DIN EN ISO/IEC 27007

ICS 03.120.20; 35.030

Einsprüche bis 2021-11-03

Entwurf

Informationstechnik – Sicherheitsverfahren – Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020); Deutsche und Englische Fassung prEN ISO/IEC 27007:2021

Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing (ISO/IEC 27007:2020); German and English version prEN ISO/IEC 27007:2021

Sécurité de l'information, cybersécurité et protection des données privées – Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information (ISO/IEC 27007:2020); Version allemande et anglaise prEN ISO/IEC 27007:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-09-03 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 101 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Nationales Vorwort

Der Text von ISO/IEC 27007:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27007:2021 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 19011:2018	siehe	DIN EN ISO 19011:2018-10
ISO 31000:2018	siehe	DIN ISO 31000:2018-10
ISO/IEC 17021-1:2015	siehe	DIN EN ISO/IEC 17021-1:2015-11
ISO/IEC 17024	siehe	DIN EN ISO/IEC 17024
ISO/IEC 27000:2018	siehe	DIN EN ISO/IEC 27000:2020-06
ISO/IEC 27001:2013	siehe	DIN EN ISO/IEC 27001:2017-06
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27006:2015	siehe	DIN EN ISO/IEC 27006:2021-05

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

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO 19011:2018-10, *Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018); Deutsche und Englische Fassung EN ISO 19011:2018*

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 17024, *Konformitätsbewertung — Allgemeine Anforderungen an Stellen, die Personen zertifizieren (ISO/IEC 17024:2012); Deutsche und Englische Fassung EN ISO/IEC 17024:2012*

DIN EN ISO/IEC 27000:2020-06, *Informationstechnik – Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020*

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*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

DIN EN ISO/IEC 27006:2021-05, *Informationstechnik — IT-Sicherheitsverfahren — Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd 1:2020); Deutsche Fassung EN ISO/IEC 27006:2020*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien (ISO 31000:2018)*

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

— Leerseite —

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

– Entwurf –

2021-09

prEN ISO/IEC 27007:2021

Titel de:	Informationstechnik — Sicherheitsverfahren — Leitfäden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020)
Titel en:	Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (ISO/IEC 27007:2020)
Titel fr:	Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information (ISO/IEC 27007:2020)

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 6
1 Anwendungsbereich 7
2 Normative Verweisungen 7
3 Begriffe 7
4 Grundsätze der Auditierung 7
5 Management eines Auditprogramms 7
5.1 Allgemeines 7
5.2 Festlegung der Ziele des Auditprogramms 7
5.3 Ermittlung und Beurteilung von Risiken und Chancen im Zusammenhang mit Auditprogrammen 8
5.4 Aufstellung des Auditprogramms 8
5.4.1 Rollen und Verantwortlichkeiten der Person(en), die das Auditprogramm managt/managen 8
5.4.2 Kompetenz von Person(en), die das Audit Programm managt/managen 8
5.4.3 Festlegung des Umfangs des Auditprogramms 8
5.4.4 Ermittlung von Auditprogrammressourcen 9
5.5 Umsetzung des Auditprogramms 9
5.5.1 Allgemeines 9
5.5.2 Definition der Ziele, des Anwendungsbereichs und der Kriterien für ein Einzelaudit 9
5.5.3 Auswahl und Festlegung von Auditverfahren 10
5.5.4 Auswahl von Mitgliedern des Auditteams 10
5.5.5 Übertragung der Verantwortung für ein Einzelaudit an den Leiter des Auditteams 10
5.5.6 Management des Ergebnisses des Auditprogramms 10
5.5.7 Management und Pflege der Auditprogrammunterlagen 11
5.6 Überwachung des Auditprogramms 11
5.7 Überprüfung und Verbesserung des Auditprogramms 11
6 Durchführung eines Audits 11
6.1 Allgemeines 11
6.2 Einleitung des Audits 11
6.2.1 Allgemeines 11
6.2.2 Herstellung des Kontakts mit der auditierten Organisation 11
6.2.3 Feststellung der Durchführbarkeit des Audits 11
6.3 Vorbereitung von Auditaktivitäten 11
6.3.1 Überprüfung dokumentierter Informationen 11
6.3.2 Planung des Audits 12
6.3.3 Übertragung von Arbeiten an das Auditteam 12
6.3.4 Vorbereitung dokumentierter Informationen für das Audit 12
6.4 Durchführung der Auditaktivitäten 12
6.4.1 Allgemeines 12
6.4.2 Zuweisung von Rollen und Verantwortlichkeiten von Guides und Beobachtern 12
6.4.3 Durchführung der Eröffnungsbesprechung 12
6.4.4 Kommunikation während des Audits 12

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

6.4.5 Verfügbarkeit von und Zugang zu Auditinformationen ... 12
6.4.6 Überprüfung der Dokumentinformationen während der Durchführung des Audits ... 12
6.4.7 Erfassung und Überprüfung von Informationen ... 13
6.4.8 Erstellung der Auditfeststellungen ... 13
6.4.9 Erarbeitung der Auditschlussfolgerungen ... 13
6.4.10 Durchführung der Abschlussbesprechung ... 13
6.5 Erarbeitung und Verteilung des Auditberichts ... 13
6.5.1 Erarbeitung des Auditberichts ... 13
6.5.2 Verteilung des Auditberichts ... 14
6.6 Abschluss des Audits ... 14
6.7 Durchführung von Auditfolgemaßnahmen ... 14

7 Kompetenz und Bewertung von ISMS-Auditoren ... 14
7.1 Allgemeines ... 14
7.2 Ermittlung der Kompetenz von Auditoren ... 14
7.2.1 Allgemeines ... 14
7.2.2 Persönliches Verhalten ... 14
7.2.3 Kenntnisse und Fertigkeiten ... 15
7.2.4 Erreichung der Kompetenz von Auditoren ... 15
7.2.5 Erreichung der Kompetenz des Leiters des Auditteams ... 15
7.3 Aufstellung von Kriterien zur Bewertung von Auditoren ... 15
7.4 Auswahl des entsprechenden Verfahrens zur Bewertung von Auditoren ... 15
7.5 Durchführung der Bewertung von Auditoren ... 15
7.6 Aufrechterhaltung und Verbesserung der Kompetenz von Auditoren ... 15

Anhang A (informativ) Leitfaden zur praktischen Durchführung von ISMS-Audits ... 16
A.1 Überblick ... 16
A.2 Allgemeines ... 16
A.2.1 Ziele, Umfang und Kriterien von Audits sowie Auditnachweise ... 16
A.2.2 Strategie zur Auditierung eines ISMS ... 16
A.2.3 Audit und dokumentierte Informationen ... 17
A.3 Leitfaden über die Anforderungen an dokumentierte Informationen nach ISO/IEC 27001 ... 17
A.3.1 Hintergrund ... 17
A.3.2 Beispiel einer impliziten Anforderung an dokumentierte Informationen ... 18
A.3.3 Beispiele, bei denen keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen ... 18
A.4 Die Erklärung zur Anwendbarkeit ... 19
A.5 Sonstige dokumentierte Informationen ... 19
A.6 Anmerkungen ... 19
A.7 Leitfaden zur Auditierung eines ISMS ... 20

Literaturhinweise ... 54

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Europäisches Vorwort

Der Text von ISO/IEC 27007:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 27007:2021 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 27007:2020 wurde von CEN als prEN ISO/IEC 27007:2021 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.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

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-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) oder der IEC-Liste der erhaltenen Patenterklärungen (siehe http://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.

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

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27007:2017), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

— das Dokument wurde an ISO 19011:2018 angepasst;

— die Einleitung wurde umformuliert und erweitert;

— in 5.1 wurde der gesamte Text entfernt;

— in 5.2.2 wurde der frühere Punkt d) entfernt;

— in 5.3 wurde der gesamte Text entfernt;

— in 5.5.2.2 wurden der frühere Punkt b) und ein Absatz unterhalb davon entfernt;

— in 6.5.2.2 wurden der erste Absatz entfernt und die ANMERKUNG umformuliert.

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 zu finden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Einleitung

Ein Audit eines Informationssicherheitsmanagementsystems (en: Information Security Management System, ISMS) kann anhand einer Reihe von Auditkriterien durchgeführt werden, die einzeln oder in Kombination angewendet werden. Zu diesen Kriterien gehören unter anderem:

— Anforderungen nach ISO/IEC 27001:2013;

— von betroffenen interessierten Parteien vorgegebene Richtlinien und Anforderungen;

— gesetzliche und behördliche Anforderungen;

— von der Organisation oder anderen Parteien festgelegte ISMS-Prozesse und -Maßnahmen;

— Managementsystempläne bezüglich der Bereitstellung bestimmter Ausgabedaten eines ISMS (z. B. Pläne zum um Umgang mit Risiken und Chancen bei der Festlegung von ISMS-Plänen, Pläne zur Erreichung von Informationssicherheitszielen, Pläne zum Umgang mit Risiken, Projektpläne).

