

ISO/IEC 27005:2008-06 (E)

Information technology - Security techniques - Information security risk management

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Structure of this International Standard	3
5	Background	3
6	Overview of the information security risk management process	4
7	Context establishment	7
7.1	General considerations	7
7.2	Basic Criteria	7
7.3	The scope and boundaries	8
7.4	Organization for information security risk management	9
8	Information security risk assessment	9
8.1	General description of information security risk assessment	9
8.2	Risk analysis	10
8.2.1	Risk identification	10
8.2.2	Risk estimation	14
8.3	Risk evaluation	16
9	Information security risk treatment	17
9.1	General description of risk treatment	17
9.2	Risk reduction	19
9.3	Risk retention	20
9.4	Risk avoidance	20
9.5	Risk transfer	20
10	Information security risk acceptance	21
11	Information security risk communication	21
12	Information security risk monitoring and review	22
12.1	Monitoring and review of risk factors	22
12.2	Risk management monitoring, reviewing and improving	23
Annex A (informative)	Defining the scope and boundaries of the information security risk management process	25
A.1	Study of the organization	25
A.2	List of the constraints affecting the organization	26
A.3	List of the legislative and regulatory references applicable to the organization	28
A.4	List of the constraints affecting the scope	28
Annex B (informative)	Identification and valuation of assets and impact assessment	30

B.1	Examples of asset identification	30
B.1.1	The identification of primary assets	30
B.1.2	List and description of supporting assets	31
B.2	Asset valuation	35
B.3	Impact assessment	38
Annex C (informative) Examples of typical threats		39
Annex D (informative) Vulnerabilities and methods for vulnerability assessment		42
D.1	Examples of vulnerabilities	42
D.2	Methods for assessment of technical vulnerabilities	45
Annex E (informative) Information security risk assessment approaches		47
E.1	High-level information security risk assessment	47
E.2	Detailed information security risk assessment	48
E.2.1	Example 1 Matrix with predefined values	48
E.2.2	Example 2 Ranking of Threats by Measures of Risk	50
E.2.3	Example 3 Assessing a value for the likelihood and the possible consequences of risks	51
Annex F (informative) Constraints for risk reduction		53
Bibliography		55