

	DIN EN ISO/IEC 27006-1	
ICS 03.120.20; 35.030	Ersatz für DIN EN ISO/IEC 27006:2021-05	
<p>Informationssicherheit, Cybersicherheit und Datenschutz – Anforderungen an Stellen, die Informationssicherheitsmanagement- systeme auditieren und zertifizieren – Teil 1: Allgemeines (ISO/IEC 27006-1:2024); Deutsche Fassung EN ISO/IEC 27006-1:2024</p> <p>Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems – Part 1: General (ISO/IEC 27006-1:2024); German version EN ISO/IEC 27006-1:2024</p> <p>Sécurité de l'information, cybersécurité et protection de la vie privée – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information – Partie 1: Généralités (ISO/IEC 27006-1:2024); Version allemande EN ISO/IEC 27006-1:2024</p>		
Gesamtumfang 70 Seiten		
DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)		

Nationales Vorwort

Dieses Dokument (EN ISO/IEC 27006-1:2024) wurde vom Technischen Komitee ISO/IEC JTC 1 „ISO/IEC Gemeinschaftskomitee für Informationstechnik“ 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).

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

ISO 9000	siehe	DIN EN ISO 9000
ISO 9001	siehe	DIN EN ISO 9001
ISO 19011	siehe	DIN EN ISO 19011
ISO/IEC 17021-1:2015	siehe	DIN EN ISO/IEC 17021-1:2015-11
ISO/IEC 27000	siehe	DIN EN ISO/IEC 27000
ISO/IEC 27001:2022	siehe	DIN EN ISO/IEC 27001:2024-01
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27006-2	siehe	DIN EN ISO/IEC 27006-2*
ISO/IEC 27007	siehe	DIN EN ISO/IEC 27007

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 EN ISO/IEC 27006:2021-05 wurden folgende Änderungen vorgenommen:

- a) Dieses Dokument wurde in den ersten Teil einer mehrteiligen Norm umgewandelt;
- b) das gesamte Dokument wurde für Fernaudits und Organisationen mit wenigen oder gar keinen relevanten Standorten aktualisiert;
- c) das Konzept von Personen, die bestimmte identische Tätigkeiten ausüben, wurde in C.3.4 eingeführt und mehrere Aktualisierungen wurden vorgenommen;
- d) dieses Dokument (insbesondere Anhang E) wurde an ISO/IEC 27001:2022 und ISO/IEC 27002:2022 angepasst;
- e) Redundanzen mit ISO/IEC 17021-1 wurden beseitigt;
- f) Der Wortlaut wurde klarer formuliert und enger an die ISO/IEC 17021-1 angeglichen.

* Zur Zeit Entwurf.

Frühere Ausgaben

DIN EN ISO/IEC 27006: 2021-05

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9000, *Qualitätsmanagementsysteme — Grundlagen und Begriffe*

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

DIN EN ISO 19011, *Leitfaden zur Auditierung von Managementsystemen*

DIN EN ISO/IEC 17021-1:2015-11, *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren — Teil 1: Anforderungen (ISO/IEC 17021-1:2015); Deutsche und Englische Fassung EN ISO/IEC 17021-1:2015*

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

DIN EN ISO/IEC 27001:2024-01, *Informationssicherheit, Cybersicherheit und Datenschutz — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023*

DIN EN ISO/IEC 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

DIN EN ISO/IEC 27006-2, *Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren — Teil 2: Datenschutz-Managementsysteme*

DIN EN ISO/IEC 27007, *Informationssicherheit, Cybersicherheit und Datenschutz — Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen*

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Datenschutz —
Anforderungen an Stellen, die Informationssicherheits-
managementsysteme auditieren und zertifizieren —
Teil 1: Allgemeines (ISO/IEC 27006-1:2024)

Information security, cybersecurity and
privacy protection —
Requirements for bodies providing audit and
certification of information security management
systems —
Part 1: General (ISO/IEC 27006-1:2024)

Sécurité de l'information, cybersécurité et
protection de la vie privée —
Exigences pour les organismes procédant à l'audit et à
la certification des systèmes de management de la
sécurité de l'information —
Partie 1: Généralités (ISO/IEC 27006-1:2024)

