DIN EN ISO/IEC 27006-1

DIN

ICS 03.120.20; 35.030

Entwurf

Einsprüche bis 2023-05-31
Vorgesehen als Ersatz für
DIN EN ISO/IEC 27006:2021-05;
Ersatz für
E DIN EN ISO/IEC
27006-1:2022-08

Informationstechnik, Cybersicherheit und Datenschutz – Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren – Teil 1: Allgemeines (ISO/IEC DIS 27006-1.2:2023); Deutsche und Englische Fassung prEN ISO/IEC 27006-1:2023

Information technology, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems – Part 1: General (ISO/IEC DIS 27006-1.2:2023); German and English version prEN ISO/IEC 27006-1:2023

Sécurité de l'information, cybersécurité et protection des données privées – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information – Partie 1: Généralités (ISO/IEC DIS 27006-1.2:2023); Version allemande et anglaise prEN ISO/IEC 27006-1:2023

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2023-03-31 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

— vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;

— oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;

— oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

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

Gesamtumfang 140 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Nationales Vorwort

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

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-04-27-01 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 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27006 (alle Teile)	siehe	DIN EN ISO/IEC 27006 (alle Teile)*
ISO/IEC 27007	siehe	DIN EN ISO/IEC 27007

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

Änderungen

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

a) Begriffsdefinitionen aus ISO/IEC 27000 aufgenommen;

b) Abschnitt B.7 „Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs“ und Abschnitt B.8 „Auditzeitaufwand für eine branchenspezifische Normerweiterung“ neu aufgenommen;

c) Norm neu benummert von EN ISO/IEC 27006 zu EN ISO/IEC 27006-1;

d) redaktionelle Überarbeitung der Norm.

---

* Zur Zeit Entwurf.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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 27002, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

DIN EN ISO/IEC 27006 (alle Teile), *Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren*

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

– Entwurf –

Februar 2023

prEN ISO/IEC 27006-1

Informationstechnik, Cybersicherheit und Datenschutz – Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren – Teil 1: Allgemeines (ISO/IEC DIS 27006-1.2:2023)

Information technology, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems – Part 1: General (ISO/IEC DIS 27006-1.2:2023)

Sécurité de l'information, cybersécurité et protection des données privées – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information – Partie 1: Généralités (ISO/IEC DIS 27006-1.2:2023)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Inhalt

Seite

Europäisches Vorwort . . . 5
Vorwort . . . 6
Einleitung . . . 8
1 Anwendungsbereich . . . 9
2 Normative Verweisungen . . . 9
3 Begriffe . . . 9
4 Grundsätze . . . 13
5 Allgemeine Anforderungen . . . 13
5.1 Rechts- und Vertragsfragen . . . 13
5.2 Handhabung der Unparteilichkeit . . . 13
5.2.1 Allgemeines . . . 13
5.2.2 Interessenkonflikte . . . 13
5.3 Haftung und Finanzierung . . . 13
6 Strukturelle Anforderungen . . . 13
7 Anforderungen an Ressourcen . . . 13
7.1 Kompetenz des Personals . . . 13
7.1.1 Allgemeines . . . 13
7.1.2 Allgemeine Betrachtungen . . . 14
7.1.3 Bestimmung der Kompetenzkriterien . . . 14
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist . . . 17
7.2.1 Allgemeines . . . 17
7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren . . . 17
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten . . . 18
7.4 Aufzeichnungen über Personal . . . 18
7.5 Ausgliederung . . . 18
8 Anforderungen an Informationen . . . 18
8.1 Öffentliche Informationen . . . 18
8.2 Zertifizierungsdokumente . . . 18
8.2.1 Allgemeines . . . 18
8.2.2 ISMS-Zertifizierungsdokumente . . . 18
8.2.3 ISMS-Zertifizierungsdokumente und branchenspezifische Normen . . . 19
8.2.4 Anforderungen an interessierte Parteien . . . 19
8.3 Verweisung auf Zertifizierung und Zeichennutzung . . . 19
8.4 Vertraulichkeit . . . 19
8.4.1 Allgemeines . . . 19
8.4.2 Zugang zu den Aufzeichnungen der Organisation . . . 19
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden . . . 20
9 Anforderungen an Prozesse . . . 20
9.1 Tätigkeiten vor der Zertifizierung . . . 20
9.1.1 Antrag . . . 20
9.1.2 Antragsprüfung . . . 20
9.1.3 Auditprogramm . . . 20
9.1.4 Ermittlung des Auditzeitaufwands . . . 22
9.1.5 Stichprobenprüfung an mehreren Standorten . . . 22
9.1.6 Mehrfach-Managementsysteme . . . 23
9.2 Planung von Audits . . . 24
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien . . . 24
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung . . . 24
9.2.3 Auditplan . . . 24
9.3 Erstzertifizierung . . . 25
9.3.1 Allgemeines . . . 25

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

9.3.2 Erstzertifizierungsaudit . . . 25
9.4 Durchführen von Audits . . . 26
9.4.1 Allgemeines . . . 26
9.4.2 Spezifische Elemente des ISMS-Audits . . . 26
9.4.3 Auditbericht . . . 26
9.5 Zertifizierungsentscheidung . . . 27
9.5.1 Allgemeines . . . 27
9.5.2 Zertifizierungsentscheidung . . . 27
9.6 Aufrechterhaltung der Zertifizierung . . . 27
9.6.1 Allgemeines . . . 27
9.6.2 Überwachungstätigkeiten . . . 27
9.6.3 Re-Zertifizierung . . . 28
9.6.4 Audits aus besonderem Anlass . . . 28
9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung 29
9.7 Einsprüche . . . 29
9.8 Beschwerden . . . 29
9.8.1 Allgemeines . . . 29
9.8.2 Beschwerden . . . 29
9.9 Aufzeichnungen zu Kunden . . . 29
10 Managementsystemanforderungen für Zertifizierungsstellen . . . 29
10.1 Optionen . . . 29
10.1.1 Allgemeines . . . 29
10.1.2 ISMS-Umsetzung . . . 29
10.2 Option A: Allgemeine Managementsystemanforderungen . . . 29
10.3 Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001 . . . 29
Anhang A (normativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung . . . 30
A.1 Übersicht . . . 30
Anhang B (normativ) Auditzeitaufwand . . . 31
B.1 Einleitung . . . 31
B.2 Konzepte . . . 32
B.2.1 Anzahl der von der Organisation gesteuerten Personen . . . 32
B.2.2 Auditortag . . . 32
B.2.3 Temporärer Standort . . . 32
B.3 Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit . . . 33
B.3.1 Allgemeines . . . 33
B.3.2 Methoden zur Durchführung von Fernaudits . . . 33
B.3.3 Berechnung des Auditzeitaufwands . . . 33
B.3.4 Bestimmung der ursprünglichen Personenanzahl . . . 33
B.3.5 Faktoren für die Anpassung des Auditzeitaufwands . . . 34
B.3.6 Einschränkung der Abweichung von der Auditzeit . . . 36
B.3.7 Vor-Ort-Auditzeitaufwand . . . 36
B.4 Auditzeitaufwand für das Überwachungsaudit . . . 36
B.5 Auditzeitaufwand für das Re-Zertifizierungsaudit . . . 36
B.6 Auditzeitaufwand für mehrere Standorte . . . 36
B.7 Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs . . . 37
B.8 Auditzeitaufwand für eine branchenspezifische Norm . . . 37
Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands . . . 38
C.1 Allgemeines . . . 38
C.2 Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands . . . 38
C.3 Beispiel für die Auditzeitaufwandberechnung . . . 41
Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2022, Anhang A . . . 44
D.1 Zweck . . . 44
D.2 Anwendung von Tabelle D.1 . . . 44
D.2.1 Allgemeines . . . 44
D.2.2 Spalte „Systemprüfung“ . . . 45
D.2.3 Spalte „Sichtprüfung“ . . . 45

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

D.2.4 Möglicher Nachweis der Gestaltung und Umsetzung von Maßnahmen 45
Anhang E (informativ) **Anforderungen und Einschränkungen bei Zertifizierungen nach branchenspezifischen Normen 63**
E.1 Allgemeines 63
Anhang F (normativ) **Anforderungen an die Zertifizierung einschließlich branchenspezifischer Normen 64**
F.1 Allgemeines 64
Anhang G (informativ) **Weitere Kompetenzbetrachtungen 65**
G.1 Allgemeine Kompetenzbetrachtungen 65
G.2 Spezielle Betrachtungen zu Wissen und Erfahrung 65
G.2.1 Typisches Wissen in Bezug auf ISMS 65
Literaturhinweise 67

Tabellen

Tabelle A.1 — Tabelle zum Wissen und zu den Fertigkeiten für ISMS-Audits und -Zertifizierung . 30
Tabelle B.1 — Auditzeitaufwandstabelle 34
Tabelle C.1 — Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands 39
Tabelle C.2 — Mit dem Geschäft und der Organisation zusammenhängende Faktoren (ohne IT) . 42
Tabelle C.3 — Mit der IT-Umgebung zusammenhängende Faktoren 42
Tabelle C.4 — Auswirkung der Faktoren auf die Auditzeit 43
Tabelle D.1 — Bewertung der Maßnahmen 46
Tabelle E.1 — Verweisung auf Anforderungen und Leitlinien für branchenspezifische Erweiterungen 63

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Europäisches Vorwort

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

Dieses Dokument ist derzeit zur zweiten parallelen Umfrage vorgelegt.

