

ISO 28000:2022-03 (E)

Security and resilience - Security management systems - Requirements

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Context of the organization	4
4.1	Understanding the organization and its context	4
4.2	Understanding the needs and expectations of interested parties	4
4.2.1	General	4
4.2.2	Legal, regulatory and other requirements	4
4.2.3	Principles	5
4.3	Determining the scope of the security management system	6
4.4	Security management system	6
5	Leadership	7
5.1	Leadership and commitment	7
5.2	Security policy	7
5.2.1	Establishing the security policy	7
5.2.2	Security policy requirements	8
5.3	Roles, responsibilities and authorities	8
6	Planning	8
6.1	Actions to address risks and opportunities	8
6.1.1	General	8
6.1.2	Determining security-related risks and identifying opportunities	9
6.1.3	Addressing security-related risks and exploiting opportunities	9
6.2	Security objectives and planning to achieve them	9
6.2.1	Establishing security objectives	9
6.2.2	Determining security objectives	10
6.3	Planning of changes	10
7	Support	10
7.1	Resources	10
7.2	Competence	10
7.3	Awareness	11
7.4	Communication	11
7.5	Documented information	11
7.5.1	General	11
7.5.2	Creating and updating documented information	11
7.5.3	Control of documented information	12
8	Operation	12
8.1	Operational planning and control	12
8.2	Identification of processes and activities	12
8.3	Risk assessment and treatment	13
8.4	Controls	13
8.5	Security strategies, procedures, processes and treatments	14
8.5.1	Identification and selection of strategies and treatments	14
8.5.2	Resource requirements	14
8.5.3	Implementation of treatments	14

8.6	Security plans.....	14
8.6.1	General.....	14
8.6.2	Response structure.....	14
8.6.3	Warning and communication.....	15
8.6.4	Content of the security plans.....	15
8.6.5	Recovery.....	16
9	Performance evaluation.....	16
9.1	Monitoring, measurement, analysis and evaluation.....	16
9.2	Internal audit.....	17
9.2.1	General.....	17
9.2.2	Internal audit programme.....	17
9.3	Management review.....	17
9.3.1	General.....	17
9.3.2	Management review inputs.....	18
9.3.3	Management review results.....	18
10	Improvement.....	18
10.1	Continual improvement.....	18
10.2	Nonconformity and corrective action.....	19
	Bibliography.....	20