

DIN EN ISO/IEC 27006-2



ICS 03.120.20; 35.030

Einsprüche bis 2023-09-21

Entwurf

**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

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 DIS 27006-2:2023);
Version allemande et anglaise prEN ISO/IEC 27006-2:2023

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-07-21 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 54 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN ISO/IEC 27006-2:2023) wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1 „Information technology“ in Zusammenarbeit mit dem Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Dieser Norm-Entwurf wird die sich aktuell in Bearbeitung befindende DIN CEN ISO/IEC/TS 27006-2 ersetzen.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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 27006-1:202x*	siehe	DIN EN ISO/IEC 27006-1:202x-xx*
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.

* Zurzeit Entwurf.

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 27006-1:202x-xx, *Informationstechnik, Cybersicherheit und Datenschutz — Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren — Teil 1: Allgemeines (ISO/IEC 27006-1:202x); Deutsche Fassung EN ISO/IEC 27006-1:202x*

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*

– *Entwurf* –

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

– Leerseite –

**Anforderungen an Stellen, die Informationssicherheits-Managementsysteme
auditieren und zertifizieren – Teil 2: Datenschutz-Managementsysteme
(ISO/IEC DIS 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)

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de manage-
ment des informations de sécurité – Partie 2: Systèmes de management des informations de sécurité
(ISO/IEC DIS 27006-2:2023)

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Grundsätze	9
5 Allgemeine Anforderungen	9
5.1 Rechts- und Vertragsfragen	9
5.2 Handhabung der Unparteilichkeit	9
5.2.1 Allgemeines	9
5.2.2 Interessenkonflikte	9
5.3 Haftung und Finanzierung	9
6 Strukturelle Anforderungen	9
7 Anforderungen an Ressourcen	10
7.1 Kompetenz des Personals	10
7.1.1 Allgemeines	10
7.1.2 Allgemeine Betrachtungen	10
7.1.3 Bestimmung der Kompetenzkriterien	10
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist	11
7.2.1 Allgemeines	11
7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren	11
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten	12
7.4 Aufzeichnungen über Personal	12
7.5 Ausgliederung	12
8 Anforderungen an Informationen	12
8.1 Öffentliche Informationen	12
8.2 Zertifizierungsdokumente	12
8.2.1 Allgemeines	12
8.2.2 PIMS-Zertifizierungsdokumente	12
8.3 Verweisung auf Zertifizierung und Zeichennutzung	13
8.4 Vertraulichkeit	13
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden	13
9 Anforderungen an Prozesse	13
9.1 Tätigkeiten vor der Zertifizierung	13
9.1.1 Antrag	13
9.1.2 Antragsprüfung	14
9.1.3 Auditprogramm	14
9.1.4 Ermittlung des Auditzeitaufwandes	14
9.1.5 Stichprobenprüfung an mehreren Standorten	14
9.1.6 Mehrfach-Managementsysteme	14
9.2 Planung von Audits	15
9.2.1 Festlegung der Auditziele, des Auditanwendungsbereichs und der Auditkriterien	15
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung	15
9.2.3 Auditplan	15
9.3 Erstzertifizierung	15
9.4 Durchführen von Audits	15
9.4.1 Allgemeines	15
9.4.2 Spezifische Elemente des ISMS-Audits	15
9.4.3 Auditbericht	15
9.5 Zertifizierungsentscheidung	16

