DIN EN ISO/IEC 27006-1

ICS 03.120.20; 35.030

Einsprüche bis 2022-09-15
Vorgesehen als Ersatz für
DIN EN ISO/IEC 27006:2021-05

Entwurf

Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren – Teil 1: Allgemeines (ISO/IEC DIS 27006-1:2022); Deutsche und Englische Fassung prEN ISO/IEC 27006-1:2022

Requirements for bodies providing audit and certification of information security management systems –
Part 1: General (ISO/IEC DIS 27006-1:2022);
German and English version prEN ISO/IEC 27006-1:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-07-15 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 125 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Nationales Vorwort

Der Text von ISO/IEC DIS 27006-1:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27006-1:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

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

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

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.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 9001, *Qualitätsmanagementsysteme — Anforderungen*

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

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

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

— Leerseite —

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

– Entwurf –

2022-07

prEN ISO/IEC 27006-1:2022

Titel de:	Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren — Teil 1: Allgemeines (ISO/IEC DIS 27006-1:2022)
Titel en:	Requirements for bodies providing audit and certification of information security management systems — Part 1: General (ISO/IEC DIS 27006-1:2022)
Titel fr:	

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Inhalt

Seite

Europäisches Vorwort 5

Vorwort 6

Einleitung 7

1 Anwendungsbereich 8

2 Normative Verweisungen 8

3 Begriffe 8

4 Grundsätze 12

5 Allgemeine Anforderungen 12
5.1 Rechts- und Vertragsfragen 12
5.2 Handhabung der Unparteilichkeit 12
5.2.1 IS 5.2 Interessenkonflikte 12
5.3 Haftung und Finanzierung 13

6 Strukturelle Anforderungen 13

7 Anforderungen an Ressourcen 13
7.1 Kompetenz des Personals 13
7.1.1 IS 7.1.1 Allgemeine Betrachtungen 13
7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien 13
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist 17
7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren 17
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten 18
7.3.1 IS 7.3 Einsatz einzelner externer Auditoren und externer Fachexperten als Teil des Auditteams 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 IS 8.2 ISMS-Zertifizierungsdokumente 18
8.3 Verweisung auf Zertifizierung und Zeichennutzung 19
8.4 Vertraulichkeit 19
8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation 19
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden 19
8.5.1 IS 8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden 19

9 Anforderungen an Prozesse 20
9.1 Tätigkeiten vor der Zertifizierung 20
9.1.1 Antrag 20
9.1.2 Antragsprüfung 20
9.1.3 Auditprogramm 20
9.1.4 Ermittlung des Auditzeitaufwands 22
9.1.5 Stichprobenprüfung an mehreren Standorten 22
9.1.6 Mehrfach-Managementsysteme 24
9.2 Planung von Audits 24
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien 24

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

9.2.2 Auswahl des Auditteams und Aufgabenzuordnung 25
9.2.3 Auditplan 26
9.3 Erstzertifizierung 26
9.3.1 IS 9.3.1 Erstzertifizierungsaudit 26
9.4 Durchführen von Audits 28
9.4.1 IS 9.4 Allgemeines 28
9.4.2 IS 9.4 Spezifische Elemente des ISMS-Audits 28
9.4.3 IS 9.4 Auditbericht 28
9.5 Zertifizierungsentscheidung 29
9.5.1 IS 9.5 Zertifizierungsentscheidung 29
9.6 Aufrechterhaltung der Zertifizierung 30
9.6.1 Allgemeines 30
9.6.2 Überwachungstätigkeiten 30
9.6.3 Re-Zertifizierung 31
9.6.4 Audits aus besonderem Anlass 31
9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung 31
9.7 Einsprüche 31
9.8 Beschwerden 32
9.8.1 IS 9.8 Beschwerden 32
9.9 Aufzeichnungen zu Kunden 32

10 Managementsystemanforderungen für Zertifizierungsstellen 32
10.1 Optionen 32
10.1.1 IS 10.1 ISMS-Umsetzung 32
10.2 Option A: Allgemeine Managementsystemanforderungen 32
10.3 Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001 32

Anhang A (informativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung 33
A.1 Übersicht 33
A.2 Allgemeine Kompetenzbetrachtungen 33
A.3 Spezielle Betrachtungen zu Wissen und Erfahrung 34
A.3.1 Typisches Wissen in Bezug auf ISMS 34

Anhang B (normativ) Auditzeitaufwand 35
B.1 Einleitung 35
B.2 Konzepte 36
B.2.1 Anzahl der von der Organisation gesteuerten Personen 36
B.2.2 Auditortag 36
B.2.3 Temporärer Standort 36
B.3 Verfahren zur Bestimmung des Auditzeitaufwands für das Erstaudit 36
B.3.1 Allgemeines 36
B.3.2 Methoden aus der Ferne zur Durchführung von Audits 36
B.3.3 Berechnung des Auditzeitaufwands 37
B.3.4 Faktoren für die Anpassung des Auditzeitaufwands 38
B.3.5 Einschränkung der Abweichung von der Auditzeit 40
B.3.6 Vor-Ort-Auditzeitaufwand 40
B.4 Auditzeitaufwand für das Überwachungsaudit 40
B.5 Auditzeitaufwand für das Re-Zertifizierungsaudit 40
B.6 Auditzeitaufwand für mehrere Standorte 40
B.7 Auditzeitaufwand bei Erweiterungen des Anwendungsbereichs 41
B.8 Auditzeitaufwand für eine branchenspezifische Normerweiterung 41

Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands 42
C.1 Allgemeines 42
C.2 Klassifizierung von Faktoren für die Berechnung des Auditzeitaufwands 42
C.3 Beispiel für die Auditzeitaufwandberechnung 44

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2022, Anhang A **47**
D.1 Zweck **47**
D.2 Anwendung von Tabelle D.1 ..... **47**
D.2.1 Allgemeines **47**
D.2.2 Spalte „Systemprüfung“ **47**
D.2.3 Spalte „Sichtprüfung“ **48**
D.2.4 Spalte „Typischer Nachweis der Gestaltung und Umsetzung von Maßnahmen“ **48**
Anhang E (informativ) Anforderungen und Einschränkungen bei Zertifizierungen nach branchenspezifischen Normerweiterungen **64**
E.1 Allgemeines **64**
Literaturhinweise **65**

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Europäisches Vorwort

Der Text von ISO/IEC DIS 27006-1:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27006-1:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC DIS 27006-1:2022 wurde von CEN als prEN ISO/IEC 27006-1:2022 ohne irgendeine Abänderung genehmigt.

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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

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

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

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

Bezüglich einer Erklärung der Bedeutung ISO-spezifischer Ausdrücke im Zusammenhang mit Konformitätsbewertung sowie Informationen über die Einhaltung der Prinzipien der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT) seitens ISO siehe folgende URL: www.iso.org/iso/foreword.html.

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology*, SC 27, *Information security, cybersecurity and privacy protection*.

ISO/IEC 27006-1 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* erarbeitet.

Dieses Dokument ersetzt die zweite Ausgabe (ISO/IEC 27006:2015), die technisch überarbeitet wurde. Es wurde neu nummeriert und ist daher die erste Ausgabe von ISO/IEC 27006-1.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Einleitung

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

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

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

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

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

Die Zertifizierungsstelle darf neben Audits und Zertifizierungen nach ISO/IEC 27001 auch Audit- und Zertifizierungsleistungen entsprechend den branchenspezifischen Normerweiterungen von ISO/IEC 27001 anbieten.

ANMERKUNG Die Erweiterung von ISO/IEC 7001 hat durch Anwendung einer branchenspezifischen Norm kein vom ISMS unabhängiges Managementsystem zur Folge.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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. Sie dient hauptsächlich der Unterstützung der Akkreditierung von Zertifizierungsstellen, die ISMS-Zertifizierungen durchführen.

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

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

3 Begriffe

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

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

3.2
branchenspezifische Norm
en sector-specific standards
Norm, die Anhang A von ISO/IEC 27001 zur Unterstützung einer spezifischen Branche erweitert

Anmerkung 1 zum Begriff: Eine branchenspezifische Norm bietet Ergänzungen zu den Maßnahmen in ISO/IEC 27002 oder Anleitung dazu, welche Elemente im Organisationsumfeld, bei den Beteiligten, deren Bedürfnissen und Erwartungen zur Umsetzung der Anforderungen in ISO/IEC 27001 zu berücksichtigen sind, oder Anleitung zur Umsetzung von Maßnahmen.

Anmerkung 2 zum Begriff: Eine branchenspezifische Erweiterungsnorm von ISO/IEC 27001 stellt keine Änderung der Anforderungen nach ISO/IEC 27001, einschließlich Ergänzung und Modifizierung, dar.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

3.3
Maßnahme
en control
Mittel zur Veränderung von *Risiken* (3.10)

Anmerkung 1 zum Begriff: Maßnahmen umfassen Prozesse, Richtlinien, Geräte, Methoden oder anderweitige Handlungen, die *Risiken* (3.10) verändern.

Anmerkung 2 zum Begriff: Maßnahmen haben nicht immer den erwünschten oder angenommenen Veränderungseffekt.

[QUELLE: ISO/IEC 27000:2018, 3.14]

3.4
Maßnahmenziel
en control objective
Beschreibung dessen, was als Ergebnis umgesetzter *Maßnahmen* (3.3) erzielt werden soll

[QUELLE: ISO/IEC 27000:2018, 3.15]

3.5
externer Kontext
en external context
externes Umfeld, in dem die Organisation 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 auswirken;

— Beziehungen zu externen Stakeholdern sowie deren Auffassungen und Werte.