Diese Europäische Norm wurde vom CEN am 29. Januar 2024 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-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	5
Vorwort	6
Einleitung	8
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Grundsätze	13
5 Allgemeine Anforderungen	13
5.1 Rechts- und Vertragsfragen	13
5.2 Handhabung der Unparteilichkeit	13
5.2.1 Allgemeines	13
5.2.2 Interessenkonflikte	13
5.3 Haftung und Finanzierung	13
6 Strukturelle Anforderungen	14
7 Anforderungen an Ressourcen	14
7.1 Kompetenz des Personals	14
7.1.1 Allgemeines	14
7.1.2 Allgemeine Kompetenzanforderungen	14
7.1.3 Bestimmung der Kompetenzkriterien	14
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist	17
7.2.1 Allgemeines	17
7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren	17
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten	18
7.4 Aufzeichnungen über Personal	18
7.5 Ausgliederung	18
8 Anforderungen an Informationen	18
8.1 Öffentliche Informationen	18
8.2 Zertifizierungsdokumente	18
8.2.1 Allgemeines	18
8.2.2 ISMS-Zertifizierungsdokumente	18
8.2.3 Verweis auf andere Normen in den ISMS-Zertifizierungsdokumenten	19
8.3 Verweisung auf Zertifizierung und Zeichennutzung	19
8.4 Vertraulichkeit	19
8.4.1 Allgemeines	19
8.4.2 Zugang zu den Aufzeichnungen der Organisation	19
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden	19
9 Anforderungen an Prozesse	20
9.1 Tätigkeiten vor der Zertifizierung	20
9.1.1 Antrag	20
9.1.2 Antragsprüfung	20
9.1.3 Auditprogramm	20
9.1.4 Ermittlung des Auditzeitaufwands	21
9.1.5 Stichprobenprüfung an mehreren Standorten	22
9.1.6 Mehrfach-Managementsysteme	23
9.2 Planung von Audits	23
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien	23
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung	24
9.2.3 Auditplan	24
9.3 Erstzertifizierung	24
9.3.1 Allgemeines	24
9.3.2 Erstzertifizierungsaudit	24

9.4	Durchführen von Audits	26
9.4.1	Allgemeines	26
9.4.2	Spezifische Elemente des ISMS-Audits	26
9.4.3	Auditbericht	26
9.5	Zertifizierungsentscheidung	27
9.5.1	Allgemeines	27
9.5.2	Zertifizierungsentscheidung	27
9.6	Aufrechterhaltung der Zertifizierung	27
9.6.1	Allgemeines	27
9.6.2	Überwachungstätigkeiten	27
9.6.3	Rezertifizierung	28
9.6.4	Audits aus besonderem Anlass	28
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung	28
9.7	Einsprüche	28
9.8	Beschwerden	28
9.8.1	Allgemeines	28
9.8.2	Beschwerden	28
9.9	Aufzeichnungen zu Kunden	28
10	Managementsystemanforderungen für Zertifizierungsstellen	29
10.1	Optionen	29
10.1.1	Allgemeines	29
10.1.2	ISMS-Umsetzung	29
10.2	Option A: Allgemeine Managementsystemanforderungen	29
10.3	Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001	29
Anhang A (normativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung		30
A.1	Übersicht	30
Anhang B (informativ) Weitere Kompetenzbetrachtungen		31
B.1	Allgemeine Betrachtungen zu Kompetenzen	31
B.2	Betrachtungen zu besonderen Kenntnissen und Erfahrungen	31
B.2.1	Typische Kenntnisse mit Bezug zu ISMS	31
Anhang C (normativ) Auditzeitaufwand		33
C.1	Allgemeines	33
C.2	Konzepte	34
C.2.1	Anzahl der von der Organisation gesteuerten Personen	34
C.2.2	Auditortag	34
C.2.3	Temporärer Standort	34
C.3	Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit	34
C.3.1	Allgemeines	34
C.3.2	Methoden zur Durchführung von Fernaudits	34
C.3.3	Berechnung des Auditzeitaufwands	35
C.3.4	Bestimmung der anfänglichen Personenanzahl	35
C.3.5	Faktoren für die Anpassung des Auditzeitaufwands	36
C.3.6	Einschränkung der Abweichung von der Auditzeit	38
C.3.7	Vor-Ort-Auditzeitaufwand	38
C.4	Auditzeitaufwand für das Überwachungsaudits	38
C.5	Auditzeitaufwand für das Rezertifizierungsaudit	38
C.6	Auditzeitaufwand für mehrere Standorte	38
C.7	Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs	39
Anhang D (informativ) Methoden für Berechnungen des Auditzeitaufwands		40
D.1	Allgemeines	40
D.2	Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	40
D.3	Beispiel für die Auditzeitaufwandberechnung	44
Anhang E (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2022, Anhang A		46
E.1	Zweck	46
E.2	Anwendung von Tabelle E.1	46
E.2.1	Allgemeines	46

