

# ISO/IEC 27005:2022-10 (E)

## Information security, cybersecurity and privacy protection - Guidance on managing information security risks

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
3.1	Terms related to information security risk .....	1
3.2	Terms related to information security risk management .....	5
4	Structure of this document .....	7
5	Information security risk management .....	7
5.1	Information security risk management process .....	7
5.2	Information security risk management cycles .....	9
6	Context establishment .....	9
6.1	Organizational considerations .....	9
6.2	Identifying basic requirements of interested parties .....	10
6.3	Applying risk assessment .....	10
6.4	Establishing and maintaining information security risk criteria .....	11
6.4.1	General .....	11
6.4.2	Risk acceptance criteria .....	11
6.4.3	Criteria for performing information security risk assessments .....	13
6.5	Choosing an appropriate method .....	15
7	Information security risk assessment process .....	16
7.1	General .....	16
7.2	Identifying information security risks .....	17
7.2.1	Identifying and describing information security risks .....	17
7.2.2	Identifying risk owners .....	18
7.3	Analysing information security risks .....	19
7.3.1	General .....	19
7.3.2	Assessing potential consequences .....	19
7.3.3	Assessing likelihood .....	20
7.3.4	Determining the levels of risk .....	22
7.4	Evaluating the information security risks .....	22
7.4.1	Comparing the results of risk analysis with the risk criteria .....	22
7.4.2	Prioritizing the analysed risks for risk treatment .....	23
8	Information security risk treatment process .....	23
8.1	General .....	23
8.2	Selecting appropriate information security risk treatment options .....	23
8.3	Determining all controls that are necessary to implement the information security risk treatment options .....	24
8.4	Comparing the controls determined with those in ISO/IEC 27001:2022, Annex A .....	27
8.5	Producing a Statement of Applicability .....	27
8.6	Information security risk treatment plan .....	28
8.6.1	Formulation of the risk treatment plan .....	28

8.6.2	Approval by risk owners .....	29
8.6.3	Acceptance of the residual information security risks .....	30
9	Operation .....	31
9.1	Performing information security risk assessment process .....	31
9.2	Performing information security risk treatment process .....	31
10	Leveraging related ISMS processes .....	32
10.1	Context of the organization .....	32
10.2	Leadership and commitment .....	32
10.3	Communication and consultation .....	33
10.4	Documented information .....	35
10.4.1	General .....	35
10.4.2	Documented information about processes .....	35
10.4.3	Documented information about results .....	35
10.5	Monitoring and review .....	36
10.5.1	General .....	36
10.5.2	Monitoring and reviewing factors influencing risks .....	37
10.6	Management review .....	38
10.7	Corrective action .....	38
10.8	Continual improvement .....	39
	Annex A (informative) Examples of techniques in support of the risk assessment process .....	41
	Bibliography .....	62