# DIN EN ISO/IEC 27006

DIN

ICS 35.030 Einsprüche bis 2020-09-24

*Entwurf*

# Informationstechnik – IT-Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd.1:2020); Deutsche und Englische Fassung prEN 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 and English version prEN 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 et anglaise prEN ISO/IEC 27006:2020

## Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-07-24 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

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

Gesamtumfang 99 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

## 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 prEN ISO/IEC 27006:2020 übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche/nationale Normungsgremium ist der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ 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 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.



AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

# 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*

AVA Documents
Document Sharing Hub



Full document details: E DIN EN ISO/IEC 27006:2020-08

— Leerseite —



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

# *– Entwurf –*

*2020-03*

***prEN ISO/IEC 27006:2020***

| | |
|---|---|
| *Titel de:* | Informationstechnik — IT-Sicherheitsverfahren — Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd. 1:2020) |
| *Titel en:* | Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems (ISO/IEC 27006:2015, including Amd. 1:2020) |
| *Titel fr:* | 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) |

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

# 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**



Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

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 ... 41

Literaturhinweise ... 52



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

# Europäisches 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 prEN ISO/IEC 27006:2020 übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

**Anerkennungsnotiz**

Der Text von ISO/IEC 27006:2015, einschließlich Amd.1:2020 wurde von CEN als prEN ISO/IEC 27006:2020 ohne irgendeine Abänderung genehmigt.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

# 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) hinsichtlich technischer Handelshemmnisse (TBT) 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.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

# 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.



Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

# 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 Akkreditiertung, 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 sowie die folgenden.

**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, 4.

# 5 Allgemeine Anforderungen

## 5.1 Rechts- und Vertragsfragen

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



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

## 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, 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 zuwiderliefen, und die Zertifizierungsstelle muss 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 Drittpartieienaudits nach Normen oder Regelungen, die nicht Teil des Akkreditierungsgeltungsbereichs 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, 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.



AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

### 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 aufweist, um den zu auditierenden ISMS-Anwendungsbereich abzudecken).

##### 7.1.2.1.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

Zusammen müssen alle Mitglieder über folgendes Wissen verfügen:

a) ISMS-spezifische Dokumentationsstrukturen, Hierarchie und Wechselbeziehungen;

b) Werkzeuge, Methoden, Techniken des Informationssicherheitsmanagements und deren Anwendung;



AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

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 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;



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

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 jeweiligenRechtssystem/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 Geschäftsfeldspraktiken.

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 Fertigkeitenzur Lenkung des Zertifizierungsauditprozesses und der Leitung des Auditteams;

b) Nachweis der Fähigkeit zu effektiver mündlicher und schriftlicher Kommunikation.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

#### 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.



AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

#### 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 Geschäftsfeldspraktiken 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.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

#### 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 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 Fertigkeitenmit Bezug zu auf Informationssicherheit und Audits pflegt;

g) über Kompetenz im Auditieren eines ISMS gemäß 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.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

### 7.5 Ausgliederung

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

## 8 Anforderungen an Informationen

### 8.1 Öffentliche Informationen

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

### 8.2 Zertifizierungsdokumente

Es gelten die Anforderungen nach ISO/IEC 17021-1, 8.2. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 8.2.1 IS 8.2 ISMS-Zertifizierungsdokumente

Zertifizierungsdokumente müssen von einem Bevollmächtigten unterschrieben werden, dem die entsprechende Befugnis zugewiesen wurde. Die Version der Erklärung zur Anwendbarkeit muss in die Zertifizierungsdokumente aufgenommen werden.

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

Die Zertifizierungsdokumente dürfen nationale und internationale Normen als Quelle(n) für Sätze an Maßnahme für Maßnahmen referenzieren, die in der Erklärung zur Anwendbarkeit der Organisation gemäß ISO/IEC 27001:2013, 6.1.3 d) als notwendig ermittelt werden. Die Referenz auf den Zertifizierungsdokumenten muss klar darstellen, dass diese nur als Quelle für Maßnahmensätze für Maßnahmen dienen, die in der Erklärung zur Anwendbarkeit referenziert werden, und nicht als Zertifizierung gemäß dieser Referenzen.