E.2.2	Spalte „Systemprüfung“	47
E.2.3	Spalte „Sichtprüfung“	47
E.2.4	Möglicher Nachweis der Gestaltung und Umsetzung von Maßnahmen	47
	Literaturhinweise	66

Tabellen

Tabelle A.1	— Tabelle zum Wissen und zu den Fertigkeiten für ISMS-Audits und -Zertifizierung	30
Tabelle C.1	— Auditzeitaufwandstabelle	36
Tabelle D.1	— Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands	41
Tabelle D.2	— Mit dem Geschäft und der Organisation zusammenhängende Faktoren (ohne IT)	44
Tabelle D.3	— Mit der IT-Umgebung zusammenhängende Faktoren	45
Tabelle D.4	— Auswirkung der Faktoren auf die Auditzeit	45
Tabelle E.1	— Bewertung der Maßnahmen	48

Europäisches Vorwort

Dieses Dokument (EN ISO/IEC 27006-1:2024) wurde vom 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.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2024, und etwaige entgegenstehende nationale Normen müssen bis September 2024 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN ISO/IEC 27006:2020.

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 und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27006-1:2024 wurde von CEN-CENELEC als EN ISO/IEC 27006-1:2024 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 oder www.iec.ch/members_experts/refdocs).

ISO und IEC weisen auf die Möglichkeit hin, dass die Anwendung dieses Dokuments mit der Verwendung eines oder mehrerer Patente verbunden sein kann. ISO und IEC beziehen jedoch in dieser Hinsicht keinerlei Stellung bezüglich Nachweis, Gültigkeit oder Anwendbarkeit jeglicher beanspruchten Patentrechte. Zum Zeitpunkt der Veröffentlichung dieses Dokuments lag ISO und IEC keine Mitteilung über ein Patent bzw. mehrere Patente vor, welche/s zur Umsetzung dieses Dokuments erforderlich sein könnte/n. Anwender werden jedoch darauf hingewiesen, dass dies möglicherweise nicht der aktuelle Informationsstand ist. Dieser kann jedoch der Patentdatenbank unter www.iso.org/patents oder <https://patents.iec.ch> entnommen werden. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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. Für IEC, siehe: www.iec.ch/understanding-standards.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* in Zusammenarbeit mit dem Europäischen Komitee für Normung (CEN), Technisches Komitee CEN/CLC/JTC 13, *Cybersicherheit und Datenschutz*, in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

Diese erste Ausgabe von ISO/IEC 27006-1 ersetzt ISO/IEC 27006:2015, die technisch überarbeitet wurde. Auch die Änderung ISO/IEC 27006:2015/Amd 1:2020 wurde mit einbezogen.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- dieses Dokument wurde in den ersten Teil einer Normenreihe überführt;
- das gesamte Dokument wurde für Fernaudits und Organisationen mit wenigen oder keinen entsprechenden physischen Standorten aktualisiert;
- das Konzept von Personen, die bestimmte identische Tätigkeiten ausüben, wurde in C.3.4 eingeführt und mehrere Aktualisierungen wurden vorgenommen;

- dieses Dokument (insbesondere Anhang E) wurden an ISO/IEC 27001:2022 und ISO/IEC 27002:2022 angeglichen;
- Redundanzen mit ISO/IEC 17021-1 wurden entfernt;
- der Wortlaut wurde verbessert und an ISO/IEC 17021-1 angeglichen.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 27006 ist auf der ISO- und auf der IEC-Internetseite abrufbar.

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 und www.iec.ch/national-committees zu finden.

Einleitung

ISO/IEC 17021-1 beschreibt Anforderungen und Leitfäden für Stellen, die Audits und Zertifizierungen von Managementsystemen anbieten. Falls solche Stellen beabsichtigen, ISO/IEC 17021-1 mit dem Ziel des Audits und der Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS) in Übereinstimmung mit ISO/IEC 27001 zu entsprechen, sind einige zusätzliche Anforderungen und Anleitung in Bezug auf ISO/IEC 17021-1 von entscheidender Bedeutung. Diese werden durch dieses Dokument zur Verfügung gestellt.

Dieses Dokument legt Anforderungen an Stellen fest, die ein ISMS auditieren und zertifizieren. Es nennt allgemeine Anforderungen an diese als Zertifizierungsstellen bezeichneten Stellen. Mit Einhaltung dieser Anforderungen soll sichergestellt werden, dass Zertifizierungsstellen die Zertifizierung von ISMS kompetent, konsistent und unparteilich durchführen und dadurch die Anerkennung solcher Stellen und die Akzeptanz ihrer Zertifizierungen auf nationaler und internationaler Ebene fördern.