Dieses Dokument enthält einen Leitfaden für alle Größen und Arten von Organisationen und ISMS-Audits verschiedener Anwendungsbereiche und Größenordnungen, zu denen Audits sowohl großer Auditteams üblicherweise in größeren Organisationen als auch einzelner Auditoren in großen oder kleinen Organisationen gehören. Dieser Leitfaden sollte entsprechend an den Anwendungsbereich, die Komplexität und die Größenordnung des ISMS-Auditprogramms angepasst werden.

Dieses Dokument befasst sich hauptsächlich mit internen ISMS-Audits (erste Partei) und ISMS-Audits, die Organisationen bei ihren externen Dienstleistern und anderen externen interessierten Parteien (zweite Partei) durchführen. Dieses Dokument kann außerdem bei externen ISMS-Audits hilfreich sein, die zu anderen Zwecken als zur Zertifizierung von Managementsystemen Dritter durchgeführt werden. ISO/IEC 27006 enthält Anforderungen zum Auditieren von ISMS zur Zertifizierung Dritter; hierzu enthält dieses Dokument unter Umständen weitere nützliche Leitfäden.

Dieses Dokument ist in Verbindung mit dem in ISO 19011:2018 enthaltenen Leitfaden anzuwenden.

Der Aufbau dieses Dokuments folgt der Struktur von ISO 19011:2018.

ISO 19011:2018 enthält einen Leitfaden für das Management von Auditprogrammen, zur Durchführung interner oder externer Audits von Managementsystemen sowie zur Kompetenz und Bewertung von Auditoren für Managementsysteme.

Anhang A enthält einen Leitfaden zur praktischen Durchführung von ISMS-Audits zusammen mit Anforderungen von ISO/IEC 27001:2013, Abschnitt 4 bis Abschnitt 10.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

1 Anwendungsbereich

Zusätzlich zu dem in ISO 19011 enthaltenen Leitfaden enthält dieses Dokument Leitfäden zum Management eines Auditprogramms für Informationssicherheitsmanagementsysteme (ISMS), zur Durchführung von Audits und zur Kompetenz von ISMS-Auditoren.

Dieses Dokument gilt für alle, die sich mit internen oder externen Audits eines ISMS vertraut machen oder diese durchführen müssen oder ein ISMS-Auditprogramm managen müssen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 19011:2018, *Guidelines for auditing management systems*

ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 19011 und ISO/IEC 27000.

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 http://www.electropedia.org/

4 Grundsätze der Auditierung

Es gelten die Grundsätze der Auditierung nach ISO 19011:2018, Abschnitt 4.

5 Management eines Auditprogramms

5.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 5.1.

5.2 Festlegung der Ziele des Auditprogramms

5.2.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.2. Außerdem gilt der Leitfaden in 5.2.2.

5.2.2 Zu ISMS-spezifischen Aspekten bei der Ermittlung[1] der Ziele des Auditprogramms können gehören:

a) identifizierte Anforderungen an die Informationssicherheit;

b) Anforderungen nach ISO/IEC 27001;

1 Im Sinne dieses Dokuments bezeichnet der Begriff „Audit“ ISMS-Audits.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

c) Leistungsfähigkeit der auditierten Organisation, die sich im Auftreten von Ereignissen und Vorfällen im Zusammenhang mit der Informationssicherheit und der Wirksamkeit des ISMS widerspiegelt;

ANMERKUNG Weitere Informationen über die Überwachung, Messung, Analyse und Bewertung der Leistung sind in ISO/IEC 27004 zu finden.

d) Informationssicherheitsrisiken für die betroffenen Parteien, d. h. die auditierte Organisation und den Auditauftraggeber.

Zu Beispielen ISMS-spezifischer Ziele von Auditprogrammen gehören:

— Nachweis der Übereinstimmung mit den einschlägigen gesetzlichen und vertraglichen Anforderungen und anderen Anforderungen sowie deren Sicherheitsauswirkungen;

— Herstellen und Aufrechterhalten des Vertrauens in die Fähigkeit der auditierten Organisation zum Risikomanagement;

— Beurteilen der Wirksamkeit der Maßnahmen zum Umgang mit Risiken und Chancen im Zusammenhang mit der Informationssicherheit.

5.3 Ermittlung und Beurteilung von Risiken und Chancen im Zusammenhang mit Auditprogrammen

5.3.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.3.

5.3.2 Es sollten Maßnahmen zum Sicherstellen der Informationssicherheit und Vertraulichkeit festgelegt werden, bei denen die Anforderungen der auditierten Organisationen und anderer betroffener Parteien berücksichtigt werden. Zu Anforderungen anderer Parteien können einschlägige gesetzliche und vertragliche Anforderungen gehören.

5.4 Aufstellung des Auditprogramms

5.4.1 Rollen und Verantwortlichkeiten der Person(en), die das Auditprogramm managt/managen

Es gilt der Leitfaden nach ISO 19011:2018, 5.4.1. Außerdem gilt der Leitfaden in 5.4.1.2.

5.4.2 Kompetenz von Person(en), die das Audit Programm managt/managen

Es gilt der Leitfaden nach ISO 19011:2018, 5.4.2.

5.4.3 Festlegung des Umfangs des Auditprogramms

5.4.3.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.4.3. Außerdem gilt der Leitfaden in 5.4.3.2.

5.4.3.2 Zum Umfang des Auditprogramms kann Folgendes gehören:

a) die Größe des ISMS, unter anderem:

1) die Gesamtzahl von Personen, die Arbeiten unter der Kontrolle der Organisation ausführen, und die Beziehungen zu interessierten Parteien und Auftragnehmern, die für das ISMS maßgeblich sind;

2) die Anzahl von Informationssystemen;

3) die Anzahl von Standorten, die durch das ISMS erfasst werden;

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

b) die Komplexität des ISMS (einschließlich der Anzahl und der Kritikalität von Prozessen und Aktivitäten) unter Berücksichtigung von Unterschieden zwischen Standorten innerhalb des Anwendungsbereichs des ISMS;

c) die Bedeutung von Informationssicherheitsrisiken des ISMS, die in Bezug auf die Geschäftstätigkeit identifiziert wurden;

d) die Bedeutung der Risiken und Chancen, die bei der Planung des ISMS ermittelt wurden;

e) die Bedeutung der Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen innerhalb des Anwendungsbereichs des ISMS;

f) die Komplexität des zu auditierenden Informationssystems einschließlich der Komplexität der eingesetzten Informationstechnologie;

g) die Anzahl ähnlicher Standorte.

Im Auditprogramm sollte die Einstellung von Prioritäten in Betracht gezogen werden, die eine detailliertere Prüfung auf der Grundlage der Bedeutung von Informationssicherheitsrisiken und Unternehmensanforderungen hinsichtlich des Anwendungsbereichs des ISMS garantieren.

ANMERKUNG Weitere Informationen über die Festlegung der Auditzeit sind in ISO/IEC 27006 zu finden. Weitere Informationen über Stichproben an mehreren Standorten sind in ISO/IEC 27006 und im obligatorischen Dokument 1 vom International Accreditation Forum (IAF MD 1, siehe Literaturhinweis [11]) zu finden. Die in ISO/IEC 27006 und IAF MD 1 enthaltenen Informationen betreffen nur Zertifizierungsaudits.

5.4.4 Ermittlung von Auditprogrammressourcen

5.4.4.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.4.4. Außerdem gilt der Leitfaden in 5.4.4.2.

5.4.4.2 Insbesondere sollte bei allen wesentlichen Risiken, die für die auditierte Organisation gelten und für die Ziele des Auditprogramms maßgeblich sind, den ISMS-Auditoren ausreichend Zeit gegeben werden, um die Wirksamkeit der Maßnahmen zum Umgang mit Informationssicherheitsrisiken und den Risiken und Chancen im Zusammenhang mit dem ISMS zu überprüfen.

5.5 Umsetzung des Auditprogramms

5.5.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 5.5.1.

5.5.2 Definition der Ziele, des Anwendungsbereichs und der Kriterien für ein Einzelaudit

5.5.2.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.5.2. Außerdem gilt der Leitfaden in 5.5.2.2.

5.5.2.2 Zu den Zielen des Audits kann Folgendes gehören:

a) Beurteilung, ob das ISMS Anforderungen und Informationssicherheit angemessen identifiziert und behandelt;

b) Ermittlung des Umfangs der Übereinstimmung von Informationssicherheitsmaßnahmen mit den Anforderungen und Verfahren des ISMS.

