

ISO/IEC 27005:2011-06 (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	5
5	Background	6
6	Overview of the information security risk management process	7
7	Context establishment	10
7.1	General considerations	10
7.2	Basic Criteria	10
7.2.1	Risk management approach	10
7.2.2	Risk evaluation criteria	10
7.2.3	Impact criteria	11
7.2.4	Risk acceptance criteria	11
7.3	Scope and boundaries	12
7.4	Organization for information security risk management	12
8	Information security risk assessment	13
8.1	General description of information security risk assessment	13
8.2	Risk identification	13
8.2.1	Introduction to risk identification	13
8.2.2	Identification of assets	14
8.2.3	Identification of threats	14
8.2.4	Identification of existing controls	15
8.2.5	Identification of vulnerabilities	15
8.2.6	Identification of consequences	16
8.3	Risk analysis	17
8.3.1	Risk analysis methodologies	17
8.3.2	Assessment of consequences	18
8.3.3	Assessment of incident likelihood	18
8.3.4	Level of risk determination	19
8.4	Risk evaluation	19
9	Information security risk treatment	20
9.1	General description of risk treatment	20
9.2	Risk modification	22
9.3	Risk retention	23
9.4	Risk avoidance	23
9.5	Risk sharing	23
10	Information security risk acceptance	24
11	Information security risk communication and consultation	24

12	Information security risk monitoring and review	25
12.1	Monitoring and review of risk factors	25
12.2	Risk management monitoring, review and improvement	26
Annex A (informative) Defining the scope and boundaries of the information security risk management process		28
A.1	Study of the organization	28
A.2	List of the constraints affecting the organization	29
A.3	List of the legislative and regulatory references applicable to the organization	31
A.4	List of the constraints affecting the scope	31
Annex B (informative) Identification and valuation of assets and impact assessment		33
B.1	Examples of asset identification	33
B.1.1	The identification of primary assets	33
B.1.2	List and description of supporting assets	34
B.2	Asset valuation	38
B.3	Impact assessment	41
Annex C (informative) Examples of typical threats		42
Annex D (informative) Vulnerabilities and methods for vulnerability assessment		45
D.1	Examples of vulnerabilities	45
D.2	Methods for assessment of technical vulnerabilities	48
Annex E (informative) Information security risk assessment approaches		50
E.1	High-level information security risk assessment	50
E.2	Detailed information security risk assessment	51
E.2.1	Example 1 Matrix with predefined values	52
E.2.2	Example 2 Ranking of Threats by Measures of Risk	54
E.2.3	Example 3 Assessing a value for the likelihood and the possible consequences of risks	54
Annex F (informative) Constraints for risk modification		56
27005:2011		58
Bibliography		68