

DIN EN ISO/IEC 27006

ICS 35.030

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

Information technology –
Security techniques –
Requirements for bodies providing audit and certification of information security
management systems (ISO/IEC 27006:2015, including Amd 1:2020);
German version EN ISO/IEC 27006:2020

Technologies de l'information –
Techniques de sécurité –
Exigences pour les organismes procédant à l'audit et à la certification des systèmes de
management de la sécurité de l'information (ISO/IEC 27006:2015, y compris Amd 1:2020);
Version allemande EN ISO/IEC 27006:2020

Gesamtumfang 53 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27006:2015, einschließlich Amd 1:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als EN ISO/IEC 27006:2020 übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

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 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06

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

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 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 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

Deutsche Fassung

Informationstechnik —
IT-Sicherheitsverfahren —
Anforderungen an Institutionen, die Audits und Zertifizierungen
von Informationssicherheits-Managementsystemen anbieten
(ISO/IEC 27006:2015, einschließlich Amd 1:2020)

Information technology —
Security techniques —
Requirements for bodies providing audit and
certification of information security management
systems (ISO/IEC 27006:2015, including Amd 1:2020)

Technologies de l'information —
Techniques de sécurité —
Exigences pour les organismes procédant à l'audit et à
la certification des systèmes de management de la
sécurité de l'information
(ISO/IEC 27006:2015, y compris Amd 1:2020)

Diese Europäische Norm wurde vom CEN am 16. November 2020 angenommen.

Diese Europäische Norm wurde vom CEN-CENELEC Management-Zentrum am 24. Februar 2021 korrigiert und neu herausgegeben.

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	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Grundsätze	7
5 Allgemeine Anforderungen	7
5.1 Rechts- und Vertragsfragen	7
5.2 Handhabung der Unparteilichkeit	8
5.2.1 IS 5.2 Interessenskonflikte	8
5.3 Haftung und Finanzierung	8
6 Strukturelle Anforderungen	8
7 Anforderungen an Ressourcen	8
7.1 Kompetenz des Personals	8
7.1.1 IS 7.1.1 Allgemeine Betrachtungen	9
7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien	9
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist	13
7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren	13
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten	14
7.3.1 IS 7.3 Einsatz einzelner externer Auditoren und externer Fachexperten als Teil des Auditteams	14
7.4 Aufzeichnungen über Personal	14
7.5 Ausgliederung	15
8 Anforderungen an Informationen	15
8.1 Öffentliche Informationen	15
8.2 Zertifizierungsdokumente	15
8.2.1 IS 8.2 ISMS-Zertifizierungsdokumente	15
8.3 Verweis auf Zertifizierung und Zeichennutzung	15
8.4 Vertraulichkeit	15
8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation	15
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden	15
9 Anforderungen an Prozesse	16
9.1 Tätigkeiten vor der Zertifizierung	16
9.1.1 Antrag	16
9.1.2 Antragsprüfung	16
9.1.3 Auditprogramm	16
9.1.4 Ermittlung des Auditzeitaufwandes	17
9.1.5 Stichprobenprüfung an mehreren Standorten	17
9.1.6 Mehrfach-Managementsysteme	19
9.2 Planung von Audits	19
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien	19
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung	19

9.2.3	Auditplan	20
9.3	Erstzertifizierung	20
9.3.1	IS 9.3.1 Erstzertifizierungsaudit	20
9.4	Durchführen von Audits.....	22
9.4.1	IS 9.4 Allgemeines	22
9.4.2	IS 9.4 Spezifische Elemente des ISMS-Audits.....	22
9.4.3	IS 9.4 Auditbericht	22
9.5	Zertifizierungsentscheidung.....	23
9.5.1	IS 9.5 Zertifizierungsentscheidung	23
9.6	Aufrechterhaltung der Zertifizierung	23
9.6.1	Allgemeines	23
9.6.2	Überwachungstätigkeiten	23
9.6.3	Re-Zertifizierung	24
9.6.4	Audits aus besonderem Anlass.....	25
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung	25
9.7	Einsprüche	25
9.8	Beschwerden.....	25
9.8.1	IS 9.8 Beschwerden.....	25
9.9	Aufzeichnungen zu Kunden	25
10	Managementsystemanforderungen für Zertifizierungsstellen.....	25
10.1	Optionen	25
10.1.1	IS 10.1 ISMS-Umsetzung.....	25
10.2	Option A: Allgemeine Managementsystemanforderungen	25
10.3	Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001	25
	Anhang A (informativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung	26
	Anhang B (normativ) Auditzeitaufwand.....	28
	Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands.....	34
	Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2013, Anhang A.....	40
	Literaturhinweise.....	51

Europäisches Vorwort

Der Text von ISO/IEC 27006:2015, inklusive Amd 1:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als EN ISO/IEC 27006:2020 übernommen, 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 Mai 2021, und etwaige entgegenstehende nationale Normen müssen bis Mai 2021 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.