9.5.1	Allgemeines	16
9.5.2	Zertifizierungsentscheidung	16
9.6	Aufrechterhaltung der Zertifizierung	16
9.6.1	Allgemeines	16
9.6.2	Überwachungstätigkeiten	16
9.6.3	Re-Zertifizierung	16
9.6.4	Audits aus besonderem Anlass	16
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Anwendungsbereichs der Zertifizierung	16
9.7	Einsprüche	16
9.8	Beschwerden	16
9.9	Aufzeichnungen zu Kunden	17
10	Managementsystemanforderungen für Zertifizierungsstellen	17
10.1	Optionen	17
10.2	Option A: Allgemeine Managementsystemanforderungen	17
10.3	Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001	17
Anhang A (normativ) Auditzeitaufwand		18
A.1	Einleitung	18
A.2	Konzepte	18
A.3	Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit	18
A.3.1	Allgemeines	18
A.3.2	Fernaudit	19
A.3.3	Berechnung des Auditzeitaufwands	19
A.3.4	Faktoren für die Anpassung des Auditzeitaufwands	20
A.3.5	Einschränkung der Abweichung vom Auditzeitaufwand	21
A.3.6	Vor-Ort-Auditzeitaufwand	21
A.4	Auditzeitaufwand für das Überwachungsaudit	21
A.5	Auditzeitaufwand für das Re-Zertifizierungsaudit	21
A.6	Auditzeitaufwand für mehrere Standorte	21
A.7	Auditzeitaufwand-Abweichungen bei ISMS-Audits, die zu verschiedenen Zeiten stattfinden	21
Anhang B (informativ) Methoden für Berechnungen des Auditzeitaufwands		22
B.1	Allgemeines	22
B.2	Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	22
B.3	Beispiel für die Auditzeitaufwandberechnung	24
Literaturhinweise		27

Tabellen

Tabelle A.1 — Auditzeitaufwandstabelle	19
Tabelle B.1 — Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	22
Tabelle B.2 — Risiken bei der Verarbeitung von pbD	25
Tabelle B.3 — Operative Risiken	26
Tabelle B.4 — Auswirkung der Faktoren auf den Auditzeitaufwand	26

Europäisches Vorwort

Dieses Dokument (prEN ISO/IEC 27006-2:2023) wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1 „Information technology“ in Zusammenarbeit mit dem Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird CEN ISO/IEC/TS 27006-2:2022 ersetzen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anerkennungsnotiz

Der Text von ISO/IEC DIS 27006-2:2023 wurde von CEN als prEN ISO/IEC 27006-2:2023 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC Directives, Teil 1, beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC Directives, Teil 2, erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC TS 27006-2:2021), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Dieses Dokument wurde von einer Technischen Spezifikation zu einer Internationalen Norm geändert.
- Die vorherige Ausgabe wurde an ISO/IEC 27006:2015 angepasst. Die neue Struktur und die neuen Inhalte wurden an ISO/IEC 27006-1:202x angepasst.
- Anhang A wurde erstellt.
- Anhang B wurde erstellt.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 27006 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

ISO/IEC 27006-1 legt Kriterien für Stellen fest, die Informationssicherheits-Managementsysteme auditieren und zertifizieren. Falls solche Stellen auch als ISO/IEC 27006-1-konform akkreditiert werden sollen, mit dem Ziel, Datenschutz-Managementsysteme (PIMS) in Übereinstimmung mit ISO/IEC 27701 zu auditieren und zu zertifizieren, sind einige zusätzliche Anforderungen und Anleitungen in Bezug auf ISO/IEC 27006-1 erforderlich. Diese werden durch dieses Dokument zur Verfügung gestellt. Der Text dieses Dokuments folgt der Struktur von ISO/IEC 27006-1.

Der wesentliche Zweck dieses Dokuments besteht darin, Akkreditierungsstellen zu befähigen, ihre Anwendung von Normen, nach denen sie Zertifizierungsstellen bewerten müssen, effektiver in Einklang zu bringen.

[Anmerkung des Herausgebers: Die Überarbeitung von ISO/IEC 27006-1 wurde eingeleitet und dementsprechend wurde der erste CD von ISO/IEC 27006-1 am 03.09.2021 zur Abstimmung vorgelegt. Entwürfe für ISO/IEC 27006-2 werden aktualisiert, um die Konsistenz mit der Überarbeitung von ISO/IEC 27006-1 zu bewahren.]

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest und bietet Anleitung für Stellen, die Audits und Zertifizierungen von Datenschutz-Managementsystemen (PIMS) nach ISO/IEC 27701 in Kombination mit ISO/IEC 27001 vornehmen. Zusätzlich gelten die Anforderungen nach ISO/IEC 27006-1.