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

3.6
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]

3.7
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* (3.6) zu bedrohen

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

3.8
Informationssystem
en information system
Anwendungen, Dienste, informationstechnische Werte oder andere Information bearbeitende Komponenten

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

3.9
interner Kontext
en internal context
interne Umgebung, innerhalb derer die Organisation 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 in Kraft sind mit dem Ziel sie einzuhalten beziehungsweise sie zu erreichen;

— das Potenzial in Form von Ressourcen und Wissen (z. B. Kapital, Zeit, Menschen, Prozesse, Systeme und Technologien);

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

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

— die Organisationskultur;

— Standards, Leitfäden und Modelle, die von der Organisation übernommen worden sind;

— Gestalt und Ausmaß vertraglicher Beziehungen.

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

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

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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* (3.11) liefert die Grundlage für die Risikobewertung und die Entscheidungen im Zuge der *Risikobehandlung* (3.14).

Anmerkung 2 zum Begriff: Die *Risikoanalyse* (3.11) 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 in Bezug auf *Risiken* (3.10)

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

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

Anmerkung 1 zum Begriff: Die Risikobehandlung kann umfassen:

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

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

— Beseitigen der Risikoquelle;

— Verändern der Wahrscheinlichkeit;

— Verändern der Folgen;

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

— Beibehalten des Risikos im Rahmen einer fundierten Wahl.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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 verändern.

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

4 Grundsätze

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

5 Allgemeine Anforderungen

5.1 Rechts- und Vertragsfragen

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

5.2 Handhabung der Unparteilichkeit

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

5.2.1 IS 5.2 Interessenkonflikte

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

a) Organisation von Schulungen und die Teilnahme daran als Ausbilder, vorausgesetzt, dass sich die Zertifizierungsstellen in Fällen, in denen sich die Schulungen auf das Informationssicherheitsmanagement, dazugehörige Managementsysteme oder Audits beziehen, auf die Bereitstellung von generischen, öffentlich zugänglichen Informationen und Ratschlägen beschränken müssen, d. h. sie dürfen keine unternehmensspezifischen Ratschläge geben;

b) Bereitstellung oder Veröffentlichung von Informationen auf Anfrage, die das Verständnis der Anforderungen von Zertifizierungsauditnormen durch die Zertifizierungsstelle darlegen;

c) dem Audit vorangehende Tätigkeiten, deren ausschließliches Ziel die Bestimmung der Bereitschaft für ein Zertifizierungsaudit ist. Derartige Tätigkeiten dürfen allerdings nicht zu Empfehlungen oder Ratschlägen führen, die diesem Abschnitt zuwiderliefen, und die Zertifizierungsstelle muss in der Lage sein zu bestätigen, dass derartige Tätigkeiten diesen Anforderungen nicht zuwiderlaufen und dass sie nicht zur Begründung der Reduzierung der letztendlichen Dauer des Zertifizierungsaudits genutzt werden;

d) Durchführung von Zweit- und Drittparteienaudits nach Normen oder Bestimmungen, die nicht Teil des Akkreditierungsgeltungsbereichs sind;

e) 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.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

5.3 Haftung und Finanzierung

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

6 Strukturelle Anforderungen

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

7 Anforderungen an Ressourcen

7.1 Kompetenz des Personals

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

7.1.1 IS 7.1.1 Allgemeine Betrachtungen

7.1.1.1 Allgemeine Kompetenzanforderungen

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

Die Zertifizierungsstelle muss die Kompetenzanforderungen für jede Zertifizierungsfunktion definieren, wie in ISO/IEC 17021-1, Tabelle A.1, angegeben. Die Zertifizierungsstelle muss alle in ISO/IEC 17021-1 und 7.1.2 und 7.2.1 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. Zu branchenspezifischen Anforderungen an die Kompetenz siehe den entsprechenden Teil der Normenreihe ISO/IEC 27006 (z. B. ISO/IEC 27006-2 zu Managementsystemen für Datenschutzinformationen).

Falls kein Teil der Normenreihe ISO/IEC 27006 anwendbar 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.

7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien

7.1.2.1 Kompetenzanforderungen für ISMS-Audits

7.1.2.1.1 Allgemeine Anforderungen

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

a) Kenntnis der Informationssicherheit;

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

c) Kenntnis der Managementsysteme;

d) Kenntnis der Auditgrundsätze;

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

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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

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

7.1.2.1.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

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

a) ISMS-spezifische Dokumentationsstrukturen, Hierarchie und Wechselbeziehungen;

b) Informationssicherheitsrisikobewertung und -risikomanagement;

c) auf ISMS anwendbare Prozesse.

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

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

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

7.1.2.1.3 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 27002 (und sofern zutreffend auch aus einschlägigen branchenspezifischen Normen) und ihre Umsetzung.

7.1.2.1.4 Praktische Unternehmensführung

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

a) gute Branchenverhaltensweisen in Bezug auf Informationssicherheit und Informationssicherheitsverfahren;

b) Politiken, Richtlinien und betriebliche Anforderungen für Informationssicherheit;

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

d) Managementprozesse und zugehörige Terminologie.

