

ISO 22301:2019-10 (E)

Security and resilience - Business continuity 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	7
4.1	Understanding the organization and its context	7
4.2	Understanding the needs and expectations of interested parties	7
4.2.1	General	7
4.2.2	Legal and regulatory requirements	7
4.3	Determining the scope of the business continuity management system	7
4.3.1	General	7
4.3.2	Scope of the business continuity management system	8
4.4	Business continuity management system	8
5	Leadership	8
5.1	Leadership and commitment	8
5.2	Policy	8
5.2.1	Establishing the business continuity policy	8
5.2.2	Communicating the business continuity policy	9
5.3	Roles, responsibilities and authorities	9
6	Planning	9
6.1	Actions to address risks and opportunities	9
6.1.1	Determining risks and opportunities	9
6.1.2	Addressing risks and opportunities	9
6.2	Business continuity objectives and planning to achieve them	9
6.2.1	Establishing business continuity objectives	9
6.2.2	Determining business continuity objectives	10
6.3	Planning changes to the business continuity management system	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	11
7.5.3	Control of documented information	12
8	Operation	12
8.1	Operational planning and control	12
8.2	Business impact analysis and risk assessment	12
8.2.1	General	12
8.2.2	Business impact analysis	13
8.2.3	Risk assessment	13

8.3	Business continuity strategies and solutions	13
8.3.1	General	13
8.3.2	Identification of strategies and solutions	13
8.3.3	Selection of strategies and solutions	14
8.3.4	Resource requirements	14
8.3.5	Implementation of solutions	14
8.4	Business continuity plans and procedures	14
8.4.1	General	14
8.4.2	Response structure	15
8.4.3	Warning and communication	15
8.4.4	Business continuity plans	16
8.4.5	Recovery	17
8.5	Exercise programme	17
8.6	Evaluation of business continuity documentation and capabilities	17
9	Performance evaluation	17
9.1	Monitoring, measurement, analysis and evaluation	17
9.2	Internal audit	18
9.2.1	General	18
9.2.2	Audit programme(s)	18
9.3	Management review	18
9.3.1	General	18
9.3.2	Management review input	18
9.3.3	Management review outputs	19
10	Improvement	19
10.1	Nonconformity and corrective action	19
10.2	Continual improvement	20
	Bibliography	21