Der Text in diesem Dokument folgt der Struktur von ISO/IEC 17021-1:2015.

In diesem Dokument werden die folgenden Verbformen verwendet:

- „müssen“ zeigt eine Anforderung an;
- „sollten“ zeigt eine Empfehlung an;
- „dürfen“ zeigt eine Erlaubnis an;
- „können“ zeigt eine Möglichkeit bzw. eine Fähigkeit an.

1 Anwendungsbereich

Dieses Dokument legt Anforderungen fest und bietet Anleitung für Stellen, die Audits und Zertifizierungen von Informationssicherheitsmanagementsystemen (ISMS) vornehmen. Zusätzlich gelten die Anforderungen nach ISO/IEC 17021-1.

Die in diesem Dokument enthaltenen Anforderungen werden von Stellen, die ISMS-Zertifizierungen durchführen, im Hinblick auf Kompetenz und Zuverlässigkeit nachgewiesen. Die in diesem Dokument enthaltene Anleitung bietet eine zusätzliche Interpretation dieser Anforderungen für Stellen, die ISMS-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 17021-1:2015, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17021-1 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

en **certification document**

Dokument, das angibt, dass das Informationssicherheitsmanagementsystem (ISMS) eines Kunden spezifizierten ISMS-Normen und jeglicher im Rahmen des Managementsystems erforderlichen zusätzlichen Dokumentation entspricht

Anmerkung 1 zum Begriff: Diese Definition schränkt die Anzahl der Dokumente, die gemeinsam als Zertifizierungsdokumente bezeichnet werden, nicht ein.

3.2

Maßnahme

en **control**

Mittel zur Beibehaltung und/oder Veränderung des *Risikos* (3.10)

Anmerkung 1 zum Begriff: Maßnahmen umfassen unter anderem Prozesse, Politik, Richtlinien, Geräte, Praktiken oder andere Bedingungen und/oder Handlungen, die das *Risiko* (3.10) beibehalten und/oder verändern.

Anmerkung 2 zum Begriff: Maßnahmen können nicht immer die beabsichtigte oder angenommene verändernde Wirkung ausüben.

[QUELLE: ISO/IEC 27002:2022, 3.1.8]

3.3

externer Kontext

en **external context**

externes Umfeld, in dem die *Organisation* (3.9) versucht, ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der externe Kontext kann Folgendes beinhalten:

- die kulturelle, soziale, politische, gesetzliche, regulatorische, finanzielle, technologische, ökonomische, natürliche und wettbewerbliche Umgebung, die internationalen, nationalen, regionalen oder lokalen Charakter haben kann;
- wesentliche Treiber und Trends, die sich auf die Ziele der *Organisation* (3.9) auswirken;
- Beziehungen zu externen interessierten Parteien sowie deren Auffassungen und Werte.

[QUELLE: ISO/IEC 27000:2018, 3.22]

3.4

Informationssicherheit

en **information security**

Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information

Anmerkung 1 zum Begriff: Zusätzlich können auch andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit einbezogen werden.

[QUELLE: ISO/IEC 27000:2018, 3.28]

3.5

Informationssicherheitsvorfall

en **information security incident**

einzelnes oder eine Reihe von ungewollten oder unerwarteten Informationssicherheitsereignissen, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die *Informationssicherheit* (3.4) zu bedrohen

[QUELLE: ISO/IEC 27000:2018, 3.31]

3.6

Informationssystem

en **information system**

Satz an Anwendungen, Dienste, informationstechnische Werte oder andere Information bearbeitende Komponenten

[QUELLE: ISO/IEC 27000:2018, 3.35]

3.7

interner Kontext

en **internal context**

interne Umgebung, in der die *Organisation* (3.9) versucht, ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der interne Kontext kann Folgendes beinhalten:

- Steuerung durch die Unternehmensführung, Organisationsstruktur, Rollen und Verantwortlichkeiten;
- Politik, Richtlinien, Ziele und Strategien, die mit dem Ziel in Kraft sind, sie einzuhalten beziehungsweise sie zu erreichen;

- die Fähigkeit in Form von Ressourcen und Wissen (z. B. Kapital, Zeit, Menschen, Prozesse, Systeme und Techniken);
- *Informationssysteme* (3.6), Informationsflüsse und Prozesse zur Entscheidungsfindung (sowohl formell als auch informell);
- Beziehungen zu internen interessierten Parteien sowie deren Auffassungen und Werte;
- die Organisationskultur (*Organisation*, 3.9);
- Standards, Leitfäden und Modelle, die von der *Organisation* (3.9) übernommen worden sind;
- Gestalt und Ausmaß vertraglicher Beziehungen.

