DIN EN ISO/IEC 27001:2024-01 (E)

Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022)

Contents

Page

European foreword 3

Foreword 4

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 7
4.4 Information security management system 7

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

6 Planning 8
6.1 Actions to address risks and opportunities 8
6.1.1 General 8
6.1.2 Information security risk assessment 9
6.1.3 Information security risk treatment 9
6.2 Information security objectives and planning to achieve them 10

7 Support 11
7.1 Resources 11
7.2 Competence 11
7.3 Awareness 11
7.4 Communication 11
7.5 Documented information 11
7.5.1 General 11
7.5.2 Creating and updating 12
7.5.3 Control of documented information 12

8 Operation 12
8.1 Operational planning and control 12
8.2 Information security risk assessment 13
8.3 Information security risk treatment 13

9 Performance evaluation 13
9.1 Monitoring, measurement, analysis and evaluation 13
9.2 Internal audit 13
9.2.1 General 13
9.2.2 Internal audit programme 14
9.3 Management review 14
9.3.1 General 14
9.3.2 Management review inputs 14
9.3.3 Management review results 15

10 Improvement **15**
10.1 Continual improvement 15
10.2 Nonconformity and corrective action 15
Annex A (normative) **Information security controls reference** **16**
Bibliography **24**