Der Auditumfang sollte Informationssicherheitsrisiken und maßgebliche Risiken und Chancen berücksichtigen, die sich auf das ISMS betroffener Parteien auswirken, d. h. des Auditauftraggebers und der auditierten Organisation.

AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

Die folgenden Themen können als Auditkriterien und als Referenz betrachtet werden, auf deren Grundlage die Konformität ermittelt wird:

a) die Informationssicherheitspolitik, die Informationssicherheitsziele, Richtlinien und Verfahren, die durch die auditierte Organisation eingeführt wurden;

b) vertragliche Anforderungen und sonstige Anforderungen, die für die auditierte Organisation maßgeblich sind;

c) Kriterien von Informationssicherheitsrisiken, Prozess zur Beurteilung von Informationssicherheitsrisiken und Prozess zur Risikobehandlung der auditierten Organisation;

d) die Erklärung zur Anwendbarkeit, die Identifizierung von sektorspezifischen und anderen notwendigen Maßnahmen, Begründung für deren Einbeziehung, ob sie umgesetzt sind oder nicht, und die Begründung für den Ausschluss von Maßnahmen nach ISO/IEC 27001:2013, Anhang A;

e) die Definition von Maßnahmen zur entsprechenden Behandlung von Risiken;

f) die Verfahren und Kriterien zur Überwachung, Messung, Analyse und Bewertung der Informationssicherheitsleistung und der Wirksamkeit des ISMS;

g) durch einen Kunden zur Verfügung gestellte Anforderungen an die Informationssicherheit;

h) durch einen Lieferanten oder ein Unternehmen, an das Tätigkeiten ausgelagert wurden, angewendete Anforderungen an die Informationssicherheit.

5.5.3 Auswahl und Festlegung von Auditverfahren

5.5.3.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.5.3. Außerdem gilt der Leitfaden in 5.5.3.2.

5.5.3.2 Bei einem gemeinschaftlichen Audit sollte besondere Aufmerksamkeit auf die Offenlegung von Informationen zwischen den betroffenen Parteien gelegt werden. Vor Beginn des Audits sollte hierzu eine Vereinbarung zwischen allen interessierten Parteien herbeigeführt werden.

5.5.4 Auswahl von Mitgliedern des Auditteams

5.5.4.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.5.4. Außerdem gilt der Leitfaden in 5.5.4.2.

5.5.4.2 Die Kompetenz des gesamten Auditteams sollte eine angemessene Kenntnis und ein entsprechendes Verständnis folgender Punkte beinhalten:

a) Informationssicherheitsrisikomanagement, das ausreicht, um die durch die auditierte Organisation verwendeten Verfahren zu beurteilen;

b) Informationssicherheit und Informationssicherheitsmanagement, die ausreichen, um die Festlegung von Maßnahmen, Planung, Umsetzung, Pflege und Wirksamkeit des ISMS zu beurteilen.

5.5.5 Übertragung der Verantwortung für ein Einzelaudit an den Leiter des Auditteams

Es gilt der Leitfaden nach ISO 19011:2018, 5.5.5.

5.5.6 Management des Ergebnisses des Auditprogramms

Es gilt der Leitfaden nach ISO 19011:2018, 5.5.6.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

5.5.7 Management und Pflege der Auditprogrammunterlagen

Es gilt der Leitfaden nach ISO 19011:2018, 5.5.7.

5.6 Überwachung des Auditprogramms

Es gilt der Leitfaden nach ISO 19011:2018, 5.6.

5.7 Überprüfung und Verbesserung des Auditprogramms

Es gilt der Leitfaden nach ISO 19011:2018, 5.7.

6 Durchführung eines Audits

6.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 6.1.

6.2 Einleitung des Audits

6.2.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 6.2.1.

6.2.2 Herstellung des Kontakts mit der auditierten Organisation

6.2.2.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.2.2. Außerdem gilt der Leitfaden in 6.2.2.2.

6.2.2.2 Gegebenenfalls sollte darauf geachtet werden, dass den Auditoren die notwendige Sicherheitsfreigabe für den Zugang zu dokumentierten Informationen oder anderen Informationen erteilt wurde, die für Aktivitäten im Rahmen des Audits erforderlich sind (einschließlich unter anderem vertraulicher oder sensibler Informationen).

6.2.3 Feststellung der Durchführbarkeit des Audits

6.2.3.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.2.3. Außerdem gilt der Leitfaden in 6.2.3.2.

6.2.3.2 Vor dem Beginn des Audits sollte die auditierte Organisation gefragt werden, ob Nachweise für das ISMS-Audit durch das Auditteam nicht geprüft werden können, weil z. B. die Nachweise personenbezogene Informationen oder andere vertrauliche/sensible Informationen enthalten. Die für das Management des Auditprogramms verantwortliche Person sollte festlegen, ob das ISMS bei Fehlen von Auditnachweisen angemessen auditiert werden kann. Sofern die Schlussfolgerung darin besteht, dass das ISMS ohne Überprüfung der betreffenden Auditnachweise nicht auditiert werden kann, sollte die für das Management des Auditprogramms zuständige Person die auditierte Organisation darüber informieren, dass das Audit so lange nicht stattfinden kann, bis entsprechende Absprachen über den Zugang getroffen wurden oder der auditierten Organisation oder durch sie alternative Mittel vorgeschlagen wurden, um die Durchführung des Audits zu erreichen. Falls das Audit fortgesetzt wird, sollten alle Zugangseinschränkungen im Auditplan berücksichtigt werden.

6.3 Vorbereitung von Auditaktivitäten

6.3.1 Überprüfung dokumentierter Informationen

Es gilt der Leitfaden nach ISO 19011:2018, 6.3.1.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

6.3.2 Planung des Audits

6.3.2.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.3.2. Außerdem gilt der Leitfaden in 6.3.2.2.

6.3.2.2 Der Leiter des Auditteams sollte sich dessen bewusst sein, dass durch die Anwesenheit der Mitglieder des Auditteams Risiken für die auditierte Organisation entstehen können. Die Anwesenheit des Auditteams kann sich auf die Informationssicherheit auswirken und eine Quelle zusätzlicher Risiken für die Informationen der auditierten Organisation darstellen, z. B. für vertrauliche oder sensible Aufzeichnungen oder für die Systeminfrastruktur (z. B. versehentliche Löschung, unbefugte Offenlegung von Informationen, unbeabsichtigte Veränderung von Informationen).

6.3.3 Übertragung von Arbeiten an das Auditteam

Es gilt der Leitfaden nach ISO 19011:2018, 6.3.3.

6.3.4 Vorbereitung dokumentierter Informationen für das Audit

6.3.4.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.3.4. Außerdem gilt der Leitfaden in 6.3.4.2.

6.3.4.2 Der Leiter des Auditteams sollte dafür sorgen, dass alle Arbeitsdokumente des Audits entsprechend klassifiziert und in Übereinstimmung mit dieser Klassifizierung behandelt werden.

6.4 Durchführung der Auditaktivitäten

6.4.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.1.

6.4.2 Zuweisung von Rollen und Verantwortlichkeiten von Guides und Beobachtern

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.2.

6.4.3 Durchführung der Eröffnungsbesprechung

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.3.

6.4.4 Kommunikation während des Audits

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.4.

6.4.5 Verfügbarkeit von und Zugang zu Auditinformationen

6.4.5.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.4.5. Außerdem gilt der Leitfaden in 6.4.5.2.

6.4.5.2 Falls Auditnachweise aufgrund der Klassifizierung oder aufgrund sensibler Daten während des Audits nicht zur Verfügung stehen, sollte der leitende Auditor das Ausmaß ermitteln, in dem sich dies auf das Vertrauen in die Auditfeststellungen und auf die Schlussfolgerung auswirkt, und dies im Auditbericht entsprechend wiedergeben, ohne den sensiblen Charakter der Nachweise zu beeinträchtigen, die nicht zur Verfügung standen.

6.4.6 Überprüfung der Dokumentinformationen während der Durchführung des Audits

6.4.6.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.4.6. Außerdem gilt der Leitfaden in 6.4.6.2.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

6.4.6.2 Die ISMS-Auditoren sollten überprüfen, ob die dokumentierten Informationen, die aufgrund der Auditkriterien erforderlich und für den Auditumfang maßgeblich sind, vorhanden sind und den Anforderungen der Auditkriterien entsprechen.

Die ISMS-Auditoren sollten bestätigen, dass die festgelegten Maßnahmen innerhalb des Umfangs des Audits im Zusammenhang mit den Ergebnissen der Risikobeurteilung und mit dem Prozess zum Umgang mit Risiken im Zusammenhang stehen und anschließend anhand der Informationssicherheitspolitik und deren Zielen zurückverfolgt werden können.

