ISO 22313:2020-02 (E)

Security and resilience - Business continuity manageme nt systems - Guidance on the use of ISO 22301

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Context of the organization 2
4.1 Understanding the organization and its context 2
4.2 Understanding the needs and expectations of interested parties 3
4.2.1 General 3
4.2.2 Legal and regulatory requirements 3
4.3 Determining the scope of the business continuity management system 4
4.3.1 General 4
4.3.2 Scope of the business continuity management system 4
4.3.3 Exclusions to scope 4
4.4 Business continuity management system 5

5 Leadership 5
5.1 Leadership and commitment 5
5.1.1 General 5
5.1.2 Top management 5
5.1.3 Other managerial roles 6
5.2 Policy 6
5.2.1 Establishing the business continuity policy 6
5.2.2 Communicating the business continuity policy 7
5.3 Roles, responsibilities and authorities 7

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 10
6.2.1 Establishing business continuity objectives 10
6.2.2 Determining business continuity objectives 10
6.3 Planning changes to the business continuity management system 10

7 Support 11
7.1 Resources 11
7.1.1 General 11
7.1.2 BCMS resources 11
7.2 Competence 11
7.3 Awareness 13
7.4 Communication 14
7.5 Documented information 15
7.5.1 General 15
7.5.2 Creating and updating 16
7.5.3 Control of documented information 16

8 Operation 17
8.1 Operational planning and control 17
8.1.1 General 17
8.1.2 Business continuity management 18
8.1.3 Maintaining business continuity 19
8.2 Business impact analysis and risk assessment 20
8.2.1 General 20
8.2.2 Business impact analysis 20

8.2.3 Risk assessment 23
8.3 Business continuity strategies and solutions 25
8.3.1 General 25
8.3.2 Identification of strategies and solutions 25
8.3.3 Selection of strategies and solutions 28
8.3.4 Resource requirements 28
8.3.5 Implementation of solutions 34
8.4 Business continuity plans and procedures 35
8.4.1 General 35
8.4.2 Response structure 35
8.4.3 Warning and communication 36
8.4.4 Business continuity plans 38
8.4.5 Recovery 43
8.5 Exercise programme 44
8.5.1 General 44
8.5.2 Design of the exercise programme 44
8.5.3 Exercising business continuity plans 45
8.6 Evaluation of business continuity documentation and capabilities 48
8.6.1 General 48
8.6.2 Measuring effectiveness 49
8.6.3 Outcomes 49

9 Performance evaluation 50
9.1 Monitoring, measurement, analysis and evaluation 50
9.1.1 General 50
9.1.2 Retention of evidence 50
9.1.3 Performance evaluation 50
9.2 Internal audit 51
9.2.1 General 51
9.2.2 Audit programme(s) 51
9.3 Management review 51
9.3.1 General 51
9.3.2 Management review input 51
9.3.3 Management review outputs 52

10 Improvement 52
10.1 Nonconformity and corrective action 52
10.1.1 General 52
10.1.2 Occurrence of nonconformity 53
10.1.3 Retention of documented information 53
10.2 Continual improvement 53

Bibliography 55