

E DIN EN ISO/IEC 27006-2:2023-08 (D/E)

Erscheinungsdatum: 2023-07-21

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren - Teil 2: Datenschutz-Managementsysteme (ISO/IEC DIS 27006-2:2023); Deutsche und Englische Fassung prEN ISO/IEC 27006-2:2023

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems (ISO/IEC DIS 27006-2:2023); German and English version prEN ISO/IEC 27006-2:2023

Inhalt	Seite
Europäisches Vorwort.....	8
Vorwort.....	9
Einleitung.....	10
1 Anwendungsbereich.....	11
2 Normative Verweisungen.....	11
3 Begriffe.....	11
4 Grundsätze.....	13
5 Allgemeine Anforderungen.....	13
5.1 Rechts- und Vertragsfragen.....	13
5.2 Handhabung der Unparteilichkeit.....	13
5.2.1 Allgemeines.....	13
5.2.2 Interessenkonflikte.....	13
5.3 Haftung und Finanzierung.....	13
6 Strukturelle Anforderungen.....	14
7 Anforderungen an Ressourcen.....	14
7.1 Kompetenz des Personals.....	14
7.1.1 Allgemeines.....	14
7.1.2 Allgemeine Betrachtungen.....	14
7.1.3 Bestimmung der Kompetenzkriterien.....	14
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist.....	15
7.2.1 Allgemeines.....	15
7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren.....	16
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten.....	16
7.4 Aufzeichnungen über Personal.....	16
7.5 Ausgliederung.....	16
8 Anforderungen an Informationen.....	16
8.1 Öffentliche Informationen.....	16
8.2 Zertifizierungsdokumente.....	17
8.2.1 Allgemeines.....	17
8.2.2 PIMS-Zertifizierungsdokumente.....	17
8.3 Verweisung auf Zertifizierung und Zeichennutzung.....	17
8.4 Vertraulichkeit.....	17
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden.....	17
9 Anforderungen an Prozesse.....	18
9.1 Tätigkeiten vor der Zertifizierung.....	18
9.1.1 Antrag.....	18

9.1.2	Antragsprüfung.....	18
9.1.3	Auditprogramm	18
9.1.4	Ermittlung des Auditzeitaufwandes.....	19
9.1.5	Stichprobenprüfung an mehreren Standorten.....	19
9.1.6	Mehrfach-Managementsysteme	19
9.2	Planung von Audits.....	19
9.2.1	Festlegung der Auditziele, des Auditanwendungsbereichs und der Auditkriterien.....	19
9.2.2	Auswahl des Auditteams und Aufgabenzuordnung	19
9.2.3	Auditplan	19
9.3	Erstzertifizierung.....	19
9.4	Durchführen von Audits.....	20
9.4.1	Allgemeines.....	20
9.4.2	Spezifische Elemente des ISMS-Audits	20
9.4.3	Auditbericht.....	20
9.5	Zertifizierungsentscheidung	20
9.5.1	Allgemeines.....	20
9.5.2	Zertifizierungsentscheidung	20
9.6	Aufrechterhaltung der Zertifizierung.....	20
9.6.1	Allgemeines.....	20
9.6.2	Überwachungstätigkeiten	20
9.6.3	Re-Zertifizierung	20
9.6.4	Audits aus besonderem Anlass	20
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Anwendungsbereichs der Zertifizierung.....	21
9.7	Einsprüche.....	21
9.8	Beschwerden	21
9.9	Aufzeichnungen zu Kunden	21
10	Managementsystemanforderungen für Zertifizierungsstellen.....	21
10.1	Optionen.....	21
10.2	Option A: Allgemeine Managementsystemanforderungen.....	21
10.3	Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001	21
Anhang A (normativ) Auditzeitaufwand		22
A.1	Einleitung.....	22
A.2	Konzepte	22
A.3	Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit	23
A.3.1	Allgemeines.....	23
A.3.2	Fernaudit	23
A.3.3	Berechnung des Auditzeitaufwands.....	23
A.3.4	Faktoren für die Anpassung des Auditzeitaufwands.....	24
A.3.5	Einschränkung der Abweichung vom Auditzeitaufwand	25
A.3.6	Vor-Ort-Auditzeitaufwand	25
A.4	Auditzeitaufwand für das Überwachungsaudit.....	25
A.5	Auditzeitaufwand für das Re-Zertifizierungsaudit	25
A.6	Auditzeitaufwand für mehrere Standorte.....	25
A.7	Auditzeitaufwand-Abweichungen bei ISMS-Audits, die zu verschiedenen Zeiten stattfinden	25
Anhang B (informativ) Methoden für Berechnungen des Auditzeitaufwands.....		26
B.1	Allgemeines.....	26
B.2	Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands.....	26
B.3	Beispiel für die Auditzeitaufwandberechnung.....	28
Literaturhinweise.....		31

Tabellen

Tabelle A.1 — Auditzeitaufwandstabelle	23
Tabelle B.1 — Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands.....	26
Tabelle B.2 — Risiken bei der Verarbeitung von pbD.....	28
Tabelle B.3 — Operative Risiken	29
Tabelle B.4 — Auswirkung der Faktoren auf den Auditzeitaufwand.....	30