ANMERKUNG Anhang A enthält einen Leitfaden zur praktischen Durchführung von ISMS-Audits, darunter auch Hinweise, wie das ISMS unter Verwendung der maßgeblichen dokumentierten Informationen zu auditieren ist.

6.4.7 Erfassung und Überprüfung von Informationen

6.4.7.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.4.7. Außerdem gilt der Leitfaden in 6.4.7.2.

6.4.7.2 Zu möglichen Verfahren zur Erfassung maßgeblicher Informationen während des Audits gehören:

a) Prüfung dokumentierter Informationen (einschließlich von Computerprotokollen und Konfigurationsdaten);

b) Besuch informationsverarbeitender Einrichtungen;

c) Beobachtung von ISMS-Prozessen und zugehörigen Maßnahmen;

d) Verwendung automatisierter Audit-Tools.

ANMERKUNG 1 Anhang A enthält einen Leitfaden zur Auditierung der ISMS-Prozesse.

ANMERKUNG 2 ISO/IEC TS 27008 enthält einen zusätzlichen Leitfaden zur Beurteilung von Informationssicherheitsmaßnahmen.

Die Mitglieder des ISMS-Auditteams sollten sicherstellen, dass alle von auditierten Organisationen erhaltenen Informationen entsprechend der zwischen dem Auditauftraggeber, dem Auditteam und der auditierten Organisation getroffenen Vereinbarung behandelt werden.

6.4.8 Erstellung der Auditfeststellungen

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.8.

6.4.9 Erarbeitung der Auditschlussfolgerungen

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.9.

6.4.10 Durchführung der Abschlussbesprechung

Es gilt der Leitfaden nach ISO 19011:2018, 6.4.10.

6.5 Erarbeitung und Verteilung des Auditberichts

6.5.1 Erarbeitung des Auditberichts

Es gilt der Leitfaden nach ISO 19011:2018, 6.5.1.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

6.5.2 Verteilung des Auditberichts

6.5.2.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.5.2. Außerdem gilt der Leitfaden in 6.5.2.2.

6.5.2.2 ANMERKUNG

ANMERKUNG Bei Verwendung elektronischer Mittel zur Verteilung des Auditberichts besteht eine mögliche Maßnahme zur Einhaltung der Vertraulichkeitsanforderungen in einer entsprechenden Verschlüsselung des Auditberichts.

6.6 Abschluss des Audits

Es gilt der Leitfaden nach ISO 19011:2018, 6.6.

6.7 Durchführung von Auditfolgemaßnahmen

Es gilt der Leitfaden nach ISO 19011:2018, 6.7.

7 Kompetenz und Bewertung von ISMS-Auditoren

7.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 7.1.

7.2 Ermittlung der Kompetenz von Auditoren

7.2.1 Allgemeines

7.2.1.1 Es gilt der Leitfaden nach ISO 19011:2018, 7.2.1. Außerdem gilt der Leitfaden in 7.2.1.2.

7.2.1.2 Bei der Entscheidung über die entsprechenden Kenntnisse und Fertigkeiten eines ISMS-Auditors sollte Folgendes berücksichtigt werden:

a) Komplexität des ISMS (z. B. Kritikalität von Informationssystemen innerhalb des ISMS, Ergebnisse der Risikobeurteilung des ISMS);

b) Art(en) der im Anwendungsbereich des ISMS durchgeführten Geschäftstätigkeit(en);

c) Umfang und Verschiedenartigkeit der bei der Realisierung der verschiedenen Komponenten des ISMS genutzten Technologie (z. B. die umgesetzten Maßnahmen, dokumentierte Informationen und/oder Prozesskontrolle, beteiligte Technologieplattformen und Lösungen usw.);

d) zuvor unter Beweis gestellte Leistung des ISMS;

e) Umfang der Ausgliederung und der mit externen Parteien getroffenen Vereinbarungen, die innerhalb des Anwendungsbereichs des ISMS verwendet werden;

f) die auf das Auditprogramm zutreffenden Normen, gesetzlichen und sonstigen Anforderungen.

7.2.2 Persönliches Verhalten

Es gilt der Leitfaden nach ISO 19011:2018, 7.2.2.

AVA Documents Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

7.2.3 Kenntnisse und Fertigkeiten

7.2.3.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2018, 7.2.3.1.

7.2.3.2 Allgemeine Kenntnisse und Fertigkeiten von Auditoren für Managementsysteme

Es gilt der Leitfaden nach ISO 19011:2018, 7.2.3.2.

7.2.3.3 Fachrichtung und sektorspezifische Kompetenz von Auditoren

7.2.3.3.1 Es gilt der Leitfaden nach ISO 19011:2018, 7.2.3.3. Außerdem gilt der Leitfaden in 7.2.3.3.2.

7.2.3.3.2 Außerdem sollten ISMS-Auditoren über das Verständnis entsprechender Unternehmensanforderungen verfügen.

7.2.3.4 Allgemeine Kompetenz eines Leiters eines Auditteams

Es gilt der Leitfaden nach ISO 19011:2018, 7.2.3.4.

7.2.3.5 Kenntnisse und Fertigkeiten zum Auditieren in mehreren Fachrichtungen

Es gilt der Leitfaden nach ISO 19011:2018, 7.2.3.5.

7.2.4 Erreichung der Kompetenz von Auditoren

7.2.4.1 Es gilt der Leitfaden nach ISO 19011:2018, 7.2.4. Außerdem gilt der Leitfaden in 7.2.4.2.

7.2.4.2 ISMS-Auditoren sollten über Kenntnisse und Fertigkeiten in der Informationstechnologie und Informationssicherheit verfügen, die beispielsweise durch entsprechende Zertifizierungen belegt sind (z. B. Akkreditierung nach ISO/IEC 17024). Die Berufserfahrung einzelner ISMS-Auditoren sollte darüber hinaus zur Weiterentwicklung ihrer Kenntnisse und Fertigkeiten auf dem Gebiet der ISMS beitragen.

ANMERKUNG Weitere Informationen über die Zertifizierung von ISMS-Auditoren sind in ISO/IEC 27006 zu finden.

7.2.5 Erreichung der Kompetenz des Leiters des Auditteams

Es gilt der Leitfaden nach ISO 19011:2018, 7.2.5.

7.3 Aufstellung von Kriterien zur Bewertung von Auditoren

Es gilt der Leitfaden nach ISO 19011:2018, 7.3.

7.4 Auswahl des entsprechenden Verfahrens zur Bewertung von Auditoren

Es gilt der Leitfaden nach ISO 19011:2018, 7.4.

7.5 Durchführung der Bewertung von Auditoren

Es gilt der Leitfaden nach ISO 19011:2018, 7.5.

7.6 Aufrechterhaltung und Verbesserung der Kompetenz von Auditoren

Es gilt der Leitfaden nach ISO 19011:2018, 7.6.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Anhang A
(informativ)

Leitfaden zur praktischen Durchführung von ISMS-Audits

A.1 Überblick

Dieser Anhang enthält einen allgemeinen Leitfaden zur Auditierung eines ISMS, für das eine Organisation Konformität mit ISO/IEC 27001 beansprucht. Da dieser Leitfaden unabhängig von der Größe oder Art der beteiligten Organisation zur Anwendung auf alle derartigen ISMS-Audits vorgesehen ist, trägt dieser Leitfaden allgemeinen Charakter. Der Leitfaden ist zur Verwendung durch Auditoren vorgesehen, die eine interne oder externe ISMS-Auditierung durchführen.

ANMERKUNG ISO/IEC 27003 enthält einen Leitfaden zur Umsetzung und zum Betrieb eines ISMS nach ISO/IEC 27001.

A.2 Allgemeines

A.2.1 Ziele, Umfang und Kriterien von Audits sowie Auditnachweise

Während der Auditaktivitäten sollten durch geeignete Stichproben Informationen erfasst und überprüft werden, die für die Ziele, den Umfang und die Kriterien des Audits maßgeblich sind, darunter Informationen im Zusammenhang mit Schnittstellen zwischen Funktionen, Aktivitäten und Prozessen. Als Auditnachweise sollten nur überprüfbare Informationen akzeptiert werden. Auditnachweise, die zu Auditfeststellungen führen, sollten aufgezeichnet werden.

Zu Methoden zum Erfassen von Informationen gehören folgende:

— Befragungen;

— Beobachtungen;

— Überprüfung von Dokumenten einschließlich Aufzeichnungen.

A.2.2 Strategie zur Auditierung eines ISMS

Einige Unterabschnitte von ISO/IEC 27001:2013 hängen eng miteinander zusammen und werden bei der praktischen Durchführung des Audits am besten auch zum selben Zeitpunkt gemeinsam behandelt. Beispiele siehe Tabelle A.2.