### 8.3 Verweis auf Zertifizierung und Zeichennutzung

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

### 8.4 Vertraulichkeit

Es gelten die Anforderungen nach ISO/IEC 17021-1, 8.4. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation

Vor dem Zertifizierungsaudit muss die Zertifizierungsstelle den Kunden darum bitten, anzugeben, ob Informationen in Bezug auf das ISMS (etwa ISMS-Aufzeichnungen oder Informationen zur Gestaltung und Effektivität 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 ISMS beim Fehlen derartiger Informationen angemessen auditiert werden kann. Falls die Zertifizierungsstelle zu dem Ergebnis kommt, dass es nicht möglich ist, das ISMS adäquat zu auditieren, ohne die identifizierten vertraulichen oder sensiblen Informationen zu bewerten, 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, 8.5.

AVA Documents
Document Sharing Hub



Full document details: E DIN EN ISO/IEC 27006:2020-08

# 9 Anforderungen an Prozesse

## 9.1 Tätigkeiten vor der Zertifizierung

### 9.1.1 Antrag

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.1.1. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.1.1.1 IS 9.1.1 Bereitschaft zum Antrag

Die Zertifizierungsstelle muss fordern, dass der Kunde über ein dokumentiertes und implementiertes ISMS verfügt, das ISO/IEC 27001 und andere für die Zertifizierung erforderliche Dokumente erfüllt.

### 9.1.2 Antragsprüfung

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

### 9.1.3 Auditprogramm

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.1.3. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.1.3.1 IS 9.1.3 Allgemeines

Das Auditprogramm für ISMS-Audits muss die festgelegten Informationssicherheitsmaßnahmen berücksichtigen.

#### 9.1.3.2 IS 9.1.3 Auditmethodologie

Die Verfahren der Zertifizierungsstelle dürfen keine besondere Art der Umsetzung eines ISMS oder ein besonderes Format für Dokumentation und Aufzeichnungen voraussetzen. Zertifizierungsverfahren müssen ihren Schwerpunkt auf den Nachweis legen, dass das ISMS des Kunden die Anforderungen nach ISO/IEC 27001 sowie die Politik, Richtlinien und Ziele des Kunden erfüllt.

ANMERKUNG ISO/IEC 27007 enthält weitere Anleitung zu Audits.

#### 9.1.3.3 IS 9.1.3 Allgemeine Vorbereitungen für das erste Audit

Die Zertifizierungsstelle muss fordern, dass ein Kunde alle erforderlichen Maßnahmen für den Zugriff auf interne Auditberichte und Berichte unabhängiger Prüfungen der Informationssicherheit ergreift.

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

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

b) eine Kopie der erforderlichen, in ISO/IEC 27001 festgelegten ISMS-Dokumentation und, ggf., zugehörige Dokumentation.

#### 9.1.3.4 IS 9.1.3 Bewertungszeiträume

Die Zertifizierungsstelle darf kein ISMS zertifizieren, sofern bei diesem nicht mindestens eine Managementbewertung und ein internes ISMS-Audit durchgeführt wurde, die den Geltungsbereich der Zertifizierung abdecken.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

#### 9.1.3.5 IS 9.1.3 Geltungsbereich der Zertifizierung

Das Auditteam muss das vom definierten Geltungsbereich abgedeckte ISMS des Kunden gegenüber allen anwendbaren Zertifizierungsanforderungen auditieren. Die Zertifizierungsstelle muss bestätigen, dass der Kunde im Rahmen seines ISMS die in ISO/IEC 27001, 4.3, festgelegten Anforderungen behandelt.

Zertifizierungsstellen müssen sicherstellen, dass die Informationssicherheitsrisikobeurteilung und -risikobehandlung des Kunden seine Tätigkeiten angemessen widerspiegelt und sich bis auf die Grenzen der Tätigkeiten, wie sie im Geltungsbereich der Zertifizierung definiert wurden, erstreckt. Zertifizierungsstellen müssen bestätigen, dass dies im ISMS-Anwendungsbereich des Kunden und der Erklärung zur Anwendbarkeit widergespiegelt wird. Die Zertifizierungsstelle muss verifizieren, dass es pro Geltungsbereich der Zertifizierung mindestens eine Erklärung zur Anwendbarkeit gibt.

