

ISO/IEC TS 27006-2:2021-02 (E)

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy in formation management systems

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Principles	2
5	General requirements	2
5.1	Legal and contractual matters	2
5.2	Management of impartiality	2
5.3	Liability and financing	2
6	Structural requirements	2
7	Resource requirements	2
7.1	Competence of personnel	2
7.1.1	PS 7.1.1 General considerations	2
7.1.2	PS 7.1.2 Determination of competence criteria	2
7.2	Personnel involved in the certification activities	3
7.2.1	PS 7.2 Demonstration of auditor knowledge and experience	4
7.2.2	PS 7.2.1.1 Selecting auditors	4
7.3	Use of individual external auditors and external technical experts	4
7.4	Personnel records	4
7.5	Outsourcing	4
8	Information requirements	4
8.1	Public information	4
8.2	Certification documents	4
8.2.1	PS 8.2 PIMS Certification documents	4
8.3	Reference to certification and use of marks	5
8.4	Confidentiality	5
8.5	Information exchange between a certification body and its clients	5
9	Process requirements	5
9.1	Pre-certification activities	5
9.1.1	Application	5
9.1.2	Application review	5
9.1.3	Audit programme	5
9.1.4	Determining audit time	6
9.1.5	Multi-site sampling	7
9.1.6	Multiple management systems	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	7

9.4	Conducting audits	7
9.4.1	IS 9.4 General	7
9.4.2	IS 9.4 Specific elements of the ISMS audit	7
9.4.3	IS 9.4 Audit report	7
9.5	Certification decision	7
9.6	Maintaining certification	8
9.6.1	General	8
9.6.2	Surveillance activities	8
9.6.3	Re-certification	8
9.6.4	Special audits	8
9.6.5	Suspending, withdrawing or reducing the scope of certification	8
9.7	Appeals	8
9.8	Complaints	8
9.9	Client records	8
10	Management system requirements for certification bodies	8
10.1	Options	8
10.2	Option A: General management system requirements	8
10.3	Option B: Management system requirements in accordance with ISO 9001	9