DIN EN ISO 22301:2020-06 (E)

Security and resilience - Business continuity management systems - Requirements (ISO 22301:2019)

Contents

Page

European foreword **4**

Foreword **5**

Introduction **6**

1 Scope **9**

2 Normative references **9**

3 Terms and definitions **9**

4 Context of the organization **15**
4.1 Understanding the organization and its context 15
4.2 Understanding the needs and expectations of interested parties 15
4.2.1 General 15
4.2.2 Legal and regulatory requirements 15
4.3 Determining the scope of the business continuity management system 15
4.3.1 General 15
4.3.2 Scope of the business continuity management system 16
4.4 Business continuity management system 16

5 Leadership **16**
5.1 Leadership and commitment 16
5.2 Policy 16
5.2.1 Establishing the business continuity policy 16
5.2.2 Communicating the business continuity policy 17
5.3 Roles, responsibilities and authorities 17

6 Planning **17**
6.1 Actions to address risks and opportunities 17
6.1.1 Determining risks and opportunities 17
6.1.2 Addressing risks and opportunities 17
6.2 Business continuity objectives and planning to achieve them 17
6.2.1 Establishing business continuity objectives 17
6.2.2 Determining business continuity objectives 18
6.3 Planning changes to the business continuity management system 18

7 Support **18**
7.1 Resources 18
7.2 Competence 18
7.3 Awareness 19
7.4 Communication 19
7.5 Documented information 19
7.5.1 General 19
7.5.2 Creating and updating 19
7.5.3 Control of documented information 20

8 Operation **20**
8.1 Operational planning and control 20
8.2 Business impact analysis and risk assessment 20
8.2.1 General 20
8.2.2 Business impact analysis 21
8.2.3 Risk assessment 21
8.3 Business continuity strategies and solutions 21
8.3.1 General 21

8.3.2 Identification of strategies and solutions 21
8.3.3 Selection of strategies and solutions 22
8.3.4 Resource requirements 22
8.3.5 Implementation of solutions 22
8.4 Business continuity plans and procedures 22
8.4.1 General 22
8.4.2 Response structure 23
8.4.3 Warning and communication 23
8.4.4 Business continuity plans 24
8.4.5 Recovery 25
8.5 Exercise programme 25
8.6 Evaluation of business continuity documentation and capabilities 25
9 Performance evaluation 25
9.1 Monitoring, measurement, analysis and evaluation 25
9.2 Internal audit 26
9.2.1 General 26
9.2.2 Audit programme(s) 26
9.3 Management review 26
9.3.1 General 26
9.3.2 Management review input 26
9.3.3 Management review outputs 27
10 Improvement 27
10.1 Nonconformity and corrective action 27
10.2 Continual improvement 28
Bibliography 29