

ISO/IEC 27033-1:2009-12 (E)

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

Contents		Page
1	Scope	1
2	Normative references	2
3	Terms and definitions	2
4	Abbreviated terms	6
5	Structure	9
6	Overview	11
6.1	Background	11
6.2	Network Security Planning and Management	12
7	Identifying Risks and Preparing to Identify Security Controls	14
7.1	Introduction	14
7.2	Information on Current and/or Planned Networking	15
7.3	Information Security Risks and Potential Control Areas	19
8	Supporting Controls	22
8.1	Introduction	22
8.2	Management of Network Security	23
8.3	Technical Vulnerability Management	26
8.4	Identification and Authentication	27
8.5	Network Audit Logging and Monitoring	28
8.6	Intrusion Detection and Prevention	29
8.7	Protection against Malicious Code	29
8.8	Cryptographic Based Services	30
8.9	Business Continuity Management	31
9	Guidelines for the Design and Implementation of Network Security	32
9.1	Background	32
9.2	Network Technical Security Architecture/Design	32
10	Reference Network Scenarios - Risks, Design, Techniques and Control Issues	34
10.1	Introduction	34
10.2	Internet Access Services for Employees	34
10.3	Enhanced Collaboration Services	35
10.4	Business to Business Services	35
10.5	Business to Customer Services	35
10.6	Outsourcing Services	35
10.7	Network Segmentation	36
10.8	Mobile Communications	36
10.9	Network Support for Traveling Users	36
10.10	Network Support for Home and Small Business Offices	36
11	'Technology' Topics - Risks, Design Techniques and Control Issues	37
12	Develop and Test Security Solution	37
13	Operate Security Solution	38
14	Monitor and Review Solution Implementation	38
Annex A (informative) 'Technology' Topics - Risks, Design Techniques and Control Issues		39

Annex B (informative) Cross-references Between ISO/IEC 27001 and ISO/IEC 27002 Network Security Related Controls, and clauses within this part of ISO/IEC 27033	64
Annex C (informative) Example Template for a SecOPs Document	69