Zertifizierungsstellen müssen sicherstellen, dass Schnittstellen zu Diensten oder Tätigkeiten, die nicht vollständig innerhalb des ISMS-Anwendungsbereiches liegen, im ISMS, das der Zertifizierung unterzogen wird, behandelt werden und in die Informationssicherheitsrisikobeurteilung des Kunden aufgenommen wurden. Ein Beispiel für eine solche Situation ist das gemeinsame Nutzen von Anlagen (z. B. IT-Systeme, Datenbanken und Telekommunikationssysteme oder die Ausgliederung einer Geschäftsfunktion) mit einer anderen Organisation.

#### 9.1.3.6 IS 9.1.3 Zertifizierungsauditkriterien

Die Kriterien, nach denen das ISMS eines Kunden auditiert wird, muss die ISMS-Norm ISO/IEC 27001 sein.. Andere Dokumente, die relevant für die durchgeführten Funktionen sind, dürfen zur Zertifizierung herangezogen werden.

### 9.1.4 Ermittlung des Auditzeitaufwandes

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.1.4. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.1.4.1 IS 9.1.4 Auditzeitaufwand

Zertifizierungsstellen müssen Auditoren genügend Zeit geben, um alle Tätigkeitenin Bezug auf ein Erstaudit, ein Überwachungsaudit oder ein Re-Zertifizierungsaudit auszuführen. Die Berechnung des Gesamtaudit-zeitaufwands muss genügend Zeit für die Auditberichterstattung enthalten.

Die Zertifizierungsstelle muss Anhang B zur Bestimmung der Auditzeitaufwand verwenden.

ANMERKUNG Anhang C enthält weitere Anleitung und Beispiele zur Berechnung des Auditzeitaufwands.

### 9.1.5 Stichprobenprüfung an mehreren Standorten

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.1.5. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.1.5.1 IS 9.1.5 Mehrere Standorte

**9.1.5.1.1** Falls ein Kunde über eine Reihe von Standorten verfügt, die die nachfolgenden Kriterien von a) bis c) erfüllen, können Zertifizierungsstellen einen stichprobenbasierten Ansatz für das Zertifizierungsaudit mehrerer Standorte erwägen:

a) alle Standorte werden unter demselben ISMS betrieben, das zentral verwaltet und auditiert wird und einer zentralen Managementbewertung unterliegt;

b) alle Standorte werden vom internen ISMS-Auditprogramm des Kunden abgedeckt;



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

c) alle Standorte werden vom ISMS-ManagementbewertungManagementbewertungsprogramm des Kunden abgedeckt.

**9.1.5.1.2** Die Zertifizierungsstelle, die einem stichprobenbasierten Ansatz folgen möchte, muss über Verfahren verfügen, um Folgendes sicherzustellen:

a) Die erstmalige Vertragsprüfung bestimmt im größtmöglichen Maße die Unterschiede zwischen den Standorten, so dass ein angemessenes Niveau der Stichprobenahme bestimmt wird.

b) Eine repräsentative Anzahl von Standorten wurde seitens der Zertifizierungsstelle einer Stichprobenahme unterzogen, wobei Folgendes berücksichtigt wurde:

   1) die Ergebnisse der internen Audits des Stammsitzes und der Standorte;

   2) die Ergebnisse der Managementbewertung;

   3) Variationen der Größe der Standorte;

   4) Variationen des Geschäftszweckes der Standorte;

   5) Komplexität der Informationssysteme an den verschiedenen Standorten;

   6) Variationen der Arbeitsmethoden;

   7) Variationen der durchgeführten Tätigkeiten;

   8) Variationen der Gestaltung und der Durchführung von Maßnahmen;

   9) potenzielle Interaktion mit kritischen Informationssystemen oder Informationen, die sensible Informationen verarbeiten;

   10) jegliche unterschiedliche rechtlichen Anforderungen;

   11) geographische und kulturelle Aspekte;

   12) Risikosituationen der Standorte;

   13) Informationssicherheitsvorfälle an den jeweiligen Standorten.

c) Von allen vom Geltungsbereich des ISMS des Kunden abgedeckten Standorten wird eine repräsentative Stichprobe ausgewählt; diese Zusammenstellung muss auf einer wertenden Auswahl basieren, um sowohl die im obigen Punkt b) dargestellten Faktoren als auch ein zufälliges Element widerzuspiegeln.

d) Jeder vom ISMS abgedeckte Standort, der erheblichen Risiken ausgesetzt ist, wird vor der Zertifizierung von der Zertifizierungsstelle auditiert.

e) Das Auditprogramm wurde unter Berücksichtigung der obigen Anforderungen ausgelegt und deckt repräsentative Stichproben aus dem Geltungsbereich der ISMS-Zertifizierung innerhalb des Zeitraums von drei Jahren ab.

f) Bei einer entweder am Stammsitz oder an einem einzelnen Standort beobachteten Nichtkonformität betrifft das Verfahren für Korrekturmaßnahmen den Stammsitz und alle vom Zertifikat abgedeckten Standorte.