[QUELLE: ISO/IEC 27000:2018, 3.38]

3.8

Managementsystem

Satz zusammenhängender oder sich gegenseitig beeinflussender Elemente einer *Organisation* (3.9), um Politik, Richtlinien, Ziele und Prozesse zum Erreichen dieser Ziele festzulegen

Anmerkung 1 zum Begriff: Ein Managementsystem kann eine oder mehrere Disziplinen behandeln, z. B. Qualitätsmanagement, Finanzmanagement oder Umweltmanagement.

Anmerkung 2 zum Begriff: Die Elemente des Managementsystems beinhalten die Struktur der *Organisation* (3.9), Rollen und Verantwortlichkeiten, Planung, Betrieb, Politik, Richtlinien, Praktiken, Regeln, Überzeugungen, Ziele und Prozesse zum Erreichen dieser Ziele.

Anmerkung 3 zum Begriff: Der Anwendungsbereich eines Managementsystems kann die ganze *Organisation* (3.9), bestimmte Funktionen der *Organisation* (3.9), bestimmte Bereiche der *Organisation* (3.9) oder eine oder mehrere Funktionsbereiche über eine Gruppe von *Organisationen* (3.9) hinweg umfassen.

Anmerkung 4 zum Begriff: Dieser Begriff stellt eine der gemeinsamen Benennungen und der Basisdefinitionen für ISO-Managementsystemnormen dar, die in ISO/IEC-Directives, Part 1, Consolidated ISO Supplement, Anhang SL enthalten sind. Die ursprüngliche Definition wurde durch Änderungen in den Anmerkungen 1 bis 3 zum Begriff geändert.

[QUELLE: ISO 9000:2015, 3.5.3]

3.9

Organisation

Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen

Anmerkung 1 zum Begriff: Der Begriff *Organisation* umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat.

[QUELLE: ISO/IEC 27000:2018, 3.50]

3.10

Risiko

en **risk**

Auswirkung von Ungewissheit auf Ziele

Anmerkung 1 zum Begriff: Eine Auswirkung ist eine Abweichung vom Erwarteten – in positiver oder negativer Hinsicht.

Anmerkung 2 zum Begriff: Ungewissheit ist der Zustand des auch teilweisen Fehlens von Information im Hinblick auf das Verständnis eines Ereignisses oder Wissen über ein Ereignis, seine Folgen oder seine Wahrscheinlichkeit.

Anmerkung 3 zum Begriff: Risiko wird häufig durch Bezugnahme auf mögliche „Ereignisse“ (wie in ISO Guide 73:2009, 3.5.1.3, definiert) und „Folgen“ (wie in ISO Guide 73:2009, 3.6.1.3, definiert) oder eine Kombination beider charakterisiert.

Anmerkung 4 zum Begriff: Risiko wird häufig mittels der Folgen eines Ereignisses (einschließlich Veränderungen der Umstände) in Verbindung mit der „Wahrscheinlichkeit“ (wie in ISO Guide 73:2009, 3.6.1.1, definiert) seines Eintretens beschrieben.

Anmerkung 5 zum Begriff: Im Kontext von Informationssicherheitsmanagementsystemen können Informationssicherheitsrisiken als Auswirkung von Ungewissheit auf Informationssicherheitsziele beschrieben werden.

Anmerkung 6 zum Begriff: Informationssicherheitsrisiko ist mit der Möglichkeit verbunden, dass Bedrohungen Schwachstellen eines Informationswerts oder einer Gruppe solcher Werte ausnutzen und damit einer *Organisation* (3.9) Schaden zufügen.

[QUELLE: ISO/IEC 27000:2018, 3.61]

3.11

Risikoanalyse

en **risk analysis**

Prozess, um die Beschaffenheit des *Risikos* (3.10) zu verstehen und das Risikoniveau zu bestimmen

Anmerkung 1 zum Begriff: Die Risikoanalyse liefert die Grundlage für die Risikobewertung und die Entscheidungen im Zuge der *Risikobehandlung* (3.14).

Anmerkung 2 zum Begriff: Die Risikoanalyse beinhaltet die Risikoabschätzung.