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 27006:2015, einschließlich Amd 1:2020 wurde von CEN als EN ISO/IEC 27006:2020 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. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, 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-Direktiven, 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).

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

Eine Erläuterung zum freiwilligen Charakter 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, enthält der folgende Link: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques* erarbeitet.

ISO/IEC 27006 wurde vom Gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques* erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27006:2011), die technisch überarbeitet wurde.

Einleitung

ISO/IEC 17021-1 legt Kriterien für Stellen fest, die Audits und Zertifizierungen von Managementsystemen vornehmen. Falls solche Stellen mit dem Ziel des Audits und der Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS) in Übereinstimmung mit ISO/IEC 27001:2013 als mit ISO/IEC 17021-1 übereinstimmend akkreditiert werden sollen, sind einige zusätzliche Anforderungen und Anleitung in Bezug auf ISO/IEC 17021-1 erforderlich. Diese werden durch diese Internationale Norm zur Verfügung gestellt.

Der Text dieser Internationalen Norm folgt der Struktur von ISO/IEC 17021-1, und die zusätzlichen ISMS-spezifischen Anforderungen und die Anleitung in Bezug auf ISO/IEC 17021-1 für die ISMS-Zertifizierung werden durch die Buchstaben „IS“ gekennzeichnet.

Der Begriff „muss“ wird in dieser Internationalen Norm verwendet, um Bestimmungen zu kennzeichnen, die, die Anforderungen nach ISO/IEC 17021-1 und ISO/IEC 27001 widerspiegelnd, obligatorisch sind. Der Begriff „sollte“ dient der Kennzeichnung von Empfehlungen.

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

In dieser Internationalen Norm werden die Begriffe „Managementsystem“ und „System“ synonym verwendet. Die Definition eines Managementsystems ist in ISO 9000:2005 enthalten. Das Managementsystem, wie es in dieser Internationalen Norm verwendet wird, sollte nicht mit anderen Arten von Systemen, etwa IT-Systemen, verwechselt werden.

1 Anwendungsbereich

Diese Internationale Norm 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 und ISO/IEC 27001. Sie dient hauptsächlich der Unterstützung der Akkreditierung von Zertifizierungsstellen, die ISMS-Zertifizierungen durchführen.

Die Anforderungen in dieser Norm bedürfen im Hinblick auf Kompetenz und Zuverlässigkeit von jeder Stelle, die ISMS-Zertifizierungen durchführt, eines Nachweises, und die Anleitungen in dieser Internationalen Norm erlauben die weitere Interpretation dieser Anforderungen für jede Stelle, die ISMS-Zertifizierungen durchführt.

ANMERKUNG Diese Internationale Norm kann als Kriteriendokument für die Akkreditierung, die Bewertung unter Gleichrangigen oder für andere Auditprozesse verwendet werden.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Begriffe

Für die Zwecke dieses Dokuments gelten die Begriffe nach ISO/IEC 17021-1, ISO/IEC 27000 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

4 Grundsätze

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

5 Allgemeine Anforderungen

5.1 Rechts- und Vertragsfragen

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

5.2 Handhabung der Unparteilichkeit

Es gelten die Anforderungen nach ISO/IEC 17021-1, 5.2. Zudem gelten die folgenden Anforderungen und Anleitungen.

5.2.1 IS 5.2 Interessenskonflikte

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

- a) Organisation von Schulungen und die Teilnahme daran als Ausbilder, vorausgesetzt, dass sich die Zertifizierungsstellen in Fällen, in denen sich die Schulungen auf das Informations-sicherheitsmanagement, dazugehörige Managementsysteme oder Audits beziehen, auf die Bereitstellung von generischen, öffentlich zugänglichen Informationen und Ratschlägen beschränken müssen, d. h. sie dürfen keine unternehmensspezifische Ratschläge geben, die den Anforderungen des nachfolgenden Punktes b) zuwiderlaufen;
- b) Bereitstellung oder Veröffentlichung von Informationen auf Anfrage, die die Interpretation der Anforderungen von Zertifizierungsauditnormen durch die Zertifizierungsstelle darlegen (siehe 9.1.3.6);
- c) dem Audit vorangehende Tätigkeiten, deren ausschließliches Ziel die Bestimmung der Bereitschaft für ein Zertifizierungsaudit. Derartige Tätigkeiten dürfen allerdings nicht zu Empfehlungen oder Ratschlägen führen, die diesem Abschnitt zuwiderliegen, und die Zertifizierungsstelle muss in der Lage sein zu bestätigen, dass derartige Tätigkeiten diesen Anforderungen nicht zuwiderlaufen und dass sie nicht zur Begründung der Reduzierung der letztendliche Dauer des Zertifizierungsaudits genutzt werden;
- d) Durchführung von Zweit- und Drittparteienaudits nach Normen oder Regelungen, die nicht Teil des Akkreditierungsbereichs sind;
- e) Erbringung von Mehrwert während Zertifizierungsaudits und Überwachungsbesuchen, z. B. durch Bestimmung von Verbesserungsmöglichkeiten, die während des Audits bekannt werden, ohne spezifische Lösungen vorzuschlagen.

