DIN EN ISO/IEC 27007

ICS 03.120.20; 35.030

Informationssicherheit, Cybersicherheit und Datenschutz – Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020); Deutsche Fassung EN ISO/IEC 27007:2022

Information security, cybersecurity and privacy protection –
Guidelines for information security management systems auditing (ISO/IEC 27007:2020);
German version EN ISO/IEC 27007:2022

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 EN ISO/IEC 27007:2022

Gesamtumfang 58 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27007:2022-10

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 EN ISO/IEC 27007:2022 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).

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

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*

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: DIN EN ISO/IEC 27007:2022-10

— Leerseite —

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27007

Januar 2022

ICS 03.120.20; 35.030

Deutsche Fassung

Informationssicherheit, Cybersicherheit und Datenschutz — Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen (ISO/IEC 27007:2020)

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (ISO/IEC 27007:2020)

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)

Diese Europäische Norm wurde vom CEN am 26. Dezember 2021 angenommen.

Diese Europäische Norm wurde korrigiert und vom CEN-CENELEC-Management-Zentrum am 26. Januar 2022 neu herausgegeben.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27007:2022-10

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 steuert (steuern) ... 8
5.4.2 Kompetenz von Person(en), die das Auditprogramm steuert (steuern) ... 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 Auditmethoden ... 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: DIN EN ISO/IEC 27007:2022-10

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 13
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 14
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 der entsprechenden Methode 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) Anleitung 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 zum Auditieren eines ISMS 16
A.2.3 Audit und dokumentierte Informationen 17
A.3 Anleitung 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 Anleitung zur Auditierung eines ISMS 20

Literaturhinweise 54

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27007:2022-10

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 EN ISO/IEC 27007:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juli 2022, und etwaige entgegenstehende nationale Normen müssen bis Juli 2022 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 27007:2020 wurde von CEN als EN ISO/IEC 27007:2022 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

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 wurde 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: DIN EN ISO/IEC 27007:2022-10

Einleitung

Ein Audit eines Informationssicherheitsmanagementsystems (ISMS, en: Information Security Management System) 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 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 eine Anleitung 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. Diese Anleitung 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 Anleitung.

Dieses Dokument ist in Verbindung mit der in ISO 19011:2018 enthaltenen Anleitung anzuwenden.

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

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

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

1 Anwendungsbereich

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

Dieses Dokument ist anzuwenden für alle, die sich mit internen oder externen Audits eines ISMS vertraut machen oder diese durchführen müssen oder ein ISMS-Auditprogramm steuern 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 https://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 die Anleitung in 5.2.2.

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

a) identifizierte Anforderungen an die Informationssicherheit;

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

b) Anforderungen nach ISO/IEC 27001;

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 den 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 steuert (steuern)

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

5.4.2 Kompetenz von Person(en), die das Auditprogramm steuert (steuern)

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 die Anleitung 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 im Auftrag der Organisation tätig sind, 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;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

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 Informationstechnik;

g) die Anzahl ähnlicher Standorte.

Im Auditprogramm sollte die Erstellung 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 verpflichtenden 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 die Anleitung 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 die Anleitung in 5.5.2.2.

5.5.2.2 Zu den Zielen des Audits darf Folgendes gehören:

a) Beurteilung, ob das ISMS Anforderungen zur 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: DIN EN ISO/IEC 27007:2022-10

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 geeigneten Behandlung von Risiken;

f) die Methoden 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 Auditmethoden

5.5.3.1 Es gilt der Leitfaden nach ISO 19011:2018, 5.5.3. Außerdem gilt die Anleitung 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 die Anleitung 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 Methoden 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: DIN EN ISO/IEC 27007:2022-10

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 die Anleitung in 6.2.2.2.

6.2.2.2 Falls notwendig 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 die Anleitung 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.

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27007:2022-10

6.3.2 Planung des Audits

6.3.2.1 Es gilt der Leitfaden nach ISO 19011:2018, 6.3.2. Außerdem gilt die Anleitung 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 die Anleitung 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 die Anleitung in 6.4.5.2.

6.4.5.2 Falls Auditnachweise aus Gründen der Klassifizierung oder Sensitivität 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 die Sensitivität der Nachweise zu gefährden, 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 die Anleitung in 6.4.6.2.

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10

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 relevanten 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 die Anleitung in 6.4.7.2.

6.4.7.2 Zu möglichen Methoden 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-Werkzeuge.

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.

6.5.2 Verteilung des Auditberichts

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

6.5.2.2 ANMERKUNG

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27007:2022-10

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 die Anleitung 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 Technik (z. B. die umgesetzten Maßnahmen, dokumentierte Informationen und/oder Prozesssteuerung, 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.

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 von Managementsystemen

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27007:2022-10