Das Audit muss die Tätigkeitenam Stammsitz des Kunden behandeln, um sicherzustellen, dass ein einzelnes ISMS alle Standorte abdeckt und auf betrieblicher Ebene ein zentrales Management bietet. Das Audit muss alle oben skizzierten Punkte behandeln.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

### 9.1.6 Mehrfach-Managementsysteme

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.1.6. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.1.6.1 IS 9.1.6 Integration der ISMS-Dokumentation in die Dokumentation für andere Managementsysteme

Die Zertifizierungsstelle darf eine kombinierte Dokumentation akzeptieren (z. B. für Informationssicherheit, Qualität, Gesundheit, Sicherheit und Umwelt), solange das ISMS zusammen mit den angemessenen Schnittstellen zu anderen Systemen eindeutig identifiziert werden kann.

#### 9.1.6.2 IS 9.1.6 Kombination von Managementsystemaudits

Das ISMS-Audit darf mit Audits anderer Managementsysteme kombiniert werden, vorausgesetzt, dass nachgewiesen werden kann, dass das Audit alle Anforderungen an die Zertifizierung des ISMS erfüllt. Alle für ein ISMS wichtigen Elemente müssen eindeutig und problemlos identifizierbar in den Auditberichten erscheinen. Die Qualität des Audits darf von der Kombination der Audits nicht beeinträchtigt werden.

## 9.2 Planung von Audits

### 9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.2.1. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.2.1.1 IS 9.2.1 Auditziele

Die Auditziele müssen die Bestimmung der Wirksamkeit des Managementsystems umfassen, um sicherzustellen, dass der Kunde auf der Grundlage der Risikobeurteilung anwendbare Maßnahmen implementiert und die festgelegten Informationssicherheitsziele erreicht hat.

### 9.2.2 Auswahl des Auditteams und Aufgabenzuordnung

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.2.2. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.2.2.1 IS 9.2.2 Auditteam

Das Auditteam muss formell benannt und mit den angemessenen Arbeitsdokumenten ausgestattet werden. Das dem Auditteam erteilte Mandat muss eindeutig definiert und dem Kunden mitgeteilt werden.

Ein Auditteam kann aus einer Einzelperson bestehen, sofern diese alle in 7.1.2.1 festgelegten Kriterien erfüllt.

#### 9.2.2.2 IS 9.2.2 Kompetenz des Auditteams

Es gelten die in 7.1.2 aufgelisteten Anforderungen. Für Überwachungsaudittätigkeiten und Tätigkeiten bei Audits aus besonderem Anlass gelten nur die Anforderungen, die für die geplante Überwachungsaudittätigkeiten und Tätigkeiten bei Audits aus besonderem Anlass relevant sind.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08

Bei der Auswahl und Leitung des Auditteams, das für ein spezifisches Zertifizierungsaudit benannt werden soll, muss die Zertifizierungsstelle sicherstellen, dass die in jede Aufgabe eingebrachten Kompetenzen angemessen sind. Das Team muss:

a) über ein angemessenes technisches Wissen über die spezifischen Tätigkeiteninnerhalb des ISMS-Anwendungsbereiches, das zertifiziert werden soll, und, falls relevant., über zugehörige Verfahren und ihre möglichen Informationssicherheitsrisiken verfügen (Fachexperten dürfen diese Funktion erfüllen);

b) ausreichendes Verständnisüber den Kunden haben, um ein zuverlässiges Zertifizierungsaudit seines ISMS in Anbetracht des Anwendungsbereiches und des Kontextes des ISMS innerhalb der Organisation bei der Handhabung von Informationssicherheitsaspekten der Tätigkeiten, Produkte und Dienstleistungen durchzuführen;

c) über ein angemessenes Verständnis über die rechtlichen und behördlichen Anforderungen verfügen, die für das ISMS des Kunden gelten.

ANMERKUNG Angemessenes Verständnis impliziert kein umfassendes rechtliches Hintergrundwissen.

