ISO/IEC 27033-1:2015-08 (E)

Information technology - Security techniques - Network security - Part 1: Overview and concepts

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 2

4 Symbols and abbreviated terms 6

5 Structure 8

6 Overview 10
6.1 Background 10
6.2 Network security planning and management 11

7 Identifying risks and preparing to identify security controls 13
7.1 Introduction 13
7.2 Information on current and/or planned networking 13
7.2.1 Security requirements in corporate information security policy 13
7.2.2 Information on current/planned networking 14
7.3 Information security risks and potential control areas 18

8 Supporting controls 21
8.1 Introduction 21
8.2 Management of network security 21
8.2.1 Background 21
8.2.2 Network security management activities 21
8.2.3 Network security roles and responsibilities 23
8.2.4 Network monitoring 24
8.2.5 Evaluating network security 25
8.3 Technical vulnerability management 25
8.4 Identification and authentication 25
8.5 Network audit logging and monitoring 26
8.6 Intrusion detection and prevention 27
8.7 Protection against malicious code 28
8.8 Cryptographic based services 28
8.9 Business continuity management 29

9 Guidelines for the design and implementation of network security 30
9.1 Background 30
9.2 Network technical security architecture/design 30

10 Reference network scenarios - Risks, design, techniques and control issues 32
10.1 Introduction 32
10.2 Internet access services for employees 33
10.3 Enhanced collaboration services 33
10.4 Business to business services 33
10.5 Business to customer services 34

10.6 Outsourced services 34
10.7 Network segmentation 34
10.8 Mobile communication 34
10.9 Networking support for travelling users 35
10.10 Networking support for home and small business offices 35

11 `Technology' topics -- Risks, design techniques and control issues 35

12 Develop and test security solution 36

13 Operate security solution 36

14 Monitor and review solution implementation 37

Annex B (informative) Example template for a SecOPs document 42

Bibliography 47