DIN EN ISO/IEC 27706

DIN

ICS 03.120.20; 35.030

Entwurf

Einsprüche bis 2024-10-30
Vorgesehen als Ersatz für
DIN CEN ISO/IEC/TS
27006-2:2023-12;
Ersatz für
E DIN EN ISO/IEC
27006-2:2023-08

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren (ISO/IEC DIS 27706.2:2024); Deutsche und Englische Fassung prEN ISO/IEC 27706:2024

Requirements for bodies providing audit and certification of privacy information management systems (ISO/IEC DIS 27706.2:2024);
German and English version prEN ISO/IEC 27706:2024

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2024-08-30 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 66 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

Nationales Vorwort

Der Text von ISO/IEC DIS 27706.2:2024 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27706:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. 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 17000	siehe	DIN EN ISO/IEC 17000
ISO/IEC 17021-1	siehe	DIN EN ISO/IEC 17021-1
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.

Änderungen

Gegenüber DIN CEN ISO/IEC/TS 27006-2:2023-12 wurden folgende Änderungen vorgenommen:

a) das Dokument wurde von einer Technischen Spezifikation in eine Internationale Norm umgewandelt;

b) die Struktur und der Inhalt wurden an ISO/IEC 27006-1:2024 angeglichen;

c) es wurden ein Anhang A, ein Anhang B und ein Anhang C erstellt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 17000, *Konformitätsbewertung — Begriffe und allgemeine Grundlagen*

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

DIN EN ISO/IEC 27701, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Datenschutz-Informationsmanagementsysteme — Anforderungen und Leitlinien*

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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

– Entwurf –

August 2024

prEN ISO/IEC 27706

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren (ISO/IEC DIS 27706.2:2024)

Requirements for bodies providing audit and certification of privacy information management systems (ISO/IEC DIS 27706.2:2024)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

E DIN EN ISO/IEC 27706:2024-10
prEN ISO/IEC 27706:2024 (D)

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe und Abkürzungen 7
4 Grundsätze 9
5 Allgemeine Anforderungen 9
5.1 Rechts- und Vertragsfragen 9
5.2 Handhabung der Unparteilichkeit 9
5.2.1 Allgemeine Betrachtungen 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 Allgemeine Betrachtungen 10
7.1.2 Bestimmung der Kompetenzkriterien 10
7.1.3 Beurteilungsprozesse 10
7.1.4 Sonstige Betrachtungen 11
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist 11
7.3 Einsatz einzelner Auditoren und externer Fachexperten 11
7.4 Aufzeichnungen über Personal 11
7.5 Ausgliederung 11
8 Anforderungen an Informationen 11
8.1 Öffentliche Informationen 11
8.2 Zertifizierungsdokumente 11
8.2.1 Allgemeines 11
8.2.2 PIMS-Zertifizierungsdokumente 11
8.3 Verweisung auf Zertifizierung und Zeichennutzung 12
8.4 Vertraulichkeit 12
8.4.1 Allgemeines 12
8.4.2 Zugang zu den Aufzeichnungen der Organisation 12
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden 12
9 Anforderung an Prozesse 12
9.1 Tätigkeiten vor der Zertifizierung 12
9.1.1 Antrag 12
9.1.2 Antragsprüfung 12
9.1.3 Auditprogramm 13
9.1.4 Ermittlung des Auditzeitaufwands 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 14
9.2.3 Auditplan 14
9.3 Erstzertifizierung 14
9.3.1 Allgemeines 14
9.4 Durchführen von Audits 15
9.4.1 Allgemeines 15
9.4.2 Spezifische Elemente des PIMS-Audits 15
9.4.3 Auditbericht 16
9.5 Zertifizierungsentscheidung 16

