DIN EN ISO/IEC 27006:2021-05 (E)

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management syste ms (ISO/IEC 27006:2015, including Amd 1:2020)

Contents

Page

European foreword 4

Foreword 5

Introduction 6

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 Principles 7

5 General requirements 8
5.1 Legal and contractual matters 8
5.2 Management of impartiality 8
5.2.1 IS 5.2 Conflicts of interest 8
5.3 Liability and financing 8

6 Structural requirements 8

7 Resource requirements 8
7.1 Competence of personnel 8
7.1.1 IS 7.1.1 General considerations 9
7.1.2 IS 7.1.2 Determination of Competence Criteria 9
7.2 Personnel involved in the certification activities 12
7.2.1 IS 7.2 Demonstration of auditor knowledge and experience 12
7.3 Use of individual external auditors and external technical experts 13
7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team 13
7.4 Personnel records 13
7.5 Outsourcing 13

8 Information requirements 14
8.1 Public information 14
8.2 Certification documents 14
8.2.1 IS 8.2 ISMS Certification documents 14
8.3 Reference to certification and use of marks 14
8.4 Confidentiality 14
8.4.1 IS 8.4 Access to organizational records 14
8.5 Information exchange between a certification body and its clients 14

9 Process requirements 14
9.1 Pre-certification activities 14
9.1.1 Application 14
9.1.2 Application review 15
9.1.3 Audit programme 15
9.1.4 Determining audit time 16
9.1.5 Multi-site sampling 16

9.1.6 Multiple management systems 17
9.2 Planning audits 17
9.2.1 Determining audit objectives, scope and criteria 17
9.2.2 Audit team selection and assignments 18
9.2.3 Audit plan 18
9.3 Initial certification 19
9.3.1 IS 9.3.1 Initial certification audit 19
9.4 Conducting audits 20
9.4.1 IS 9.4 General 20
9.4.2 IS 9.4 Specific elements of the ISMS audit 20
9.4.3 IS 9.4 Audit report 20
9.5 Certification decision 21
9.5.1 IS 9.5 Certification decision 21
9.6 Maintaining certification 21
9.6.1 General 21
9.6.2 Surveillance activities 21
9.6.3 Re-certification 22
9.6.4 Special audits 23
9.6.5 Suspending, withdrawing or reducing the scope of certification 23
9.7 Appeals 23
9.8 Complaints 23
9.8.1 IS 9.8 Complaints 23
9.9 Client records 23

10 Management system requirements for certification bodies 23
10.1 Options 23
10.1.1 IS 10.1 ISMS implementation 23
10.2 Option A: General management system requirements 23
10.3 Option B: Management system requirements in accordance with ISO 9001 23

Annex A (informative) Knowledge and skills for ISMS auditing and certification 24

Annex B (normative) Audit time 26

Annex C (informative) Methods for audit time calculations 31

Annex D (informative) Guidance for review of implemented ISO/IEC 27001:2013, Annex A controls 34

Bibliography 41