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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

b) mit dem Geschäftsfeld zusammenhängende Informationssicherheitsrisiken;

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

d) relevante Geschäftsfeldpraktiken.

Kriterium a) darf im Auditteam verteilt sein.

7.1.2.1.6 Produkte, Prozesse und Organisation des Kunden

Die Mitglieder des Auditteams müssen gemeinschaftlich über folgendes Wissen verfügen:

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

b) komplexer Betrieb im Rahmen einer breiten Perspektive;

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

7.1.2.2 Anforderungen an die Kompetenz für die Durchführung der Antragsprüfung

7.1.2.2.1 Informationssicherheitsmanagementsystemnormen und normative Dokumente

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

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

7.1.2.2.2 Geschäftsfeld des Kunden

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

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

7.1.2.2.3 Produkte, Prozesse und Organisation des Kunden

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

a) 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.

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

7.1.2.3.1 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 Effektivität des Audits, insbesondere die fortdauernde Gültigkeit der Bestimmung der Schnittstellen, Abhängigkeiten und zugehörigen Risiken, zu verifizieren.

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

a) Managementsysteme allgemein;

b) Auditprozesse und -verfahren;

c) Auditgrundsätze, -praktiken und -verfahren.

7.1.2.3.2 Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren

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

a) die in 7.1.2.1.2 a), c) und d) aufgelisteten Punkte;

b) für die Informationssicherheit relevante gesetzliche und behördliche Anforderungen.

7.1.2.3.3 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.

7.1.2.3.4 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.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

7.1.2.3.5 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

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

7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren

Die Zertifizierungsstelle muss nachweisen, dass jeder Auditor zu jedem der folgenden Punkte 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 Nachweise;

d) aktuelle Aufzeichnungen der beruflichen Entwicklung;

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

7.2.1.1 Auswahl von Auditoren

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

a) über eine berufliche Ausbildung oder Schulung auf einem mit einer universitären Ausbildung vergleichbaren Niveau verfügt;

b) eine mindestens vierjährige praktische Vollzeitberufserfahrung im Bereich der Informationstechnologie vorweisen kann, bei der er mindestens zwei Jahre lang eine Rolle oder Funktion mit Bezug zu Informationssicherheit innehatte;

c) mindestens eine fünftägige Schulung erfolgreich absolviert hat, die ISMS-Audits und das Auditmanagement umfasst;

d) Erfahrung im Auditieren eines ISMS vor der Tätigkeit als Auditor zur Durchführung von ISMS-Audits gesammelt hat. Diese Erfahrung muss als Auditor-in-Ausbildung unter Überwachung durch einen ISMS-Evaluator (siehe ISO/IEC 17021-1:2015, 9.2.2.1.4) im Rahmen der Teilnahme an mindestens einem ISMS-Erstzertifizierungs- (Stufe 1 und Stufe 2) oder Re-Zertifizierungsaudit und mindestens einem Überwachungsaudit gesammelt worden sein. Diese Erfahrung muss in mindestens 10 ISMS-Vor-Ort-Audittagen und innerhalb der letzten 5 Jahre erlangt worden sein. Die Teilnahme muss Prüfungen der Dokumentation und Risikobeurteilungen, Umsetzungsbewertungen und Auditberichterstattung umfassen;

e) über relevante und aktuelle Erfahrung verfügt;

f) durch ständige berufliche Entwicklung aktuelles Wissen und Fertigkeiten mit Bezug zu auf Informationssicherheit und Audits pflegt;

g) über Kompetenz im Auditieren eines ISMS nach ISO/IEC 27001 verfügt.

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

7.2.1.2 Auswahl von Auditoren für die Teamleitung

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

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

7.3 Einsatz einzelner externer Auditoren und externer Fachexperten

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

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

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

7.4 Aufzeichnungen über Personal

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

7.5 Ausgliederung

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

8 Anforderungen an Informationen

8.1 Öffentliche Informationen

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

8.2 Zertifizierungsdokumente

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

8.2.1 IS 8.2 ISMS-Zertifizierungsdokumente

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

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

Die Zertifizierungsdokumente dürfen nur dann nationale und internationale branchenspezifische Normen als Quellen für Referenzmaßnahmen referenzieren, wenn:

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 27001:2013, 6.1.3 c), weggelassen hat;

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

b) eine Begründung für ausgeschlossene Referenzmaßnahmen wird in der Erklärung zur Anwendbarkeit nach ISO/IEC 27001:2013, 6.1.3 d), aufgeführt.

Die Referenz auf die Zertifizierungsdokumenten muss klar darstellen, dass diese nur als Quelle für Maßnahmensätze für Maßnahmen dienen, die in der Erklärung zur Anwendbarkeit referenziert werden, und nicht als Zertifizierung nach diesen Referenzen.

In Fällen, in denen der physische Standort für die Tätigkeiten der Organisation unerheblich ist, muss/müssen das/die Zertifizierungsdokument(e) angeben, dass alle Tätigkeiten der Organisation aus der Ferne durchgeführt wurden. Die Zertifizierungsdokumente müssen in diesem Fall sicherstellen, dass die Organisation eindeutig ist.