#### 9.2.3 Auditplan

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.2.3. Zudem gelten die folgenden Anforderungen und Anleitungen.

##### 9.2.3.1 IS 9.2.3 Allgemeines

Der Auditplan für ISMS-Audits muss die festgelegten Informationssicherheitsmaßnahmen berücksichtigen.

##### 9.2.3.2 IS 9.2.3 Netzwerkgestützte Auditverfahren

Der Auditplan muss die netzwerkgestützten Auditverfahren bestimmen, die, sofern geeignet, im Rahmen des Audits angewandt werden.

Netzwerkgestützte Auditverfahren können beispielsweise Telefonkonferenzen, Webmeetings, interaktive webbasierte Kommunikation und elektronischen Fernzugriff auf die ISMS-Dokumentationen oder -Verfahren umfassen. Der Schwerpunkt derartiger Prozesse sollte auf der Verbesserung der Auditeffektivität und -effizienz liegen und sollte die Integrität des Auditprozesses unterstützen.

##### 9.2.3.3 IS 9.2.3 Zeitplanung des Audits

Eine Zertifizierungsstelle sollte die Zeitplanung des Audits, die den vollen Geltungsbereich einer Organisation am besten darstellt, mit der zu auditierenden Organisation vereinbaren. Die Betrachtung sollte sofern geeignet Jahreszeit, Monat, Tag/Daten und Schichten umfassen.

### 9.3 Erstzertifizierung

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.3. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.3.1 IS 9.3.1 Erstzertifizierungsaudit

##### 9.3.1.1 IS 9.3.1.1 Stufe 1

In dieser Stufe des Audits muss die Zertifizierungsstelle die Dokumentation zur Gestaltung des ISMS beschaffen, die die nach ISO/IEC 27001 erforderliche Dokumentation abdeckt.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

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

Die Ergebnisse von Stufe 1 müssen in einem schriftlichen Bericht aufgezeichnet werden. Die Zertifizierungsstelle muss den Auditbericht der Stufe 1 vor der Entscheidung, mit Stufe 2 fortzufahren, prüfen und bestätigen, ob die Auditteammitglieder für Stufe 2 über die notwendigen Kompetenzen verfügen; dies darf durch den Auditor, der das Audit der Stufe 1 leitete, erfolgen, falls dieser als kompetent und geeignet betrachtet wird.

ANMERKUNG Unabhängige Prüfung (d. h. von einer Person in der Zertifizierungsstelle, die nicht am Audit beteiligt ist) ist eine Maßnahme, um die Risiken bei der Entscheidung ob und mit wem in Stufe 2 fortgesesetzt wird, zu reduzieren. Es können allerdings bereits andere Risikominimierungsmaßnahmen vorhanden sein, die das gleiche Ziel erreichen.

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

### 9.3.1.2 IS 9.3.1.2 Stufe 2

**9.3.1.2.1** Die Zertifizierungsstelle entwickelt auf Grundlage der im Auditbericht für Stufe 1 dokumentierten Ergebnisse einen Auditplan für die Durchführung von Stufe 2. Neben der Beurteilung der wirksamen Umsetzung des ISMS bestehen die Ziele von Stufe 2 in Folgendem:

a) in der Bestätigung, dass das Kunde seine eigene Politik sowie Richtlinien, Ziele und Verfahren einhält.

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

a) Führung durch die oberste Leitung und Verpflichtung zur Informationssicherheitspolitik und zu den Informationssicherheitszielen;

b) die in ISO/IEC 27001 aufgelisteten Dokumentationsanforderungen;

c) Bewertungder mit der Informationssicherheit zusammenhängenden Risiken und dass die Bewertungenbei Wiederholung konsistente, gültige und vergleichbare Ergebnisse erbringen;

d) Bestimmung der Maßnahmenziele und Maßnahmen basierend auf der Informationssicherheitsrisikobeurteilung und des Risikobehandlungsprozesses;

e) Informationssicherheitsleistung und die Wirksamkeit des ISMS, beurteilt gegenüber Informationssicherheitszielen;

f) Korrespondenz zwischen festgelegten Maßnahmen, der Erklärung zur Anwendbarkeit und den Ergebnissen der Informationssicherheitsrisikobeurteilung und des Risikobehandlungsprozesses sowie der Informationssicherheitspolitik und -ziele;

g) Umsetzung der Maßnahmen (siehe Anhang D) unter Berücksichtigung des externen und internen Kontextes und zugehöriger Risiken sowie der Überwachung, Messung und Analyse der Informationssicherheitsverfahren und -Maßnahmen der Organisation zur Bestimmung, ob Maßnahmen umgesetzt wurden und wirksam sind und ihre angegebenen Informationssicherheitsziele erfüllen;

h) Programme, Prozesse, Verfahren, Aufzeichnungen, interne Audits und Bewertung der ISMS-Wirksamkeit um sicherzustellen, dass diese auf Entscheidungen der obersten Leitung sowie die Informationssicherheitspolitik und -ziele zurückzuführen sind.