Beispiele sind die Abschnitte ISO/IEC 27001:2013:6.1.3 und 8.3 und 6.2, 5.1, 5.2, 5.3, 7.1, 7.4, 7.5, 9.1, 9.3 sowie 10.2. Es ist sinnvoll, diese Unterabschnitte mit den verknüpften und zugehörigen Unterabschnitten zu auditieren.

ISO/IEC 27001:2013, 7.5, enthält die Anforderungen bezüglich dokumentierter Informationen. Wie in Tabelle A.2, A.4.5, erläutert, bietet die Norm bei jeder Überprüfung dokumentierter Informationen durch Auditoren die Möglichkeit zur Bestätigung der Einhaltung der Anforderungen nach ISO/IEC 27001:2013, 7.5. Der Leitfaden hierzu ist in Tabelle A.2, A.4.5, zu finden. In der Tabelle werden die Anforderungen bezüglich dokumentierter Informationen nicht bei jedem Auftreten „dokumentierter Informationen“ wiederholt.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

A.2.3 Audit und dokumentierte Informationen

Auditaktivitäten können folgende dokumentierte Informationen beinhalten:

a) Anforderungsangaben zu dokumentierten Informationen in ISO/IEC 27001 können als Auditkriterien verwendet werden;

b) durch ISO/IEC 27001:2013, 7.5.1 b), geforderte dokumentierte Informationen;

c) dokumentierte Informationen, die nach ISO/IEC 27001:2013, 7.5.1 c), durch die Organisation als notwendig für die Wirksamkeit des ISMS festgelegt wurden.

Auch andere Auditnachweise als nach A.2.3 b) sind möglich, die Auditoren über Befragungen, Beobachtungen und Überprüfung von Dokumenten einschließlich Aufzeichnungen erhalten.

Eine ausführliche Erläuterung dokumentierter Informationen hinsichtlich ISO/IEC 27001 ist in A.3 zu finden.

A.3 Leitfaden über die Anforderungen an dokumentierte Informationen nach ISO/IEC 27001

A.3.1 Hintergrund

Bei der Anforderung dokumentierter Informationen als Konformitätsnachweis sollten Auditoren vorsichtig vorgehen.

Es bestehen:

a) 16 explizite Anforderungen an dokumentierte Informationen einschließlich der Erklärung zur Anwendbarkeit, wie in Tabelle A.1 aufgeführt;

b) bei den übrigen Anforderungen handelt es sich um Anforderungen, bei denen:

   1) erwartet werden kann, dass der Konformitätsnachweis in den oben aufgeführten dokumentierten Informationen zu finden ist;

   2) keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen.

Tabelle A.1 – Anforderungen an dokumentierte Informationen in ISO/IEC 27001

Anforderung an dokumentierte Informationen bezüglich	Unterabschnitt in ISO/IEC 27001:2013
Anwendungsbereich des ISMS	4.3
Informationssicherheitspolitik	5.2
Prozess zur Beurteilung von Informationssicherheitsrisiken	6.1.2
Prozess zur Informationssicherheitsrisikobehandlung	6.1.3
Erklärung zur Anwendbarkeit	6.1.3 d)
Informationssicherheitsziele	6.2
Kompetenznachweis	7.2 d)
Dokumentierte Informationen, die durch die Organisation als für die Wirksamkeit des ISMS notwendig festgelegt wurden	7.5.1 b)

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Anforderung an dokumentierte Informationen bezüglich	Unterabschnitt in ISO/IEC 27001:2013
Betriebliche Planung und Steuerung	8.1
Ergebnisse der Beurteilungen von Informationssicherheitsrisiken	8.2
Ergebnisse der Informationssicherheitsrisikobehandlung	8.3
Nachweis der Überwachung und Messung von Ergebnissen	9.1
Nachweis des Auditprogramms/der Auditprogramme und der Auditergebnisse	9.2 g)
Nachweis der Ergebnisse von Managementbewertungen	9.3
Nachweis der Art von Nichtkonformitäten und der ergriffenen Folgemaßnahmen	10.1 f)
Nachweis der Ergebnisse von Korrekturmaßnahmen	10.1 g)

ANMERKUNG In der Definition eines Audits ist festgelegt, dass es sich um einen dokumentierten Prozess handelt. Ein Auditor kann daher erwarten, dass die Anforderung nach ISO/IEC 27001:2013, 9.2, zu einem dokumentierten Auditprozess führt.

A.3.2 Beispiel einer impliziten Anforderung an dokumentierte Informationen

Als Beispiel für A.3.1 b) 1) soll ISO/IEC 27001:2013, 6.1.2, betrachtet werden, der von Organisationen verlangt, „dokumentierte Informationen über den Informationssicherheitsrisikobeurteilungsprozess“ aufzubewahren. Alle vorhergehenden Anforderungen [ISO/IEC 27001:2013, 6.1.2 a) bis e)] betreffen den Risikobeurteilungsprozess. Es kann daher erwartet werden, dass der Nachweis der Konformität mit diesen Anforderungen in den geforderten dokumentierten Informationen zu finden ist, die den Risikobeurteilungsprozess betreffen.

A.3.3 Beispiele, bei denen keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen

Als Beispiel für A.3.1 b) 2) soll ISO/IEC 27001:2013, 4.1.1, betrachtet werden. Es liegen keine Anforderungen an dokumentierte Informationen vor, die interne und externe Aspekte betreffen. Auditoren sollten daher keine Einsichtnahme verlangen. Wenn die Organisation unabhängig davon nicht nachweist, dass sie diese Aspekte ermittelt hat, würde dies eine Nichtkonformität mit ISO/IEC 27001:2013, 4.1.1, darstellen. Die Pflicht zur Festlegung der Art und Weise, in der sie die Konformität nachweist, liegt jedoch bei der Organisation. Eventuell kann die oberste Leitung die Konformität erläutern (d. h., dass jemand über entsprechende Kenntnisse verfügt); eventuell liegt ein Protokoll einer Besprechung vor, bei der das Thema erörtert wurde; eventuell kann die Konformität in den dokumentierten Informationen nachgewiesen werden, die dem formalen Konfigurationsmanagement unterliegen, oder die Konformität kann auf andere Weise nachgewiesen werden. Tatsächlich besteht die Wahrscheinlichkeit, dass der Nachweis über die dokumentierten Informationen des ISMS hinweg verteilt ist. Beispielsweise besteht der Zweck von ISO/IEC 27001:2013, 4.1.1, darin, der Organisation das Verständnis des Kontextes ihres ISMS zu erleichtern. Dieser Kontext ist für das gesamte ISMS maßgebend, insbesondere bei der Festlegung des Anwendungsbereichs und der Politik und bei der Durchführung der Prozesse zur Risikobeurteilung und Risikobehandlung. Sofern die Organisation die Anforderungen nach ISO/IEC 27001:2013, 4.1.1, erfüllt hat, besteht die Wahrscheinlichkeit, dass ihre Kenntnisse externer und interner Aspekte in diesen anderen Bereichen des ISMS verwendet werden, dessen Verwendung konsistent ist und ein Konformitätsnachweis in den dokumentierten Informationen vorliegt, die diese anderen Bereiche betreffen.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

A.4 Die Erklärung zur Anwendbarkeit

Die Erklärung zur Anwendbarkeit (en: Statement of Applicability (SoA)) ist ein weiterer Bereich, der Sorgfalt erfordert. Die SoA sollte alle notwendigen Maßnahmen enthalten, d. h. die Maßnahmen, die die Organisation im Ergebnis ihres Risikobehandlungsprozesses [ISO/IEC 27001:2013, 6.1.3 c)] als zur Änderung des Informationssicherheitsrisikos notwendig festgelegt hat, um ihre Risikoakzeptanzkriterien zu erfüllen. Bei allen notwendigen Maßnahmen handelt es sich um die organisationseigenen Anforderungen.

Notwendige Maßnahmen können Maßnahmen nach ISO/IEC 27001:2013, Anhang A, sein, sind jedoch nicht obligatorisch. Diese können Maßnahmen aus anderen Normen (z. B. ISO/IEC 27017) oder anderen Quellen entnommen oder durch die Organisation speziell konzipiert worden sein.

In einigen Fällen nutzt die Organisation eine Maßnahme, bei der es sich um eine Variante einer Maßnahme nach ISO/IEC 27001:2013, Anhang A, unter Ausschluss der ursprünglichen Maßnahmen nach ISO/IEC 27001:2013, Anhang A, handelt, wobei der Hintergrund des Ausschlusses darin besteht, dass die Maßnahme durch die Maßnahmenvariante der Organisation ersetzt wurde. Alternativ kann in der Variante eine Maßnahme nach ISO/IEC 27001:2013, Anhang A, enthalten sein, sodass sie nicht ausgeschlossen würde.