Die in diesem Dokument enthaltenen Anforderungen werden von Stellen, die PIMS-Zertifizierungen durchführen, im Hinblick auf Kompetenz und Zuverlässigkeit nachgewiesen. Die in diesem Dokument enthaltene Anleitung bietet eine zusätzliche Interpretation dieser Anforderungen für Stellen, die PIMS-Zertifizierungen durchführen.

ANMERKUNG Dieses Dokument kann als Kriteriendokument für die Akkreditierung, die Bewertung unter Gleichrangigen oder für andere Auditprozesse verwendet werden.

[Anmerkung des Herausgebers: Der Text dieser überarbeiteten Ausgabe von ISO/IEC 27006-2 (einschließlich des Anwendungsbereichs) unterliegt während des gesamten Projektlebenszyklus einer Überprüfung durch ISO/CASCO. Alle Anmerkungen und Rückmeldungen von CASCO und seiner Mitglieder werden bei WG 5-Meetings besprochen und gelöst. Es ist ebenfalls zu beachten, dass der Anwendungsbereich mit ISO/IEC 27006:2015 konsistent ist und die Konsistenz mit der Überarbeitung von ISO/IEC 27006 (d. h. 27006-1) während der Überarbeitung von ISO/IEC 27006-2 gewahrt bleibt.]

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 17021-1, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27006-1:202x, *Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General*

ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17021-1, ISO/IEC 27006-1 und die folgenden Begriffe.

3.1

Zertifizierungsdokumente

Dokumente, die angeben, dass das ISMS eines Kunden spezifizierten ISMS-Normen und jeglicher im Rahmen des Systems erforderlichen zusätzlichen Dokumentation entspricht

Anmerkung 1 zum Begriff: Im Zusammenhang dieser Norm kann ein ISMS als das PIMS einschließlich verstanden werden.

[QUELLE: ISO/IEC 27006-1:202x, 3.1]

3.2

personenbezogene Daten

pbD

sämtliche Informationen, die (a) verwendet werden können, um die betroffene Person, auf die sich solche Informationen beziehen, zu identifizieren, oder die (b) im direkten oder indirekten Zusammenhang mit einer betroffenen Person stehen oder stehen könnten

Anmerkung 1 zum Begriff: Um festzustellen, ob eine betroffene Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von Betroffenen, Verantwortlichen und anderen Interessengruppen des Datenschutzes, die im Besitz der Daten sind, oder von einer beliebigen anderen Partei angewendet werden können, um diese natürliche Person zu identifizieren.

[QUELLE: ISO/IEC 29100:2011, 2.9]

3.3

verantwortliche Stelle

Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die die Zwecke und Mittel zum Verarbeiten von personenbezogenen Daten (pbD) bestimmen, und keine natürliche Personen sind, die Daten für persönliche Zwecke verwenden

Anmerkung 1 zum Begriff: Eine verantwortliche Stelle weist manchmal andere (beispielsweise Auftragsdatenverarbeiter) an, pbD in ihrem Namen zu verarbeiten, wobei die Verantwortung für die Verarbeitung bei der verantwortlichen Stelle bleibt.

[QUELLE: ISO/IEC 29100:2011, 2.10]

3.4

betroffene Person

natürliche Person, auf die sich die personenbezogenen Daten (pbD) beziehen

Anmerkung 1 zum Begriff: Abhängig von der Rechtsprechung und der jeweiligen Gesetzgebung zum Datenschutz und zum Schutz personenbezogener Daten kann anstelle der Benennung „betroffene Person (en: PII principal)“ auch das Synonym „Datensubjekt (en: data subject)“ verwendet werden.