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

9.6 Aufrechterhaltung der Zertifizierung . . . 16
9.6.1 Allgemeines . . . 16
9.6.2 Überwachungstätigkeiten . . . 16
9.7 Einsprüche . . . 17
9.8 Beschwerden . . . 17
9.9 Aufzeichnungen zu Kunden . . . 17
10 Managementsystemanforderungen für Zertifizierungsstellen . . . 17
10.1 Optionen . . . 17
10.2 Option A: Allgemeine Managementsystemanforderungen . . . 18
10.3 Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001 . . . 18
Anhang A (normativ) **Auditzeitaufwand** . . . 19
A.1 Einleitung . . . 19
A.2 Konzepte . . . 19
A.2.1 Anzahl der von der Organisation gesteuerten Personen . . . 19
A.2.2 Auditortag . . . 20
A.2.3 Temporärer Standort . . . 20
A.3 Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit . . . 20
A.3.1 Allgemeines . . . 20
A.3.2 Fernaudit . . . 20
A.3.3 Berechnung des Auditzeitaufwands . . . 20
A.3.4 Bestimmung der ursprünglichen Personenanzahl . . . 22
A.3.5 Faktoren für die Anpassung des Auditzeitaufwands . . . 23
A.3.6 Einschränkung der Abweichung vom Auditzeitaufwand . . . 23
A.3.7 Vor-Ort-Auditzeitaufwand . . . 23
A.4 Auditzeitaufwand für das Überwachungsaudit . . . 24
A.5 Auditzeitaufwand für das Re-Zertifizierungsaudit . . . 24
A.6 Auditzeitaufwand für mehrere Standorte . . . 24
A.7 Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs . . . 24
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
Anhang C (normativ) **Erforderliche Kenntnisse und Fertigkeiten** . . . 31
C.1 Allgemeines . . . 31
C.2 Kompetenzanforderungen an Managementsystem-Auditoren und -Auditteams . . . 31
C.2.1 Allgemeines . . . 31
C.3 Anforderungen an die Kompetenz des Personals, das Auditberichte überprüft und Zertifizierungsentscheidungen trifft . . . 32
C.3.1 Allgemeines . . . 32
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 . . . 32
Literaturhinweise . . . 33

Tabellen

Tabelle A.1 — Auditzeitaufwandstabelle . . . 21
Tabelle B.1 — Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands . . . 26
Tabelle B.2 — Risiken bei der Auftragsverarbeitung . . . 28
Tabelle B.3 — Operative Risiken . . . 30
Tabelle B.4 — Auswirkung der Faktoren auf den Auditzeitaufwand . . . 30

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

Europäisches Vorwort

Der Text von ISO/IEC DIS 27706.2:2024 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27706:2024 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC DIS 27706.2:2024 wurde von CEN als prEN ISO/IEC 27706:2024 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

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 (https://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.

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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

Einleitung

Dieses Dokument legt die Anforderungen für Stellen fest, die Datenschutz-Managementsysteme auditieren und zertifizieren.

Diese Norm ist auch dazu bestimmt, Akkreditierungsstellen und Peer-Prüfer dabei zu unterstützen, die Mindestanforderungen an die Kompetenz des Personals in Zertifizierungsstellen und die Zertifizierungsprozesse in diesen Zertifizierungsstellen auf effiziente und harmonisierte Weise zu beurteilen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

1 Anwendungsbereich

Dieses Dokument legt, zusätzlich zu den Anforderungen in ISO/IEC 17021-1, Anforderungen fest und bietet eine Anleitung für Stellen, die Audits und Zertifizierungen von Datenschutz-Managementsystemen (PIMS) nach ISO/IEC 27701 vornehmen.

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.

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 17000, *Conformity assessment — Vocabulary and general principles*

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

ISO/IEC 27701, *Information security, cybersecurity and privacy protection — Requirements and guidance*

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17000, ISO/IEC 17021-1, ISO/IEC 27701, ISO/IEC 29100 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

3.1
Zertifizierungsdokument
Dokumente, die angeben, dass das PIMS eines Kunden ISO/IEC 27701 und jeglicher im Rahmen des Managementsystems erforderlichen zusätzlichen Dokumentation entspricht

Anmerkung 1 zum Begriff: Diese Definition ist nicht auf die Anzahl der Dokumente begrenzt, die allgemein als Zertifizierungsdokumente bekannt sind.