Falls die Zertifizierungsdokumente auf branchenspezifische Normerweiterungen verweisen, gilt Folgendes:

Das Ablaufdatum der Zertifizierung in Übereinstimmung mit einer branchenspezifischen Normerweiterung der Zertifizierung nach ISO/IEC 27001 darf nicht nach dem Ablaufdatum der Zertifizierung nach ISO/IEC 27001 liegen, für die die Erweiterung gilt.

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

Die Zertifizierungsstelle muss sicherstellen, dass alle für die Zertifizierungsdokumente nach ISO/IEC 27001 erforderlichen Änderungen auf die Zertifizierungsdokumente entsprechend der branchenspezifischen Normerweiterung von ISO/IEC 27001 (siehe 9.6.5.1) übertragen werden.

8.3 Verweisung auf Zertifizierung und Zeichennutzung

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

8.4 Vertraulichkeit

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

8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation

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

8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden

Es gelten die Anforderungen nach ISO/IEC 17021-1, 8.5. Zudem gelten die folgenden Anforderungen und Anleitungen.

8.5.1 IS 8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden

Falls die Zertifizierungsstelle Audits für branchenspezifische Erweiterungsnormen anbietet, gilt Folgendes:

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Die Zertifizierungsstelle muss sicherstellen, dass ihre Kunden sich der Möglichkeit und der damit verbundenen Auswirkungen bewusst sind, so auditiert zu werden, dass sie nur Konformität mit ISO/IEC 27001 angeben oder dass sie Konformität sowohl mit ISO/IEC 27001 als auch mit der branchenspezifischen Erweiterungsnorm angeben.

9 Anforderungen an Prozesse

9.1 Tätigkeiten vor der Zertifizierung

9.1.1 Antrag

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

9.1.1.1 IS 9.1.1 Bereitschaft zum Antrag

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

9.1.2 Antragsprüfung

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

9.1.3 Auditprogramm

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

9.1.3.1 IS 9.1.3 Allgemeines

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

9.1.3.2 IS 9.1.3 Auditmethodologie

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

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

Falls die Zertifizierungsstelle branchenspezifische Normerweiterungen einschließt, gilt Folgendes:

Alle Anforderungen nach ISO/IEC 27001 hinsichtlich der Risikobeurteilung gelten bei Aufnahme der branchenspezifischen Normen in das ISMS. Es können insbesondere nur die Maßnahmen in der Erklärung zur Anwendbarkeit als erforderlich gekennzeichnet werden, die zur Behandlung der ermittelten Risiken in der Risikobeurteilung als notwendig bestimmt und angegeben werden.

ANMERKUNG 2 Die Zertifizierung nach ISO/IEC 27001 kann vor oder parallel zur Zertifizierung nach der Norm für branchenspezifische Erweiterung erhalten werden.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

ANMERKUNG 3 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, Anhang A, oder aus einer branchenspezifischen Erweiterung stammen.

Die Zertifizierungsstelle muss Prozesse pflegen, um gleichzeitig mit der Zertifizierung des ISMS nach ISO/IEC 27001 die branchenspezifische Normerweiterung von ISO/IEC 27001 zu zertifizieren bzw. sie zu unterschiedlichen Zeitpunkten zu zertifizieren.

9.1.3.3 IS 9.1.3 Einsatz eines Fernaudits

Die Zertifizierungsstelle muss Verfahren bestimmen, um den Umfang von Fernaudittätigkeiten („Fernaudits“) festzulegen, die zum Auditieren des ISMS einer Organisation 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 die Organisation;

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 hat.

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

ANMERKUNG Falls die Organisation einen virtuellen Standort (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 IS 9.1.3 Allgemeine Vorbereitungen für das erste Audit

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

9.1.3.5 IS 9.1.3 Bewertungszeiträume

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.

ANMERKUNG Die jeweiligen Anforderungen an die Zertifizierungsentscheidung sind in 9.5.1 aufgeführt.

9.1.3.6 IS 9.1.3 Geltungsbereich der Zertifizierung

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

Zertifizierungsstellen müssen sicherstellen, dass die Informationssicherheitsrisikobeurteilung und –risikobehandlung des Kunden seine Tätigkeiten angemessen widerspiegelt und sich bis auf die Grenzen der Tätigkeiten, wie sie im Geltungsbereich der Zertifizierung definiert wurden, erstreckt. Zertifizierungsstellen

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

müssen bestätigen, dass dies im ISMS-Anwendungsbereich des Kunden und der Erklärung zur Anwendbarkeit widergespiegelt wird. Die Zertifizierungsstelle muss verifizieren, dass es für den Geltungsbereich der Zertifizierung eine Erklärung zur Anwendbarkeit 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 branchenspezifische Normerweiterungen einschließt, gilt Folgendes:

Der Geltungsbereich der Zertifizierung in Übereinstimmung mit einer branchenspezifischen Normerweiterung der Zertifizierung nach ISO/IEC 27001 darf nicht den Geltungsbereich der Zertifizierung nach ISO/IEC 27001 überschreiten, für den die Erweiterung gilt.

