TECHNICAL REPORT

ISO/IEC TR 13335-5

First edition
2001-11-01

Information technology — Guidelines for the management of IT Security —

Part 5: Management guidance on network security

Technologies de l'information — Lignes directrices pour la gestion de sécurité IT —

Partie 5: Guide pour la gestion de sécurité du réseau

Reference number
ISO/IEC TR 13335-5:2001(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.ch
Web www.iso.ch

Printed in Switzerland

TABLE OF 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.

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

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.

In exceptional circumstances, the joint 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 the joint 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.

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 13335-5, which is a Technical Report of type 3, was prepared by 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 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: Management guidance on network security*

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 five 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 relevant to those involved with management activities during a project life cycle, such as planning, designing, implementing, testing, acquisition or operations.

Part 4 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 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 5:
Management guidance on network security

1. Scope

ISO/IEC TR 13335-5 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.

This part of ISO/IEC TR 13335 builds upon Part 4 of this Technical Report by providing an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks.

It is not within the scope of this TR to provide advice on the detailed design and implementation aspects of the technical safeguard areas. That advice will be dealt with in future ISO documents.

2. References

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

ISO/IEC TR 13335-2:1997, *Information technology — Guidelines for the management of IT Security — Part 2: Managing and planning IT Security*

ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security*

ISO/IEC TR 13335-4:2000, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

ISO/IEC TR 14516:—[1], *Information technology — Guidelines on the use and management of Trusted Third Party (TTP) services*

ISO/IEC 13888 (all parts), *Information technology — Security techniques — Non-repudiation*

ISO/IEC 15947:—[1], *Information technology — Security techniques — IT intrusion detection framework*

ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[1] To be published.

ISO/IEC 7498-3:1997, *Information technology — Open Systems Interconnection — Basic Reference Model: Naming and addressing*

ISO/IEC 7498-4:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework*

(Other relevant, non ISO/IEC, references are given in the Bibliography.)

3. Definitions

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

4. Abbreviations

EDI	-	Electronic Data Interchange
IP	-	Internet Protocol
IT	-	Information Technology
PC	-	Personal Computer
PIN	-	Personal Identification Number
SecOPs	-	Security Operating Procedures
TR	-	Technical Report

5. Structure

The approach taken in TR 13335-5 is to first summarize the overall process for identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and then provide an indication of the potential safeguard areas (in doing so indicating where relevant content of other parts of TR 13335 may be used).

This document describes three simple criteria to aid those persons responsible for IT security to identify potential safeguard areas. These criteria identify (1) the different types of network connections, (2) the different networking characteristics and related trust relationships, and (3) the potential types of security risk associated with network connections (and the use of services provided via those connections). The results of combining these criteria are then utilised to indicate potential safeguard areas. Subsequently, a brief introductory description is provided of the potential safeguard areas, with indications to sources of more detail.

6. Aim

The aim of this document is to provide guidance for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and to provide an indication of the potential safeguard areas.

7. Overview

7.1 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 an organization's business operations. Consequently, there is a critical need to protect information and to manage the security of IT systems within organizations.

This critical need to protect information is particularly important in today's environment because many organizations' IT systems are connected by networks. These network connections can be within the organization, between different organizations, and sometimes between the organization and the general public. Both governmental and commercial organizations conduct business globally. Therefore they depend on all kinds of communication from computerized to other 'classical' means. Their network needs have to be fulfilled, with network security playing an increasing significant role.

Clause 7.2 summarises the recommended process for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and the provision of an indication of the potential safeguard areas. Subsequent clauses then provide further detail of this process.

7.2 Identification Process

When considering network connections, all those persons in the organization who have responsibilities associated with the connections should be clear about the business requirements and benefits. In addition, they and all other users of the connections should be aware of the security risks to, and related safeguard areas for, such network connections. The business requirements and benefits are likely to influence many decisions and actions taken in the process of considering network connections, identifying potential safeguard areas, and then eventually selecting, designing, implementing and maintaining security safeguards. Thus, these business requirements and benefits need to be kept in mind throughout the process. In order to identify the appropriate network related security requirements and safeguard areas, the following tasks will need to be completed:

- review the general security requirements for network connections as set out in the organization’s corporate IT security policy (see clause 8),
- review the network architectures and applications that relate to the network connections, to provide the necessary background to conduct subsequent tasks (see clause 9),
- identify the type or types of network connection that should be considered (see clause 10),
- review the characteristics of the networking proposed (aided as necessary by the information available on network and application architectures), and the associated trust relationships (see clause 11),
- determine the related types of security risk, where possible with the help of risk analysis and management review results - including consideration of the value to business operations of the information to be transferred via the connections, and any other information potentially accessible in an unauthorized way through these connections (see clause 12),
- identify the references to the potential safeguard areas that may be appropriate, on the basis of the type(s) of network connection, the networking characteristics and associated trust relationships, and the types of security risk, determined (see clause 13),
- document and review security architecture options (see clause 14),
- prepare to allocate tasks for the detailed safeguard selection, design, implementation and maintenance, using the identified references to potential safeguard areas and the agreed security architecture (see clause 15).

It should be noted that general advice on the identification of safeguards is contained in Part 4 of TR 13335. This Part (5) of TR 13335 complements Part 4 and provides an introduction on how to identify appropriate safeguard areas with respect to security associated with connections to communications networks.

Figure 1 below explains the overall process of identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and the provision of indications of potential safeguard areas. Each step of the process is described in further detail in the clauses following the figure.