3.2
personenbezogene Daten
pbD, personenbezogene Daten
Informationen, die (a) dazu verwendet werden können, eine Verbindung zwischen den Informationen und der natürlichen Person, auf die sie sich beziehen, herzustellen, oder (b) direkt oder indirekt mit einer natürlichen Person verknüpft sind oder verknüpft werden könnten

Anmerkung 1 zum Begriff: Die „natürliche Person“ in der Definition entspricht dem/der *betroffenen Person* (3.4). Um festzustellen, ob eine betroffene Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von Betroffenen,

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

Verantwortlichen und anderen Interessengruppen des Datenschutzes, die im Besitz der Daten sind, oder von einer beliebigen anderen Partei angewendet werden können, um eine Verbindung zwischen den pbD und der natürlichen Person herzustellen.

[QUELLE: ISO/IEC 29100:2024, 3.7]

3.3
verantwortliche Stelle
Betroffene, Verantwortliche und andere Interessensgruppen des Datenschutzes, die die Zwecke und Mittel für die Verarbeitung der *personenbezogenen Daten (pbD)* (3.2) festlegen, ausgenommen natürliche Personen, die Daten für persönliche Zwecke nutzen

Anmerkung 1 zum Begriff: In einigen Fällen weist eine verantwortliche Stelle andere [z. B. *Auftragsdatenverarbeiter* (3.5)] an, *personenbezogene Daten* in ihrem Namen *zu verarbeiten* (3.8), während die Verantwortung für die Verarbeitung weiterhin bei der verantwortlichen Stelle liegt.

[QUELLE: ISO/IEC 29100:2024, 3.8]

3.4
betroffene Person
Datensubjekt
natürliche Person, auf die sich die *personenbezogenen Daten (pbD)* (3.2) beziehen

[QUELLE: ISO/IEC 29100:2024, 3.9]

3.5
Auftragsdatenverarbeiter
Betroffene, Verantwortliche und andere Interessengruppen des Datenschutzes, die *personenbezogene Daten (pbD)* (3.2) im Namen und nach den Anweisungen einer *verantwortlichen Stelle* (3.3) verarbeiten

[QUELLE: ISO/IEC 29100:2024, 3.10]

3.6
Managementsystem für Datenschutzinformationen
PIMS, en: Privacy Information Management System
Managementsystem, das sich mit dem Schutz der durch die *Verarbeitung personenbezogener Daten* (3.8) möglicherweise beeinträchtigten Privatsphäre befasst

[QUELLE: ISO/IEC 27701:201X, 3.2]

3.7
Datenschutz-Folgenabschätzung
Gesamtprozess aus Identifizieren, Analysieren, Bewerten, Beraten, Kommunizieren und Planen der Behandlung von möglichen Datenschutzfolgen unter Bezug auf die Verarbeitung *personenbezogener Daten* (3.2), eingebettet in den unternehmensweiten Rahmen zum Risikomanagement

[QUELLE: ISO/IEC 29100:2024, 3.18]

3.8
Verarbeitung von personenbezogenen Daten
Vorgänge oder Reihe von Vorgängen, die auf *personenbezogene Daten (pbD)* (3.7) angewendet wird

Anmerkung 1 zum Begriff: Beispiele für Vorgänge zur Verarbeitung von pbD sind unter anderem: das Erheben, Speichern, Ändern, Auswerten, Hinzuziehen, Offenlegen, Anonymisieren, Pseudonymisieren, Verbreiten oder sonstige Verfügbarmachen, Löschen oder Zerstören von pbD.

[QUELLE: ISO/IEC 29100:2024, 3.21]

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

3.9
Erklärung zur Anwendbarkeit
Dokumentation aller notwendigen Maßnahmen und Begründung der Aufnahme oder des Ausschlusses von Maßnahmen

Anmerkung 1 zum Begriff: Organisationen benötigen möglicherweise nicht alle in Anhang A aufgeführten Maßnahmen oder können sogar die Liste in Anhang A durch zusätzliche, durch die Organisation selbst eingeführte Maßnahmen erweitern.

