

ISO/IEC 27006:2011-12 (E)

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Principles	2
5	General requirements	2
5.1	Legal and contractual matter	2
5.2	Management of impartiality	2
5.3	Liability and financing	3
6	Structural requirements	3
6.1	Organizational structure and top management	3
6.2	Committee for safeguarding impartiality	3
7	Resource requirements	3
7.1	Competence of management and personnel	3
7.2	Personnel involved in the certification activities	4
7.3	Use of individual external auditors and external technical experts	6
7.4	Personnel records	6
7.5	Outsourcing	6
8	Information requirements	6
8.1	Publicly accessible information	6
8.2	Certification documents	7
8.3	Directory of certified clients	7
8.4	Reference to certification and use of marks	7
8.5	Confidentiality	7
8.6	Information exchange between a certification body and its clients	7
9	Process requirements	8
9.1	General requirements	8
9.2	Initial audit and certification	11
9.3	Surveillance activities	15
9.4	Recertification	16
9.5	Special audits	16
9.6	Suspending, withdrawing or reducing scope of certification	16
9.7	Appeals	17
9.8	Complaints	17
9.9	Records of applicants and clients	17
10	Management system requirements for certification bodies	17
10.1	Options	17
10.2	Option 1 - Management system requirements in accordance with ISO 9001	17
10.3	Option 2 - General management system requirements	17

Annex A (informative) Analysis of a client organization's complexity and sector-specific aspects ...	19
Annex B (informative) Example areas of auditor competence	22
Annex C (informative) Audit time	24