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

Anerkennungsnotiz

Der Text von ISO/IEC DIS 27006-1.2:2023 wurde von CEN als prEN ISO/IEC 27006-1:2023 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Vorwort

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

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

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

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

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

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

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

Die wesentlichen Änderungen sind folgende:

— dieses Dokument wurde für branchenspezifische Erweiterungen verallgemeinert;

— das gesamte Dokument wurde für Fernaudits und Organisationen mit wenigen oder keinen entsprechenden physischen Standorten aktualisiert;

— in Anhang B wurde ein neues Konzept eingeführt und mehrere Aktualisierungen wurden vorgenommen;

— dieses Dokument wurde an ISO/IEC 27001:2022 und ISO/IEC 27022 angeglichen, einschließlich der Aktualisierung von Anhang D;

— Redundanzen mit ISO/IEC 17021-1 wurden entfernt;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

— der Wortlaut wurde erläutert und verbessert, um eine bessere Konsistenz zu erreichen, unter anderem mit ISO/IEC 17021-1;

— strukturelle Änderungen zur Erfüllung der ISO/IEC-Directives wurden vorgenommen.

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

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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 der Norm ISO/IEC 17021-1 und möglicherweise branchenspezifischen Normerweiterungen von ISO/IEC 27001 entsprechen sollten, sind einige zusätzliche Anforderungen und Anleitung in Bezug auf ISO/IEC 17021-1 von entscheidender Bedeutung. Diese werden durch dieses Dokument zur Verfügung gestellt.

Der Text dieses Dokuments folgt der Struktur von ISO/IEC 17021-1.

In diesem Teil von ISO/IEC 27006 bezeichnet die Verbform:

— „müssen“ eine Anforderung;

— „sollten“ eine Empfehlung;

— „dürfen“ eine Erlaubnis;

— „können“ eine Möglichkeit bzw. eine Fähigkeit.

Weitere Einzelheiten hierzu sind in den ISO/IEC-Directives, Teil 2 zu finden.

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

In diesem Dokument werden die Begriffe „Managementsystem“ und „System“ synonym verwendet. Das Managementsystem, wie es in diesem Dokument verwendet wird, sollte nicht mit anderen Arten von Systemen, etwa IT-Systemen, verwechselt werden.

Die Zertifizierungsstelle darf ein Audit und eine Zertifizierung nach ISO/IEC 27001 anbieten, wenn der Zertifizierungskunde branchenspezifische Normen als Quelle für einen oder mehrere zusätzliche Maßnahmensätze angegeben hat, mit denen die bestimmten Maßnahmen verglichen werden können. Wenn Normen zur Erweiterung von Informationssicherheitsmaßnahmen verwendet werden, gilt weiterhin die Zertifizierungsnorm ISO/IEC 27001.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

1 Anwendungsbereich

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

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

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

2 Normative Verweisungen

Die folgenden Dokumente, 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 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

3 Begriffe

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

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

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

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

3.1
Zertifizierungsdokumente
en **certification documents**
Dokumente, die angeben, dass das Informationssicherheitsmanagementsystem (ISMS) eines Kunden spezifizierten ISMS-Normen und jeglicher im Rahmen des Systems erforderlichen zusätzlichen Dokumentation entspricht

3.2
Maßnahme
en **control**
Mittel zur Beibehaltung und/oder Veränderung des *Risikos* (3.10)

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

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

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

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

3.3
externer Kontext
en **external context**
externes Umfeld, in dem die *Organisation* (3.9) versucht, ihre Ziele zu erreichen

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

— die kulturelle, soziale, politische, gesetzliche, regulatorische, finanzielle, technologische, ökonomische, natürliche und wettbewerbliche Umgebung, die internationalen, nationalen, regionalen oder lokalen Charakter haben kann;

— wesentliche Treiber und Trends, die sich auf die Ziele der *Organisation* (3.9) auswirken;

— Beziehungen zu externen interessierten Parteien sowie deren Auffassungen und Werte.

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

3.4
Informationssicherheit
en **information security**
Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information

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

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

3.5
Informationssicherheitsvorfall
en **information security incident**
einzelnes oder eine Reihe von ungewollten oder unerwarteten Informationssicherheitsereignissen, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die *Informationssicherheit* (3.4) zu bedrohen

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

3.6
Informationssystem
en **information system**
Anwendungen, Dienste, informationstechnische Werte oder andere Information bearbeitende Komponenten

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

3.7
interner Kontext
en **internal context**
interne Umgebung, in der die *Organisation* (3.9) versucht, ihre Ziele zu erreichen

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

— Steuerung durch die Unternehmensführung, Organisationsstruktur, Rollen und Verantwortlichkeiten;

— Richtlinien, Ziele und Strategien, die mit dem Ziel in Kraft sind, sie einzuhalten beziehungsweise sie zu erreichen;

— die Fähigkeit in Form von Ressourcen und Wissen (z. B. Kapital, Zeit, Menschen, Prozesse, Systeme und Techniken);

— *Informationssysteme* (3.6), Informationsflüsse und Prozesse zur Entscheidungsfindung (sowohl formell als auch informell);

— Beziehungen zu internen interessierten Parteien sowie deren Auffassungen und Werte;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

— die Organisationskultur (*Organisation,* 3.9);

— Standards, Leitfäden und Modelle, die von der *Organisation* (3.9) übernommen worden sind;

— Gestalt und Ausmaß vertraglicher Beziehungen.

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

3.8
Managementsystem
Satz zusammenhängender oder sich gegenseitig beeinflussender Elemente einer *Organisation* (3.9), um Politiken, Ziele und Prozesse zum Erreichen dieser Ziele festzulegen

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

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

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

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

[QUELLE: ISO/IEC 9000:2015, 3.5.3]

3.9
Organisation
Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen

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

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

3.10
Risiko
en **risk**
Auswirkung von Ungewissheit auf Ziele

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

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

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

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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

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

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

3.11
Risikoanalyse
en **risk analysis**
Prozess, um die Beschaffenheit des *Risikos* (3.10) zu verstehen und das Risikoniveau zu bestimmen

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

Anmerkung 2 zum Begriff: Die Risikoanalyse beinhaltet die Risikoabschätzung.

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

3.12
Risikobeurteilung
en **risk assessment**
übergreifender Prozess, der aus Risikoidentifizierung, *Risikoanalyse* (3.11) und Risikobewertung besteht

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

3.13
Risikomanagement
en **risk management**
koordinierte Tätigkeiten zum Zwecke der Führung und Steuerung einer *Organisation* (3.9) in Bezug auf *Risiken* (3.10)

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

3.14
Risikobehandlung
en **risk treatment**
Prozess, um *Risiken* (3.10) zu verändern

Anmerkung 1 zum Begriff: Die Risikobehandlung kann umfassen:

— Vermeiden des Risikos, indem entschieden wird, die Tätigkeit, die Anlass zu dem *Risiko* (3.10) gibt, nicht zu beginnen oder fortzusetzen;

— Eingehen oder Vergrößern des Risikos mit dem Ziel, eine Chance wahrzunehmen;

— Beseitigen der Risikoquelle;

— Verändern der Wahrscheinlichkeit;

— Verändern der Folgen;

— Teilen des *Risikos* (3.10) mit einer anderen Partei oder anderen Parteien (einschließlich Verträgen und Finanzierung von Risiken);

— Beibehalten des *Risikos* (3.10) im Rahmen einer fundierten Entscheidung.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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

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

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

4 Grundsätze

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

5 Allgemeine Anforderungen

5.1 Rechts- und Vertragsfragen

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

5.2 Handhabung der Unparteilichkeit

5.2.1 Allgemeines

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

5.2.2 Interessenkonflikte

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

a) Erbringung von Mehrwert während Zertifizierungen und Überwachungsaudits, 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 17021-1:2015, 5.3.

6 Strukturelle Anforderungen

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

7 Anforderungen an Ressourcen

7.1 Kompetenz des Personals

7.1.1 Allgemeines

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

7.1.2 Allgemeine Betrachtungen

7.1.2.1 Allgemeine Kompetenzanforderungen

Die Zertifizierungsstelle muss die Kompetenzanforderungen für jede Zertifizierungsfunktion definieren, wie in ISO/IEC 17021-1:2015, Tabelle A.1, angegeben. Die Zertifizierungsstelle muss alle in ISO/IEC 17021-1 und 7.1.3 und 7.2.2 dieses Dokuments angegebenen Anforderungen berücksichtigen, die entsprechend den Festlegungen der Zertifizierungsstelle für die technischen Bereiche des ISMS relevant sind.

ANMERKUNG Anhang A enthält eine Zusammenfassung der Kompetenzanforderungen an das Personal, das in bestimmte Zertifizierungsfunktionen einbezogen ist. Der entsprechende Teil der Normenreihe ISO/IEC 27006 enthält Informationen zu branchenspezifischen Anforderungen an die Kompetenz.

