DIN ISO/IEC 27001:2015-03 (E)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 + Cor. 1:2014)

Contents

Page

National foreword 3

National Annex NA (informative) Bibliography 4

0 Introduction 5

1 Scope 6

2 Normative references 6

3 Terms and definitions 6

4 Context of the organization 6
4.1 Understanding the organization and its context 6
4.2 Understanding the needs and expectations of interested parties 6
4.3 Determining the scope of the information security management system 6
4.4 Information security management system 7

5 Leadership 7
5.1 Leadership and commitment 7
5.2 Policy 7
5.3 Organizational roles, responsibilities and authorities 8

6 Planning 8
6.1 Actions to address risks and opportunities 8
6.2 Information security objectives and planning to achieve them 10

7 Support 10
7.1 Resources 10
7.2 Competence 10
7.3 Awareness 10
7.4 Communication 11
7.5 Documented information 11

8 Operation 12
8.1 Operational planning and control 12
8.2 Information security risk assessment 12
8.3 Information security risk treatment 12

9 Performance evaluation 12
9.1 Monitoring, measurement, analysis and evaluation 12
9.2 Internal audit 13
9.3 Management review 13

10 Improvement 14
10.1 Nonconformity and corrective action 14
10.2 Continual improvement 14

Annex A (normative) Reference control objectives and controls 15

Bibliography 28