Falls der Kunde eine branchenspezifische Normerweiterung einschließen möchte, muss die Zertifizierungsstelle sicherstellen, dass seine Erklärung zur Anwendbarkeit und sein Risikobehandlungsprozess gleichermaßen alle Maßnahmen der branchenspezifischen Normerweiterung wie die Maßnahmen in ISO/IEC 27001, Anhang A, berücksichtigen.

9.1.4 Ermittlung des Auditzeitaufwands

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

9.1.4.1 IS 9.1.4 Auditzeitaufwand

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

Die Zertifizierungsstelle muss Anhang B zur Bestimmung des Auditzeitaufwands verwenden.

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

Falls das Audit branchenspezifische Normerweiterungen einschließt, gilt Folgendes:

Die Zertifizierungsstelle muss die Anforderungen an den Auditzeitaufwand für jede Audittätigkeit auf Grundlage der branchenspezifischen Normerweiterung von ISO/IEC 27001, einschließlich des Prozesses zur Berechnung des Auditzeitaufwands, bestimmen. Sowohl die Methodik als auch die einzelnen Berechnungen müssen dokumentiert werden.

9.1.5 Stichprobenprüfung an mehreren Standorten

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

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

9.1.5.1 IS 9.1.5 Mehrere Standorte

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

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

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

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

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

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

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

   1) die Ergebnisse der internen Audits des Stammsitzes (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;

   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.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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

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

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

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

ANMERKUNG Falls das ISMS durch Anforderungen und Anleitungen einer branchenspezifischen Norm erweitert wird, ist das daraus resultierende Managementsystem per se immer noch ein ISMS, weshalb dieser Abschnitt hinsichtlich der branchenspezifischen Normerweiterung keine Anwendung findet.

9.1.6.2 IS 9.1.6 Kombination von Managementsystemaudits

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

ANMERKUNG Falls das ISMS durch Anforderungen und Anleitungen einer branchenspezifischen Norm erweitert wird, ist das daraus resultierende Managementsystem per se immer noch ein ISMS, weshalb dieser Abschnitt hinsichtlich der branchenspezifischen Normerweiterung keine Anwendung findet.

9.2 Planung von Audits

9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien

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

9.2.1.1 IS 9.2.1 Auditziele

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

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

9.2.1.2 IS 9.2.1 Auditkriterien

Die Kriterien, nach denen das ISMS eines Kunden auditiert wird, muss die ISMS-Norm ISO/IEC 27001 sein. Die Auditkriterien dürfen um den Vergleich der Maßnahmen, die zusätzlich zu ISO/IEC 27001, Anhang A, in der branchenspezifischen Norm enthalten sind, erweitert werden. Andere Dokumente, die relevant für die durchgeführten Funktionen sind, dürfen zur Zertifizierung herangezogen werden.

Falls die Auditkriterien branchenspezifische Normerweiterungen einschließen, gilt Folgendes:

Die Zertifizierungsstelle muss eine internationale, regionale oder nationale Norm anwenden, die gegebenenfalls Anforderungen an Audit und Zertifizierung in Übereinstimmung mit der Zertifizierung nach der branchenspezifischen Erweiterung von ISO/IEC 27001 festlegt. Zusätzlich findet weiterhin dieses Dokument Anwendung.

ANMERKUNG 1 Nachfolgende Teile der Normenreihe ISO/IEC 27006, z. B. ISO/IEC 27006-2, sind Beispiele für eine solche Norm.

ANMERKUNG 2 Immer wenn in diesem Dokument der Begriff „ISMS“ verwendet wird, gilt er gleichermaßen für das ISMS nach ISO/IEC 27001 wie für die branchenspezifischen Normerweiterungen des ISMS nach ISO/IEC 27001.

Bei der Auswahl einer Norm, die die Anforderung an die Durchführung von Audits und Zertifizierungen nach einer branchenspezifischen Erweiterungsnorm gibt, muss die Zertifizierungsstelle sicherstellen, dass die Norm mindestens die folgenden Punkte abdeckt:

a) die genaue Verweisung auf die Norm, die die branchenspezifische Erweiterung von ISO/IEC 27001 beschreibt (um die Anforderungen in 9.1.3.7 dieses Dokuments zu erweitern);

b) die Kompetenzkriterien der Auditoren (als Erweiterung von Abschnitt 7 dieses Dokuments);

c) die Berechnung des Auditzeitaufwands (als Erweiterung von 9.1.4 und/oder Anhang B).

