

E DIN EN ISO/IEC 27006-1:2022-08 (D/E)

Erscheinungsdatum: 2022-07-15

Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren - Teil 1: Allgemeines (ISO/IEC DIS 27006-1:2022); Deutsche und Englische Fassung prEN ISO/IEC 27006-1:2022

Requirements for bodies providing audit and certification of information security management systems - Part 1: General (ISO/IEC DIS 27006-1:2022); German and English version prEN ISO/IEC 27006-1:2022

Inhalt	Seite
Europäisches Vorwort.....	5
Vorwort.....	6
Einleitung.....	7
1 Anwendungsbereich.....	8
2 Normative Verweisungen.....	8
3 Begriffe.....	8
4 Grundsätze.....	12
5 Allgemeine Anforderungen.....	12
5.1 Rechts- und Vertragsfragen.....	12
5.2 Handhabung der Unparteilichkeit.....	12
5.2.1 IS 5.2 Interessenkonflikte.....	12
5.3 Haftung und Finanzierung.....	13
6 Strukturelle Anforderungen.....	13
7 Anforderungen an Ressourcen.....	13
7.1 Kompetenz des Personals.....	13
7.1.1 IS 7.1.1 Allgemeine Betrachtungen.....	13
7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien.....	13
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist.....	17
7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren.....	17
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten.....	18
7.3.1 IS 7.3 Einsatz einzelner externer Auditoren und externer Fachexperten als Teil des Auditteams.....	18
7.4 Aufzeichnungen über Personal.....	18
7.5 Ausgliederung.....	18
8 Anforderungen an Informationen.....	18
8.1 Öffentliche Informationen.....	18
8.2 Zertifizierungsdokumente.....	18
8.2.1 IS 8.2 ISMS-Zertifizierungsdokumente.....	18
8.3 Verweisung auf Zertifizierung und Zeichennutzung.....	19
8.4 Vertraulichkeit.....	19
8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation.....	19
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden.....	19
8.5.1 IS 8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden.....	19
9 Anforderungen an Prozesse.....	20
9.1 Tätigkeiten vor der Zertifizierung.....	20
9.1.1 Antrag.....	20

9.1.2	Antragsprüfung.....	20
9.1.3	Auditprogramm	20
9.1.4	Ermittlung des Auditzeitaufwands.....	22
9.1.5	Stichprobenprüfung an mehreren Standorten.....	22
9.1.6	Mehrfach-Managementsysteme	24
9.2	Planung von Audits.....	24
9.2.1	Festlegung der Auditziele, des Auditumfangs und der Auditkriterien.....	24
9.2.2	Auswahl des Auditteams und Aufgabenzuordnung	25
9.2.3	Auditplan	26
9.3	Erstzertifizierung.....	26
9.3.1	IS 9.3.1 Erstzertifizierungsaudit.....	26
9.4	Durchführen von Audits.....	28
9.4.1	IS 9.4 Allgemeines	28
9.4.2	IS 9.4 Spezifische Elemente des ISMS-Audits.....	28
9.4.3	IS 9.4 Auditbericht	28
9.5	Zertifizierungsentscheidung	29
9.5.1	IS 9.5 Zertifizierungsentscheidung.....	29
9.6	Aufrechterhaltung der Zertifizierung.....	30
9.6.1	Allgemeines.....	30
9.6.2	Überwachungstätigkeiten	30
9.6.3	Re-Zertifizierung	31
9.6.4	Audits aus besonderem Anlass	31
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung....	31
9.7	Einsprüche.....	31
9.8	Beschwerden	32
9.8.1	IS 9.8 Beschwerden.....	32
9.9	Aufzeichnungen zu Kunden	32
10	Managementsystemanforderungen für Zertifizierungsstellen.....	32
10.1	Optionen.....	32
10.1.1	IS 10.1 ISMS-Umsetzung	32
10.2	Option A: Allgemeine Managementsystemanforderungen.....	32
10.3	Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001	32
Anhang A (informativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung.....		33
A.1	Übersicht.....	33
A.2	Allgemeine Kompetenzbetrachtungen.....	33
A.3	Spezielle Betrachtungen zu Wissen und Erfahrung	34
A.3.1	Typisches Wissen in Bezug auf ISMS	34
Anhang B (normativ) Auditzeitaufwand		35
B.1	Einleitung.....	35
B.2	Konzepte	36
B.2.1	Anzahl der von der Organisation gesteuerten Personen	36
B.2.2	Auditortag.....	36
B.2.3	Temporärer Standort.....	36
B.3	Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit	36
B.3.1	Allgemeines.....	36
B.3.2	Methoden aus der Ferne zur Durchführung von Audits	36
B.3.3	Berechnung des Auditzeitaufwands.....	37
B.3.4	Faktoren für die Anpassung des Auditzeitaufwands.....	38
B.3.5	Einschränkung der Abweichung von der Auditzeit.....	40
B.3.6	Vor-Ort-Auditzeitaufwand	40
B.4	Auditzeitaufwand für das Überwachungsaudit.....	40
B.5	Auditzeitaufwand für das Re-Zertifizierungsaudit	40
B.6	Auditzeitaufwand für mehrere Standorte.....	40
B.7	Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs	41
B.8	Auditzeitaufwand für eine branchenspezifische Normerweiterung.....	41
Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands		42

C.1	Allgemeines	42
C.2	Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	42
C.3	Beispiel für die Auditzeitaufwandberechnung	44
Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach		
	ISO/IEC 27001:2022, Anhang A	47
D.1	Zweck	47
D.2	Anwendung von Tabelle D.1	47
D.2.1	Allgemeines	47
D.2.2	Spalte „Systemprüfung“	47
D.2.3	Spalte „Sichtprüfung“	48
D.2.4	Spalte „Typischer Nachweis der Gestaltung und Umsetzung von Maßnahmen“	48
Anhang E (informativ) Anforderungen und Einschränkungen bei Zertifizierungen nach		
	branchenspezifischen Normerweiterungen	64
E.1	Allgemeines	64
Literaturhinweise		65