Falls kein Teil der Normenreihe ISO/IEC 27006 vorhanden ist, muss die Zertifizierungsstelle für jede Zertifizierungsfunktion Anforderungen an die Kompetenz für Tätigkeiten festlegen, die die branchenspezifische(n) Norm(en) zur Erweiterung der Auditkriterien enthalten.

7.1.3 Bestimmung der Kompetenzkriterien

7.1.3.1 Kompetenzanforderungen für ISMS-Audits

7.1.3.1.1 Allgemeine Anforderungen

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

a) Wissen über Informationssicherheit;

b) technisches Wissen in Bezug auf die Tätigkeit, die auditiert werden soll;

c) Wissen über Managementsysteme;

d) Wissen über Auditgrundsätze;

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

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

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

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

Die Mitglieder des Auditteams müssen gemeinsam über eine angemessene Arbeitserfahrung in Bezug auf die oben genannten Anforderungen und die praktische Anwendung dieser Anforderungen verfügen. Einzelne Auditoren müssen nicht über eine umfassende Erfahrung in allen Bereichen der Informationssicherheit verfügen, aber das Auditteam muss insgesamt über angemessene Kompetenzen verfügen, um den zu auditierenden ISMS-Anwendungsbereich abzudecken.

7.1.3.1.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

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

a) ISMS-spezifische Dokumentationsstrukturen, Hierarchie und Wechselbeziehungen;

b) Informationssicherheitsrisikobeurteilung und -risikomanagement;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

c) auf ISMS anwendbare Prozesse.

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

d) Werkzeuge, Methoden, Verfahren des Informationssicherheitsmanagements und deren Anwendung;

e) aktuelle Technik, bei der die Informationssicherheit relevant oder ein Problem sein kann.

7.1.3.1.3 Informationssicherheitsmanagementsystemnormen und normative Dokumente

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

a) alle Anforderungen in ISO/IEC 27001.

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

b) alle Maßnahmen in ISO/IEC 27001:2022, Anhang A (und sofern zutreffend auch aus einschlägigen branchenspezifischen Normen) und ihre Umsetzung.

7.1.3.1.4 Praktische Unternehmensführung

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

a) bewährte Informationssicherheitspraktiken und Informationssicherheitsprozeduren aus der Industrie;

b) Richtlinien und betriebliche Anforderungen an die Informationssicherheit;

c) allgemeine Konzepte und Praktiken zur Unternehmensführung und die Wechselbeziehung zwischen Politik, Zielen und Ergebnissen;

d) Managementprozesse und zugehörige Terminologie.

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

7.1.3.1.5 Geschäftsfeld des Kunden

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

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

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

b) mit dem Geschäftsfeld zusammenhängende Informationssicherheitsrisiken;

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

d) relevante Geschäftsfeldpraktiken.

Kriterium a) darf im Auditteam verteilt sein.

7.1.3.1.6 Produkte, Prozesse und Organisation des Kunden

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

a) Einfluss der Art, Größe, Führung, Struktur, Funktionen und Beziehungen einer Organisation auf die Entwicklung und Implementierung des ISMS und der Zertifizierungstätigkeiten, einschließlich Ausgliederung;

b) komplexer Betrieb im Rahmen einer weiten Perspektive;

c) auf die Produkte oder Dienstleistungen anzuwendende gesetzliche und behördliche Anforderungen.

7.1.3.2 Anforderungen an die Kompetenz für die Durchführung der Antragsprüfung

7.1.3.2.1 Geschäftsfeld des Kunden

Das Personal, das die Antragsprüfung zur Bestimmung der erforderlichen Kompetenz des Auditteams, zur Auswahl der Mitglieder des Auditteams und zur Bestimmung der Auditzeit durchführt, muss über folgendes Wissen verfügen:

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

7.1.3.2.2 Produkte, Prozesse und Organisation des Kunden

Das Personal, das die Antragsprüfung zur Bestimmung der erforderlichen Kompetenz des Auditteams, zur Auswahl der Mitglieder des Auditteams und zur Bestimmung der Auditzeit durchführt, muss über folgendes Wissen verfügen:

a) Einfluss von Kundenprodukten, Prozessen, Art der Organisation, Größe, Führung, Struktur, Funktionen und Beziehungen einer Organisation zur Entwicklung und Implementierung des ISMS und der Zertifizierungstätigkeiten, einschließlich Ausgliederungsfunktionen.

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

7.1.3.3.1 Allgemeines

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

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

a) Managementsysteme allgemein;

b) Auditprozesse und -verfahren;

c) Auditgrundsätze, -praktiken und -verfahren.

7.1.3.3.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

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

a) die in 7.1.3.1.2 a), b) und c) aufgelisteten Punkte;

b) für die Informationssicherheit relevante gesetzliche und behördliche Anforderungen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

7.1.3.3.3 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.

7.1.3.3.4 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.

7.1.3.3.5 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

7.2.1 Allgemeines

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

7.2.2 Nachweis des Wissens und der Erfahrung der Auditoren

7.2.2.1 Allgemeine Betrachtungen

Die Zertifizierungsstelle muss nachweisen, dass jeder Auditor zu folgenden Punkten über Wissen und Erfahrung verfügt:

a) anerkannte ISMS-spezifische Qualifikationen;

b) Registrierung als Auditor, soweit anwendbar;

c) Teilnahme an ISMS-Schulungen und Erlangung relevanter persönlicher Qualifikationen;

d) aktuelle Aufzeichnungen der beruflichen Entwicklung;

e) ISMS-Audits, die ein anderer ISMS-Auditor überwacht hat.

7.2.2.2 Auswahl von Auditoren

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

a) über einen ausreichenden Bildungsstand und praktische Berufserfahrung in den Bereichen Informationstechnologie und Informationssicherheit verfügt, um als Auditor für ISMS tätig zu sein;

b) eine ausreichende Schulung zur Auditierung von ISMS erhalten und seine Fertigkeiten zur Auditierung eines ISMS nach ISO/IEC 27001 nachgewiesen hat;

c) relevantes und aktuelles Wissen sowie Fertigkeiten im Bereich der Informationssicherheit und der Auditierung pflegt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

ANMERKUNG Die Pflege der Fertigkeiten kann durch kontinuierliche berufliche Weiterbildung nachgewiesen werden.

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

d) über einen ausreichenden Bildungsstand und praktische Berufserfahrung in den Bereichen Informationstechnologie und Informationssicherheit verfügt, um als Fachexperte tätig zu sein;

e) relevantes und aktuelles Wissen sowie Fertigkeiten im Bereich der Informationssicherheit pflegt.

ANMERKUNG Die Pflege der Fertigkeiten kann durch kontinuierliche berufliche Weiterbildung nachgewiesen werden.

7.2.2.3 Auswahl von Auditoren für die Teamleitung

Neben 7.2.2.1 müssen die Kriterien zur Auswahl eines Auditors für die Teamleitung sicherstellen, dass der 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 17021-1:2015, 7.3.

7.4 Aufzeichnungen über Personal

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

7.5 Ausgliederung

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

8 Anforderungen an Informationen

8.1 Öffentliche Informationen

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

8.2 Zertifizierungsdokumente

8.2.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1, 8.2. Außerdem gelten die Anforderungen und der Leitfaden in 8.2.2, 8.2.3 und 8.2.4.

8.2.2 ISMS-Zertifizierungsdokumente

Zertifizierungsdokumente müssen von einem Bevollmächtigten unterschrieben werden, dem diese 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 nur dann nationale und internationale branchenspezifische Normen referenzieren, wenn:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

a) die Organisation alle ihre erforderlichen Maßnahmen mit denen in der/n Quelle(n) für Referenzmaßnahmen verglichen hat, um zu sehen, dass sie nicht versehentlich eine solche Referenzmaßnahme in Übereinstimmung mit ISO/IEC 27001:2022, 6.1.3 c) weggelassen hat;

b) eine Begründung für ausgeschlossene Referenzmaßnahmen wird in der Erklärung zur Anwendbarkeit (SoA, en: Statement of Applicability) nach ISO/IEC 27001:2022, 6.1.3 d) aufgeführt.

Die Bezugsnormen für die Maßnahmen können auf ISO/IEC 27001:2022, Anhang A, beruhen oder Normen sein, die Sicherheitsmaßnahmen beinhalten.

In den Zertifizierungsdokumenten muss angegeben werden, dass die im SoA angewandten Maßnahmensätze nur als Referenz für die Relevanz der Aufnahme oder des Ausschlusses von Maßnahmen in das ISMS und nicht für die Konformitätsbewertung verwendet werden.

Wenn die Tätigkeiten der Organisation nicht an einem bestimmten physischen Standort durchgeführt werden, muss in den Zertifizierungsdokumenten angegeben werden, dass alle Tätigkeiten der Organisation aus der Ferne durchgeführt werden.

