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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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.