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, 5.3.

6 Strukturelle Anforderungen

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

7 Anforderungen an Ressourcen

7.1 Kompetenz des Personals

Es gelten die Anforderungen nach ISO/IEC 17021-1, 7.1. Zudem gelten die folgenden Anforderungen und Anleitungen.

7.1.1 IS 7.1.1 Allgemeine Betrachtungen

7.1.1.1 Allgemeine Kompetenzanforderungen

Die Zertifizierungsstelle muss sicherstellen, dass sie Kenntnisse zu den technologischen, gesetzlichen und behördlichen Entwicklungen hat, die das ISMS des Kunden betreffen, den sie bewertet.

Die Zertifizierungsstelle muss die Kompetenzanforderungen für jede Zertifizierungsfunktion definieren, wie in ISO/IEC 17021-1, Tabelle A.1, angegeben. Die Zertifizierungsstelle muss alle in ISO/IEC 17021-1 und 7.1.2 und 7.2.1 dieser Internationalen Norm angegebenen Anforderungen berücksichtigen, die entsprechend den Festlegungen der Zertifizierungsstelle für die technischen Bereiche des ISMS relevant sind.

ANMERKUNG Anhang A enthält eine Zusammenfassung der Kompetenzanforderungen an das Personal, das in bestimmte Zertifizierungsfunktionen einbezogen ist.

7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien

7.1.2.1 Kompetenzanforderungen für ISMS-Audits

7.1.2.1.1 Allgemeine Anforderungen

Die Zertifizierungsstelle muss über Kriterien zur Verifizierung des Erfahrungshintergrundes, der spezifischen Schulung oder der Unterweisung der Auditteammitglieder verfügen, so dass mindestens Folgendes sichergestellt ist:

- a) Kenntnis der Informationssicherheit;
- b) technisches Wissen in Bezug auf die Tätigkeit, die auditiert werden soll;
- c) Kenntnis der Managementsysteme;
- d) Kenntnis der Auditgrundsätze;

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

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

Die voranstehenden Anforderungen a) bis e) gelten für jeden Auditoren, der Teil des Auditteams ist, mit Ausnahme von b), die gemeinsam von allen Auditoren des Teams abgedeckt werden kann.

Das Auditteam muss über die Kompetenz verfügen, Anzeichen von Informationssicherheitsvorfällen im ISMS des Kunden zu den entsprechenden ISMS-Elementen zurückzuverfolgen.

Das Auditteam muss in Bezug auf die obigen Punkte und ihre praktische Anwendung über eine angemessene Arbeitserfahrung verfügen (dies bedeutet nicht, dass ein Auditor über eine umfassende Erfahrung in allen Bereichen der Informationssicherheit verfügen muss, aber dass das Auditteam insgesamt genügend Verständnis und Erfahrung aufweisen muss, um den zu auditierenden ISMS-Anwendungsbereich abzudecken).

7.1.2.1.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

Zusammen müssen alle Mitglieder des Auditteams über folgendes Wissen verfügen:

- a) ISMS-spezifische Dokumentationsstrukturen, Hierarchie und Wechselbeziehungen;
- b) Werkzeuge, Methoden, Techniken des Informationssicherheitsmanagements und deren Anwendung;
- c) Informationssicherheitsrisikobewertung und -risikomanagement;
- d) auf ISMS anwendbare Prozesse;
- e) aktuelle Technologie, bei der die Informationssicherheit relevant oder ein Problem sein kann.

Jeder Auditor muss die Punkte a), c) und d) erfüllen.

7.1.2.1.3 Informationssicherheitsmanagementsystemnormen und normative Dokumente

An ISMS-Audits beteiligte Auditoren müssen über folgendes Wissen verfügen:

- a) alle Anforderungen in ISO/IEC 27001.

