ISO/IEC 27001:2013-10 (E)

Information technology - Security techniques - Information security management systems - Requirements

Contents

Page

Foreword iv

0 Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Context of the organization 1
4.1 Understanding the organization and its context 1
4.2 Understanding the needs and expectations of interested parties 1
4.3 Determining the scope of the information security management system 1
4.4 Information security management system 2

5 Leadership 2
5.1 Leadership and commitment 2
5.2 Policy 2
5.3 Organizational roles, responsibilities and authorities 3

6 Planning 3
6.1 Actions to address risks and opportunities 3
6.2 Information security objectives and planning to achieve them 5

7 Support 5
7.1 Resources 5
7.2 Competence 5
7.3 Awareness 5
7.4 Communication 6
7.5 Documented information 6

8 Operation 7
8.1 Operational planning and control 7
8.2 Information security risk assessment 7
8.3 Information security risk treatment 7

9 Performance evaluation 7
9.1 Monitoring, measurement, analysis and evaluation 7
9.2 Internal audit 8
9.3 Management review 8

10 Improvement 9
10.1 Nonconformity and corrective action 9
10.2 Continual improvement 9

Annex A (normative) Reference control objectives and controls 10

Bibliography 23