AVA Documents
Document Sharing Hub



Full document details: E DIN EN ISO/IEC 27006:2020-08

## 9.4 Durchführen von Audits

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.4. Zudem gelten die folgenden Anforderungen und Anleitungen.

### 9.4.1 IS 9.4 Allgemeines

Die Zertifizierungsstelle muss über dokumentierte Verfahren für Folgendes verfügen:

a) das Erstzertifizierungsaudit des ISMS eines Kunden, in Übereinstimmung mit den Vorgaben nach ISO/IEC 17021-1;

b) regelmäßige Überwachungs- und Re-Zertifizierungsaudits des ISMS eines Kunden in Übereinstimmung mit ISO/IEC 17021-1 für fortdauernde Einhaltung der relevanten Anforderungen und zur Überprüfung und Aufzeichnung, dass ein Kunde rechtzeitig Korrekturmaßnahmen zur Behebung aller Nichtkonformitäten ergreift.

### 9.4.2 IS 9.4 Spezifische Elemente des ISMS-Audits

Die vom Auditteam repräsentierte Zertifizierungsstelle muss:

a) vom Kunden den Nachweis fordern, dass die Bewertung der mit der Informationssicherheit zusammenhängenden Risiken für den vom Anwendungsbereich des ISMS abgedeckten ISMS-Betrieb relevant und angemessen ist;

b) festlegen, ob die Verfahren des Kunden zur Bestimmung, Untersuchung und Bewertung der mit der Informationssicherheit zusammenhängenden Risiken und die Ergebnisse der Umsetzung mit der Politik und den Zielen des Kunden in Einklang stehen.

Die Zertifizierungsstelle muss auch feststellen, ob die im Rahmen der Risikobeurteilung eingesetzten Verfahren gründlich und angemessen umgesetzt wurden.

### 9.4.3 IS 9.4 Auditbericht

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

a) eine Darstellung des Audits, einschließlich einer Zusammenfassung der Dokumentenprüfung;

b) eine Darstellung des Zertifizierungsaudits der Informationssicherheitsrisikoanalyse des Kunden;

c) Abweichungen vom Auditplan (z. B. höherer oder geringerer Zeitaufwand bei bestimmten geplanten Tätigkeiten);

d) der ISMS-Anwendungsbereich.

**9.4.3.2** Der Auditbericht muss eine ausreichende Detailtiefe aufweisen, um die Zertifizierungsentscheidung zu erleichtern und zu unterstützen. Er muss Folgendes enthalten:

a) wesentliche verfolgte Auditpfade und angewandte Auditmethoden (siehe 9.1.3.2);

b) Beobachtungen, sowohl positiv (z. B. nennenswerte Merkmale) als auch negativ (z. B. potenzielle Nichtkonformitäten);

c) Kommentare zur Einhaltung der Zertifizierungsanforderungen seitens des ISMS des Kunden mit einer eindeutigen Aussage zur Nichtkonformität, einem Verweis auf die Erklärung zur Anwendbarkeit und, sofern zutreffend, jeder nützliche Vergleich mit den Ergebnissen vorangegangener Zertifizierungsaudits des Kunden.



AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

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

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

Zusätzlich zu den Anforderungen in ISO/IEC 17021-1, 9.4.8, an die Berichterstattung muss der Auditbericht die folgenden Informationen enthalten:

— eine Zusammenfassung der wichtigsten Beobachtungen, sowohl positiver als auch negativer Art, in Bezug auf die Umsetzung und Wirksamkeit der ISMS-Anforderungen und IS-Maßnahmen;

— die Empfehlungen des Auditteams im Hinblick darauf, ob das ISMS des Kunden zertifiziert werden sollte, einschließlich Informationen zur Begründung dieser Empfehlung.