Zusammen müssen alle Mitglieder des Auditteams über folgendes Wissen verfügen:

- b) alle Maßnahmen in ISO/IEC 27002 (falls als erforderlich bestimmt auch aus branchenspezifischen Normen) und ihre Umsetzung, kategorisiert als:
 - 1) Informationssicherheitsrichtlinien;
 - 2) Organisation der Informationssicherheit;
 - 3) Personalsicherheit;
 - 4) Verwaltung der Werte;
 - 5) Zugangssteuerung, einschließlich Befugnis;
 - 6) Kryptographie;
 - 7) Physische und umgebungsbezogene Sicherheit;
 - 8) Betriebssicherheit, einschließlich IT-Dienstleistungen;
 - 9) Kommunikationssicherheit, einschließlich Netzwerksicherheitsmanagement und Informationsübertragung;
 - 10) Anschaffung, Entwicklung und Instandhaltung von Systemen;
 - 11) Lieferantenbeziehungen, einschließlich ausgegliederte Dienstleistungen;
 - 12) Handhabung von Informationssicherheitsvorfällen;
 - 13) Informationssicherheitsaspekte beim Business Continuity Management, einschließlich Redundanzen;
 - 14) Compliance, einschließlich Informationssicherheitsprüfungen.

7.1.2.1.4 Praktische Unternehmensführung

An ISMS-Audits beteiligte Auditoren müssen über folgendes Wissen verfügen:

- a) gute Branchenverhaltensweisen in Bezug auf Informationssicherheit und Informationssicherheitsverfahren;
- b) Politiken, Richtlinien und betriebliche Anforderungen für 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 Personalmanagement, interne und externe Kommunikation sowie andere relevante Unterstützungsprozesse.

7.1.2.1.5 Geschäftsfeld des Kunden

An ISMS-Audits beteiligte Auditoren müssen über folgendes Wissen verfügen:

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

ANMERKUNG Die Kenntnis gesetzlicher und behördlicher Anforderungen impliziert kein umfassendes rechtliches Hintergrundwissen.

- b) mit dem Geschäftsfeld zusammenhängende Informationssicherheitsrisiken;
- c) generische Terminologie, Prozesse und Technologien, die mit dem Geschäftsfeld des Kunden zusammenhängen;
- d) relevante Geschäftsfeldpraktiken.

Kriterium a) darf im Auditteam verteilt sein.

7.1.2.1.6 Produkte, Prozesse und Organisation des Kunden

Zusammen müssen an ISMS-Audits beteiligte Auditoren 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 breiten Perspektive;
- c) auf die Produkte oder Dienstleistungen anzuwendende gesetzliche und behördliche Anforderungen.

7.1.2.2 Anforderungen an die Kompetenz für das Leiten des Auditteams

Neben den Anforderungen in 7.1.2.1 müssen die Leiter der Auditteams die folgenden Anforderungen erfüllen, die in Audits unter Anleitung und Aufsicht nachgewiesen werden müssen:

- a) Wissen und Fertigkeiten zur Lenkung des Zertifizierungsauditprozesses und der Leitung des Auditteams;
- b) Nachweis der Fähigkeit zu effektiver mündlicher und schriftlicher Kommunikation.

7.1.2.3 Anforderungen an die Kompetenz für die Durchführung der Antragsprüfung

7.1.2.3.1 Informationssicherheitsmanagementsystemnormen und normative Dokumente

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 folgendes Wissen verfügen:

- a) relevante ISMS-Normen und normative Dokumente, die im Rahmen des Zertifizierungsprozesses angewandt werden.

7.1.2.3.2 Geschäftsfeld des Kunden

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 folgendes Wissen verfügen:

- a) generische Terminologie, Prozesse, Technologien und Risiken, die mit dem Geschäftsfeld des Kunden zusammenhängen.

7.1.2.3.3 Produkte, Prozesse und Organisation des Kunden

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 folgendes Wissen verfügen:

- a) Kundenprodukte, Prozesse, Art der Organisation, Größe, Führung, Struktur, Funktionen und Beziehungen einer Organisation zur Entwicklung und Implementierung des ISMS und der Zertifizierungstätigkeiten, einschließlich Ausgliederungsfunktionen.

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

7.1.2.4.1 Allgemeines

Das Personal, das Auditberichte bewertet und Zertifizierungsentscheidungen trifft muss über Wissen verfügen, das es ihm ermöglicht, die Angemessenheit des Geltungsbereiches der Zertifizierung sowie Änderungen des Geltungsbereiches und ihre Auswirkungen auf die Effektivität 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;
- c) Auditgrundsätze, -praktiken und -verfahren.