[QUELLE: ISO/IEC 27701:202X, 3.24]

4 Grundsätze

Es gelten die Grundsätze nach ISO/IEC 17021-1:2015, Abschnitt 4.

5 Allgemeine Anforderungen

5.1 Rechts- und Vertragsfragen

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 5.1.

5.2 Handhabung der Unparteilichkeit

5.2.1 Allgemeine Betrachtungen

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 5.2. Außerdem gelten die Anforderungen und der Leitfaden in 5.2.2.

5.2.2 Interessenkonflikte

Zusätzlich zu den Anforderungen nach ISO/IEC 17021-1:2015, 5.2.5, dürfen Zertifizierungsstellen keine Beratung für Managementsysteme in Zusammenhang mit der Privatsphäre, dem Datenschutz (z. B. in Form eines externen Datenschutzbeauftragten oder einer Datenschutzprüfung) oder dem Risikomanagement anbieten.

Zertifizierungsstellen dürfen die folgenden Tätigkeiten durchführen, ohne dass sie als Beratung betrachtet werden oder dass sie einen potenziellen Interessenkonflikt darstellen:

a) wenn bei der Organisation von und der Teilnahme als Dozent an Schulungskursen, die sich auf Datenschutz-Managementsysteme, Managementsysteme oder Audits beziehen, nur allgemeine und öffentlich zugängliche Informationen von Zertifizierungsstellen bereitgestellt werden;

b) Tätigkeiten, die dem Audit vorausgehen, um den Gegenstand der Zertifizierung zu ermitteln, dessen einziger Zweck darin besteht, den Anwendungsbereich und die Fähigkeit für ein Zertifizierungsaudit zu bestimmen;

c) Erbringung von Mehrwert während Zertifizierungen und Überwachungsaudits, z. B. durch Bestimmung von Verbesserungsmöglichkeiten, die während des Audits bekannt werden.

5.3 Haftung und Finanzierung

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 5.3.

6 Strukturelle Anforderungen

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, Abschnitt 6.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

7 Anforderungen an Ressourcen

7.1 Kompetenz des Personals

7.1.1 Allgemeine Betrachtungen

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.1.

7.1.2 Bestimmung der Kompetenzkriterien

7.1.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.1.2. Außerdem gelten die Anforderungen in 7.1.2.2.

7.1.2.2 Allgemeine Kompetenzanforderungen

Die Zertifizierungsstelle muss die Kompetenzanforderungen für jede Zertifizierungsfunktion definieren, wie in ISO/IEC 17021-1:2015, Tabelle A.1, angegeben.

Die Zertifizierungsstelle muss auch die in Anhang C dieses Dokuments festgelegten Anforderungen (für die technischen Bereiche von PIMS) berücksichtigen.

Hinsichtlich der Kompetenz in Bezug auf die Informationssicherheit kann die Zertifizierungsstelle die in ISO/IEC 27006-1:2024, 7.1.3, festgelegten Kompetenzanforderungen berücksichtigen, die für die Informationssicherheit in Bezug auf die Anforderungen in ISO/IEC 27701 für ein Informationssicherheitsprogramm maßgeblich sind.

7.1.3 Beurteilungsprozesse

7.1.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.1.3. Außerdem gelten die Anforderungen und der Leitfaden in 7.1.3.2, 7.1.3.3 und 7.1.3.4.

7.1.3.2 Beurteilen von Auditoren

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-Schulungen und Erlangung relevanter persönlicher Qualifikationen;

c) aktuelle Aufzeichnungen der beruflichen Entwicklung;

d) PIMS-Audits, die ein anderer kompetenter und zugelassener Auditor überwacht hat.

ANMERKUNG Wissen und Fertigkeiten mit Bezug auf 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.

