

# DIN CEN ISO/IEC/TS 27006-2:2023-12 (D)

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren - Teil 2: Datenschutz-Managementsysteme (ISO/IEC TS 27006-2:2021); Deutsche Fassung CEN ISO/IEC/TS 27006-2:2022

---

Inhalt	Seite
Europäisches Vorwort.....	7
Vorwort.....	8
Einleitung.....	9
1 Anwendungsbereich.....	10
2 Normative Verweisungen.....	10
3 Begriffe.....	10
4 Grundsätze.....	10
5 Allgemeine Anforderungen.....	11
5.1 Rechts- und Vertragsfragen.....	11
5.2 Handhabung der Unparteilichkeit.....	11
5.3 Haftung und Finanzierung.....	11
6 Strukturelle Anforderungen.....	11
7 Anforderungen an Ressourcen.....	11
7.1 Kompetenz des Personals.....	11
7.1.1 PS 7.1.1 Allgemeine Betrachtungen.....	11
7.1.2 PS 7.1.2 Bestimmung von Kompetenzkriterien.....	11
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist.....	13
7.2.1 PS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren.....	13
7.2.2 PS 7.2.1.1 Auswahl von Auditoren.....	13
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten.....	13
7.4 Aufzeichnungen über Personal.....	13
7.5 Ausgliederung.....	13
8 Anforderungen an Informationen.....	14
8.1 Öffentliche Informationen.....	14
8.2 Zertifizierungsdokumente.....	14
8.2.1 PS 8.2 PIMS-Zertifizierungsdokumente.....	14
8.3 Verweisung auf Zertifizierung und Zeichennutzung.....	14
8.4 Vertraulichkeit.....	14
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden.....	15
9 Anforderungen an Prozesse.....	15
9.1 Tätigkeiten vor der Zertifizierung.....	15
9.1.1 Antrag.....	15
9.1.2 Antragsprüfung.....	15
9.1.3 Auditprogramm.....	15
9.1.4 Ermittlung des Auditzeitaufwandes.....	16
9.1.5 Stichprobenprüfung an mehreren Standorten.....	16
9.1.6 Mehrfach-Managementsysteme.....	16
9.2 Planung von Audits.....	16
9.2.1 Festlegung der Auditziele, des Auditanwendungsbereichs und der Auditkriterien.....	16
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung.....	16
9.2.3 Auditplan.....	17

9.3	<b>Erstzertifizierung</b> .....	17
9.4	<b>Durchführen von Audits</b> .....	17
9.4.1	<b>IS 9.4 Allgemeines</b> .....	17
9.4.2	<b>IS 9.4 Spezifische Elemente des ISMS-Audits</b> .....	17
9.4.3	<b>IS 9.4 Auditbericht</b> .....	17
9.5	<b>Zertifizierungsentscheidung</b> .....	17
9.6	<b>Aufrechterhaltung der Zertifizierung</b> .....	17
9.6.1	<b>Allgemeines</b> .....	17
9.6.2	<b>Überwachungstätigkeiten</b> .....	18
9.6.3	<b>Re-Zertifizierung</b> .....	18
9.6.4	<b>Audits aus besonderem Anlass</b> .....	18
9.6.5	<b>Aussetzung, Zurückziehung oder Einschränkung des Anwendungsbereichs der Zertifizierung</b> .....	18
9.7	<b>Einsprüche</b> .....	18
9.8	<b>Beschwerden</b> .....	18
9.9	<b>Aufzeichnungen zu Kunden</b> .....	18
10	<b>Managementsystemanforderungen für Zertifizierungsstellen</b> .....	18
10.1	<b>Optionen</b> .....	18
10.2	<b>Option A: Allgemeine Managementsystemanforderungen</b> .....	18
10.3	<b>Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001</b> .....	18