7.1.2.4.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

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

- a) die in 7.1.2.1.2 a), c) und d) aufgelisteten Punkte;
- b) für die Informationssicherheit relevante gesetzliche und behördliche Anforderungen.

7.1.2.4.3 Informationssicherheitsmanagementsystemnormen und normative Dokumente

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

- a) relevante ISMS-Normen und weitere normative Dokumente, die im Rahmen des Zertifizierungsprozesses angewandt werden.

7.1.2.4.4 Geschäftsfeld des Kunden

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

- a) generische Terminologie und Risiken, die mit den relevanten Geschäftsfeldpraktiken zusammenhängen.

7.1.2.4.5 Produkte, Prozesse und Organisation des Kunden

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

- a) Kundenprodukte, Prozesse, Art der Organisation, Größe, Führung, Struktur, Funktionen und Beziehungen.

7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist

Es gelten die Anforderungen nach ISO/IEC 17021-1, 7.2. Zudem gelten die folgenden Anforderungen und Anleitungen.

7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren

Die Zertifizierungsstelle muss durch Folgendes nachweisen, dass die Auditoren über Wissen und Erfahrung verfügen:

- a) anerkannte ISMS-spezifische Qualifikationen;
- b) Registrierung als Auditor soweit anwendbar;
- c) Teilnahme an ISMS-Schulungen und Erlangung relevanter persönlicher Nachweise;
- d) aktuelle Aufzeichnungen der beruflichen Entwicklung;
- e) ISMS-Audits, die ein anderer ISMS-Auditor überwacht hat.

7.2.1.1 Auswahl von Auditoren

Neben 7.1.2.1 müssen die Kriterien zur Auswahl von Auditoren sicherstellen, dass jeder Auditor:

- a) über eine berufliche Ausbildung oder Schulung auf einem mit einer universitären Ausbildung vergleichbaren Niveau verfügt;
- b) eine mindestens vierjährige praktische Vollzeitberufserfahrung im Bereich der Informationstechnologie vorweisen kann, bei der er mindestens zwei Jahre lang eine Rolle oder Funktion mit Bezug zu Informationssicherheit innehatte;
- c) mindestens eine fünftägige Schulung erfolgreich absolviert hat, die ISMS-Audits und das Auditmanagement umfasst;
- d) Erfahrung zum Auditieren eines ISMS vor der Tätigkeit als Auditor zur Durchführung von ISMS-Audits gesammelt hat. Diese Erfahrung muss als Auditor-in-Ausbildung unter Überwachung durch einen ISMS-Evaluator (siehe ISO/IEC 17021-1:2015, 9.2.2.1.4) im Rahmen der Teilnahme an mindestens einem ISMS-Erstzertifizierungs- (Stufe 1 und Stufe 2) oder Re-Zertifizierungsaudit und mindestens einem Überwachungsaudit gesammelt worden sein. Diese Erfahrung muss in mindestens 10 ISMS-Vorort-Audittagen und innerhalb der letzten 5 Jahre erlangt worden sein. Die Teilnahme muss Prüfungen der Dokumentation und Risikobeurteilungen, Umsetzungsbewertungen und Auditberichterstattung umfassen;
- e) über relevante und aktuelle Erfahrung verfügt;
- f) durch ständige berufliche Entwicklung aktuelles Wissen und Fertigkeiten mit Bezug zu auf Informationssicherheit und Audits pflegt;
- g) über Kompetenz im Auditieren eines ISMS nach ISO/IEC 27001 verfügt.

Fachexperten müssen die Kriterien a), b) und e) erfüllen.

7.2.1.2 Auswahl von Auditoren für die Teamleitung

Neben 7.1.2.2 und 7.2.1.1 müssen die Kriterien zur Auswahl eines Auditors für die Teamleitung sicherstellen, dass dieser Auditor:

- a) aktiv an allen Stufen von mindestens drei ISMS-Audits teilgenommen hat. Die Teilnahme muss die anfängliche Festlegung des Umfangs und Planung, Prüfungen der Dokumentation und Risikobeurteilungen, Umsetzungsbewertungen und formale Auditberichterstattung umfassen.

7.3 Einsatz einzelner externer Auditoren und externer Fachexperten

Es gelten die Anforderungen nach ISO/IEC 17021-1, 7.3. Zudem gelten die folgenden Anforderungen und Anleitungen.

7.3.1 IS 7.3 Einsatz einzelner externer Auditoren und externer Fachexperten als Teil des Auditteams

Fachexperten müssen unter der Aufsicht eines Auditors arbeiten. Die Mindestanforderungen an Fachexperten werden in 7.2.1.1 aufgelistet.

7.4 Aufzeichnungen über Personal

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