

DIN CEN ISO/IEC/TS 27006-2



ICS 03.120.20; 35.030

**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**

Requirements for bodies providing audit and certification of information security management systems –

Part 2: Privacy information management systems (ISO/IEC TS 27006-2:2021);
German version CEN ISO/IEC/TS 27006-2:2022

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité –

Partie 2: Systèmes de management des informations de sécurité
(ISO/IEC TS 27006-2:2021);
Version allemande CEN ISO/IEC/TS 27006-2:2022

Gesamtumfang 19 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC TS 27006-2:2021 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als CEN ISO/IEC/TS 27006-2:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Zu diesem Dokument ist bereits ein Nachfolgedokument in Erarbeitung, dessen Entwurf als DIN EN ISO/IEC 27006-2:2023-08, *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* erschienen ist.

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Erfahrungen mit dieser Technischen Spezifikation sind erbeten:

- vorzugsweise als Datei per E-Mail an nia@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <http://www.din.de/stellungnahme> abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss „Informationstechnik und Anwendungen“ (NIA), 10772 Berlin (Hausanschrift: Burggrafenstraße 6, 10787 Berlin).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 17021-1	siehe	DIN EN ISO/IEC 17021-1
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27006:2015	siehe	DIN EN ISO/IEC 27006:2021-05
ISO/IEC 27701	siehe	DIN EN ISO/IEC 27701
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 17021-1, *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren — Teil 1: Anforderungen*

DIN EN ISO/IEC 27000, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie*

DIN EN ISO/IEC 27001, *Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27006:2021-05, *Informationstechnik — IT-Sicherheitsverfahren — Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd 1:2020); Deutsche Fassung EN ISO/IEC 27006:2020*

DIN EN ISO/IEC 27701, *Sicherheitstechniken — Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz — Anforderungen und Leitlinien*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

– Leerseite –

Deutsche Fassung

Anforderungen an Stellen, die Informationssicherheits-
Managementsysteme auditieren und zertifizieren —
Teil 2: Datenschutz-Managementsysteme
(ISO/IEC TS 27006-2:2021)

Requirements for bodies providing audit and certification
of information security management systems —
Part 2: Privacy information management systems
(ISO/IEC TS 27006-2:2021)

Exigences pour les organismes procédant à l'audit et à
la certification des systèmes de management des
informations de sécurité —
Partie 2: Systèmes de management des informations de
sécurité (ISO/IEC TS 27006-2:2021)

Diese Technische Spezifikation (CEN/TS) wurde vom CEN am 30. Oktober 2022 als eine künftige Norm zur vorläufigen Anwendung angenommen.

Die Gültigkeitsdauer dieser CEN/TS ist zunächst auf drei Jahre begrenzt. Nach zwei Jahren werden die Mitglieder von CEN und CENELEC gebeten, ihre Stellungnahmen abzugeben, insbesondere über die Frage, ob die CEN/TS in eine Europäische Norm umgewandelt werden kann.

Die CEN- und CENELEC-Mitglieder sind verpflichtet, das Vorhandensein dieser CEN/TS in der gleichen Weise wie bei einer EN anzukündigen und die CEN/TS verfügbar zu machen. Es ist zulässig, entgegenstehende nationale Normen bis zur Entscheidung über eine mögliche Umwandlung der CEN/TS in eine EN (parallel zur CEN/TS) beizubehalten.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Grundsätze	7
5 Allgemeine Anforderungen	8
5.1 Rechts- und Vertragsfragen	8
5.2 Handhabung der Unparteilichkeit	8
5.3 Haftung und Finanzierung	8
6 Strukturelle Anforderungen	8
7 Anforderungen an Ressourcen	8
7.1 Kompetenz des Personals	8
7.1.1 PS 7.1.1 Allgemeine Betrachtungen	8
7.1.2 PS 7.1.2 Bestimmung von Kompetenzkriterien	8
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist	10
7.2.1 PS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren	10
7.2.2 PS 7.2.1.1 Auswahl von Auditoren	10
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten	10
7.4 Aufzeichnungen über Personal	10
7.5 Ausgliederung	10
8 Anforderungen an Informationen	10
8.1 Öffentliche Informationen	10
8.2 Zertifizierungsdokumente	10
8.2.1 PS 8.2 PIMS-Zertifizierungsdokumente	11
8.3 Verweisung auf Zertifizierung und Zeichennutzung	11
8.4 Vertraulichkeit	11
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden	11
9 Anforderungen an Prozesse	11
9.1 Tätigkeiten vor der Zertifizierung	11
9.1.1 Antrag	11
9.1.2 Antragsprüfung	11
9.1.3 Auditprogramm	12
9.1.4 Ermittlung des Auditzeitaufwandes	12
9.1.5 Stichprobenprüfung an mehreren Standorten	13
9.1.6 Mehrfach-Managementsysteme	13
9.2 Planung von Audits	13
9.2.1 Festlegung der Auditziele, des Auditanwendungsbereichs und der Auditkriterien	13
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung	13
9.2.3 Auditplan	13
9.3 Erstzertifizierung	13
9.4 Durchführen von Audits	13
9.4.1 IS 9.4 Allgemeines	13
9.4.2 IS 9.4 Spezifische Elemente des ISMS-Audits	13
9.4.3 IS 9.4 Auditbericht	14
9.5 Zertifizierungsentscheidung	14
9.6 Aufrechterhaltung der Zertifizierung	14
9.6.1 Allgemeines	14
9.6.2 Überwachungstätigkeiten	14
9.6.3 Re-Zertifizierung	14