

ISO/IEC 27032:2012-07 (E)

Information technology - Security techniques - Guidelines for cybersecurity

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Applicability	1
2.1	Audience	1
2.2	Limitations	1
3	Normative references	2
4	Terms and definitions	2
5	Abbreviated terms	8
6	Overview	9
6.1	Introduction	9
6.2	The nature of the Cyberspace	10
6.3	The nature of Cybersecurity	10
6.4	General model	11
6.5	Approach	13
7	Stakeholders in the Cyberspace	14
7.1	Overview	14
7.2	Consumers	14
7.3	Providers	14
8	Assets in the Cyberspace	15
8.1	Overview	15
8.2	Personal assets	15
8.3	Organizational assets	15
9	Threats against the security of the Cyberspace	16
9.1	Threats	16
9.2	Threat agents	17
9.3	Vulnerabilities	17
9.4	Attack mechanisms	18
10	Roles of stakeholders in Cybersecurity	20
10.1	Overview	20
10.2	Roles of consumers	20
10.3	Roles of providers	21
11	Guidelines for stakeholders	22
11.1	Overview	22
11.2	Risk assessment and treatment	22
11.3	Guidelines for consumers	23
11.4	Guidelines for organizations and service providers	25
12	Cybersecurity controls	28
12.1	Overview	28

12.2	Application level controls	28
12.3	Server protection	29
12.4	End-user controls	29
12.5	Controls against social engineering attacks	30
12.6	Cybersecurity readiness	33
12.7	Other controls	33
13	Framework of information sharing and coordination	33
13.1	General	33
13.2	Policies	34
13.3	Methods and processes	35
13.4	People and organizations	36
13.5	Technical	37
13.6	Implementation guidance	38
Annex A (informative) Cybersecurity readiness		40
Annex B (informative) Additional resources		44
Annex C (informative) Examples of related documents		47
Bibliography		50