[QUELLE: ISO/IEC 27000:2018, 3.63]

3.12

Risikobeurteilung

en **risk assessment**

übergreifender Prozess, der aus Risikoidentifizierung, *Risikoanalyse* (3.11) und Risikobewertung besteht

[QUELLE: ISO/IEC 27000:2018, 3.64]

3.13

Risikomanagement

en **risk management**

koordinierte Tätigkeiten zum Zwecke der Führung und Steuerung einer *Organisation* (3.9) in Bezug auf *Risiken* (3.10)

[QUELLE: ISO/IEC 27000:2018, 3.69]

3.14

Risikobehandlung

en **risk treatment**

Prozess, um *Risiken* (3.10) zu verändern

Anmerkung 1 zum Begriff: Die Risikobehandlung kann umfassen:

- Vermeiden des Risikos, indem entschieden wird, die Tätigkeit, die Anlass zu dem Risiko gibt, nicht zu beginnen oder fortzusetzen;
- Eingehen oder Vergrößern des Risikos mit dem Ziel, eine Chance wahrzunehmen;
- Beseitigen der Risikoquelle;
- Verändern der Wahrscheinlichkeit;

- Verändern der Folgen;
- Teilen des Risikos mit einer anderen Partei oder anderen Parteien (einschließlich Verträgen und Finanzierung von Risiken);
- Beibehalten des Risikos im Rahmen einer fundierten Entscheidung.

Anmerkung 2 zum Begriff: Risikobehandlungen, die sich mit negativen Folgen beschäftigen, heißen auch „Risikominderung“, „Risikoeliminierung“, „Risikovorsorge“ und „Risikoreduzierung“.

Anmerkung 3 zum Begriff: Die Risikobehandlung kann zu neuen Risiken führen oder vorhandene *Risiken* (3.10) verändern.

[QUELLE: ISO/IEC 27000:2018, 3.72]

3.15

Regel

en **rule**

anerkannter Grundsatz oder Anweisung, der die Erwartungen der *Organisation* (3.9) in Bezug auf das, was zu tun ist, was erlaubt oder nicht erlaubt ist, festlegt

[QUELLE: ISO/IEC 27002:2022, 3.1.32 – modifiziert, Anmerkung 1 zum Begriff wurde gestrichen]

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 Allgemeines

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

Zertifizierungsstellen dürfen einen Mehrwert während Zertifizierungen und Überwachungsaudits erbringen, (z. B. durch Bestimmung von Verbesserungsmöglichkeiten, die während des Audits bekannt werden, ohne spezifische Lösungen vorzuschlagen), ohne dass dies als Beratung betrachtet wird oder dass dies einen potenziellen Interessenkonflikt darstellt.

Die Zertifizierungsstelle darf keine internen Prüfungen der Informationssicherheit des ISMS des Kunden, das zertifiziert werden soll, durchführen. Des Weiteren muss die Zertifizierungsstelle von der Stelle oder den Stellen (einschließlich Einzelpersonen) unabhängig sein, die das interne ISMS-Audit durchführen.

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.

7 Anforderungen an Ressourcen

7.1 Kompetenz des Personals

7.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.1. Außerdem gelten die Anforderungen und der Leitfaden in 7.1.2 und 7.1.3.

7.1.2 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 alle in ISO/IEC 17021-1 und 7.1.3 und 7.2.2 dieses Dokuments angegebenen Anforderungen berücksichtigen, die entsprechend den Festlegungen der Zertifizierungsstelle für die technischen Bereiche des ISMS relevant sind. Anhang B gibt hier weitere Hilfestellungen zu Kompetenzen.

Die Zertifizierungsstelle muss die Kenntnisse und Fähigkeiten, die für bestimmte Funktionen erforderlich sind, nach Anhang A festlegen.

Wenn in einer spezifischen Norm (z. B. ISO/IEC 27006-2) zusätzliche spezifische Kriterien einschließlich Kompetenzanforderungen festgelegt wurden, müssen diese angewendet werden.

7.1.3 Bestimmung der Kompetenzkriterien

7.1.3.1 Kompetenzanforderungen für ISMS-Audits

7.1.3.1.1 Allgemeine Anforderungen

Die Zertifizierungsstelle muss über Kriterien zur Verifizierung der Kompetenz der Auditteammitglieder verfügen, so dass sichergestellt ist, dass diese zumindest die Fertigkeiten besitzen, ihr Wissen über folgendes anzuwenden:

- a) Informationssicherheit;
- b) die technischen Aspekte in Bezug auf die Tätigkeit, die auditiert werden soll;
- c) Managementsysteme;
- d) Auditgrundsätze;

ANMERKUNG ISO 19011 enthält weitere Informationen zu den Grundsätzen des Auditierens.

