
9.8 Contingency Plans and Disaster Recovery	14
10. Models	14
11. Summary	18

© ISO/IEC 1996

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

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 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*

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.