TECHNICAL REPORT

ISO/IEC TR 13335-4

First edition
2000-03-01

Information technology — Guidelines for the management of IT Security —

Part 4: Selection of safeguards

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

Partie 4: Sélection de sauvegardes

Reference number
ISO/IEC TR 13335-4:2000(E)

© ISO/IEC 2000

This is a preview. Click here to purchase the full publication.

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/IEC 2000

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 either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

EC 2000 – All rights reserved

This is a preview. Click here to purchase the full publication.

Table of Contents

FOREWORD vi

INTRODUCTION vii

1 SCOPE 1

2 REFERENCES 1

3 DEFINITIONS 1

4 AIM 1

5 OVERVIEW 2

6 INTRODUCTION TO SAFEGUARD SELECTION AND THE CONCEPT OF BASELINE SECURITY 4

7 BASIC ASSESSMENTS 8

7.1 IDENTIFICATION OF THE TYPE OF IT SYSTEM 8
7.2 IDENTIFICATION OF PHYSICAL/ENVIRONMENTAL CONDITIONS 8
7.3 ASSESSMENT OF EXISTING/PLANNED SAFEGUARDS 9

8 SAFEGUARDS 9

8.1 ORGANIZATIONAL AND PHYSICAL SAFEGUARDS 10
8.1.1 IT Security Management and Policies *10*
8.1.2 Security Compliance Checking *10*
8.1.3 Incident Handling *11*
8.1.4 Personnel *11*
8.1.5 Operational Issues *12*
8.1.6 Business Continuity Planning *13*
8.1.7 Physical Security *13*
8.2 IT SYSTEM SPECIFIC SAFEGUARDS 18
8.2.1 Identification and Authentication (I&A) *18*
8.2.2 Logical Access Control and Audit *19*
8.2.3 Protection against Malicious Code *19*
8.2.4 Network Management *20*
8.2.5 Cryptography *21*

9 BASELINE APPROACH: SELECTION OF SAFEGUARDS ACCORDING TO THE TYPE OF IT SYSTEM 24

9.1 GENERALLY APPLICABLE SAFEGUARDS 25
9.2 IT SYSTEM SPECIFIC SAFEGUARDS 26

10 SELECTION OF SAFEGUARDS ACCORDING TO SECURITY CONCERNS AND THREATS 27

10.1 ASSESSMENT OF SECURITY CONCERNS 27
10.1.1 Loss of confidentiality *28*
10.1.2 Loss of integrity *28*
10.1.3 Loss of availability *28*
10.1.4 Loss of accountability *29*
10.1.5 Loss of authenticity *29*
10.1.6 Loss of reliability *29*
10.2 SAFEGUARDS FOR CONFIDENTIALITY 30
10.2.1 Eavesdropping *30*

© ISO/IEC 2000 – All rights

This is a preview. Click here to purchase the full publication.

10.2.2 Electromagnetic radiation ... *30*
10.2.3 Malicious code ... *31*
10.2.4 Masquerading of user identity ... *31*
10.2.5 Misrouting/re-routing of messages ... *31*
10.2.6 Software failure ... *31*
10.2.7 Theft ... *32*
10.2.8 Unauthorized access to computers, data, services and applications ... *32*
10.2.9 Unauthorized access to storage media ... *32*
10.3 SAFEGUARDS FOR INTEGRITY ... 33
10.3.1 Deterioration of storage media ... *33*
10.3.2 Maintenance error ... *33*
10.3.3 Malicious code ... *33*
10.3.4 Masquerading of user identity ... *33*
10.3.5 Misrouting/re-routing of messages ... *34*
10.3.6 Non-Repudiation ... *34*
10.3.7 Software failure ... *34*
10.3.8 Supply failure (power, air conditioning) ... *34*
10.3.9 Technical failure ... *35*
10.3.10 Transmission errors ... *35*
10.3.11 Unauthorized access to computers, data, services and applications ... *35*
10.3.12 Use of unauthorized programmes and data ... *36*
10.3.13 Unauthorized access to storage media ... *36*
10.3.14 User error ... *36*
10.4 SAFEGUARDS FOR AVAILABILITY ... 36
10.4.1 Destructive attack ... *37*
10.4.2 Deterioration of storage media ... *37*
10.4.3 Failure of communication equipment and services ... *37*
10.4.4 Fire, water ... *38*
10.4.5 Maintenance error ... *38*
10.4.6 Malicious code ... *38*
10.4.7 Masquerading of user identity ... *38*
10.4.8 Misrouting/re-routing of messages ... *39*
10.4.9 Misuse of resources ... *39*
10.4.10 Natural disasters ... *39*
10.4.11 Software failures ... *39*
10.4.12 Supply failure (power, air conditioning) ... *40*
10.4.13 Technical failures ... *40*
10.4.14 Theft ... *40*
10.4.15 Traffic overloading ... *40*
10.4.16 Transmission errors ... *41*
10.4.17 Unauthorized access to computers, data, services and applications ... *41*
10.4.18 Use of unauthorized programmes and data ... *41*
10.4.19 Unauthorized access to storage media ... *42*
10.4.20 User error ... *42*
10.5 SAFEGUARDS FOR ACCOUNTABILITY, AUTHENTICITY AND RELIABILITY ... 42
10.5.1 Accountability ... *42*
10.5.2 Authenticity ... *42*
10.5.3 Reliability ... *43*

11 SELECTION OF SAFEGUARDS ACCORDING TO DETAILED ASSESSMENTS ... 43

11.1 RELATION BETWEEN PART 3 AND PART 4 OF THIS TECHNICAL REPORT ... 43
11.2 PRINCIPLES OF SELECTION ... 43

12 DEVELOPMENT OF AN ORGANIZATION-WIDE BASELINE ... 45

13 SUMMARY ... 46

BIBLIOGRAPHY ... 46

EC 2000 – All rights reserved
This is a preview. Click here to purchase the full publication.

ANNEX A CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT 47

ANNEX B ETSI BASELINE SECURITY STANDARD FEATURES AND MECHANISMS 49

ANNEX C IT BASELINE PROTECTION MANUAL 51

ANNEX D NIST COMPUTER SECURITY HANDBOOK 53

ANNEX E MEDICAL INFORMATICS: SECURITY CATEGORISATION AND PROTECTION FOR HEALTHCARE INFORMATION SYSTEMS 55

ANNEX F TC68 BANKING AND RELATED FINANCIAL SERVICES - INFORMATION SECURITY GUIDELINES 56

ANNEX G PROTECTION OF SENSITIVE INFORMATION NOT COVERED BY THE OFFICIAL SECRETS ACT - RECOMMENDATIONS FOR COMPUTER WORKSTATIONS. 58

ANNEX H CANADIAN HANDBOOK ON INFORMATION TECHNOLOGY SECURITY 60

© ISO/IEC 2000 – All rights r

This is a preview. Click here to purchase the full publication.

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.

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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, 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), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides 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 13335-4 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: Safeguards for external connections*

EC 2000 – All rights reserved
This is a preview. Click here to purchase the full publication.

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 have responsibility 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 the 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.

© ISO/IEC 2000 – All rights r

This is a preview. Click here to purchase the full publication.

This is a preview. Click here to purchase the full publication.