7.1.3.3 Auswahl von Auditoren

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

a) über praktische Berufserfahrung im Bereich Datenschutz verfügt, um als Auditor für PIMS tätig zu sein;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

b) eine Schulung zu Auditierung von PIMS und Auditmanagement erhält und seine Fertigkeiten zur Auditierung eines PIMS 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.

7.1.3.4 Auswählen von Fachexperten

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

a) über praktische Berufserfahrung im Bereich Datenschutz verfügt, um als Fachexperte tätig zu sein;

b) durch ständige berufliche Entwicklung relevantes und aktuelles Wissen und Fertigkeiten mit Bezug auf das Datenschutzmanagement pflegt.

ANMERKUNG Wissen und Fertigkeiten mit Bezug auf 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.

7.1.4 Sonstige Betrachtungen

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.1.4.

7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.2.

7.3 Einsatz einzelner Auditoren und externer Fachexperten

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.3.

7.4 Aufzeichnungen über Personal

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.4.

7.5 Ausgliederung

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.5.

8 Anforderungen an Informationen

8.1 Öffentliche Informationen

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 8.1.

8.2 Zertifizierungsdokumente

8.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 8.2. Außerdem gelten die Anforderungen und der Leitfaden in 8.2.2.

8.2.2 PIMS-Zertifizierungsdokumente

Zertifizierungsunterlagen müssen Folgendes enthalten:

a) den Begriff „Datenschutz-Managementsystem“;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

b) die Rolle der Organisation für jede Aktivität, jedes Produkt und jeden Dienst im Anwendungsbereich (d. h. ob die Organisation als verantwortliche Stelle oder Auftragsverarbeiter oder beides auftritt);

c) die Version der Erklärung zur Anwendbarkeit (SoA, en: statement of applicability) für das PIMS der Organisation.

ANMERKUNG Eine Änderung der Erklärung zur Anwendbarkeit, die nicht die Abdeckung der Maßnahmen im Anwendungsbereich der Zertifizierung ändert, erfordert keine Aktualisierung der Zertifizierungsdokumente.

Wenn keine Tätigkeit der Organisation im Anwendungsbereich der Zertifizierung an einem bestimmten physischen Standort durchgeführt wird, muss in dem/den Zertifizierungsdokument(en) angegeben werden, dass alle Tätigkeiten der Organisation aus der Ferne durchgeführt werden.

8.3 Verweisung auf Zertifizierung und Zeichennutzung

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 8.3.

8.4 Vertraulichkeit

8.4.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 8.4. Außerdem gelten die Anforderungen in 8.4.2.

8.4.2 Zugang zu den Aufzeichnungen der Organisation

Vor dem Zertifizierungsaudit muss die Zertifizierungsstelle den Kunden darum bitten, anzugeben, ob Informationen in Bezug auf PIMS (z. B. PIMS-Aufzeichnungen oder Informationen zur Gestaltung und Wirksamkeit von Maßnahmen) zur Prüfung durch das Auditteam nicht zur Verfügung gestellt werden können, da sie vertrauliche oder sensible Informationen enthalten. Die Zertifizierungsstelle muss bestimmen, ob das PIMS beim Fehlen derartiger Informationen angemessen auditiert werden kann. Falls die Zertifizierungsstelle zu dem Ergebnis kommt, dass es nicht möglich ist, das PIMS adäquat zu auditieren, ohne die identifizierten vertraulichen oder sensiblen Informationen zu überprüfen, muss sie den Kunden darüber in Kenntnis setzen, dass das Zertifizierungsaudit nicht stattfinden kann, bis angemessene Zugangsvereinbarungen bereitgestellt werden.

8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 8.5.

9 Anforderung an Prozesse

9.1 Tätigkeiten vor der Zertifizierung

9.1.1 Antrag

9.1.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.1. Außerdem gelten die Anforderungen 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 kein PIMS dokumentiert und eingeführt hat, das den Anforderungen nach ISO/IEC 27701 entspricht.

9.1.2 Antragsprüfung

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.2.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

9.1.3 Auditprogramm

9.1.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.3.2.

