

DIN EN ISO/IEC 27006-1:2024-08 (E)

Information security, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of information security management systems - Part 1: General (ISO/IEC 27006-1:2024)

Contents	Page
European foreword	4
Foreword	5
Introduction	6
1 Scope	7
2 Normative references	7
3 Terms and definitions	7
4 Principles	10
5 General requirements	11
5.1 Legal and contractual matters	11
5.2 Management of impartiality	11
5.2.1 General	11
5.2.2 Conflicts of interest	11
5.3 Liability and financing	11
6 Structural requirements	11
7 Resource requirements	11
7.1 Competence of personnel	11
7.1.1 General	11
7.1.2 Generic competence requirements	11
7.1.3 Determination of competence criteria	12
7.2 Personnel involved in the certification activities	14
7.2.1 General	14
7.2.2 Demonstration of auditor knowledge and experience	14
7.3 Use of individual external auditors and external technical experts	15
7.4 Personnel records	15
7.5 Outsourcing	15
8 Information requirements	15
8.1 Public information	15
8.2 Certification documents	15
8.2.1 General	15
8.2.2 ISMS Certification documents	16
8.2.3 Reference of other standards in the ISMS certification documents	16
8.3 Reference to certification and use of marks	16
8.4 Confidentiality	16
8.4.1 General	16
8.4.2 Access to organizational records	16
8.5 Information exchange between a certification body and its clients	16
9 Process requirements	17
9.1 Pre-certification activities	17
9.1.1 Application	17
9.1.2 Application review	17
9.1.3 Audit programme	17
9.1.4 Determining audit time	18
9.1.5 Multi-site sampling	19
9.1.6 Multiple management systems	20

9.2	Planning audits.....	20
9.2.1	Determining audit objectives, scope and criteria.....	20
9.2.2	Audit team selection and assignments.....	20
9.2.3	Audit plan.....	21
9.3	Initial certification.....	21
9.3.1	General.....	21
9.3.2	Initial certification audit.....	21
9.4	Conducting audits.....	22
9.4.1	General.....	22
9.4.2	Specific elements of the ISMS audit.....	22
9.4.3	Audit report.....	22
9.5	Certification decision.....	23
9.5.1	General.....	23
9.5.2	Certification decision.....	23
9.6	Maintaining certification.....	23
9.6.1	General.....	23
9.6.2	Surveillance activities.....	23
9.6.3	Re-certification.....	24
9.6.4	Special audits.....	24
9.6.5	Suspending, withdrawing or reducing the scope of certification.....	24
9.7	Appeals.....	25
9.8	Complaints.....	25
9.8.1	General.....	25
9.8.2	Complaints.....	25
9.9	Client records.....	25
10	Management system requirements for certification bodies.....	25
10.1	Options.....	25
10.1.1	General.....	25
10.1.2	ISMS implementation.....	25
10.2	Option A: General management system requirements.....	25
10.3	Option B: Management system requirements in accordance with ISO 9001.....	25
	Annex A (normative) Knowledge and skills for ISMS auditing and certification.....	26
	Annex B (informative) Further competence considerations.....	27
	Annex C (normative) Audit time.....	28
	Annex D (informative) Methods for audit time calculations.....	34
	Annex E (informative) Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls.....	38
	Bibliography.....	52