[QUELLE: ISO/IEC 29100:2011, 2.11]

3.5

Auftragsdatenverarbeiter

Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die personenbezogene Daten (pbD) im Namen und nach den Anweisungen einer verantwortlichen Stelle verarbeiten

[QUELLE: ISO/IEC 29100:2011, 2.12]

3.6

Managementsystem für Datenschutzinformationen

PIMS

Informationssicherheits-Managementsystem, das den Datenschutz bei potentieller Auswirkung durch die Verarbeitung von personenbezogenen Daten behandelt

[QUELLE: ISO/IEC 27701:2019, 3.2]

3.7

Datenschutz-Folgenabschätzung

gesamter Prozess der Risikoidentifikation, Risikoanalyse und Risikobewertung mit Bezug auf die Verarbeitung von personenbezogenen Daten (pbD)

Anmerkung 1 zum Begriff: Dieser Prozess wird auch als Datenschutz-Risikobeurteilung bezeichnet.

[QUELLE: ISO/IEC 29100:2011, 2.20]

3.8

Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes

natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die eine Entscheidung oder Tätigkeit mit Bezug auf die Verarbeitung von personenbezogenen Daten (pbD) beeinflussen kann, die davon beeinflusst sein kann oder die sich davon beeinflusst fühlen kann

[QUELLE: ISO/IEC 29100:2011, 2.22]

3.9

Verarbeitung von personenbezogenen Daten

Handlung oder Folge von Handlungen, die an personenbezogenen Daten (pbD) durchgeführt wird

Anmerkung 1 zum Begriff: Beispiele für Handlungen zur Verarbeitung von pbD sind unter anderem das Sammeln, Speichern, Ändern, Abrufen, Konsultieren, Offenlegen, Anonymisieren, Pseudonymisieren, Verbreiten oder anderweitiges Bereitstellen, Löschen oder Vernichten von pbD.

[QUELLE: ISO/IEC 29100:2011, 2.23]

4 Grundsätze

Es gelten die Grundsätze nach ISO/IEC 27006-1:202x, Abschnitt 4.

5 Allgemeine Anforderungen

5.1 Rechts- und Vertragsfragen

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 5.1.

5.2 Handhabung der Unparteilichkeit

5.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 5.2.1. Außerdem gelten die Anforderungen und der Leitfaden in 5.2.2.

5.2.2 Interessenkonflikte

Die Zertifizierungsstelle darf keine Managementsystemberatung in Bezug auf PIMS anbieten (z. B. Dienstleistungen als externer Datenschutzbeauftragter oder dergleichen, Beratungen zu Managementprozessen oder Datenschutzprozessen).

Die Ausrichtung von oder die Teilnahme als ein Vortragender an Schulungen für Managementsysteme zur Sicherheit personenbezogener Daten wird nicht als Beratung oder als Ursache von Interessenkonflikten betrachtet, vorausgesetzt, die Vorgaben in ISO/IEC 27006-1:202x, 5.2.2 a) werden beachtet.

5.3 Haftung und Finanzierung

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 5.3.

6 Strukturelle Anforderungen

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, Abschnitt 6.

7 Anforderungen an Ressourcen

7.1 Kompetenz des Personals

7.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.1.1.

7.1.2 Allgemeine Betrachtungen

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.1.2.

7.1.3 Bestimmung der Kompetenzkriterien

7.1.3.1 Kompetenzanforderungen für PIMS-Audits

7.1.3.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.1.3.1. Außerdem gelten die Anforderungen und der Leitfaden in 7.1.3.1.2, 7.1.3.1.3.

7.1.3.1.2 Allgemeine Anforderungen

Die Zertifizierungsstelle muss über Kriterien zur Verifizierung des Erfahrungshintergrundes, der spezifischen Schulung oder der Unterweisung der Auditteammitglieder verfügen, sodass mindestens das Wissen sichergestellt ist über:

- a) Datenschutz-Informationsmanagement;
- b) Identifikation, Management und Handhabung personenbezogener Daten (pbd);
- c) Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen;
- d) PIMS-Überwachung, -Messung, -Analyse und -Bewertung;
- e) Informationssicherheitsrisiken im Zusammenhang mit Datenschutzmanagement und der Verarbeitung personenbezogener Daten;
- f) Richtlinien und betriebliche Anforderungen für das Datenschutzmanagement.

