

November 2019

ICS 03.100.70; 35.030

Deutsche Fassung

Informationstechnik - Sicherheitsverfahren - Leitfäden für
das Auditieren von
Informationssicherheitsmanagementsystemen (ISO/IEC
27007:2017)

Information technology - Security techniques -
Guidelines for information security management
systems auditing (ISO/IEC 27007:2017)

Technologies de l'information - Techniques de sécurité
- Lignes directrices pour l'audit des systèmes de
management de la sécurité de l'information (ISO/IEC
27007:2017)

Dieser Europäische Norm-Entwurf wird den CEN-Mitgliedern zur Umfrage vorgelegt. Er wurde vom Technischen Komitee CEN/CLC/JTC 13 erstellt.

Wenn aus diesem Norm-Entwurf eine Europäische Norm wird, sind die CEN und CENELEC-Mitglieder gehalten, die CEN und 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.

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

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees 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.

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

Warnvermerk : Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäischen Norm in Bezug genommen werden.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

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
5.1.1 IS 5.1 Allgemeines.....	7
5.2 Festlegung der Ziele des Auditprogramms.....	8
5.2.1 IS 5.2 Festlegung der Ziele des Auditprogramms.....	8
5.3 Aufstellung des Auditprogramms.....	8
5.3.1 Rollen und Verantwortlichkeiten der Person, die das Auditprogramm managt.....	8
5.3.2 Kompetenz der Person, die das Audit Programm managt.....	8
5.3.3 Festlegung des Umfangs des Auditprogramms.....	8
5.3.4 Identifikation und Beurteilung von Auditprogrammrisiken.....	9
5.3.5 Erstellung von Verfahren für das Auditprogramm.....	9
5.3.6 Identifikation von Auditprogrammressourcen.....	9
5.4 Umsetzung des Auditprogramms.....	10
5.4.1 Allgemeines.....	10
5.4.2 Definition der Ziele, des Anwendungsbereichs und der Kriterien für ein Einzelaudit.....	10
5.4.3 Auswahl der Auditverfahren.....	11
5.4.4 Auswahl der Mitglieder des Auditteams.....	11
5.4.5 Übertragung der Verantwortung für ein Einzelaudit an den Leiter des Auditteams.....	11
5.4.6 Management des Ergebnisses des Auditprogramms.....	11
5.4.7 Management und Pflege der Auditprogrammunterlagen.....	11
5.5 Überwachung des Auditprogramms.....	11
5.6 Überprüfung und Verbesserung des Auditprogramms.....	11
6 Durchführung eines Audits.....	12
6.1 Allgemeines.....	12
6.2 Einleitung des Audits.....	12
6.2.1 Allgemeines.....	12
6.2.2 Herstellung des Erstkontakts mit der auditierten Organisation.....	12
6.2.3 Feststellung der Durchführbarkeit des Audits.....	12
6.3 Vorbereitung von Auditaktivitäten.....	12
6.3.1 Durchführung der Dokumentenüberprüfung bei der Vorbereitung auf das Audit.....	12
6.3.2 Erarbeitung des Auditplans.....	12
6.3.3 Übertragung von Arbeiten an das Auditteam.....	13
6.3.4 Erarbeitung von Arbeitsdokumenten.....	13
6.4 Durchführung der Auditaktivitäten.....	13
6.4.1 Allgemeines.....	13
6.4.2 Durchführung der Eröffnungsbesprechung.....	13
6.4.3 Durchführung der Dokumentenüberprüfung bei der Durchführung des Audits.....	13

