

ISO/IEC 27033-2:2012-08 (E)

Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security

Contents		Page
Foreword		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviations	2
5	Document structure	2
6	Preparing for design of network security	3
6.1	Introduction	3
6.2	Asset identification	3
6.3	Requirements collection	3
6.3.1	Legal and regulatory requirements	3
6.3.2	Business requirements	4
6.3.3	Performance requirements	4
6.4	Review requirements	4
6.5	Review of existing designs and implementations	5
7	Design of network security	5
7.1	Introduction	5
7.2	Design principles	6
7.2.1	Introduction	6
7.2.2	Defence in depth	6
7.2.3	Network Zones	7
7.2.4	Design resilience	7
7.2.5	Scenarios	8
7.2.6	Models and Frameworks	8
7.3	Design Sign off	8
8	Implementation	8
8.1	Introduction	8
8.2	Criteria for Network component selection	9
8.3	Criteria for product or vendor selection	9
8.4	Network management	10
8.5	Logging, monitoring and incident response	11
8.6	Documentation	11
8.7	Test plans and conducting testing	11
8.8	Sign off	12
Annex B (informative)	Example documentation templates	14
B.1	An example network security architecture document template	14
B.1.1	Introduction	14
B.1.2	Business related requirements	14
B.1.3	Technical architecture	14
B.1.4	Network services	17
B.1.5	Hardware/physical layout	17

B.1.6	Software	18
B.1.7	Performance	19
B.1.8	Known issues	19
B.1.9	References	19
B.1.10	Appendices	20
B.1.11	Glossary	20
B.2	An example template for a Functional Security requirements document	20
B.2.1	Introduction	20
B.2.2	Firewall configuration	21
B.2.3	Security risks	21
B.2.4	Security management	22
B.2.5	Security administration	22
B.2.6	Authentication and access control	22
B.2.7	(Audit) Logging	23
B.2.8	Information Security incident management	23
B.2.9	Physical security	23
B.2.10	Personnel security	23
B.2.11	Appendices	23
B.2.12	Glossary	23
Bibliography		28