ANMERKUNG Im Rahmen des Auditprogramms sollten Fernauditmethoden in Betracht gezogen werden. Hinsichtlich weiterer Informationen können sich Zertifizierungsstellen auf die Leitfäden für die Verwendung von Fernauditmethoden in Auditmanagementsystemen in ISO/IEC 17012 beziehen.

9.1.3.2 PIMS-Maßnahmen

Das Auditprogramm für PIMS-Audits muss die vom Kunden festgelegten Maßnahmen (nach ISO/IEC 27701, 6.1.3 b und c) berücksichtigen.

9.1.4 Ermittlung des Auditzeitaufwands

9.1.4.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015,9.1.4. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.4.2.

9.1.4.2 Auditzeitaufwand

Die Zertifizierungsstelle muss den Auditzeitaufwand bestimmen, der für die ISO/IEC 27701-Zertifizierungsaudits (einschließlich Erstzertifizierung, Überwachung und Re-Zertifizierung) erforderlich ist.

Die Zertifizierungsstelle muss Anhang A zur Bestimmung des Auditzeitaufwands verwenden.

9.2 Planung von Audits

9.2.1 Festlegung der Auditziele, des Auditanwendungsbereichs und der Auditkriterien

9.2.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.2.1. Außerdem gelten die Anforderungen und der Leitfaden in 9.2.1.2 und 9.2.1.3.

9.2.1.2 Ermittlung des Auditaufwands

Die Zertifizierungsstelle muss sicherstellen, dass der Anwendungsbereich der ISO/IEC 27701-Zertifizierung wie im Anwendungsbereich des PIMS definiert innerhalb der Grenzen der Tätigkeiten des Kunden liegt.

Im Auditprogramm für ein ISO/IEC 27701-Audit muss die Rolle des Kunden im Verhältnis zu verantwortlichen Stellen oder Auftragsverarbeitern oder beiden festgelegt werden.

Die Zertifizierungsstelle muss verifizieren, dass die Verarbeitung von pbD innerhalb des Anwendungsbereichs des Kunden-PIMS liegt (siehe ISO/IEC 27701:202X, 5.2.3).

Zertifizierungsstellen müssen sicherstellen, dass die Datenschutz-Risikobeurteilung und -Risikobehandlung des Kunden seine Tätigkeiten widerspiegelt und sich bis auf die Grenzen der Tätigkeiten, wie sie im Anwendungsbereich des PIMS definiert wurden, erstreckt. Zertifizierungsstellen müssen bestätigen, dass dies im PIMS-Anwendungsbereich des Kunden und der Erklärung zur Anwendbarkeit widergespiegelt wird.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

9.2.1.3 Auditziele

Die Auditziele müssen Folgendes auch sicherstellen, dass der Kunde auf der Grundlage der Risikobeurteilung die erforderlichen Maßnahmen ermittelt hat.

9.2.2 Auswahl des Auditteams und Aufgabenzuordnung

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.2.2.

9.2.3 Auditplan

9.2.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.2.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.2.3.2.

9.2.3.2 Allgemeine Betrachtungen

Der Auditplan muss die bestimmten PIMS-Maßnahmen berücksichtigen.

9.3 Erstzertifizierung

9.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.3.1.1.1 und 9.3.1.1.2.

9.3.1.1 Erstzertifizierungsaudit

9.3.1.1.1 Stufe 1:

In dieser Stufe des Audits muss die Zertifizierungsstelle die Dokumentation zur Gestaltung des PIMS beschaffen, die die nach ISO/IEC 27701 erforderliche Dokumentation abdeckt.

Vom Kunden müssen während Stufe 1 des Zertifizierungsaudits mindestens die folgenden Informationen bereitgestellt werden:

a) allgemeine Informationen in Bezug auf das PIMS und die Tätigkeiten, die es abdeckt;

b) eine Kopie der erforderlichen, in ISO/IEC 27701 festgelegten PIMS-Dokumentation und gegebenenfalls andere zugehörige Dokumentation.