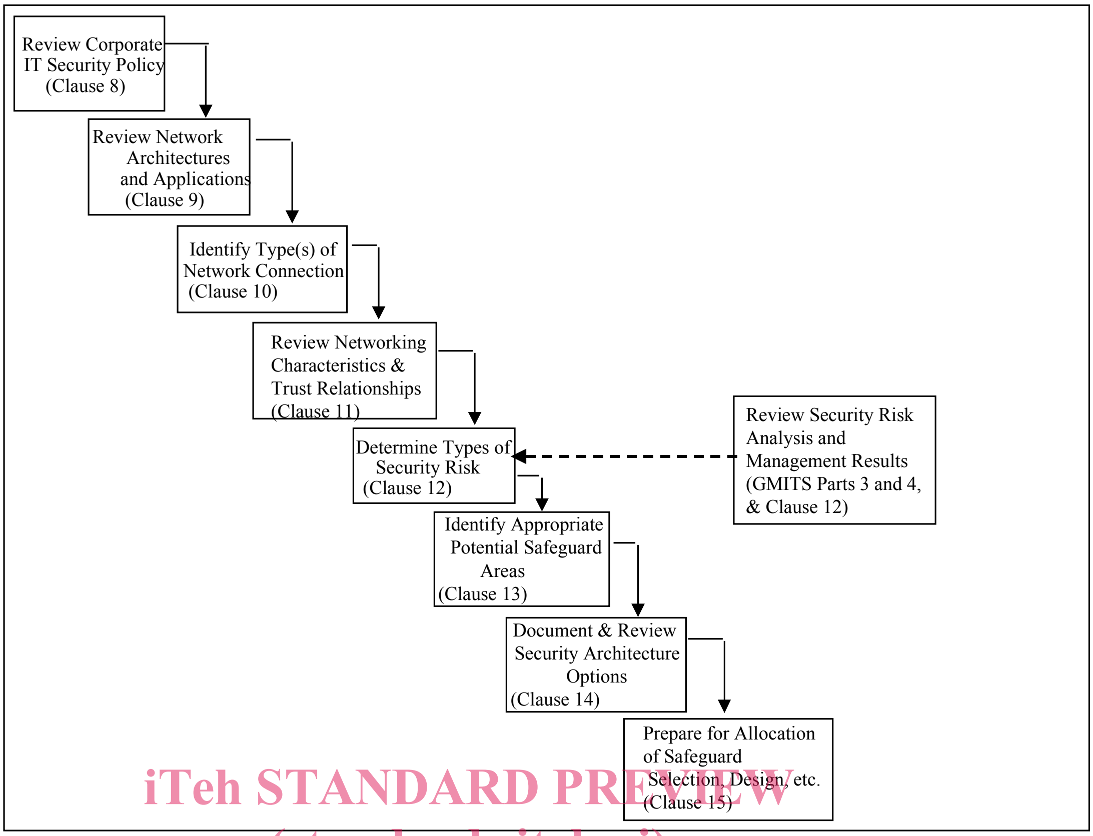
Review Corporate IT Security Policy (Clause 8)
Review Network Architectures and Applications (Clause 9)
Identify Type(s) of Network Connection (Clause 10)
Review Networking Characteristics & Trust Relationships (Clause 11)
Determine Types of Security Risk (Clause 12)
Review Security Risk Analysis and Management Results (GMITS Parts 3 and 4, & Clause 12)
Identify Appropriate Potential Safeguard Areas (Clause 13)
Document & Review Security Architecture Options (Clause 14)
Prepare for Allocation of Safeguard Selection, Design, etc. (Clause 15)

Figure 1: Process for the Identification and Analysis of Communications Related Factors Leading to the Establishment of Network Security Requirements

It should be noted that, in Figure 1, the solid lines represent the main path of the process, and the dotted line where the types of security risk may be determined with the aid of results from a security risk analysis and management review.

In addition to the main path of the process, in certain steps there will be a need to re-visit the results of earlier steps to ensure consistency, in particular the steps ”Review Corporate IT Security Policy” and ”Review Network Architectures and Applications”. For example,

- after types of security risk have been determined there may be a need to review corporate IT security policy because something has arisen that is in fact not covered at that policy level,
- in identifying potential safeguard areas, the corporate IT security policy should be taken into account, because it may, for example, specify that a particular safeguard has to be implemented across the organization regardless of the risks,
- in reviewing security architecture options, to ensure compatibility there will be a need to consider the network architectures and applications.

8 Review Corporate IT Security Policy Requirements

The organization's corporate IT security policy may include statements on the need for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, as well as views on types of threat, and safeguard requirements, that relate directly to network connections.

For example, such a policy could state that:

- availability of certain types of information or services is a major concern,
- no connections via dial-up lines are permitted,
- all connections to the Internet must be made through a security gateway,
- a particular type of security gateway must be used,
- no payment instruction is valid without a digital signature.

Such statements, views and requirements, being applicable organization-wide, must be accounted for in the determination of the types of security risk (see clause 12 below) and the identification of potential safeguard areas for network connections (see clause 13 below). If there are any such security requirements then these can be documented in the draft list of potential safeguard areas, and as necessary reflected in security architecture options. Guidance on the positioning of a corporate IT security policy document within an organization's approach to IT security, and on its content and relationships with other security documentation, is provided in Parts 2 and 3 of TR 13335.

9 Review Network Architectures and Applications

9.1 Introduction

Later steps in the process of moving towards the confirmation of potential safeguard areas, i.e. identification of the:

- type(s) of network connection that will be used,
- networking characteristics and associated trust relationships involved,
- types of security risk,

and indeed the development of the list of potential safeguard areas (and later the related designs for securing a particular connection), should always be done in the context of the network architecture and applications that already exist or are planned.