Auditoren sollten auf die Konformität mit der Spezifikation der notwendigen Maßnahmen der Organisation und nicht auf mit der in ISO/IEC 27001:2013, Anhang A, aufgeführten Spezifikation achten. Sofern die Spezifikation der Organisation ein dokumentiertes Verfahren verlangt, bildet dies einen Teil der Konformität der Organisation mit ISO/IEC 27001:2013, 7.5.1 b). Sofern dies nicht zutrifft, sollten Auditoren keine Einsichtnahme verlangen. Auditoren sollten jedoch die Anforderung [ISO/IEC 27001:2013, 8.1)] beachten, dass die Organisation „dokumentierte Informationen im notwendigen Umfang aufbewahren [sollte], sodass darauf vertraut werden kann, dass die Prozesse wie geplant umgesetzt wurden“. Da sich ISO/IEC 27001:2013, 8.1, auf ISO/IEC 27001:2013, 6.1, bezieht, fallen der Risikobehandlungsplan der Organisation und daher dessen notwendige Maßnahmen in den Geltungsbereich dieser Anforderung an dokumentierte Informationen.

Beim Auditieren der Auswahl von Maßnahmen ist es besser, anhand des Plans/der Pläne zur Informationssicherheitsrisikobehandlung [wie in ISO/IEC 27001:2013, 6.1.3 e), angegeben] und nicht anhand der individuellen notwendigen Maßnahmen zu auditieren, die in der Erklärung zur Anwendbarkeit aufgeführt sind. Der Grund hierfür liegt darin, dass der/die Plan/Pläne zur Informationssicherheitsrisikobehandlung wahrscheinlich die Wechselwirkung zwischen notwendigen Maßnahmen angibt/angeben. Dies ist ein Gesichtspunkt, der übersehen werden kann, wenn lediglich die Erklärung zur Anwendbarkeit verwendet wurde.

A.5 Sonstige dokumentierte Informationen

Das Hauptaugenmerk von ISO/IEC 27001 ist auf Ergebnisse gerichtet. Von den 16 expliziten Anforderungen an dokumentierte Informationen (siehe Tabelle A.1) treffen lediglich drei auf Spezifikationen zu (den Informationssicherheitsrisikobeurteilungsprozess, den Informationssicherheitsrisikobehandlungsprozess und das Auditprogramm). Dies hindert eine Organisation jedoch nicht daran, über dokumentierte Verfahren zu verfügen. Eine derartige unterstützende Dokumentation fällt in den Anwendungsbereich von ISO/IEC 27001:2013, 7.5.1 b) (dokumentierte Informationen, die die Organisation als notwendig für die Wirksamkeit des Managementsystems festgelegt hat). Sie wird dadurch zu einer Anforderung an eine Organisation und sollte daher in den Anwendungsbereich eines Audits fallen.

A.6 Anmerkungen

Die geforderten Informationen können Teil einer Webseite sein oder dem Leser in Form von Ergebnissen einer Datenbankabfrage dargestellt werden. Darüber hinaus werden durch ISO/IEC 27001 für die Dokumente mit Ausnahme der Erklärung zur Anwendbarkeit keine Namen vergeben. Die dokumentierten Informationen, die die Informationssicherheitspolitik betreffen, sind daher möglicherweise nicht in einem Dokument oder auf einer Webseite mit dem Namen „Informationssicherheitspolitik“ enthalten. Die

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

Organisationen sind berechtigt, die Informationssicherheitspolitik anders zu bezeichnen. Die Person(en), die verantwortlich und befugt ist/sind sicherzustellen, dass das Informationssicherheitsmanagementsystem den Anforderungen nach ISO/IEC 27001:2013, 5.3 a), entspricht, ist/sind ebenfalls dazu berechtigt und sollte(n) die Beziehung zwischen den von ISO/IEC 27001 vorgeschriebenen Anforderungen an dokumentierte Informationen und ihren dokumentierten Informationen kennen.

A.7 Leitfaden zur Auditierung eines ISMS

In Tabelle A.2 sind die folgenden Informationen aufgeführt:

— erste Zeile: Nummer und Überschrift des entsprechenden Unterabschnitts von ISO/IEC 27001:2013;

— zweite Zeile: zugehörige Abschnitte (Informationen zur Verwendung dieser Zeile siehe A.2.2);

— dritte Zeile: maßgebliche Definitionen von ISO/IEC 27000:2018 für den entsprechenden Unterabschnitt von ISO/IEC 27001:2013;

— vierte Zeile: „Auditnachweis" – mögliche Informationsquellen über den entsprechenden Unterabschnitt von ISO/IEC 27001:2013;

— fünfte Zeile: „Audit-Praxisanleitung" – Leitfaden für das Auditieren (siehe A.3);

— sechste Zeile: „Unterstützende Dokumente" – Verweisungen auf weitere Dokumente, die beim Auditieren anhand des entsprechenden Unterabschnitts von ISO/IEC 27001:2013 hilfreich sein können.

Tabelle A.2 – Leitfaden für das Auditieren nach ISO/IEC 27001

A.1 Kontext der Organisation (ISO/IEC 27001:2013, Abschnitt 4)	
A.1.1 Verständnis der Organisation und ihres Kontextes (ISO/IEC 27001:2013, 4.1)	
Zugehörige Unterabschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 6.1, 9.3
Zutreffende Definitionen nach ISO/IEC 27000	Externer Kontext, Informationssicherheit, interner Kontext, Managementsystem, Organisation
Auditnachweis	Ein Auditnachweis ist anhand dokumentierter Informationen oder anderer Informationen möglich über: a) die wichtigen Aspekte, die sich positiv oder negativ auf das ISMS auswirken können; b) die Organisation; c) den Zweck der Organisation; d) das angestrebte Ergebnis des ISMS. Zu möglichen Quellen wichtiger Aspekte können gehören: a) Umgebungsmerkmale oder -bedingungen im Zusammenhang mit Klima, Umweltverschmutzung, Ressourcenverfügbarkeit und Biodiversität sowie die Wirkung, die diese Bedingungen auf die Fähigkeit der Organisation zur Erreichung ihrer Ziele haben können; b) der kulturelle, soziale, politische, gesetzliche, behördliche, finanzielle, technologische, ökonomische, natürliche und wettbewerbliche Kontext, der internationalen, nationalen, regionalen oder lokalen Charakter haben kann;

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

	c) Merkmale oder Bedingungen der Organisation wie beispielsweise organisatorische Führung, Informationsflüsse und Entscheidungsfindungsprozesse; — organisatorische Richtlinien, Ziele und in Kraft befindliche Strategien zu deren Einhaltung bzw. Erreichung; — die Kultur der Organisation; — durch die Organisation übernommene Normen, Leitfäden und Modelle; — der Lebenszyklus der Produkte und Dienstleistungen der Organisation; — Informationssysteme, Prozesse, Wissenschaft und Technik, die dem Informationssicherheitsmanagement zugrunde liegen; d) Trends bei Audits und Risikobeurteilung.
Audit-Praxis-anleitung	Auditoren sollten bestätigen, dass die Organisation: a) auf der Führungsebene ein Verständnis (z. B. strategisches Verständnis) der wichtigen Aspekte hat, die sich positiv oder negativ auf das ISMS auswirken können; b) die externen und internen Aspekte kennt, die für ihren Zweck maßgeblich sind und sich auf ihre Fähigkeit zur Erreichung der angestrebten Ergebnisse ihres ISMS auswirken. ANMERKUNG 1 Die Anforderung in ISO/IEC 27001:2013, 4.3, besteht darin, „die unter ISO/IEC 27001:2013, 4.1, genannten externen und internen Themen [zu] berücksichtigen". Eine Organisation kann Punkte berücksichtigen, die nicht unbedingt im Ergebnis aufgeführt sind. Auditoren sollten außerdem bestätigen, dass zu den angestrebten Ergebnissen die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gehört, indem ein Risikomanagementprozess angewendet wird und Risiken entsprechend behandelt werden.
	Auditoren sollten außerdem überprüfen, ob zu den Aspekten die für die Organisation wichtigen Themen, zu beratende und erörternde Probleme und sich ändernde Umstände gehören. Außerdem sollte überprüft werden, ob die gewonnenen Kenntnisse verwendet werden, um bei den Bemühungen der Organisation zur Planung, Umsetzung und zum Betrieb des Managementsystems als Anleitung zu dienen.
Unterstützende Dokumente	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.1
A.1.2 Verständnis der Bedürfnisse und Erwartungen interessierter Parteien (ISO/IEC 27001:2013, 4.2)	
Zugehörige Unterabschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 4.1, 4.3
Zutreffende Definitionen nach ISO/IEC 27000	Interessierte Partei
Auditnachweis	Ein Auditnachweis ist anhand dokumentierter Informationen oder anderer Informationen möglich über: a) die interessierten Parteien; b) die Bedürfnisse und Erwartungen betroffener interessierter Parteien, die für das ISMS und ISO/IEC 27001 gelten.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