8.2.3 ISMS-Zertifizierungsdokumente und branchenspezifische Normen

Falls die Zertifizierungsdokumente auf branchenspezifische Normen verweisen, gilt Folgendes:

Die branchenspezifische Norm der Zertifizierungsdokumente muss deutlich die Zertifizierungsdokumente nach ISO/IEC 27001 referenzieren, für die die Erweiterung gilt.

Die Zertifizierungsstelle darf ein zusätzliches Dokument zur Beschreibung der referenzierten branchenspezifischen Norm nur als Teil der Zertifizierungsdokumente nach ISO/IEC 27001 herausgeben, das auf die Hauptzertifizierungsdokumente verweisen und an diese angeglichen sein muss.

ANMERKUNG Anhang E enthält die prägnante Übersicht über die Anforderungen sowie Leitlinien für branchenspezifische Normerweiterungen.

8.2.4 Anforderungen an interessierte Parteien

Die Zertifizierungsstelle muss sicherstellen, dass die Erklärung zum Geltungsbereich der Zertifizierung eindeutig sein muss, wenn der Zertifizierungskunde Anforderungen, die für die Informationssicherheit der interessierten Parteien relevant sind, aus dem Anwendungsbereich des ISMS ausgeschlossen hat.

8.3 Verweisung auf Zertifizierung und Zeichennutzung

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

8.4 Vertraulichkeit

8.4.1 Allgemeines

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

8.4.2 Zugang zu den Aufzeichnungen der Organisation

Vor dem Zertifizierungsaudit muss die Zertifizierungsstelle den Kunden darum bitten, anzugeben, ob Informationen in Bezug auf das ISMS (etwa ISMS-Aufzeichnungen oder Informationen zur Gestaltung und Wirksamkeit von Maßnahmen) zur Prüfung durch das Auditteam nicht zur Verfügung gestellt werden können, da sie vertrauliche oder sensible Informationen enthalten. Die Zertifizierungsstelle muss bestimmen, ob das 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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

das Zertifizierungsaudit nicht stattfinden kann, bis angemessene Zugangsvereinbarungen bereitgestellt werden.

8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden

8.5.1 Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 8.5. Außerdem gelten die Anforderungen und der Leitfaden in 8.5.2.

8.5.2 Falls die Zertifizierungsstelle Audits für branchenspezifische Normen anbietet, gilt Folgendes:

Die Zertifizierungsstelle muss sicherstellen, dass ihre Kunden über die Möglichkeit informiert sind, eine oder mehrere branchenspezifische Normen in die Zertifizierung nach ISO/IEC 27001 aufzunehmen.

9 Anforderungen an Prozesse

9.1 Tätigkeiten vor der Zertifizierung

9.1.1 Antrag

9.1.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.1. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.1.2.

9.1.1.2 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 die Bestätigung legen, dass das ISMS des Kunden die Anforderungen nach ISO/IEC 27001 sowie Richtlinien und Ziele des Kunden erfüllt.

ANMERKUNG 1 ISO/IEC 27007 enthält weitere Anleitung zu Audits.

ANMERKUNG 2 Eine Organisation kann ihre eigenen notwendigen Maßnahmen entwerfen oder sie aus einer beliebigen Quelle auswählen; daher ist es möglich, dass eine Organisation nach ISO/IEC 27001 zertifiziert ist, auch wenn keine ihrer notwendigen Maßnahmen aus ISO/IEC 27001:2022, Anhang A, oder aus einer branchenspezifischen Norm stammen.

9.1.2 Antragsprüfung

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

9.1.3 Auditprogramm

9.1.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.3.2, 9.1.3.3, 9.1.3.4, 9.1.3.5 und 9.1.3.6.

9.1.3.2 Allgemeine Betrachtungen

Das Auditprogramm für ISMS-Audits muss die vom Kunden festgelegten Informationssicherheitsmaßnahmen berücksichtigen, die aus ISO/IEC 27001:2022, Anhang A, und gegebenenfalls aus der/den sektorspezifischen Norm(en) stammen können.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

9.1.3.3 Einsatz eines Fernaudits

Die Zertifizierungsstelle muss Verfahren bestimmen, um den Umfang von Fernaudittätigkeiten („Fernaudits“) festzulegen, die zum Auditieren des ISMS eines Kunden eingesetzt werden können. Die Verfahren müssen den Auditprozess während des Lebenszyklus der Zertifizierung vom Erstaudit bis zum Re-Zertifizierungsaudit berücksichtigen. Zu den Verfahren muss die Analyse gehören von:

a) Risiken in Bezug auf den Einsatz von Fernaudits für den Kunden;

b) Branche, in der der Kunde tätig ist;

c) Auditart(en) während des Zertifizierungszyklus.

Die Ergebnisse der Analyse und die Begründung für den Einsatz eines Fernaudits während des Zertifizierungszyklus müssen dokumentiert werden.

Fernaudits dürfen nicht eingesetzt werden, wenn die Risikobeurteilung für die Wirksamkeit des Auditprozesses nicht annehmbare Risiken ermittelt.

Die Risikobeurteilung muss während des Zertifizierungszyklus erneut geprüft werden, um sicherzustellen, ob dieser weiterhin geeignet ist.

ANMERKUNG Falls der Kunde virtuelle Standorte (d. h. ein Ort, an dem eine Organisation mithilfe einer Online-Umgebung Arbeit ausführt oder eine Dienstleistung erbringt, damit die Beteiligten ungeachtet ihres physischen Standorts die Prozesse durchführen können) nutzt, sind Fernauditverfahren ein maßgebender Bestandteil des Auditplans.

9.1.3.4 Allgemeine Vorbereitungen für das Erstaudit

Die Zertifizierungsstelle muss fordern, dass ein Kunde alle erforderlichen Maßnahmen zur Sicherstellung des Zugriffs auf interne Auditberichte und Berichte unabhängiger Prüfungen der Informationssicherheit ergreift.

9.1.3.5 Überprüfungszeiträume

Die Zertifizierungsstelle darf ISMS nicht zertifizieren, bis es ausreichende Nachweise gibt, die darlegen, dass Vorkehrungen für Managementbewertungen und interne ISMS-Audits umgesetzt und wirksam sind sowie zur Abdeckung des Zertifizierungsbereichs aufrechterhalten werden.

9.1.3.6 Geltungsbereich der ISMS-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 27001:2022, 4.3, festgelegten Anforderungen behandelt.

Zertifizierungsstellen müssen sicherstellen, dass die Informationssicherheitsrisikobeurteilung und –risikobehandlung des Kunden seine Tätigkeiten angemessen widerspiegeln und sich bis auf die Grenzen der Tätigkeiten, wie sie im Geltungsbereich der Zertifizierung definiert wurden, erstrecken. Zertifizierungsstellen müssen bestätigen, dass dies im ISMS-Anwendungsbereich des Kunden und der SoA widergespiegelt wird. Die Zertifizierungsstelle muss verifizieren, dass es für den Geltungsbereich der Zertifizierung eine SoA gibt.

Zertifizierungsstellen müssen sicherstellen, dass Schnittstellen zu Diensten oder Tätigkeiten, die nicht vollständig innerhalb des ISMS-Anwendungsbereichs 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.

Falls die Zertifizierung auf branchenspezifische Normen verweisen soll, gilt Folgendes:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Die Zertifizierungsstelle muss sicherstellen, dass die SoA und der Risikobehandlungsprozess des Kunden gleichermaßen alle Maßnahmen der branchenspezifischen Norm wie die Maßnahmen in ISO/IEC 27001:2022, Anhang A berücksichtigen.

Der Anwendungsbereich der einzelnen branchenspezifischen Normen muss festgelegt werden und darf nicht über den Geltungsbereich der Zertifizierung nach ISO/IEC 27001 hinausgehen.

9.1.4 Ermittlung des Auditzeitaufwands

9.1.4.1 Allgemeines

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

9.1.4.2 Auditzeitaufwand

Die Zertifizierungsstelle muss Anhang B zur Bestimmung des Auditzeitaufwands verwenden.

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

9.1.5 Stichprobenprüfung an mehreren Standorten

9.1.5.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.5. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.5.2.

9.1.5.2 Mehrere Standorte

9.1.5.2.1 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;

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

9.1.5.2.2 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 Hauptsitzes (sofern zutreffend) und der Standorte;

   2) die Ergebnisse der Managementbewertung;

   3) Variationen der Größe der Standorte;

   4) Variationen des Geschäftszwecks der Standorte;

   5) Komplexität der Informationssysteme an den verschiedenen Standorten;

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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 Informationssystemen, die sensible Informationen verarbeiten;

10) jegliche unterschiedlichen rechtlichen Anforderungen;

11) geographische und kulturelle Aspekte;

12) Risikosituationen der Standorte;

13) Informationssicherheitsvorfälle an den jeweiligen Standorten.

c) Von allen vom Anwendungsbereich 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 an einem einzelnen Standort beobachteten Nichtkonformität betrifft das Verfahren für Korrekturmaßnahmen alle vom Zertifikat abgedeckten Standorte.

Das Audit muss die Tätigkeiten 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.

9.1.6 Mehrfach-Managementsysteme

9.1.6.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.1.6. Außerdem gelten die Anforderungen und der Leitfaden in 9.1.6.2 und 9.1.6.3.

