DIN EN ISO 22301:2014-12 (E)

Societal security - Business continuity management systems - Requirements (ISO 22301:2012)

Contents

Page

Foreword 3

0 Introduction 4
0.1 General 4
0.2 The Plan-Do-Check-Act (PDCA) model 4
0.3 Components of PDCA in this International Standard 5

1 Scope 7

2 Normative references 7

3 Termsanddefinitions 7

4 Context of the organization 14
4.1 Understanding of the organization and its context 14
4.2 Understanding the needs and expectations of interested parties 15
4.3 Determining the scope of the business continuity management system 15
4.4 Business continuity management system 16

5 Leadership 16
5.1 Leadership and commitment 16
5.2 Management commitment 16
5.3 Policy 17
5.4 Organizational roles, responsibilities and authorities 17

6 Planning 18
6.1 Actions to address risks and opportunities 18
6.2 Business continuity objectives and plans to achieve them 18

7 Support 18
7.1 Resources 18
7.2 Competence 19
7.3 Awareness 19
7.4 Communication 19
7.5 Documented information 20

8 Operation 21
8.1 Operational planning and control 21
8.2 Business impact analysis and risk assessment 21
8.3 Business continuity strategy 22
8.4 Establish and implement business continuity procedures 23
8.5 Exercising and testing 25

9 Performance evaluation 25
9.1 Monitoring, measurement, analysis and evaluation 25
9.2 Internal audit 26
9.3 Management review 27

10 Improvement 28
10.1 Nonconformity and corrective action 28
10.2 Continual improvement 29

Bibliography 30