Die Zertifizierungsstelle muss ein ausreichendes Verständnis der Gestaltung des PIMS im Kontext der Organisation, Risikobeurteilung und -handhabung (einschließlich der festgelegten Maßnahmen), Datenschutzrichtlinie und -ziele des Kunden und insbesondere der Bereitschaft des Kunden für das Audit erlangen. Dies muss für die Planung des Audits der Stufe 2 verwendet werden.

Die Ergebnisse von Stufe 1 müssen in einem schriftlichen Bericht aufgezeichnet werden. Die Zertifizierungsstelle muss den Auditbericht der Stufe 1 überprüfen, bevor sie über die Fortsetzung der Stufe 2 entscheidet. Die Zertifizierungsstelle muss bestätigen, dass die Mitglieder des Auditteams der Stufe 2 über die erforderliche Kompetenz verfügen. Dies darf der Auditor tun, der das Team des Audits der Stufe 1 leitet, wenn er dies für kompetent und geeignet hält.

ANMERKUNG Die Tatsache, dass eine Person in der Zertifizierungsstelle, die nicht an dem Audit beteiligt ist, den Bericht überprüft und entscheidet, ob das Audit fortgesetzt wird, und bestätigt, dass die Mitglieder des Auditteams für Stufe 2 kompetent sind, bietet eine gewisse Risikominderung. Es können allerdings bereits andere Risikominderungsmaßnahmen vorhanden sein, um das gleiche Ziel zu erreichen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

Die Zertifizierungsstelle muss den Kunden über die weiteren Arten von Informationen und Aufzeichnungen, die für eine detaillierte Untersuchung in Stufe 2 erforderlich sein können, in Kenntnis setzen.

9.3.1.1.2 Stufe 2

Die Zertifizierungsstelle muss auf Grundlage der im Auditbericht für Stufe 1 dokumentierten Ergebnisse einen Auditplan für die Durchführung von Stufe 2 entwickeln. Neben der Beurteilung der wirksamen Umsetzung des PIMS besteht das Ziel von Stufe 2 darin, zu bestätigen, dass der Kunde seine eigenen Richtlinien, Ziele und Verfahren einhält.

Dazu muss das Audit den Schwerpunkt auf folgende Aspekte des Kunden legen:

a) Führung durch die oberste Leitung und Verpflichtung zu den Datenschutzzielen;

b) Bewertung der mit dem Datenschutz zusammenhängenden Risiken; das Audit muss außerdem sicherstellen, dass die Bewertungen bei Wiederholung konsistente, gültige und vergleichbare Ergebnisse erbringen;

c) Bestimmung der Maßnahmen basierend auf der Datenschutz-Risikobeurteilung und des Risikobehandlungsprozesses;

d) Datenschutzleistung und Wirksamkeit des PIMS, beurteilt gegenüber den Datenschutzzielen;

e) Übereinstimmung zwischen den festgelegten Maßnahmen, der Erklärung zur Anwendbarkeit, den Ergebnissen der Datenschutz-Risikobeurteilung, des Risikobehandlungsprozesses sowie der Datenschutzrichtlinie und -ziele;

f) Umsetzung der Maßnahmen unter Berücksichtigung des externen und internen Kontextes und zugehöriger Risiken sowie der Überwachung, Messung und Analyse der Datenschutzverfahren und -maßnahmen der Organisation zur Bestimmung, ob Maßnahmen, die als umgesetzt erklärt werden, tatsächlich umgesetzt wurden und wirksam sind;

g) Programme, Prozesse, Verfahren, Aufzeichnungen, interne Audits und Überprüfungen der PIMS-Wirksamkeit, um sicherzustellen, dass diese auf Entscheidungen der obersten Leitung sowie die Datenschutzrichtlinie und -ziele zurückzuführen sind.

9.4 Durchführen von Audits

9.4.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.4. Außerdem gelten die Anforderungen und der Leitfaden in 9.4.2 und 9.4.3.