9.1.6.2 Integration der Dokumentation des ISMS und anderer 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.

9.1.6.3 Kombination von Managementsystemaudits

Das ISMS-Audit darf mit Audits anderer Managementsysteme kombiniert werden, falls 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.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

9.2 Planung von Audits

9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien

9.2.1.1 Allgemeines

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

9.2.1.2 Auditziele

Die Auditziele müssen Folgendes umfassen:

a) Bestimmen der Wirksamkeit des Managementsystems;

b) Sicherstellen, dass der Kunde auf der Grundlage der Risikobeurteilung die erforderlichen Maßnahmen ermittelt hat; und

c) Bestimmen, ob die festgelegten Informationssicherheitsziele erreicht worden sind.

9.2.1.3 Auditkriterien

Die Kriterien zur Auditierung des ISMS eines Kunden müssen ISO/IEC 27001 einschließen. Die Auditkriterien dürfen um branchenspezifische Normen erweitert werden, die ISO/IEC 27001:2022, Anhang A, über eine zusätzliche Quelle von Referenzmaßnahmen zum Vergleich hinaus erweitern. In diesem Fall gilt Anhang F.

Andere für die durchgeführten Funktionen relevanten Dokumente dürfen zur Zertifizierung herangezogen werden.

9.2.2 Auswahl des Auditteams und Aufgabenzuordnung

9.2.2.1 Allgemeines

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

9.2.3 Auditplan

9.2.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.2.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.2.3.2, 9.2.3.3 und 9.2.3.4.

9.2.3.2 Allgemeine Betrachtungen

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

9.2.3.3 Fernauditverfahren

Das Ziel von Fernauditverfahren sollte auf der Verbesserung der Auditwirksamkeit und -effizienz liegen und darauf, die Integrität des Auditprozesses zu unterstützen.

Der Auditplan muss Werkzeuge aufführen, die zur Unterstützung der Fernaudits eingesetzt werden.

9.2.3.4 Zeitplanung des Audits

ANMERKUNG Es empfiehlt sich für eine Zertifizierungsstelle, die Zeitplanung des Audits, das den vollen Umfang der Organisation bestmöglich darstellt, mit der zu auditierenden Organisation zu vereinbaren. Betrachtungen können, sofern geeignet, Jahreszeit, Monat, Tag/Daten und Schichten umfassen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

9.3 Erstzertifizierung

9.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.3.2.

9.3.2 Erstzertifizierungsaudit

9.3.2.1 Stufe 1

In dieser Stufe des Audits muss die Zertifizierungsstelle die Dokumentation zur Gestaltung des ISMS beschaffen, die die nach ISO/IEC 27001 (und gegebenenfalls der branchenspezifischen Norm) erforderliche Dokumentation abdeckt.

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, gegebenenfalls der durch die branchenspezifische Norm, festgelegten ISMS-Dokumentation und, ggf., andere zugehörige Dokumentation.

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 soll für die Planung des Audits der Stufe 2 verwendet werden.

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

ANMERKUNG Die Tatsache, dass eine Person in der Zertifizierungsstelle, die nicht an dem Audit beteiligt ist, den Bericht überprüft, über die Fortsetzung entscheidet und die Kompetenz der Mitglieder des Auditteams für Stufe 2 bestätigt, bietet eine gewisse Risikominderung. 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.

9.3.2.2 Stufe 2

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

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

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

b) Bewertung der mit der Informationssicherheit zusammenhängenden Risiken und dass die Bewertungen bei Wiederholung konsistente, gültige und vergleichbare Ergebnisse erbringen;

c) Bestimmung der Maßnahmen basierend auf der Informationssicherheitsrisikobeurteilung und des Risikobehandlungsprozesses;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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

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

f) Umsetzung der Maßnahmen (siehe Anhang D; mit Beispielen für die Auditierung von Maßnahmen und, soweit vorhanden, ähnliche Anleitung in anderen Teilen der Normenreihe ISO/IEC 27006) müssen den externen und internen Kontext und die zugehörige Risiken sowie die Überwachung, Messung und Analyse der Informationssicherheitsverfahren und -maßnahmen der Organisation zur Bestimmung berücksichtigen, ob Maßnahmen, die als umgesetzt erklärt werden, umgesetzt wurden und wirksam sind;

g) 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.

9.4 Durchführen von Audits

9.4.1 Allgemeines

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

9.4.2 Spezifische Elemente des ISMS-Audits

Das Auditteam der 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) darlegen, 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 darlegen, ob die im Rahmen der Risikobeurteilung eingesetzten Verfahren gut fundiert und angemessen umgesetzt wurden.

9.4.3 Auditbericht

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

a) eine Darstellung des Zertifizierungsaudits der Informationssicherheitsrisikoanalyse des Kunden;

b) sämtliche von der Organisation für den Vergleich nach ISO/IEC 27001:2022, 6.1.3. c) eingesetzten Sätze von Maßnahmen.

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

a) wesentliche verfolgte Auditpfade und angewandte Auditmethoden (siehe 9.1.1.2);

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

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Ausgefüllte Fragebögen, Checklisten, Beobachtungen, Protokolle oder Auditornotizen können einen integralen Bestandteil des Auditberichts 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.

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

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

Der Bericht muss die Angemessenheit der internen Organisation und der vom Kunden 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.

— eine Zusammenfassung der wichtigsten Beobachtungen, sowohl positiver als auch negativer Art, in Bezug auf die Umsetzung und Wirksamkeit der ISMS-Anforderungen und Informationssicherheitsmaßnahmen enthalten.

9.5 Zertifizierungsentscheidung

9.5.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.5. Außerdem gelten die Anforderungen und der Leitfaden in 9.5.2.

9.5.2 Zertifizierungsentscheidung

Zusätzlich zu den Anforderungen der ISO/IEC 17021-1 muss die Zertifizierungsentscheidung auf der Zertifizierungsempfehlung des Auditteams beruhen, wie sie im Bericht über das Zertifizierungsaudit vorgelegt wird (siehe 9.4.3).

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 17021-1:2015, 9.6.1.

9.6.2 Überwachungstätigkeiten

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

9.6.2.2 Überwachungsauditverfahren müssen eine Teilmenge der Verfahren für das Zertifizierungsaudit des ISMS des Kunden sein, wie in diesem Dokument dargelegt.

Zweck der Überwachung ist die Überprüfung, ob das freigegebene ISMS weiterhin umgesetzt wird, die Betrachtung der Auswirkungen von Änderungen dieses ISMS, die aufgrund von Änderungen in den betrieblichen Abläufen des Kunden vorgenommen wurden, und die Bestätigung der fortlaufenden Einhaltung der Zertifizierungsanforderungen. Überwachungsauditprogramme müssen mindestens Folgendes abdecken:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

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

b) Mitteilungen externer Parteien, wie von ISO/IEC 27001 und anderen für die Zertifizierung erforderlichen Dokumenten gefordert;

9.6.2.3 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 Erklärung zur Anwendbarkeit (SoA, en: Statement of Applicability);

d) Umsetzung und Wirksamkeit der im Auditprogramm angegebenen Maßnahmen.

9.6.2.4 Die Zertifizierungsstelle muss in der Lage sein, ihr Programm der Überwachungstätigkeiten anzupassen, um die Informationssicherheitsprobleme in Bezug auf die Risiken und Auswirkungen auf den Kunden zu berücksichtigen und dieses Programm zu begründen.

Überwachungsaudits dürfen mit den Audits anderer Managementsysteme kombiniert werden. Auditberichte müssen die für jedes Managementsystem relevanten Aspekte eindeutig kennzeichnen.

Im Rahmen von Überwachungsaudits müssen Zertifizierungsstellen die Aufzeichnungen von den der Zertifizierungsstelle vorgelegten Einsprüchen 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, die Version der SoA und wichtige Änderungen seit dem letzten Audit enthalten. Die aus der Überwachung stammenden Berichte müssen insgesamt mindestens die Anforderungen aus 9.6.2.2 und 9.6.2.3 abdecken.

9.6.3 Re-Zertifizierung

9.6.3.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.6.3. Außerdem gelten die Anforderungen und der Leitfaden in 9.6.3.2.

9.6.3.2 Re-Zertifizierungsaudits

Re-Zertifizierungsauditverfahren müssen eine Teilmenge der Verfahren für das Erstzertifizierungsaudit des ISMS des Kunden, wie in diesem Dokument dargelegt, sein.

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 17021-1:2015, 9.6.4.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung

9.6.5.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.6.5. Außerdem gelten die Anforderungen und der Leitfaden in 9.6.5.2.

9.6.5.2 Auswirkungen auf branchenspezifische Normen

Falls die Zertifizierung branchenspezifische Normen einschließt, gilt Folgendes:

Die Zertifizierungsstelle muss eindeutig bestimmen, ob die Reduzierung des Geltungsbereiches der Zertifizierung den geltenden Anwendungsbereich der branchenspezifischen Norm beeinflusst.

9.7 Einsprüche

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.7.

9.8 Beschwerden

9.8.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.8. Außerdem gelten die Anforderungen und der Leitfaden in 9.8.2.