## 9.5 Zertifizierungsentscheidung

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.5. Zudem gelten die folgenden Anforderungen und Anleitungen.

### 9.5.1 IS 9.5 Zertifizierungsentscheidung

Die Zertifizierungsentscheidung muss auf der im Zertifizierungsauditbericht angegebenen Zertifizierungsempfehlung des Auditteams (siehe 9.4.3) sowie auf den Anforderungen in ISO/IEC 17021-1 basieren.

Die Personen oder Komitees, die die Entscheidung zur Erteilung einer Zertifizierung treffen, sollten üblicherweise eine negative Entscheidung des Auditteams nicht umkehren. Falls eine derartige Situation zustande kommt, muss die Zertifizierungsstelle die Grundlage der Entscheidung zur Umkehrung der Empfehlung dokumentieren und begründen.

Die Zertifizierung darf dem Kunden nicht erteilt werden, bis es ausreichende Nachweise gibt, die darlegen, dass Vorkehrungen für Managementbewertungen und interne ISMS-Audits umgesetzt und wirksam sind sowie aufrechterhalten werden.

## 9.6 Aufrechterhaltung der Zertifizierung

### 9.6.1 Allgemeines

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

### 9.6.2 Überwachungstätigkeiten

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.6.2. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.6.2.1 IS 9.6.2 Überwachungstätigkeiten

**9.6.2.1.1** Überwachungsauditverfahren müssen mit den Verfahren in Bezug auf das Zertifizierungsaudit des ISMS des Kunden, wie in dieser Internationalen Norm dargelegt, übereinstimmen.

Zweck der Überwachung ist die Überprüfung, dass das freigegebene ISMS weiterhin umgesetzt wird, die Betrachtung der Auswirkungen von Änderungen dieses Systems, die aufgrund von Änderungen der



AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

Organisation des Kunden vorgenommen wurden, und die Bestätigung der weiteren Einhaltung der Zertifizierungsanforderungen. Überwachungsauditprogramme müssen mindestens Folgendes abdecken:

a) Elemente der Systempflege, z. B. Informationssicherheitsrisikobeurteilung und Maßnahmenpflege, internes ISMS-Audit, Managementbewertung und Korrekturmaßnahmen;

b) Kommunikation externer Parteien, wie von der ISMS-Norm ISO/IEC 27001 und anderen für die Zertifizierung erforderlichen Dokumenten gefordert;

c) Änderungen des dokumentierten Systems;

d) Bereiche, die Änderungen unterworfen sind;

e) ausgewählte Anforderungen nach ISO/IEC 27001;

f) andere ausgewählte Bereiche, sofern angebracht.

**9.6.2.1.2** Jede Überwachung durch die Zertifizierungsstelle muss mindestens Folgendes prüfen:

a) die Wirksamkeit des ISMS in Bezug auf die Erfüllung der Ziele der Informationssicherheitspolitik des Kunden;

b) die Funktionsweise der Verfahren zur regelmäßigen Bewertung und Prüfung der Einhaltung relevanter Gesetze und Vorschriften zur Informationssicherheit;

c) Änderungen an den festgelegten Maßnahmen und daraus resultierende Änderungen an der SoA;

d) Umsetzung und Wirksamkeit der Maßnahmen gemäß dem Auditprogramm.

**9.6.2.1.3** Die Zertifizierungsstelle muss in der Lage sein, ihr Überwachungsprogramm an die Informationssicherheitsprobleme in Bezug auf die Risiken und Auswirkungen auf den Kunden anzupassen und dieses Programm zu begründen.

Überwachungsaudits dürfen mit den Audits anderer Managementsysteme kombiniert werden. Die Berichterstattung muss die für jedes Managementsystem relevanten Aspekte eindeutig kennzeichnen.

Im Rahmen von Überwachungsaudits müssen Zertifizierungsstellen die Aufzeichnungen von denen der Zertifizierungsstelle vorgelegten Einsprüche und Beschwerden prüfen. In Fällen von erkannten Nichtkonformitäten und nicht erfüllten Anforderungen der Zertifizierung muss geprüft werden, ob der Kunde sein eigenes ISMS und Verfahren untersucht und angemessene Korrekturmaßnahmen ergriffen hat.