7.1.3.1.3 PIMS-Terminologie, -Grundsätze, -Praktiken und -Verfahren

Zusammen müssen die Mitglieder des Auditteams über folgendes Wissen verfügen:

- a) Werkzeuge, Verfahren und Techniken im Zusammenhang mit Datenschutz-Informationsmanagement und der Verarbeitung personenbezogener Daten und ihrer Anwendung;
- b) Datenschutz-Risikobeurteilung, Datenschutz-Folgenabschätzung und damit zusammenhängende Verfahren und Risikomanagement;
- c) auf PIMS anwendbare Prozesse;
- d) aktuelle Technologie, bei der der Datenschutz relevant oder ein Problem sein kann;
- e) alle Maßnahmen in ISO/IEC 27701 und ihre Umsetzung;

- f) die für das Datenschutzmanagement oder die Verarbeitung von personenbezogenen Daten geltenden rechtlichen Anforderungen (z. B. branchenspezifische Gesetze und örtliche Datenschutzgesetze) oder beides;

ANMERKUNG Das Wissen um gesetzliche und behördliche Anforderungen setzt keinen spezifischen Bildungsabschluss in juristischen oder verwandten Studiengängen voraus.

- g) gute Branchenverhaltensweisen in Bezug auf Datenschutz und Datenschutzverfahren.

7.1.3.2 Anforderungen an die Kompetenz für die Bewertung von Auditberichten und das Treffen von Zertifizierungsentscheidungen

7.1.3.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.1.3.2. Außerdem gelten die Anforderungen und der Leitfaden in 7.1.3.2.2.

7.1.3.2.2 Allgemeine Anforderungen

Das Personal, das Auditberichte bewertet und Zertifizierungsentscheidungen trifft, muss über Folgendes verfügen:

- a) Wissen über ISO/IEC 27701;
- b) Wissen um für den Datenschutz relevante gesetzliche und behördliche Anforderungen;

ANMERKUNG Das Wissen um gesetzliche und behördliche Anforderungen setzt keinen spezifischen Bildungsabschluss in juristischen oder verwandten Studiengängen voraus.

- c) Wissen über die für die Verarbeitung von pbD spezifischen Zertifizierungsanwendungsbereichsanforderungen nach ISO/IEC 27701, um die Angemessenheit des Zertifizierungsanwendungsbereichs oder die Änderungen an diesem verifizieren zu können;
- d) allgemeines Verständnis von Datenschutz-Risikobeurteilung, Datenschutz-Folgenabschätzung und Datenschutz-Risikomanagement;
- e) allgemeines Verständnis von auf PIMS anwendbaren Prozessen.

7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist

7.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.2.1. Außerdem gelten die Anforderungen und der Leitfaden in 7.2.2.1 und 7.2.2.2.

7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren

7.2.2.1 Allgemeine Betrachtungen

Die Zertifizierungsstelle muss durch Folgendes nachweisen, dass die Auditoren über das notwendige Wissen und die Erfahrung durch wenigstens eines der folgenden Elemente verfügen:

- a) anerkannte PIMS-spezifische Qualifikationen;
- b) Teilnahme an PIMS-Schulung(en) und Erlangung relevanter persönlicher Qualifikationen;
- c) PIMS-Audits, die ein anderer kompetenter Auditor überwacht hat.

7.2.2.2 Auswahl von Auditoren

Neben 7.1.3.1 muss der Prozess zur Auswahl von Auditoren sicherstellen, dass jeder Auditor:

- a) über einen ausreichenden Bildungsstand und praktische Berufserfahrung in den Bereichen Informationssicherheit und Datenschutz verfügt, um als Auditor für PIMS tätig zu sein;
- b) eine ausreichende Schulung zu Auditierung von PIMS und Auditmanagement erhalten und seine Fertigkeiten zur Auditierung eines ISMS nach ISO/IEC 27701 nachgewiesen hat;
- c) durch ständige berufliche Entwicklung relevantes und aktuelles Wissen und Fertigkeiten mit Bezug auf das Datenschutzmanagement und Auditierung pflegt.