	ANMERKUNG 2 Zu möglichen interessierten Parteien können gehören: a) Rechtsinstanzen und Kontrollbehörden (lokale, regionale, bundesstaatliche/bezirkliche, nationale oder internationale); b) übergeordnete Organisationen; c) Kunden; d) Fach- und Berufsverbände; e) Kommunalverbände; f) Nichtregierungsorganisationen; g) Lieferanten; h) Nachbarn; i) Angehörige der Organisation und andere, die im Auftrag der Organisation tätig sind; j) Informationssicherheitsexperten. ANMERKUNG 3 Zu Anforderungen interessierter Parteien können gehören: a) Gesetze; b) Bewilligungen, Lizenzen oder andere Genehmigungsformen; c) durch Behörden erteilte Aufträge; d) Urteile von Gerichten oder Verwaltungsgerichten; e) Abkommen, Konventionen und Protokolle; f) zutreffende Industrievorschriften und -normen; g) abgeschlossene Verträge; h) Vereinbarungen mit Kommunalverbänden oder Nichtregierungsorganisationen; i) Vereinbarungen mit Behörden und Kunden; j) organisatorische Anforderungen; k) freiwillige Prinzipien oder Verhaltensvorschriften; l) freiwillige Verpflichtungen zur Kennzeichnung oder zum Umweltschutz; m) Pflichten, die sich aus vertraglichen Vereinbarungen mit der Organisation ergeben; n) Informations- und Nachrichtenaustausch. ANMERKUNG 4 Interessierte Parteien können unterschiedliche Interessen haben, die vollständig oder teilweise mit den Geschäftszielen der Organisation übereinstimmen oder diesen entgegengesetzt sind. Ein Beispiel, bei dem eine interessierte Partei Interessen hat, die den Zielen der Organisation entgegengesetzt sind, ist der Hacker. Der Hacker erwartet von der Organisation eine schwache Sicherheit. Die Organisation sollte die Anforderung dieser interessierten Partei berücksichtigen, indem sie eine genau entgegengesetzte, d. h. starke, Sicherheit praktiziert. Auditoren sollten sich der Tatsache bewusst sein, dass das ISMS alle internen und externen Risikoquellen berücksichtigt. Daher ist das Verständnis der Organisation hinsichtlich interessierter Parteien und ihrer Anforderungen von hoher Bedeutung, die den Zielen der Organisation entgegengesetzt sind.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

Audit-Praxis-anleitung	Auditoren sollten bestätigen, dass die Organisation auf der Führungsebene ein Verständnis (z. B. strategisches Verständnis) der Bedürfnisse und Erwartungen betroffener interessierter Parteien hat, die für das ISMS und ISO/IEC 27001 gelten. Auditoren sollten überprüfen, ob die Organisation die Anforderungen interessierter Parteien, die sie freiwillig übernimmt oder über die sie freiwillig eine Vereinbarung oder einen Vertrag schließt, sowie die obligatorischen Bedürfnisse und Erwartungen identifiziert hat, da diese durch staatliche oder gerichtliche Verfahren in Gesetze, Vorschriften, Zulassungen und Lizenzen aufgenommen wurden. Es wird angemerkt, dass nicht alle Anforderungen interessierter Parteien Anforderungen der Organisation sind und einige nicht für die Organisation gelten oder für das ISMS maßgeblich sind. Manche Bedürfnisse interessierter Parteien (z. B. die eines Hackers) stehen im Widerspruch zum Zweck des ISMS, und von der Organisation wird erwartet, dass sie durch geeignete Informationssicherheitsmaßnahmen sicherstellt, dass derartige Bedürfnissen und Erwartungen nicht erfüllt werden. Auditoren können außerdem bestätigen, dass es interessierte Parteien gibt, die sich selbst als durch das ISMS betroffen wahrnehmen, und die Organisation in einem derartigen Fall darüber in Kenntnis setzen. Auditoren können außerdem überprüfen, ob die Organisation die gewonnenen Kenntnisse bei ihren Bemühungen zur Planung, Umsetzung und zum Betrieb des ISMS verwendet.
Unterstützende Dokumente	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.2
A.1.3 Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems (ISO/IEC 27001:2013, 4.3)	
Zugehörige Unter-abschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 4.1, 4.2
Zutreffende Definitionen nach ISO/IEC 27000	Ausgliedern
Auditnachweis	Ein Auditnachweis ist anhand dokumentierter Informationen oder anderer Informationen möglich über: — den Anwendungsbereich des Managementsystems der Organisation (entsprechend der Definition nach ISO/IEC 27001:2013, 4.3); — gegebenenfalls den Geltungsbereich einer Zertifizierung der Organisation; — die Erklärung zur Anwendbarkeit. ANMERKUNG 5 Der Geltungsbereich einer Zertifizierung der Organisation ist nicht unbedingt mit dem Anwendungsbereich ihres ISMS identisch. Im Allgemeinen ist der Geltungsbereich der Zertifizierung auf die ISMS-Organisation beschränkt.
Audit-Praxis-anleitung	Auditoren sollten bestätigen, dass die Organisation eigenständig die physischen, informationstechnischen, gesetzlichen und organisatorischen Grenzen festlegt, auf die das ISMS angewendet wird, und dass sie die ISO/IEC 27001 innerhalb der gesamten Organisation oder als spezielle Einheit oder bestimmte Funktion(en) innerhalb einer Organisation umsetzt.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

	Auditoren sollten überprüfen, ob das Verständnis der Organisation hinsichtlich ihres Kontextes (ISO/IEC 27001:2013, 4.1), der Anforderungen betroffener interessierter Parteien (ISO/IEC 27001:2013, 4.2) sowie von Schnittstellen und Abhängigkeiten zwischen Aktivitäten, die durch die Organisation durchgeführt werden, und denen, die durch andere Organisationen durchgeführt werden [ISO/IEC 27001:2013,4.3 c)], bei der Festlegung des Anwendungsbereichs des ISMS entsprechend berücksichtigt wurden. Soweit dies auf den Auditumfang zutrifft, sollten Auditoren ferner bestätigen, dass die Informationssicherheitsrisikobeurteilung und die Risikobehandlung der Organisation ihre Aktivitäten ordnungsgemäß widerspiegeln und sich bis zu den Grenzen ihrer Aktivitäten erstrecken, die im Anwendungsbereich des ISMS definiert sind. Auditoren sollten überprüfen, ob je Anwendungsbereich mindestens eine Erklärung zur Anwendbarkeit vorliegt und alle im Risikomanagementprozess festgelegten Maßnahmen in der/den Erklärung(en) zur Anwendbarkeit enthalten sind. Bei diesen Maßnahmen handelt es sich um die in ISO/IEC 27001:2013, 6.1.3 b), aufgeführten notwendigen Maßnahmen und nicht unbedingt um Maßnahmen nach ISO/IEC 27001:2013, Anhang A. Hierzu können sektorspezifische Maßnahmen sowie Maßnahmen gehören, die durch die Organisation konzipiert oder aus einer anderen Quelle identifiziert wurden. Auditoren sollten außerdem bestätigen, dass Schnittstellen mit Dienstleistungen oder Aktivitäten, die nicht vollständig im Anwendungsbereich des ISMS liegen, vorbehaltlich der Auditierung in das ISMS einbezogen und in der Informations-sicherheitsrisikobeurteilung der Organisation enthalten sind. Ein Beispiel einer derartigen Situation ist die gemeinsame Nutzung von Einrichtungen (z. B. IT-Systeme, Datenbanken und Telekommunikationssysteme oder die Ausgliederung einer Geschäftsfunktion) mit anderen Organisationen. Es sollte überprüft werden, ob die Dokumentation des Anwendungsbereichs in Übereinstimmung mit den Anforderungen an dokumentierte Informationen (ISO/IEC 27001:2013, 7.5) erstellt und kontrolliert wird.
Unterstützende Dokumente	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.3 ISO/IEC 27006:2015, 8.2, 9.1.3.5 (IS 9.1.3 Geltungsbereich der Zertifizierung) ISO/IEC 17021-1:2015, 8.2.2
A.1.4 Informationssicherheitsmanagementsystem (ISO/IEC 27001:2013, 4.4)	
Zugehörige Abschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 6.1.1, 6.1.2, 6.1.3, 8.1, 8.2, 8.3
Zutreffende Definitionen nach ISO/IEC 27000	Fortlaufende Verbesserung, Informationssicherheit, Managementsystem