Ein Überwachungsauditbericht muss insbesondere Informationen zur Behebung von zuvor entdeckten Nichtkonformitäten sowie die Version der SoA und wichtige Änderungen seit dem letzten Audit enthalten. Die aus der Überwachung stammenden Berichte müssen insgesamt mindestens die Anforderungen aus 9.6.2.1.1 und 9.6.2.1.2 abdecken.

### 9.6.3 Re-Zertifizierung

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.6.3. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.6.3.1 IS 9.6.3 Re-Zertifizierungsaudits

Re-Zertifizierungsauditverfahren müssen mit den Verfahren in Bezug auf das Erstzertifizierungsaudit des ISMS des Kunden, wie in dieser Internationalen Norm dargelegt, übereinstimmen.



Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006:2020-08

Die zur Umsetzung von Korrekturmaßnahmen gestattete Zeit muss in Relation zur Schwere der Nichtkonformität und zu den zugehörigen Informationssicherheitsrisiken stehen.

#### 9.6.4 Audits aus besonderem Anlass

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.6.4. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.6.4.1 IS 9.6.4 Sonderfälle

Die notwendigen Tätigkeiten für die Durchführung von Audits aus besonderem Anlass müssen besonderen Vorkehrungen unterliegen, falls ein Kunde mit einem zertifizierten ISMS wesentliche Änderungen an seinem System vornimmt oder falls andere Änderungen stattfinden, die die Grundlage der Zertifizierung beeinflussen können.

#### 9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.6.5.

### 9.7 Einsprüche

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.7.

### 9.8 Beschwerden

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.8. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 9.8.1 IS 9.8 Beschwerden

Beschwerden stellen potenzielle Vorfälle und Anzeichen für mögliche Nichtkonformitäten dar.

### 9.9 Aufzeichnungen zu Kunden

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.9.

## 10 Managementsystemanforderungen für Zertifizierungsstellen

### 10.1 Optionen

Es gelten die Anforderungen nach ISO/IEC 17021-1, 10.1. Zudem gelten die folgenden Anforderungen und Anleitungen.

#### 10.1.1 IS 10.1 ISMS-Umsetzung

Es wird empfohlen, dass Zertifizierungsstellen ein ISMS in Übereinstimmung mit ISO/IEC 27001 umsetzen.

### 10.2 Option A: Allgemeine Managementsystemanforderungen

Es gelten die Anforderungen nach ISO/IEC 17021-1, 10.2.

### 10.3 Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001

Es gelten die Anforderungen nach ISO/IEC 17021-1, 10.3.

AVA Documents
Document Sharing Hub



Full document details: E DIN EN ISO/IEC 27006:2020-08

# Anhang A
(informativ)

# Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung

## A.1 Übersicht

Tabelle A.1 enthält eine Zusammenfassung des Wissens und der Fertigkeiten, das bzw. die für Audits und die Zertifizierung von ISMS erforderlich ist bzw. sind. Die Tabelle ist informativ, da sie nur die Wissens- und Fertigkeitsbereiche für spezifische Zertifizierungsfunktionen kennzeichnet.

Die Kompetenzanforderungen für jede Funktion sind im Haupttext dieser Internationalen Norm angegeben, und diese Tabelle verweist auf die spezifische Anforderung.

**Tabelle A.1 — Wissen für ISMS-Audits und die Zertifizierung**

| | **Zertifizierungsfunktion** | | |
|---|---|---|---|
| | Durchführung der Antragsprüfung, um die erforderliche Kompetenz des Auditteams zu ermitteln, die Mitglieder des Auditteams auszuwählen und den Auditzeitaufwand festzulegen | Überprüfung der Auditberichte und Treffen von Zertifizierungs-entscheidungen | Auditierung und Leitung des Auditteams |
| **Wissen** | | | |
| Informationssicherheits-managementterminologie, -grundsätze, -praktiken und -verfahren | | 7.1.2.4.2 | 7.1.2.1.2 |
| Normen/normative Dokumente in Bezug auf Informationssicherheits-managementsysteme | 7.1.2.3.1 | 7.1.2.4.3 | 7.1.2.1.3 |
| Praktische Unternehmensführung | | | 7.1.2.1.4 |
| Geschäftsfelddes Kunden | 7.1.2.3.2 | 7.1.2.4.4 | 7.1.2.1.5 |
| Produkte, Prozesse und Organisation des Kunden | 7.1.2.3.3 | 7.1.2.4.5 | 7.1.2.1.6 |



AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006:2020-08