- e) ISMS-Überwachung, -Messung, -Analyse und -Beurteilung.

Die voranstehenden Anforderungen a) bis e) gelten für jeden Auditor im Auditteam. Dabei kann b) gemeinsam von allen Auditoren im Team abgedeckt werden.

Die Mitglieder des Auditteams müssen gemeinsam über die für die oben genannten Anforderungen erforderlichen Fähigkeiten verfügen, die durch Erfahrung in ihrer Anwendung nachgewiesen werden können.

Die Mitglieder des Auditteams müssen gemeinsam über die Kompetenz verfügen, Anzeichen von Informationssicherheitsvorfällen im ISMS des Kunden zu den entsprechenden ISMS-Elementen zurückzuverfolgen.

Einzelne Auditoren müssen nicht über eine umfassende Erfahrung in allen Bereichen der Informationssicherheit verfügen, aber das Auditteam muss insgesamt über angemessene Kompetenzen verfügen, um den zu auditierenden ISMS-Anwendungsbereich abzudecken.

7.1.3.1.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

Jeder Auditor in einem ISMS-Auditteam muss über folgendes Wissen verfügen:

- a) ISMS-spezifische Dokumentationsstrukturen, Hierarchie und Wechselbeziehungen;
- b) Informationssicherheitsrisikobeurteilung und -risikomanagement;
- c) auf ISMS anwendbare Prozesse.

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

- d) Werkzeuge, Methoden, Verfahren des Informationssicherheitsmanagements und deren Anwendung;
- e) aktuelle Technik, bei der die Informationssicherheit relevant oder ein Aspekt sein kann.

7.1.3.1.3 Informationssicherheitsmanagementsystemnormen und normative Dokumente

Jeder Auditor in einem ISMS-Auditteam muss über das Wissen bezüglich aller Anforderungen in ISO/IEC 27001 verfügen.

Die Mitglieder des Auditteams müssen gemeinschaftlich über das Wissen bezüglich aller Maßnahmen in ISO/IEC 27001:2022, Anhang A und ihrer Umsetzung verfügen.

7.1.3.1.4 Praktische Unternehmensführung

Jeder Auditor in einem ISMS-Auditteam muss über folgendes Wissen verfügen:

- a) bewährte Informationssicherheitspraktiken und Informationssicherheitsprozeduren aus der Industrie;
- b) Richtlinien und betriebliche Anforderungen an die Informationssicherheit;
- c) allgemeine Konzepte und Praktiken zur Unternehmensführung und die Wechselbeziehung zwischen Politik, Zielen und Ergebnissen;
- d) Managementprozesse und zugehörige Terminologie.

ANMERKUNG Diese Prozesse umfassen auch Personalführung, interne und externe Kommunikation sowie andere relevante Unterstützungsprozesse.

7.1.3.1.5 Geschäftsfeld des Kunden

Jeder Auditor in einem ISMS-Auditteam muss über folgendes Wissen verfügen:

- a) gesetzliche und behördliche Anforderungen im jeweiligen Informationssicherheitsgebiet, im jeweiligen geographischen Gebiet und im jeweiligen Rechtssystem/in den Rechtssystemen;

ANMERKUNG Das Wissen über gesetzliche und regulatorische Anforderungen impliziert kein umfassendes rechtliches Hintergrundwissen.

- b) mit dem Geschäftsfeld zusammenhängende Informationssicherheitsrisiken;
- c) generische Terminologie, Prozesse und Techniken, die mit dem Geschäftsfeld des Kunden zusammenhängen;

d) relevante Geschäftsfeldpraktiken.

Kriterium a) darf im Auditteam verteilt sein.

7.1.3.1.6 Produkte, Prozesse und Organisation des Kunden

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

- a) Einfluss der Art, Größe, Führung, Struktur, Funktionen und Beziehungen einer Organisation auf die Entwicklung und Implementierung des ISMS und der Zertifizierungstätigkeiten, einschließlich Ausgliederung;
- b) komplexer Betrieb im Rahmen einer weiten Perspektive;
- c) auf die Produkte oder Dienstleistungen anzuwendende gesetzliche und behördliche Anforderungen.

7.1.3.2 Anforderungen an die Kompetenz für die Durchführung der Antragsprüfung

7.1.3.2.1 Geschäftsfeld des Kunden

Das Personal, das die Antragsprüfung zur Bestimmung der erforderlichen Kompetenz des Auditteams, zur Auswahl der Mitglieder des Auditteams und zur Bestimmung der Auditzeit durchführt, muss über Wissen über generische Terminologie, Prozesse, Techniken und Risiken, die mit dem Geschäftsfeld des Kunden zusammenhängen verfügen.