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

Auditnachweis	Ein Auditnachweis ist anhand dokumentierter Informationen oder anderer Informationen über die nach ISO/IEC 27001 festzulegenden Prozesse möglich, zu denen gehören: a) Prozesse für das Managementsystem (ISO/IEC 27001:2013, 4.4); b) Prozesse zur betrieblichen Planung und Steuerung einschließlich ausgegliederter Prozesse (ISO/IEC 27001:2013, 8.1); c) Prozesse zur Behandlung von Risiken und Chancen bei der Planung des ISMS einschließlich der Prozesse zur Informationssicherheitsrisikobeurteilung (ISO/IEC 27001:2013, 6.1.2 und/oder 8.1.2) und der Prozesse zur Informationssicherheitsrisikobehandlung (ISO/IEC 27001:2013, 6.1.3 und/oder 8.1.3); d) Prozesse zur Erreichung der Informationssicherheitsziele.
Audit-Praxis-anleitung	Auditoren sollten bestätigen, dass die Organisation den „notwendigen, aber ausreichenden" Satz von Prozessen und Maßnahmen erstellt, die zusammen ein wirksames Managementsystem in Übereinstimmung mit ISO/IEC 27001 bilden, und das ISMS aus dem Satz dieser miteinander zusammenhängenden bzw. in Wechselwirkung stehenden Elemente einrichtet. Auditoren sollten außerdem bestätigen, dass die Organisation in ihrer vorhandenen Kapazität die Entscheidungsgewalt, Verantwortung und Eigenständigkeit behält, um Entscheidungen über die Art und Weise der Erfüllung der ISMS-Anforderungen zu treffen, einschließlich der Detailliertheit und des Ausmaßes, mit der/in dem sie die ISMS-Anforderungen in ihre Geschäftstätigkeit integriert.
Unterstützende Dokumente	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.4
A.2 Führung (ISO/IEC 27001:2013, Abschnitt 5)	
A.2.1 Führung und Verpflichtung (ISO/IEC 27001:2013, 5.1)	
Zugehörige Abschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 4.1, 4.2, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.1, 7.4, 8.1, 9.3, 10.2
Zutreffende Definitionen nach ISO/IEC 27000	Informationssicherheit, oberste Leitung
Auditnachweis	Ein Auditnachweis ist anhand dokumentierter Informationen oder anderer Informationen möglich über: a) die Informationssicherheitspolitik [ISO/IEC 27001:2013, 5.1 a)]; b) die Informationssicherheitsziele [ISO/IEC 27001:2013, 5.1 a)]; c) die Prozesse der Organisation; d) die Ergebnisse von Managementbewertungen [ISO/IEC 27001:2013, 5.1 c), e) und g)]; e) Beurteilung des Ressourcenbedarfs; f) Kommunikation der Bedeutung eines wirksamen Informationssicherheitsmanagements und der Einhaltung der Anforderungen an das Informationssicherheitsmanagementsystem. Ein Nachweis ist außerdem mit Hilfe von Befragungen der obersten Leitung möglich. Die Ergebnisse von Managementbewertungen können außerdem zur Erbringung von Nachweisen bei anderen Unterabschnitten als ISO/IEC 27001:2013, 5.1 c), e) und g) dienen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 27007:2021-10

Audit-Praxis-anleitung	Auditoren sollten die wahrnehmbare Unterstützung, Einbeziehung und das wahrnehmbare Engagement der obersten Leitung der Organisation bestätigen, die für die erfolgreiche Umsetzung von ISO/IEC 27001 wichtig sind. Auditoren sollten außerdem überprüfen, ob: a) delegierte Aufgaben der obersten Leitung klar benannt sind; b) die oberste Leitung für die zufriedenstellende Durchführung von Aktivitäten verantwortlich bleibt, die der Organisation zugewiesen sind; c) die oberste Leitung sicherstellt, dass die Informationssicherheitspolitik und deren Ziele festgelegt und an die strategische Ausrichtung der gesamten Organisation angeglichen sind; d) die oberste Leitung die Bedeutung eines wirksamen Informationssicherheits-managements und der Einhaltung der ISMS-Anforderungen kommuniziert; e) die oberste Leitung sicherstellt, dass das ISMS seine angestrebten Ergebnisse erreicht, indem es die Umsetzung aller Prozesse des Informationssicherheitsmanagements unterstützt, und insbesondere, indem sie Berichte über den Zustand und die Wirksamkeit des ISMS anfordert und überprüft [siehe ISO/IEC 27001:2013, 5.3 b)]; f) die oberste Leitung die Menschen in der Organisation anleitet und unterstützt, die direkt mit der Informationssicherheit und dem ISMS zu tun haben; g) die oberste Leitung die Integration der ISMS-Anforderungen in die Prozesse der Organisation sicherstellt; h) die oberste Leitung die Verfügbarkeit von Ressourcen sicherstellt, sodass ein wirksames ISMS zur Verfügung steht; i) die oberste Leitung bei Managementbewertungen den Ressourcenbedarf beurteilt und Ziele zur fortlaufenden Verbesserung und zur Überwachung der Wirksamkeit geplanter Aktivitäten festlegt; j) die oberste Leitung eine Kultur und Umgebung schafft, die Menschen dazu anregt, aktiv an der Umsetzung der Anforderungen des ISMS mitzuwirken und sich zu bemühen, die Informationssicherheitsziele zu erreichen.
Unterstützende Dokumente	ISO 31000:2018, 4.2 ISO/IEC 27003:2017, 5.1
A.2.2 Politik (ISO/IEC 27001:2013, 5.2)	
Zugehörige Abschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 6.2, 7.4
Zutreffende Definitionen nach ISO/IEC 27000	Informationssicherheit, Politik
Auditnachweis	Ein Auditnachweis ist anhand dokumentierter Informationen oder anderer Informationen möglich über: a) Informationssicherheitspolitik (ISO/IEC 27001:2013, 5.1); b) Informationssicherheitsziele [ISO/IEC 27001:2013, 5.2 b) und ISO/IEC 27001:2013, 6.2].

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10

Audit-Praxis-anleitung	Auditoren sollten bestätigen, dass: a) die Informationssicherheitspolitik die von ISO/IEC 27001 geforderten organisatorischen Verpflichtungen der Führungsebene festlegt, wobei der Zweck der Organisation berücksichtigt wird; b) die Informationssicherheitspolitik verwendet wird, um entweder die Informationssicherheitsziele zu formulieren oder festzulegen, die sich die Organisation selbst gibt oder die als Teil der Informationssicherheitspolitik angegeben sind; c) dokumentierte Informationen der Informationssicherheitspolitik in Übereinstimmung mit den Anforderungen an dokumentierte Informationen (ISO/IEC 27001:2013, 7.5) erstellt und kontrolliert werden; d) die Informationssicherheitspolitik in Übereinstimmung mit den Anforderungen des Kommunikationsabschnitts (ISO/IEC 27001:2013, 7.4) intern kommuniziert wird; e) die Informationssicherheitspolitik gegebenenfalls auch anderen interessierten Parteien zur Verfügung gestellt wird. Da die Informationssicherheitspolitik eine Verpflichtung zur Erfüllung geltender Anforderungen enthält, insbesondere hinsichtlich einschlägiger Gesetze und Vorschriften, sollte das ISMS als konform angesehen werden, solange es zur unverzüglichen Erkennung und zu Korrekturmaßnahmen an den Systemmängeln führt, die zu den Fällen von Nichtkonformität beigetragen haben.
Unterstützende Dokumente	ISO 31000:2018, 4.3.2 ISO/IEC 27003:2017, 5.2
A.2.3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse (ISO/IEC 27001:2013, 5.3)	
Zugehörige Abschnitte von ISO/IEC 27001	ISO/IEC 27001:2013, 7.4, 9.2, 9.3
Zutreffende Definitionen nach ISO/IEC 27000	Informationssicherheit, Organisation, oberste Leitung
Auditnachweis	Unter Berücksichtigung von ISO/IEC 27001:2013, 7.5.1 b), ist ein Auditnachweis anhand dokumentierter Informationen oder anderer Informationen möglich über: a) die organisatorischen Rollen; b) die Arbeitsplatzbeschreibung von unter Kontrolle der Organisation arbeitenden Personen, die einen Einfluss auf die Informationssicherheitsleistung der Organisation haben können; c) die Umsetzung des Programms für interne Audits und die Auditergebnisse; d) den Anwendungsbereich des ISMS und die Struktur der Organisation. Zusätzlich ist ein weiterer Auditnachweis anhand dokumentierter Informationen oder anderer Informationen über die Ergebnisse von Managementbewertungen möglich.
Audit-Praxis-anleitung	Auditoren sollten anhand der Überprüfung dokumentierter Informationen und/oder anhand von Befragungen bestätigen, dass: a) Verantwortlichkeiten und Befugnisse zur Umsetzung der ISMS-Anforderungen den betreffenden Rollen innerhalb der Organisation zugewiesen sind;

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 27007:2021-10