TECHNICAL REPORT

ISO/IEC TR 13335-2

First edition
1997-12-15

Information technology — Guidelines for the management of IT Security —

Part 2:
Managing and planning IT Security

Technologies de l'information — Lignes directrices pour le management de sécurité IT —

Partie 2: Management et planning de sécurité IT

Reference number
ISO/IEC TR 13335-2:1997(E)

Contents

1 Scope 1
2 Reference 1
3 Terms and definitions 1
4 Structure 1
5 Aim 1
6 Background 1
7 Management of IT Security 2
7.1 Planning and Management Process Overview 2
7.2 Risk Management Overview 3
7.3 Implementation Overview 3
7.4 Follow-up Overview 3
7.5 Integrating IT Security 3
8 Corporate IT Security Policy 3
8.1 Objectives 3
8.2 Management Commitment 4
8.3 Policy Relationships 4
8.4 Corporate IT Security Policy Elements 4
9 Organizational Aspects of IT Security 5
9.1 Roles and Responsibilities 5
9.1.1 IT Security Forum 6
9.1.2 Corporate IT Security Officer 7
9.1.3 IT Project Security Officer and IT System Security Officer 7
9.2 Commitment 7
9.3 Consistent Approach 7
10 Corporate Risk Analysis Strategy Options 8
10.1 Baseline Approach 8
10.2 Informal Approach 8
10.3 Detailed Risk Analysis 9
10.4 Combined Approach 9
11 IT Security Recommendations 9
11.1 Safeguard Selection 9
11.2 Risk Acceptance 10
12 IT System Security Policy 10
13 IT Security Plan 11
14 Implementation of Safeguards 11
15 Security Awareness 11
16 Follow-up 12
16.1 Maintenance 12
16.2 Security Compliance 13
16.3 Monitoring 13
16.4 Incident Handling 13
17 Summary 14