

DIN EN ISO/IEC 27706:2026-08 (E)

Information technology, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of privacy information management systems (ISO/IEC 27706:2025)

Contents

Page

Foreword.....	v
Introduction.....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Principles.....	3
5 General requirements.....	3
5.1 Legal and contractual matters.....	3
5.2 Management of impartiality.....	3
5.2.1 General considerations.....	3
5.2.2 Conflicts of interest.....	3
5.3 Liability and financing.....	3
6 Structural requirements.....	3
7 Resource requirements.....	3
7.1 Competence of personnel.....	3
7.1.1 General considerations.....	3
7.1.2 Determination of competence criteria.....	4
7.1.3 Evaluation processes.....	4
7.1.4 Other considerations.....	5
7.2 Personnel involved in the certification activities.....	5
7.3 Use of individual auditors and external technical experts.....	5
7.4 Personnel records.....	5
7.5 Outsourcing.....	5
8 Information Requirements.....	5
8.1 Public information.....	5
8.2 Certification documents.....	5
8.2.1 General.....	5
8.2.2 PIMS certification documents.....	5
8.3 Reference to certification and use of marks.....	5
8.4 Confidentiality.....	6
8.4.1 General.....	6
8.4.2 Access to organizational records.....	6
8.5 Information exchange between a certification body and its clients.....	6
9 Process requirements.....	6
9.1 Pre-certification activities.....	6
9.1.1 Application.....	6
9.1.2 Application review.....	6
9.1.3 Audit programme.....	6
9.1.4 Determining audit time.....	7
9.2 Planning audits.....	7
9.2.1 Determining audit objectives, scope and criteria.....	7
9.2.2 Audit team selection and assignments.....	7
9.2.3 Audit plan.....	7

9.3	Initial certification.....	8
9.3.1	General.....	8
9.3.2	Initial certification audit.....	8
9.4	Conducting audits.....	9
9.4.1	General.....	9
9.4.2	Specific elements of the PIMS audit.....	9
9.4.3	Audit report.....	9
9.5	Certification decision.....	10
9.6	Maintaining certification.....	10
9.6.1	General.....	10
9.6.2	Surveillance activities.....	10
9.7	Appeals.....	10
9.8	Complaints.....	10
9.9	Client records.....	11
10	Management system requirements for certification bodies.....	11
10.1	Options.....	11
10.2	Option A: General management system requirements.....	11
10.3	Option B: Management system requirements in accordance with ISO 9001.....	11
	Annex A (normative) Audit time.....	12
	Annex B (informative) Methods for audit time calculations.....	17
	Annex C (normative) Required knowledge and skills.....	22
	Bibliography.....	24