prEN ISO/IEC 27007:2019 - Preview only Copy via ILNAS e-Shop

6.4.4	Kommunikation während des Audits	13
6.4.5	Zuweisung von Rollen und Verantwortlichkeiten von Guides und Beobachtern.....	13
6.4.6	Erfassung und Überprüfung von Informationen.....	14
6.4.7	Erstellung der Auditfeststellungen.....	14
6.4.8	Erarbeitung der Auditschlussfolgerungen.....	14
6.4.9	Durchführung der Abschlussbesprechung.....	14
6.5	Erarbeitung und Verteilung des Auditberichts	14
6.5.1	Erarbeitung des Auditberichts.....	14
6.5.2	Verteilung des Auditberichts.....	15
6.6	Abschluss des Audits	15
6.7	Durchführung von Auditfolgemassnahmen.....	15
7	Kompetenz und Bewertung von ISMS-Auditoren	15
7.1	Allgemeines	15
7.2	Ermittlung der Kompetenz von Auditoren zur Erfüllung der Belange des Auditprogramms	15
7.2.1	Allgemeines.....	15
7.2.2	Persönliches Verhalten	16
7.2.3	Kenntnisse und Fertigkeiten	16
7.2.4	Erreichung der Kompetenz von Auditoren.....	16
7.2.5	Leiter des Auditteams	16
7.3	Aufstellung von Kriterien zur Bewertung von Auditoren	16
7.4	Auswahl des entsprechenden Verfahrens zur Bewertung von Auditoren.....	16
7.5	Durchführung der Bewertung von Auditoren.....	17
7.6	Aufrechterhaltung und Verbesserung der Kompetenz von Auditoren.....	17
Anhang A (informativ) Leitfaden zur praktischen Durchführung von ISMS-Audits.....		18
A.1	Überblick.....	18
A.2	Allgemeines	18
A.2.1	Ziele, Umfang und Kriterien von Audits sowie Auditnachweise	18
A.2.2	Strategie zur Auditierung eines ISMS	18
A.2.3	Audit und dokumentierte Informationen	19
A.3	Leitfaden über die Anforderungen an dokumentierte Informationen nach ISO/IEC 27001 ...	19
A.3.1	Hintergrund	19
A.3.2	Beispiel einer impliziten Anforderung an dokumentierte Information	20
A.3.3	Beispiele, bei denen keine expliziten oder impliziten Anforderungen an dokumentierte Informationen vorliegen.....	20
A.4	Die Erklärung zur Anwendbarkeit.....	21
A.5	Sonstige dokumentierte Information	21
A.6	Anmerkungen.....	21
A.7	Leitfaden zur Auditierung eines ISMS.....	22
Literaturhinweise		57

Europäisches Vorwort

Der Text von ISO/IEC 27007:2017 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als prEN ISO/IEC 27007:2019 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 27007:2017 wurde von CEN als prEN ISO/IEC 27007:2019 ohne irgendeine Abänderung genehmigt.

Vorwort

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

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

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

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

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, *IT Security techniques* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27007:2011), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Anhang A wurde umformuliert, um eine Übereinstimmung mit ISO/IEC 27001:2013 zu erreichen;
- der überwiegende Teil dieses Dokuments wurde an ISO/IEC 27001:2013 angepasst.

Einleitung

Dieses Dokument dient als Leitfaden für:

- a) das Management eines Auditprogramms für Informationssicherheitsmanagementsysteme (en: Information Security Management System, ISMS);
- b) die Durchführung interner und externer ISMS-Audits in Übereinstimmung mit ISO/IEC 27001;
- c) die Kompetenz und Bewertung von ISMS-Auditoren.

Dieses Dokument sollte in Verbindung mit dem in ISO 19011:2011 enthaltenen Leitfaden angewendet werden.

Der Aufbau dieses Dokuments folgt der Struktur von ISO 19011:2011. Zusätzliche ISMS-spezifische Leitfäden zur Anwendung von ISO 19011:2011 bei ISMS-Audits sind durch die Buchstaben „IS“ gekennzeichnet.

ISO 19011:2011 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.

ANMERKUNG Anforderungen zur akkreditierten Zertifizierung von Auditoren sind in ISO/IEC 27006 zu finden.

Dieses Dokument legt keine Anforderungen fest und ist für alle Anwender einschließlich kleiner und mittelgroßer Organisationen gedacht.

1 Anwendungsbereich

Zusätzlich zu dem in ISO 19011:2011 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 19011:2011, *Guidelines for auditing management systems*

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 19011:2011 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 <http://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>

4 Grundsätze der Auditierung

Es gelten die Grundsätze der Auditierung nach ISO 19011:2011, Abschnitt 4.

5 Management eines Auditprogramms

5.1 Allgemeines

Es gilt der Leitfaden nach ISO 19011:2011, 5.1. Außerdem gilt der folgende Leitfaden.

5.1.1 IS 5.1 Allgemeines

Eine Organisation, die Audits durchführen muss, sollte beim Aufstellen des Auditprogramms¹ die Risiken und Chancen berücksichtigen, die bei der Planung des ISMS festgestellt wurden.

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