Der Prozess zur Auswahl von Fachexperten muss sicherstellen, dass jeder Fachexperte:

- d) über einen ausreichenden Bildungsstand und praktische Berufserfahrung in den Bereichen Informationssicherheit und Datenschutz verfügt, um als Fachexperte tätig zu sein;
- e) durch ständige berufliche Entwicklung relevantes und aktuelles Wissen und Fertigkeiten mit Bezug auf das Datenschutzmanagement pflegt.

ANMERKUNG Wissen und Fertigkeiten mit Bezug auf Informationssicherheit und Datenschutz können das Absolvieren von PIMS-Audits unter der Aufsicht von anderen qualifizierten PIMS-Auditoren sowie spezifisches Wissen und spezifische Fertigkeiten mit Bezug auf Managementsysteme für Datenschutzinformationen einschließen.

7.3 Einsatz einzelner externer Auditoren und externer Fachexperten

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.3.

7.4 Aufzeichnungen über Personal

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.4.

7.5 Ausgliederung

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 7.5.

8 Anforderungen an Informationen

8.1 Öffentliche Informationen

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 8.1.

8.2 Zertifizierungsdokumente

8.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 8.2.1. Außerdem gelten die Anforderungen und der Leitfaden in 8.2.2.

8.2.2 PIMS-Zertifizierungsdokumente

Wenn ein separates Zertifikat für ISO/IEC 27701 ausgestellt wird, müssen die Zertifizierungsdokumente einen klaren Bezug zur ISO/IEC 27001-Zertifikats-ID (z. B. Zertifizierungsnummer) enthalten, auf der die ISO/IEC 27701-Zertifizierung beruht.

Die Version der Erklärung zur Anwendbarkeit (SoA) (en: Statement of Applicability) für ISO/IEC 27001 und, falls getrennt ausgestellt, die Version der SoA für ISO/IEC 27701 müssen in die Zertifizierungsdokumente aufgenommen werden.

ANMERKUNG 1 Die SoA für ISO/IEC 27701 kann in die SoA für ISO/IEC 27001 integriert sein oder getrennt von der SoA für ISO/IEC 27001 erstellt werden.

Das Datum der ursprünglichen Zertifizierung nach ISO/IEC 27701 muss auf oder nach dem Datum der Zertifizierung nach ISO/IEC 27001 liegen, auf der sie basiert. Das Ablaufdatum des ISO/IEC 27701-Zertifikats darf nicht nach dem Ablaufdatum des ISO/IEC 27001-Zertifikats liegen, auf der sie basiert.

Der im Zertifizierungsdokument von ISO/IEC 27701 genannte Anwendungsbereich der Zertifizierung muss innerhalb des Anwendungsbereichs der Zertifizierung für die Zertifizierung nach ISO/IEC 27001 liegen oder mit diesem identisch sein, siehe 9.1.3.2.

Die Zertifizierung nach ISO/IEC 27001 kann vor oder gleichzeitig mit der Zertifizierung nach ISO/IEC 27701 erfolgen.

Zertifizierungsunterlagen müssen Folgendes enthalten:

- a) den Begriff „Datenschutz-Managementsystem“;
- b) die Rolle der Organisation für jede Aktivität, jedes Produkt und jeden Dienst im Anwendungsbereich (d. h. ob die Organisation als verantwortliche Stelle oder Auftragsdatenverarbeiter oder beides auftritt);
- c) die Tatsache, dass die Organisation sowohl nach ISO/IEC 27001 als auch nach ISO/IEC 27701 zertifiziert ist.

8.3 Verweisung auf Zertifizierung und Zeichennutzung

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 8.3.

8.4 Vertraulichkeit

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 8.4.

8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 8.5.

9 Anforderungen an Prozesse

9.1 Tätigkeiten vor der Zertifizierung

9.1.1 Antrag

9.1.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 27006-1:202x, 9.1.1. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.1.2.

9.1.1.2 Bereitschaft zum Antrag

Die Zertifizierungsstelle darf die Anträge vom Kunden nicht annehmen, wenn der Kunde noch über kein dokumentiertes und eingeführtes PIMS verfügt, das den Anforderungen nach ISO/IEC 27701 entspricht.