DIN EN ISO/IEC 27706:2026-08 (D)

Informationssicherheit, Cybersicherheit und Datenschutz - Anforderungen an Stellen, die Datenschutz-Managementsysteme auditieren und zertifizieren (ISO/IEC 27706:2025); Deutsche Fassung EN ISO/IEC 27706:2025

Inhalt

Seite

Europäisches Vorwort 7
Vorwort 8
Einleitung 10
1 Anwendungsbereich 11
2 Normative Verweisungen 11
3 Begriffe und Definitionen 11
4 Grundsätze 13
5 Allgemeine Anforderungen 13
5.1 Rechts- und Vertragsfragen 13
5.2 Handhabung der Unparteilichkeit 13
5.2.1 Allgemeine Betrachtungen 13
5.2.2 Interessenkonflikte 13
5.3 Haftung und Finanzierung 14
6 Strukturelle Anforderungen 14
7 Anforderungen an Ressourcen 14
7.1 Kompetenz des Personals 14
7.1.1 Allgemeine Betrachtungen 14
7.1.2 Bestimmung der Kompetenzkriterien 14
7.1.3 Beurteilungsprozesse 14
7.1.4 Sonstige Betrachtungen 15
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist 15
7.3 Einsatz einzelner Auditoren und externer Fachexperten 15
7.4 Aufzeichnungen über Personal 15
7.5 Ausgliederung 15
8 Anforderungen an Informationen 15
8.1 Öffentliche Informationen 15
8.2 Zertifizierungsdokumente 16
8.2.1 Allgemeines 16
8.2.2 DSMS-Zertifizierungsdokumente 16
8.3 Verweisung auf Zertifizierung und Zeichennutzung 16
8.4 Vertraulichkeit 16
8.4.1 Allgemeines 16
8.4.2 Zugang zu den Aufzeichnungen der Organisation 16
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden 16
9 Prozessanforderungen 17
9.1 Tätigkeiten vor der Zertifizierung 17
9.1.1 Antrag 17
9.1.2 Antragsprüfung 17
9.1.3 Auditprogramm 17
9.1.4 Ermittlung des Auditzeitaufwands 17
9.2 Planung von Audits 17

9.2.1 Festlegung der Auditziele, des Auditanwendungsbereichs und der Auditkriterien ... 17
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung ... 18
9.2.3 Auditplan ... 18
9.3 Erstzertifizierung ... 18
9.3.1 Allgemeines ... 18
9.3.2 Erstzertifizierungsaudit ... 18
9.4 Durchführen von Audits ... 20
9.4.1 Allgemeines ... 20
9.4.2 Spezifische Elemente des DSMS-Audits ... 20
9.4.3 Auditbericht ... 20
9.5 Zertifizierungsentscheidung ... 21
9.6 Aufrechterhaltung der Zertifizierung ... 21
9.6.1 Allgemeines ... 21
9.6.2 Überwachungstätigkeiten ... 21
9.7 Einsprüche ... 22
9.8 Beschwerden ... 22
9.9 Aufzeichnungen zu Kunden ... 22

10 Managementsystemanforderungen für Zertifizierungsstellen ... 22
10.1 Optionen ... 22
10.2 Option A: Allgemeine Managementsystemanforderungen ... 22
10.3 Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001 ... 22

Anhang A (normativ) Auditzeitaufwand ... 23
A.1 Einleitung ... 23
A.2 Konzepte ... 24
A.2.1 Anzahl der von der Organisation gesteuerten Personen ... 24
A.2.2 Auditortag ... 24
A.2.3 Temporärer Standort ... 24
A.3 Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit ... 24
A.3.1 Allgemeines ... 24
A.3.2 Fernaudit ... 24
A.3.3 Berechnung des Auditzeitaufwands ... 25
A.3.4 Bestimmung der ursprünglichen Personenanzahl ... 26
A.3.5 Faktoren für die Anpassung des Auditzeitaufwands ... 27
A.3.6 Einschränkung der Abweichung vom Auditzeitaufwand ... 27
A.3.7 Vor-Ort-Auditzeitaufwand ... 27
A.4 Auditzeitaufwand für das Überwachungsaudit ... 28
A.5 Auditzeitaufwand für das Re-Zertifizierungsaudit ... 28
A.6 Auditzeitaufwand für mehrere Standorte ... 28
A.7 Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs ... 28

Anhang B (informativ) Verfahren für Berechnungen des Auditzeitaufwands ... 30
B.1 Allgemeines ... 30
B.2 Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands ... 30
B.3 Beispiel für die Auditzeitaufwandberechnung ... 32

Anhang C (normativ) Erforderliche Kenntnisse und Fertigkeiten ... 35
C.1 Allgemeines ... 35
C.2 Kompetenzanforderungen an Managementsystem-Auditoren und -Auditteams ... 35
C.2.1 Allgemeines ... 35
C.2.2 Kompetenzanforderungen an DSMS-Auditoren und -Auditteams ... 35
C.3 Anforderungen an die Kompetenz des Personals, das Auditberichte überprüft und Zertifizierungsentscheidungen trifft ... 36
C.3.1 Allgemeines ... 36
C.3.2 Anforderungen an die Kompetenz des Personals, das Auditberichte überprüft und Zertifizierungsentscheidungen für DSMS trifft ... 36
C.4 Anforderungen an die Kompetenz des Personals, das Antragsprüfungen durchführt, um die erforderliche Kompetenz des Auditteams zu ermitteln, die Mitglieder des Auditteams auszuwählen und den Auditzeitaufwand zu ermitteln ... 36

Literaturhinweise **37**

Tabellen

Tabelle A.1 — Auditzeitaufwandstabelle **25**

Tabelle B.1 — Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands **30**

Tabelle B.2 — Risiken bei der Verarbeitung von pbD **32**

Tabelle B.3 — Operative Risiken **33**

Tabelle B.4 — Auswirkung der Faktoren auf den Auditzeitaufwand **34**