9.8.2 Beschwerden

Beschwerden stellen potenzielle Vorfälle und Anzeichen für mögliche Nichtkonformitäten dar.

9.9 Aufzeichnungen zu Kunden

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 9.9.

10 Managementsystemanforderungen für Zertifizierungsstellen

10.1 Optionen

10.1.1 Allgemeines

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 10.1. Außerdem gelten die Anforderungen und der Leitfaden in 10.1.2.

10.1.2 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 17021-1:2015, 10.2.

10.3 Option B: Managementsystemanforderungen in Übereinstimmung mit ISO 9001

Es gelten die Anforderungen nach ISO/IEC 17021-1:2015, 10.3.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Anhang A
(normativ)

Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung

A.1 Übersicht

Tabelle A.1 legt Wissen und Fertigkeiten fest, die eine Zertifizierungsstelle für spezielle Funktionen zusätzlich zu den Anforderungen nach ISO/IEC 17021-1 festlegen muss. „X“ weist darauf hin, dass die Zertifizierungsstelle die Kriterien und den Umfang des Wissens und der Fertigkeiten festlegen muss. Die in Tabelle A.1 spezifizierten Anforderungen an Wissen und Fertigkeiten werden im relevanten Text in Abschnitt 7 ausgeführt, worauf mithilfe der Nummer in Klammern verwiesen wird.

Tabelle A.1 — Tabelle zum Wissen und zu den Fertigkeiten für ISMS-Audits und -Zertifizierung

Zertifizierungsfunktion Wissen und Fertigkeiten	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 Zertifizierungsentscheidungen	Auditierung und Leitung des Auditteams
Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren		X (siehe 7.1.3.3.2)	X (siehe 7.1.3.1.2)
Normen/normative Dokumente in Bezug auf Informationssicherheitsmanagementsysteme		X (siehe 7.1.3.3.3)	X (siehe 7.1.3.1.3)
Praktische Unternehmensführung			X (siehe 7.1.3.1.4)
Geschäftsfeld des Kunden	X (siehe 7.1.3.2.1)	X (siehe 7.1.3.3.4)	X (siehe 7.1.3.1.5)
Produkte, Prozesse und Organisation des Kunden	X (siehe 7.1.3.2.2)	X (siehe 7.1.3.3.5)	X (siehe 7.1.3.1.6)

ANMERKUNG Weitere Überlegungen zur Zuständigkeit sind in Anhang G enthalten.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Anhang B
(normativ)

Auditzeitaufwand

B.1 Einleitung

Dieser Anhang enthält weitere, mit ISO/IEC 17021-1:2015, 9.1.4, zusammenhängende Anforderungen. Dieser Anhang enthält die Mindestanforderungen und Anleitung für eine Zertifizierungsstelle zur Entwicklung ihrer eigenen Verfahren zur Bestimmung der Zeitdauer, die für die Zertifizierung der Anwendungsbereiche der ISMS für verschiedene Größen und Komplexitätsgrade über eine breite Palette an Tätigkeiten erforderlich ist.

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

Zertifizierungsstellen müssen den für die Erstzertifizierung, Überwachung und Re-Zertifizierung erforderlichen Auditzeitaufwand für jeden Kunden und jedes zertifizierte ISMS bestimmen. Die Anwendung dieses Anhangs während der Auditplanungsphase führt zu einem einheitlichen Ansatz bei der Bestimmung des angemessenen Auditzeitaufwands. Außerdem darf der Auditzeitaufwand auf Grundlage der Ergebnisse während des Audits angepasst werden, insbesondere in Stufe 1 (z. B. unterschiedliche Bewertung der Komplexität des ISMS-Anwendungsbereichs oder zusätzliche Standorte im Anwendungsbereich).

Dieser Anhang stellt Folgendes dar:

— Konzepte, die für die Berechnung des Auditzeitaufwands verwendet werden (B.2);

— Anforderungen an Verfahren zur Bestimmung des Auditzeitaufwands für die verschiedenen Phasen des Erstaudits (B.3);

— Anforderungen an den Auditzeitaufwand für Überwachungs- und Re-Zertifizierungsaudits (B.4 bzw. B.5);

— Anforderungen in Bezug auf Audits mehrerer Standorte (B.6);

— Anforderungen an den Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs (B.7) und an branchenspezifische Normen (B.8).

Beispiele für die Berechnung des Auditzeitaufwands zur Verdeutlichung der Anwendung von Anhang B sind in Anhang C enthalten.

Eine grundlegende Annahme des Ansatzes in diesem Anhang besteht darin, dass ein Berechnungsplan zur Bestimmung des Auditzeitaufwands Folgendes leisten sollte:

a) er sollte nur Attribute berücksichtigen, die begründet werden können;

b) er sollte einfach genug sein, um von Zertifizierungsstellen effizient verwendet werden zu können;

c) er sollte komplex genug sein, um eine ausreichende Unterscheidung zu ermöglichen.

Die Bestimmung des Auditzeitaufwands basiert auf den in der folgenden Tabelle B.1 („Auditzeitaufwandstabelle“) dargelegten Zahlen und muss zur Anpassung beitragende Faktoren berücksichtigen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Falls die Zertifizierung branchenspezifische Normen einschließt, gilt Folgendes:

Die Zertifizierungsstelle muss die Anforderungen an den Auditzeitaufwand für jede Audittätigkeit festlegen und über ein Verfahren zur Berechnung der Auditzeit auf der Grundlage der branchenspezifischen Norm verfügen. Sowohl die Methodik als auch die einzelnen Berechnungen müssen dokumentiert werden (siehe B.8).

Der für die branchenspezifische Norm erforderliche Auditzeitaufwand muss unabhängig berechnet werden. Siehe B.8 und 9.1.4.2 sowie gegebenenfalls den entsprechenden Teil der Normenreihe ISO/IEC 27006 zu weiteren Informationen.

B.2 Konzepte

B.2.1 Anzahl der von der Organisation gesteuerten Personen

Die Gesamtzahl der Personen, die in allen Schichten von der Organisation im Geltungsbereich der Zertifizierung gesteuert werden, ist der Ausgangspunkt für die Bestimmung des Auditzeitaufwands.

ANMERKUNG Zu den Personen, die unter der Steuerung der Organisation Tätigkeiten verrichten, zählen alle Mitarbeiter (unabhängig davon, ob sie der Organisation angehören oder nicht) im Geltungsbereich der Zertifizierung, die verpflichtet sind, nach den Anforderungen des ISMS zu arbeiten.

Teilzeitbeschäftigte, die von der Organisation gesteuert werden, tragen gegenüber einem Vollzeitbeschäftigten, der von der Organisation gesteuert wird, proportional zur Anzahl ihrer Arbeitsstunden im Verhältnis der Arbeitsstunden der von der Organisation gesteuerten Vollzeitbeschäftigten bei. Diese Ermittlung muss von der Anzahl der mit einem Vollzeitangestellten verglichenen Arbeitsstunden abhängen.

Wenn ein hoher Prozentsatz von Personen, die von der Organisation innerhalb des Geltungsbereichs der Zertifizierung gesteuert werden, bestimmte identische Tätigkeiten durchführt, ist eine geringere Anzahl an Personen vor Verwendung von Tabelle B.1 für die Berechnung des Auditzeitaufwands zulässig. Zertifizierungsstellen müssen die in B.3.4 genannten Faktoren verwenden und den Einfluss der Tätigkeiten auf das Informationssicherheitsrisiko berücksichtigen, um zu bestimmen, wie eine Verringerung der Anzahl an Personen innerhalb des Geltungsbereichs der Zertifizierung umgesetzt wird. Stringente(s) und widerspruchsfreie(s) Verfahren, das/die wiederholbar und auf unternehmensindividueller Basis anwendbar ist/sind, müssen dokumentiert werden.

B.2.2 Auditortag

Der in der Tabelle referenzierte „Auditzeitaufwand“ wird in auf das Audit verwendeten „Auditortagen“ ausgedrückt. Die Grundlage der Berechnung in Anhang B ist ein Acht-Stunden-Arbeitstag.

B.2.3 Temporärer Standort

Ein temporärer Standort ist ein von den in den Zertifizierungsdokumenten bestimmten Standorten abweichender Ort, an dem über einen festgelegten Zeitraum Tätigkeiten im Geltungsbereich der Zertifizierung umgesetzt werden. Diese Standorte können von größeren Projektmanagementstandorten bis zu kleineren Dienstleistungs-/Installationsstandorten reichen. Der Bedarf des Besuchs derartiger Standorte und das Ausmaß der Stichprobenahme sollten auf einer Beurteilung der Risiken der Nichterfüllung der Informationssicherheitsziele aufgrund einer vom temporären Standort ausgehenden Nichtkonformität basieren. Die Auswahl der derartigen ausgewählten Standorte sollte die Breite des Kompetenzbedarfs der Organisation sowie Dienstleistungsvariationen im Hinblick auf die Größen und Arten von Tätigkeiten sowie die verschiedenen Phasen laufender Projekte darstellen. Bezüglich allgemeiner Probennahme siehe 9.1.5.2.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

B.3 Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit

B.3.1 Allgemeines

Die Zertifizierungsstelle muss über ein dokumentiertes Verfahren zur Berechnung des Auditzeitaufwands verfügen und dieses befolgen.