7.1.3.2.2 Produkte, Prozesse und Organisation des Kunden

Das Personal, das die Antragsprüfung zur Bestimmung der erforderlichen Kompetenz des Auditteams, zur Auswahl der Mitglieder des Auditteams und zur Bestimmung der Auditzeit durchführt, muss über Wissen über den Einfluss von Kundenprodukten, Prozessen, Art der Organisation, Größe, Führung, Struktur, Funktionen und Beziehungen einer Organisation zur Entwicklung und Implementierung des ISMS und der Zertifizierungstätigkeiten, einschließlich extern bereitgestellter Funktionen.

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

7.1.3.3.1 Allgemeines

Das Personal, das Auditberichte bewertet und Zertifizierungsentscheidungen trifft, muss über Wissen verfügen, das es ihm ermöglicht, die Angemessenheit des Geltungsbereichs der Zertifizierung sowie Änderungen des Geltungsbereichs und ihre Auswirkungen auf die Wirksamkeit des Audits, insbesondere die fortdauernde Gültigkeit der Bestimmung der Schnittstellen, Abhängigkeiten und zugehörigen Risiken, zu verifizieren.

Zudem muss das Personal, das Auditberichte bewertet und Zertifizierungsentscheidungen trifft, über folgendes Wissen verfügen:

- a) Managementsysteme allgemein;
- b) Auditprozesse und -verfahren;

7.1.3.3.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

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

- a) die in 7.1.3.1.2 a), b) und c) aufgelisteten Punkte;
- b) für die Informationssicherheit relevante gesetzliche und behördliche Anforderungen.

7.1.3.3.3 Geschäftsfeld des Kunden

Das Personal, das Auditberichte bewertet und Zertifizierungsentscheidungen trifft, muss über Wissen verfügen bezüglich generischer Terminologie und Risiken, die mit den relevanten Geschäftsfeldpraktiken zusammenhängen.

7.1.3.3.4 Produkte, Prozesse und Organisation des Kunden

Das Personal, das Auditberichte bewertet und Zertifizierungsentscheidungen trifft, muss über Wissen bezüglich Kundenprodukten, Prozessen, Arten der Organisation, Größe, Führung, Struktur, Funktionen und Beziehungen verfügen.

7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist

7.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 7.2. Außerdem gelten die Anforderungen und der Leitfaden in 7.2.2.

7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren

7.2.2.1 Allgemeine Betrachtungen

Die Zertifizierungsstelle muss durch folgende Punkte nachweisen, dass jeder Auditor über Wissen und Erfahrung verfügt:

- a) anerkannte ISMS-spezifische Qualifikationen;
- b) Registrierung als Auditor, soweit anwendbar;
- c) Teilnahme an ISMS-Schulungen und Erlangung relevanter persönlicher Qualifikationen;
- d) aktuelle Aufzeichnungen der beruflichen Entwicklung;
- e) ISMS-Audits, die ein anderer ISMS-Auditor überwacht (engl. Witness-Audit) 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) eine berufliche Ausbildung oder Weiterbildung erfahren hat, gleichwertig mit einer universitären Ausbildung;
- b) über praktische Berufserfahrung in den Bereichen Informationstechnik und Informationssicherheit verfügt, die ausreicht, um als Auditor für ISMS tätig zu sein;
- c) eine ausreichende Schulung zur Auditierung von ISMS erhalten und seine Fertigkeiten zur Auditierung eines ISMS nach ISO/IEC 27001 nachgewiesen hat. Diese Erfahrung muss durch die Durchführung von mindestens einem ISMS-Erstzertifizierungsaudit (Stufe 1 und Stufe 2) oder einer Rezertifizierung und mindestens einem Überwachungsaudit als Auditor in Ausbildung unter Aufsicht eines ISMS-Evaluators (siehe ISO/IEC 17021-1:2015, 9.2.2.1.4) erworben werden. Diese Erfahrung muss in mindestens 10 ISMS-Vorort-Audittagen gesammelt werden, die in den letzten fünf Jahren durchgeführt wurden. Die Teilnahme muss die Überprüfung von Dokumenten, die Überprüfung der Risikobewertung und deren Umsetzung sowie die Auditberichterstattung umfassen;
- d) relevantes und aktuelles Wissen sowie Fertigkeiten im Bereich der Informationssicherheit und der Auditierung pflegt.