INTERNATIONAL STANDARD

ISO/IEC 13335-1

First edition
2004-11-15

Information technology — Security techniques — Management of information and communications technology security —

Part 1: Concepts and models for information and communications technology security management

Technologies de l'information — Techniques de sécurité — Gestion de la sécurité des technologies de l'information et des communications — Partie 1: Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications

Reference number
ISO/IEC 13335-1:2004(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document 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 13335-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 13335-1 cancels and replaces ISO/IEC TR 13335-1:1996 and ISO/IEC TR 13335-2:1997, which have been technically revised.

ISO/IEC 13335 consists of the following parts, under the general title *Information technology — Security techniques — Management of information and communications technology security*:

— *Part 1: Concepts and models for information and communications technology security management*

The following part is under preparation:

— *Part 2: Techniques for information and communications technology security risk management*

ISO/IEC 13335-2, when published, will cancel and replace ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000. ISO/IEC TR 13335-5:2001 is currently under revision. In the course of the revision process it will be merged with ISO/IEC 18028-1. When it is published, ISO/IEC 18028-1 will consequently cancel and replace ISO/IEC TR 13335-5:2001.

Introduction

ISO/IEC 13335-1, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management, is the first in a series that deals with the management aspects of planning, implementation and operations, including maintenance, of information and communications technology (ICT) security.

Government and commercial organizations rely heavily on the use of information to conduct their business activities. Compromise of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of an organization's assets can have an adverse impact. Consequently, there is a critical need to protect information and to manage the security of ICT 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 ICT systems not necessarily controlled by their organizations. As well, legislation in many countries requires that management take appropriate action to mitigate risk related to the business and the use of ICT systems. Such legislation may cover not only privacy/data protection but also healthcare and financial markets, among others.

Part 1 provides a high-level management overview. This material is suitable for managers and those who have responsibility for ICT security, for an organization's overall security program or an organization's ICT systems. Part 1 focuses its attention on concepts and models for managing the planning, implementation and operations of ICT security. This Part contains:

- definitions applicable to all parts of this International Standard (Clause 2);
- descriptions of the major security elements and their relationships that are involved in ICT security management (Clause 3);
- corporate security objectives, strategies and policies needed for effective organizational ICT security (Clause 4);
- organization for effective ICT security, models for accountability, explicit assignment and acknowledgement of security responsibilities (Clause 5);
- an overview of ICT security management functions (Clause 6).

The information provided in ISO/IEC 13335-1 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.

ISO/IEC 13335 is organized into two parts.

Part 1 (ISO/IEC 13335-1 Information technology – Security techniques – Management of information

and communications technology security – Part 1: Concepts and models for information and communications technology security management) provides an overview of the fundamental concepts and models used to describe the management of ICT security.

Part 2 (ISO/IEC 13335-2 Information technology – Security techniques - Management of information and communications technology security - Part 2: Techniques for information and communications technology security risk management, to be published) describes security risk management techniques appropriate for use by those involved with management activities.

Note that Parts 3, 4 and 5 are Technical Reports. As noted in the Foreword, ISO/IEC 13335 Part 1 supersedes ISO/IEC TR 13335 Part 1 and Part 2. ISO/IEC 13335 Part 2, when published, will supersede ISO/IEC TR 13335 Part 3 and Part 4.

Part 3 (ISO/IEC TR 13335-3 Information technology – Security techniques - Guidelines for the management of Information Technology security - Part 3: Techniques for the management of Information Technology security) describes security risk management techniques appropriate for use by those involved with management activities.

Part 4 (ISO/IEC TR 13335-4 Information technology – Security techniques - Guidelines for the management of Information Technology 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 2, and how additional assessment methods can be used for the selection of safeguards.

Part 5 (ISO/IEC TR 13335-5 Information technology – Security techniques - Guidelines for the management of Information Technology 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 — Security techniques — Management of information and communications technology security —

Part 1: Concepts and models for information and communications technology security management

1 Scope

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

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

2 Definitions

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

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

2.2
asset
anything that has value to the organization

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

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

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

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

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

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

2.9
impact
the result of an information security incident

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

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

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

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

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

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

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

2.17
reliability
the property of consistent intended behaviour and results

2.18
residual risk
the risk that remains after risk treatment

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

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

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

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

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

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

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

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

3 Security concepts and relationships

3.1 Security principles

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

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

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

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

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

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

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

3.2 Assets

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

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

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

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

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

3.3 Threats

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