B.3.2 Methoden zur Durchführung von Fernaudits

Falls Fernauditmethoden, z. B. interaktive webbasierte Zusammenarbeit, Webmeetings, Telefonkonferenzen und/oder elektronische Überprüfung der Verfahren der Organisation, angewandt werden, um Schnittstellen zur Organisation zu bilden, sollten diese Tätigkeiten im Auditplan (siehe 9.2.3) gekennzeichnet werden. Sie dürfen als Teilbeitrag zum gesamten „Vor-Ort-Auditzeitaufwand“ betrachtet werden.

ANMERKUNG Der Vor-Ort-Auditzeitaufwand bezieht sich auf den Vor-Ort-Auditzeitaufwand, der einzelnen Standorten zugewiesen wurde. Elektronische Audits von fernen Standorten werden als Fernaudits betrachtet, selbst wenn die elektronischen Audits physisch in den Räumlichkeiten der Organisation ausgeführt werden.

B.3.3 Berechnung des Auditzeitaufwands

Die folgende Auditzeitaufwandstabelle legt den Startpunkt für eine durchschnittliche Anzahl von Tagen für das Erstaudit (hier und im Folgenden umfasst diese Anzahl die Tage für ein Erstaudit (Stufe 1 und Stufe 2)) fest, die erfahrungsgemäß für einen ISMS-Anwendungsbereich mit einer gegebenen Anzahl von der Organisation gesteuerter Personen angemessen ist. Die Erfahrung hat auch gezeigt, dass bei ISMS-Anwendungsbereichen einer ähnlichen Größe manche mehr und manche weniger Zeit benötigen.

Die nachstehende Auditzeitaufwandtabelle gibt den Rahmen vor, der für die Auditplanung verwendet werden muss. Der Ausgangspunkt basiert auf der Gesamtzahl der Personen, die unter der Steuerung der Organisation in allen Schichten arbeiten. Die Anzahl der Auditortage wird auf der Grundlage der wesentlichen Faktoren, die für den zu auditierenden Anwendungsbereich des ISMS gelten, angepasst, wobei für jeden Faktor eine additive oder subtraktive Gewichtung vorgenommen wird, um die Basiszahl zu ändern. Diese Auditzeitaufwandstabelle muss unter Berücksichtigung der beitragenden Faktoren und Einschränkungen der zulässigen Abweichung (siehe nachfolgend B.3.5 und B.3.6) angewandt werden. Die in dieser Tabelle verwendeten Begriffe werden im voranstehenden Abschnitt B.2 erläutert, und Anhang C enthält Beispiele zur Anwendung.

B.3.4 Bestimmung der ursprünglichen Personenanzahl

Zertifizierungsstellen müssen vom Kunden Informationen zu einer großen Anzahl an Personen, die bestimmte identische Tätigkeiten verrichten, einholen und Folgendes berücksichtigen:

— Anzahl der an der Tätigkeit beteiligten Personen;

— Art der Tätigkeit oder des Prozesses.

Beispiele für Faktoren, die eine geringere Personenanzahl als Berechnungsgrundlage für die Personen, die bestimmte identische Tätigkeiten verrichten, zulassen, u. a.:

— Personen mit reinem Lesezugriff auf Informationen zur Erfüllung ihrer Aufgaben;

— Personen ohne Zugang zur IT-Infrastruktur der Organisation;

— Personen mit einem spezifischen, nachweislich eingeschränkten Zugang zur IT-Infrastruktur des Unternehmens.

Die Verringerung der Anzahl an Personen, die bestimmte identische Tätigkeiten ausführen, muss auf der Grundlage des Risikos der mit den Aufgaben verbundenen Tätigkeiten erfolgen, und die Quadratwurzel aus der Anzahl der Personen, die dieselben Aufgaben ausführen, kann zur Bestimmung der effektiven Anzahl an

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Personen herangezogen werden, die für die Berechnung des Auditzeitaufwands zu verwenden ist – dies muss die höchstzulässige Verringerung der Anzahl an Personen sein.

Beachtung muss jedoch auch der Art der Aufgaben und Informationen geschenkt werden, auf die sie Zugriff haben; dies könnte die Verringerung einschränken. Die nach diesem Verfahren bestimmte Personenanzahl ist der Ausgangspunkt für die Tabelle B.1.

Tabelle B.1 — Auditzeitaufwandstabelle

Anzahl der von der Organisation gesteuerten Personen	Auditzeitaufwand für das Erstaudit des Qualitäts-management-systems (Auditortage)	Auditzeitaufwand für das Erstaudit des Umweltmanagement-systems (Auditortage)	ISMS-Audit-zeitaufwand für das Erstaudit (Auditortage)	Additive und subtraktive Faktoren	Gesamtaudit-zeitaufwand
1~10	1.5–2	2.5–3	5	Siehe B.3.5	
11~15	2.5	3.5	6	Siehe B.3.5	
16~25	3	4.5	7	Siehe B.3.5	
26~45	4	5.5	8.5	Siehe B.3.5	
46~65	5	6	10	Siehe B.3.5	
66~85	6	7	11	Siehe B.3.5	
86~125	7	8	12	Siehe B.3.5	
126~175	8	9	13	Siehe B.3.5	
176~275	9	10	14	Siehe B.3.5	
276~425	10	11	15	Siehe B.3.5	
426~625	11	12	16.5	Siehe B.3.5	
626~875	12	13	17.5	Siehe B.3.5	
876~1 175	13	15	18.5	Siehe B.3.5	
1 176~1 550	14	16	19.5	Siehe B.3.5	
1 551~2 025	15	17	21	Siehe B.3.5	
2 026~2 675	16	18	22	Siehe B.3.5	
2 676~3 450	17	19	23	Siehe B.3.5	
3 451~4 350	18	20	24	Siehe B.3.5	
4 351~5 450	19	21	25	Siehe B.3.5	
5 451~6 800	20	23	26	Siehe B.3.5	
6 801~8 500	21	25	27	Siehe B.3.5	
8 501~10 700	22	27	28	Siehe B.3.5	
> 10,700	Der obigen Entwicklung folgen	Der obigen Entwicklung folgen	Der obigen Entwicklung folgen	Siehe B.3.5	

B.3.5 Faktoren für die Anpassung des Auditzeitaufwands

Die Auditzeitaufwandtabelle darf nicht isoliert verwendet werden. Bei der zugeteilten Zeit müssen auch die folgenden Faktoren berücksichtigt werden, die mit der Komplexität des ISMS und daher mit dem für das Audit des ISMS erforderlichen Aufwand zusammenhängen:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

a) Komplexität des ISMS (z. B. Kritikalität der Information, mit dem ISMS verbundene Risiken usw.);

b) Art(en) der im ISMS-Anwendungsbereich getätigten Geschäfte;

c) zuvor demonstrierte Leistung des ISMS;

d) Umfang und Vielfältigkeit der bei der Umsetzung der verschiedenen Komponenten des ISMS angewandten Techniken (z. B. Anzahl der unterschiedlichen IT-Plattformen, Anzahl der getrennten Netzwerke);

e) Ausmaß der innerhalb des ISMS-Anwendungsbereichs angewandten Ausgliederung und Bestimmungen in Bezug auf Dritte;

f) Ausmaß der Informationssystementwicklung;

g) Anzahl der Standorte und Anzahl der Notfallwiederherstellungsstandorte (DR, en: Disaster Recovery);

h) nach Stufe 1 prüft die Zertifizierungsstelle die Anzahl und Komplexität der Maßnahmen;

i) bei Überwachungs- oder Re-Zertifizierungsaudits: Die Menge und das Ausmaß der für das ISMS in Übereinstimmung mit ISO/IEC 17021-1, 8.5.3, relevanten Änderungen.

Anhang C enthält Beispiele dazu, wie diese verschiedenen Faktoren bei der Berechnung der Auditzeit berücksichtigt werden können.

Beispiele für Faktoren, die zusätzlichen Auditzeitaufwand erfordern, sind:

— komplizierte Logistik, die mehr als ein Gebäude oder einen Standort im ISMS-Anwendungsbereich betrifft;

— Personal, das mehr als eine Sprache spricht (wodurch Dolmetscher erforderlich werden oder einzelne Auditoren nicht unabhängig arbeiten können), oder Dokumentation, die in mehr als einer Sprache vorliegt;

— Tätigkeiten, die den Besuch temporärer Standorte zur Bestätigung der Tätigkeiten an permanenten Standorten, deren Managementsystem zertifiziert werden soll, erfordern (siehe Absatz unter der nächsten Liste);

— große Anzahl an Normen und Vorschriften, die für das ISMS gelten.

Beispiele für Faktoren, die einen Abzug des Auditzeitaufwands zulässig machen, sind:

— Produkte/Prozesse ohne/mit geringem Risiko;

— Prozesse, die eine einzelne allgemeine Tätigkeit betreffen (z. B. ausschließlich Dienstleistungen);

— Vorkenntnisse in Bezug auf die Organisation (z. B. ob die Organisation bereits von derselben Zertifizierungsstelle nach einer anderen Norm zertifiziert wurde);

— gute Vorbereitung des Kunden auf die Zertifizierung (z. B. bereits zertifiziert oder durch ein anderes Programm dritter Parteien anerkannt);

— hoher Reifegrad des vorhandenen Managementsystems.