9.2.2 Auswahl des Auditteams und Aufgabenzuordnung

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

9.2.2.1 IS 9.2.2 Auditteam

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

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

9.2.2.2 IS 9.2.2 Kompetenz des Auditteams

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

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

a) über ein angemessenes technisches Wissen über die spezifischen Tätigkeiten innerhalb des Anwendungs-bereichs des zu zertifizierenden ISMS und, falls relevant, über zugehörige Verfahren und ihre möglichen Informationssicherheitsrisiken verfügen (Fachexperten dürfen diese Funktion erfüllen);

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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

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

ANMERKUNG Angemessenes Verständnis impliziert kein umfassendes rechtliches Hintergrundwissen.

9.2.3 Auditplan

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

9.2.3.1 IS 9.2.3 Allgemeines

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

9.2.3.2 IS 9.2.3 Fernauditverfahren

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

Der Schwerpunkt derartiger Prozesse sollte auf der Verbesserung der Auditeffektivität und -effizienz liegen und die Integrität des Auditprozesses unterstützen.

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

9.2.3.3 IS 9.2.3 Zeitplanung des Audits

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

9.3 Erstzertifizierung

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

9.3.1 IS 9.3.1 Erstzertifizierungsaudit

9.3.1.1 IS 9.3.1.1 Stufe 1

In dieser Stufe des Audits muss die Zertifizierungsstelle die Dokumentation zur Gestaltung des ISMS beschaffen, die die nach ISO/IEC 27001 (und gegebenenfalls der branchenspezifischen Normerweiterung) 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 (und gegebenenfalls der branchenspezifischen Norm-erweiterung) festgelegten ISMS-Dokumentation und, ggf., zugehörige Dokumentation.

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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

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

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

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

9.3.1.2 IS 9.3.1.2 Stufe 2

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

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

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

b) die in ISO/IEC 27001 und gegebenenfalls in den branchenspezifischen Normerweiterungen aufgelisteten Dokumentationsanforderungen;

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

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

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

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

g) Umsetzung der Maßnahmen (siehe Anhang D; zu den branchenspezifischen Maßnahmen siehe gegebenenfalls den entsprechenden Teil des Dokuments) unter Berücksichtigung des externen und internen Kontextes und zugehöriger Risiken sowie der Überwachung, Messung und Analyse der Informationssicherheitsverfahren und -maßnahmen der Organisation zur Bestimmung, ob Maßnahmen, die als umgesetzt erklärt werden, umgesetzt wurden und wirksam sind;

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

9.4 Durchführen von Audits

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

9.4.1 IS 9.4 Allgemeines

Die Zertifizierungsstelle muss über dokumentierte Verfahren für Folgendes verfügen:

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

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

9.4.2 IS 9.4 Spezifische Elemente des ISMS-Audits

Die vom Auditteam repräsentierte Zertifizierungsstelle muss:

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

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

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

9.4.3 IS 9.4 Auditbericht

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

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

b) eine Darstellung des Zertifizierungsaudits der Informationssicherheitsrisikoanalyse des Kunden;

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

d) den ISMS-Anwendungsbereich;

e) gegebenenfalls die im Audit berücksichtigten branchenspezifischen Normerweiterungen von ISO/IEC 27001;

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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

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

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

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

Ausgefüllte Fragebögen, Checklisten, Beobachtungen, Protokolle oder Auditornotizen können einen integralen Bestandteil des Auditberichts bilden. Falls diese Methoden 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.

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

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

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

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

9.5 Zertifizierungsentscheidung

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

9.5.1 IS 9.5 Zertifizierungsentscheidung

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

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

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

9.6 Aufrechterhaltung der Zertifizierung

9.6.1 Allgemeines

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

9.6.2 Überwachungstätigkeiten

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

9.6.2.1 IS 9.6.2 Überwachungstätigkeiten

9.6.2.1.1 Überwachungsauditverfahren müssen mit den Verfahren in Bezug auf das Zertifizierungsaudit des ISMS des Kunden, wie in diesem Dokument dargelegt, übereinstimmen.

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

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

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

c) Änderungen des dokumentierten Systems;

d) Bereiche, die Änderungen unterworfen sind;

e) ausgewählte Anforderungen nach ISO/IEC 27001 und gegebenenfalls nach branchenspezifischen Normerweiterungen;

f) andere ausgewählte Bereiche, sofern angebracht.

9.6.2.1.2 Jede Überwachung durch die Zertifizierungsstelle muss mindestens Folgendes prüfen:

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

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

c) Änderungen an den festgelegten Maßnahmen und daraus resultierende Änderungen an der SoA (en: Statement of Applicability);

d) Umsetzung und Wirksamkeit der Maßnahmen entsprechend dem Auditprogramm.

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

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

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 sowie die Version der SoA und wichtige Änderungen seit dem letzten Audit enthalten. Die aus der Überwachung stammenden Berichte müssen insgesamt mindestens die Anforderungen aus 9.6.2.1.1 und 9.6.2.1.2 abdecken.

