ISO/IEC 27006-1:2024-03 (E)

Information security, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of information security management systems - Part 1: General

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Principles 4

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

6 Structural requirements 5

7 Resource requirements 5
7.1 Competence of personnel 5
7.1.1 General 5
7.1.2 Generic competence requirements 5
7.1.3 Determination of competence criteria 6
7.2 Personnel involved in the certification activities 8
7.2.1 General 8
7.2.2 Demonstration of auditor knowledge and experience 8
7.3 Use of individual external auditors and external technical experts 9
7.4 Personnel records 9
7.5 Outsourcing 9

8 Information requirements 9
8.1 Public information 9
8.2 Certification documents 9
8.2.1 General 9
8.2.2 ISMS Certification documents 10
8.2.3 Reference of other standards in the ISMS certification documents 10
8.3 Reference to certification and use of marks 10
8.4 Confidentiality 10
8.4.1 General 10
8.4.2 Access to organizational records 10
8.5 Information exchange between a certification body and its clients 10

9 Process requirements 11
9.1 Pre-certification activities 11
9.1.1 Application 11
9.1.2 Application review 11

9.1.3 Audit programme ... 11
9.1.4 Determining audit time ... 12
9.1.5 Multi-site sampling ... 13
9.1.6 Multiple management systems ... 14
9.2 Planning audits ... 14
9.2.1 Determining audit objectives, scope and criteria ... 14
9.2.2 Audit team selection and assignments ... 14
9.2.3 Audit plan ... 15
9.3 Initial certification ... 15
9.3.1 General ... 15
9.3.2 Initial certification audit ... 15
9.4 Conducting audits ... 16

9.4.1 General ... 16
9.4.2 Specific elements of the ISMS audit ... 16
9.4.3 Audit report ... 16
9.5 Certification decision ... 17
9.5.1 General ... 17
9.5.2 Certification decision ... 17
9.6 Maintaining certification ... 17
9.6.1 General ... 17
9.6.2 Surveillance activities ... 17
9.6.3 Re-certification ... 18
9.6.4 Special audits ... 18
9.6.5 Suspending, withdrawing or reducing the scope of certification ... 18
9.7 Appeals ... 19
9.8 Complaints ... 19
9.8.1 General ... 19
9.8.2 Complaints ... 19
9.9 Client records ... 19

10 Management system requirements for certification bodies ... 19
10.1 Options ... 19
10.1.1 General ... 19
10.1.2 ISMS implementation ... 19
10.2 Option A: General management system requirements ... 19
10.3 Option B: Management system requirements in accordance with ISO 9001 ... 19

Annex A (normative) Knowledge and skills for ISMS auditing and certification ... 20

Annex B (informative) Further competence considerations ... 21

Annex C (normative) Audit time ... 23

Annex D (informative) Methods for audit time calculations ... 29

Annex E (informative) Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls ... 33

Bibliography ... 47