In Situationen, in denen der Zertifizierungskunde oder die zertifizierte Organisation sein(e) bzw. ihr(e) Produkt(e) oder Dienstleistungen an temporären Standorten anbietet/anbieten, ist es wichtig, dass Bewertungen derartiger Standorte in das Zertifizierungsaudit und Überwachungsprogramme aufgenommen werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Für die oben genannten Faktoren können Anpassungen vorgenommen werden. Faktoren, die eine Addition oder Subtraktion des Auditzeitaufwands erfordern, können sich gegenseitig ausgleichen. In allen Fällen, in denen Anpassungen an der in Tabelle B.1 vorgesehenen Zeit vorgenommen werden, müssen zur Begründung dieser Änderungen ausreichend Nachweise und Aufzeichnungen gepflegt werden.

B.3.6 Einschränkung der Abweichung von der Auditzeit

Zur Sicherstellung der Durchführung wirksamer Audits sowie zur Sicherstellung zuverlässiger und vergleichbarer Ergebnisse darf die in der Auditzeittabelle angegebene Auditzeit höchstens um 30 % verringert werden.

Angemessene Gründe für Abweichungen müssen festgelegt und dokumentiert werden.

B.3.7 Vor-Ort-Auditzeitaufwand

Es wird erwartet, dass die für die Planung und das Erstellen des Berichts berechnete Zeit üblicherweise nicht den gesamten „Vor-Ort-Auditzeitaufwand“ (physisch/virtuell) auf unter 70 % der nach B.3.3, B.3.4 und B.3.5 berechneten Zeit verringern sollte. Falls zusätzliche Zeit für die Planung und/oder das Erstellen des Berichts erforderlich ist, darf dies nicht als Rechtfertigung zur Reduzierung des Vor-Ort-Auditzeitaufwands dienen. Die Reisezeit des Auditors ist nicht Teil dieser Berechnung, sondern ist zusätzlich zu dem in der Tabelle referenzierten Auditzeitaufwand.

ANMERKUNG 70 % sind ein Faktor, der auf Erfahrung mit ISMS-Audits basiert.

B.4 Auditzeitaufwand für das Überwachungsaudit

Bei einem Erstzertifizierungsauditzyklus sollte der Überwachungszeitaufwand für eine gegebene Organisation proportional zum Zeitaufwand für das Erstaudit sein, wobei der Gesamtzeitaufwand, der jährlich auf die Überwachung verwendet wird, etwa ein Drittel des Zeitaufwands für das Erstaudit betragen sollte. Der geplante Überwachungszeitaufwand sollte gelegentlich überprüft werden, um Änderungen Rechnung zu tragen, die möglicherweise Auswirkungen auf den Auditzeitaufwand haben. Der für ein Überwachungsaudit benötigte Zeitaufwand muss erhöht werden, um das Audit der Änderungen am ISMS zu ermöglichen (etwa das Audit neuer oder geänderter Maßnahmen).

B.5 Auditzeitaufwand für das Re-Zertifizierungsaudit

Der Gesamtzeitaufwand für die Durchführung des Re-Zertifizierungsaudits muss, wie in 9.4.3 und ISO/IEC 17021-1:2015, 9.6.3, festgelegt, von den Ergebnissen jeglicher vorherigen Audits abhängen. Der Zeitaufwand für ein Re-Zertifizierungsaudit sollte proportional dazu sein, aber mindestens zwei Drittel des Zeitaufwands betragen, der für ein Erstzertifizierungsaudit derselben Organisation zum Zeitpunkt des Re-Zertifizierungsaudits erforderlich wäre.

B.6 Auditzeitaufwand für mehrere Standorte

Im Allgemeinen muss der Gesamtauditzeitaufwand für ein Vor-Ort-Audit anhand der Gesamtzahl der von der Organisation gesteuerten Personen berechnet werden, unabhängig von ihrem Standort.

Aus berechtigten Gründen, die zu dokumentieren sind, ist alternativ eine Addierung der Auditzeiten, die für jeden Standort einzeln berechnet werden, zulässig, sofern diese Gesamtauditzeit größer ist als die nach dem ersten Absatz dieses Abschnitts festgelegte. Reduzierungen dürfen vorgenommen werden, um Teile des Audits zu berücksichtigen, die für den Hauptsitz oder (gegebenenfalls) die lokalen Standorte nicht relevant sind. Gründe für derartige Reduzierungen müssen von der Zertifizierungsstelle aufgezeichnet werden.

Die Gesamtzahl der Vor-Ort-Auditortage, wie diese für den Geltungsbereich nach der in B.3.3 und B.3.4 sowie diesem Abschnitt angegebenen Vorgehensweise berechnet wurde, muss den verschiedenen Standorten nach der Relevanz des Standorts für das Managementsystem, der am Standort durchgeführten Tätigkeiten und der identifizierten Risiken zugeteilt werden. Die Gründe für die Zuteilung müssen von der Zertifizierungsstelle aufgezeichnet werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

B.7 Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs

Der für die Erweiterung des Anwendungsbereichs eines ISMS erforderliche Auditzeitaufwand muss auf Grundlage der Art der Erweiterung, der Tätigkeit(en) der aktuellen Zertifizierung, der Anzahl der Standorte, an denen die Tätigkeit(en) verrichtet wird/werden, der mit der/den Tätigkeiten(en) verbundenen Informationssicherheitsrisiken, der Anzahl der für die Erweiterung relevanten Maßnahmen, der Anzahl der von der Organisation gesteuerten Personen im neuen Anwendungsbereich, des Zeitaufwands für die Überprüfung der Integration des erweiterten Anwendungsbereichs in das ISMS usw. berechnet werden.

Zertifizierungsstellen müssen über Verfahren verfügen, die einen einheitlichen Ansatz für die Erweiterung des Anwendungsbereichs bieten.

Für das Erstaudit des neuen Anwendungsbereichs muss der Zeitaufwand basierend auf der Anzahl an Personen und Standorten im Anwendungsbereich nach B.3.3, B.3.4 und B.3.5 berechnet werden.

Es muss zur berechneten Dauer für die Überprüfung des ISMS des Kunden Auditzeitaufwand addiert werden. Dieser zusätzliche Zeitaufwand muss mindestens einen halben Tag betragen, falls das Audit des erweiterten Anwendungsbereichs gleichzeitig mit dem ISMS-Audit durchgeführt wird, bzw. einen Tag, wenn die Erweiterung eigenständig durchgeführt wird.

B.8 Auditzeitaufwand für eine branchenspezifische Norm

Falls das Audit für die branchenspezifische Norm zusammen mit einem Audit derselben Art (z. B. Erstaudit, Überwachungsaudit) für ISO/IEC 27001 durchgeführt wird, ist der Gesamtauditzeitaufwand die Summe des Auditzeitaufwands für das ISMS nach ISO/IEC 27001 und des Auditzeitaufwands für die branchenspezifische Norm.

Falls jedoch das Audit für die branchenspezifische Norm nicht zusammen mit einem Audit derselben Art (z. B. Erstaudit, Überwachungsaudit) durchgeführt wird, bleibt der Auditzeitaufwand für das ISMS nach ISO/IEC 27001 unverändert, während der Auditzeitaufwand für die branchenspezifische Norm um mindestens einen halben Tag vergrößert wird, um die Schnittstellen und die Ausrichtung der Erweiterung am ISMS sowie insbesondere die Informationssicherheitsrisikobeurteilung, internen Audits und Managementbewertung zu verifizieren.

Soweit ein eigenständiges branchenspezifisches Audit erforderlich erscheint, darf dieses nur für die Erweiterung des Zertifikats (Stufe 1 und Stufe 2) durchgeführt werden.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05

Anhang C
(informativ)

Methoden für Berechnungen des Auditzeitaufwands

C.1 Allgemeines

Dieser Anhang enthält weitere Anleitung zur Herleitung einer Formel für die Berechnung des Auditzeitaufwands. C.2 enthält ein Beispiel der Klassifizierung von Faktoren, die als Grundlage für die Berechnung des Auditzeitaufwands herangezogen werden können, und C.3 enthält ein Beispiel für die Berechnung des Auditzeitaufwands.

ANMERKUNG Dieser Anhang beginnt nach der Anwendung etwaiger Reduzierungen für Personen, die bestimmte identische Tätigkeiten ausüben, wie unter B.3.4 beschrieben.

C.2 Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands

Tabelle C.1 enthält Beispiele für die Klassifizierung der wesentlichen Faktoren für die Berechnung des Auditzeitaufwands, wie in B.3.5, a) bis h), aufgelistet. Diese Klassifizierung kann von Zertifizierungsstellen zur Herleitung eines mit 9.1.4.2 übereinstimmenden Berechnungsplans für den Auditzeitaufwand verwendet werden:

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2023-05