9.6.3 Re-Zertifizierung

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

9.6.3.1 IS 9.6.3 Re-Zertifizierungsaudits

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

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

9.6.4 Audits aus besonderem Anlass

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

9.6.4.1 IS 9.6.4 Sonderfälle

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

9.6.5 Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung

Es gelten die Anforderungen nach ISO/IEC 17021-1, 9.6.5. Zudem gelten die folgenden Anforderungen und Anleitungen.

9.6.5.1 IS 9.6.5 Auswirkungen auf branchenspezifische Normerweiterungen

Falls die Zertifizierung branchenspezifische Normerweiterungen einschließt, gilt Folgendes:

Die Zertifizierungsstelle muss eindeutig feststellen, ob die Aussetzung, Rücknahme oder Einschränkung des Anwendungsbereichs nur ISMS nach der branchenspezifischen Normerweiterung oder sowohl das ISMS nach ISO/IEC 27001 als auch das ISMS nach der branchenspezifischen Normerweiterung betrifft.

ANMERKUNG Falls die Aussetzung, Rücknahme oder Einschränkung des Anwendungsbereichs das ISMS nach ISO/IEC 27001 betrifft, dann ist automatisch auch die branchenspezifische Normerweiterung betroffen (was aber nicht notwendigerweise im umgekehrten Fall gilt).

9.7 Einsprüche

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

9.8 Beschwerden

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

9.8.1 IS 9.8 Beschwerden

Beschwerden stellen potenzielle Vorfälle und Anzeichen für mögliche Nichtkonformitäten dar.

9.9 Aufzeichnungen zu Kunden

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

10 Managementsystemanforderungen für Zertifizierungsstellen

10.1 Optionen

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

10.1.1 IS 10.1 ISMS-Umsetzung

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

10.2 Option A: Allgemeine Managementsystemanforderungen

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

10.3 Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001

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

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08

Anhang A
(informativ)

Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung

A.1 Übersicht

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

Die Kompetenzanforderungen für jede Funktion sind im Haupttext dieses Dokuments angegeben, und diese Tabelle verweist auf die spezifische Anforderung.

Tabelle A.1 — Wissen für ISMS-Audits und die Zertifizierung<Tbl_large_--></Tbl_large_-->

	Zertifizierungsfunktion		
	Durchführung der Antragsprüfung 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
Wissen			
Informationssicherheitsmanagementterminologie, -grundsätze, -praktiken und -verfahren		7.1.2.3.2	7.1.2.1.2
Normen/normative Dokumente in Bezug auf Informationssicherheitsmanagementsysteme	7.1.2.2.1	7.1.2.3.3	7.1.2.1.3
Praktische Unternehmensführung			7.1.2.1.4
Geschäftsfeld des Kunden	7.1.2.2.2	7.1.2.3.4	7.1.2.1.5
Produkte, Prozesse und Organisation des Kunden	7.1.2.2.3	7.1.2.3.5	7.1.2.1.6

A.2 Allgemeine Kompetenzbetrachtungen

Auditoren können ihr Wissen und Erfahrung auf mehrere Arten nachweisen. Wissen und Erfahrung können bewertet werden, z. B. durch Anwendung anerkannter Qualifikationen. Registrierungsaufzeichnungen für Personalzertifizierungsprogramme können ebenfalls zur Bewertung des erforderlichen Wissens und der Erfahrung verwendet werden. Das für das Auditteam erforderliche Kompetenzniveau sollte in Übereinstimmung mit dem Industrie-/Technikfeld der Organisation und der Komplexität des ISMS festgelegt werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27006-1:2022-08

A.3 Spezielle Betrachtungen zu Wissen und Erfahrung

A.3.1 Typisches Wissen in Bezug auf ISMS

Zusätzlich zu den Anforderungen nach 7.1.2 sollte Folgendes berücksichtigt werden. Auditoren sollten über Wissen und Verständnis zu folgenden Audit- und ISMS-Themen verfügen:

— Auditprogrammerstellung und -planung;

— Auditarten und -methoden;

— Auditrisiken;

— Analyse der Informationssicherheitsprozesse;

— fortlaufende Verbesserung;

— interne Audits der Informationssicherheit.

Auditoren sollten über Wissen und Verständnis zu folgenden behördlichen Anforderungen verfügen:

— geistiges Eigentum;

— Inhalt, Schutz und Aufbewahrung von Aufzeichnungen der Organisation;

— Datensicherheit und Datenschutz;

— Regulierung kryptographischer Maßnahmen;

— elektronischer Handel;

— elektronische und digitale Signaturen;

— Arbeitsplatzüberwachung;

— Abfangen von Telekommunikation und Datenüberwachung (z. B. E-Mail);

— Computermissbrauch;

— Sammeln von elektronischen Beweisen;

— Penetrationsprüfung;

— internationale und nationale branchenspezifische Anforderungen (z. B. Bankwesen).

Zu branchenspezifischem Wissen und Verständnis siehe den entsprechenden Teil der Normenreihe ISO/IEC 27006, sofern vorhanden.

BEISPIEL ISO/IEC 27006-2 für Managementsysteme für Datenschutzinformationen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27006-1:2022-08