9.4.2 Spezifische Elemente des PIMS-Audits

Das Auditteam der Zertifizierungsstelle muss:

a) vom Kunden den Nachweis fordern, dass die Bewertung der mit dem Datenschutz zusammenhängenden Risiken für den vom Anwendungsbereich des PIMS abgedeckten PIMS-Betrieb maßgeblich und angemessen ist;

b) darlegen, ob die Verfahren des Kunden zur Bestimmung, Untersuchung und Bewertung der mit dem Datenschutz zusammenhängenden Risiken und die Ergebnisse der Umsetzung mit der Richtlinie und den Zielen des Kunden im Einklang stehen.

Die Zertifizierungsstelle muss auch darlegen, ob die im Rahmen der Risikobeurteilung eingesetzten Verfahren gut fundiert und angemessen umgesetzt wurden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10

9.4.3 Auditbericht

Zusätzlich zu ISO/IEC 17021-1:2015, 9.4.8, muss die Rolle des Kunden (verantwortliche Stelle, Auftragsverarbeiter oder beides) im Auditbericht beschrieben werden.

9.4.3.1 Zusätzlich zu den Anforderungen in ISO/IEC 17021-1:2015, 9.4.8, muss der Auditbericht die folgenden Informationen oder Verweisungen zu ihnen enthalten:

a) eine Darstellung des Audits der Datenschutzrisikoanalyse des Kunden;

b) sämtliche von der Organisation für den Vergleich nach ISO/IEC 27701, 6.1.3, eingesetzten Maßnahmensammlungen;

c) die Beschreibung der Rolle des Kunden (verantwortliche Stelle, Auftragsverarbeiter oder beides).

9.4.3.2 Der Auditbericht muss ausreichend detailliert sein, um die Zertifizierungsentscheidung zu ermöglichen und zu unterstützen. Er muss Folgendes enthalten:

a) die wesentlichen verfolgten Auditpfade und angewendeten Auditmethoden;

b) eine Verweisung auf die Version der Erklärung zur Anwendbarkeit und, sofern zutreffend, jedem nützlichen Vergleich mit den Ergebnissen vorangegangener Zertifizierungsaudits des Kunden.

Ausgefüllte Fragebögen, Checklisten, Beobachtungen, Protokolle oder Auditornotizen können einen integralen Bestandteil des Auditberichts bilden. Falls diese Methoden angewendet werden, müssen diese Dokumente als Nachweis zur Unterstützung der Zertifizierungsentscheidung an die Zertifizierungsstelle weitergegeben werden. Informationen zu den während des Audits bewerteten Stichproben müssen in den Auditbericht oder in andere Zertifizierungsdokumentation aufgenommen werden.

Bei Einsatz von Fernaudits muss der Bericht den Umfang angeben, in dem diese bei der Durchführung des Audits eingesetzt wurden, sowie deren Wirksamkeit zum Erreichen der Auditziele.

Wenn die Tätigkeiten der Organisation nicht an einem bestimmten physischen Standort durchgeführt und daher alle Tätigkeiten der Organisation aus der Ferne durchgeführt werden, muss im Auditbericht angegeben werden, dass alle Tätigkeiten der Organisation aus der Ferne durchgeführt werden.

Der Bericht muss die Angemessenheit der internen Organisation und der vom Kunden angewendeten Verfahren berücksichtigen, um Vertrauen in das PIMS zu erlangen.

Der Bericht muss eine Zusammenfassung der wichtigsten Beobachtungen, sowohl positiver als auch negativer Art, in Bezug auf die Umsetzung und Wirksamkeit der PIMS-Anforderungen und Steuerungsmaßnahmen für den Datenschutz enthalten.

9.5 Zertifizierungsentscheidung

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.5.

9.6 Aufrechterhaltung der Zertifizierung

9.6.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.6.1.

9.6.2 Überwachungstätigkeiten

9.6.2.1 Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.6.2. Außerdem gelten die Anforderungen und der Leitfaden in 9.6.2.2, 9.6.2.3 und 9.6.2.4.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27706:2024-10