



Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 27006:2020

Informationstechnik - IT- Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von

Technologies de l'information -
Techniques de sécurité - Exigences pour
les organismes procédant à l'audit et à la
certification des systèmes de

Information technology - Security
techniques - Requirements for bodies
providing audit and certification of
information security management

11/2020



Nationales Vorwort

Diese Europäische Norm EN ISO/IEC 27006:2020 wurde als luxemburgische Norm ILNAS-EN ISO/IEC 27006:2020 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

DIESES WERK IST URHEBERRECHTLICH GESCHÜTZT

Kein Teil dieser Veröffentlichung darf ohne schriftliche Einwilligung weder vervielfältigt noch in sonstiger Weise genutzt werden - sei es elektronisch, mechanisch, durch Fotokopien oder auf andere Art!

ICS 03.120.20; 35.030

Deutsche Fassung

**Informationstechnik - IT-Sicherheitsverfahren -
Anforderungen an Institutionen, die Audits und
Zertifizierungen von Informationssicherheits-
Managementsystemen anbieten (ISO/IEC 27006:2015,
einschließlich Amd.1:2020)**

Information technology - Security techniques -
Requirements for bodies providing audit and
certification of information security management
systems (ISO/IEC 27006:2015, including Amd 1:2020)

Technologies de l'information - Techniques de sécurité
- Exigences pour les organismes procédant à l'audit et
à la certification des systèmes de management de la
sécurité de l'information (ISO/IEC 27006:2015, y
compris Amd 1:2020)

Diese Europäische Norm wurde vom CEN am 16. November 2020 angenommen.

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 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.



**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	7
5 Allgemeine Anforderungen	7
5.1 Rechts- und Vertragsfragen	7
5.2 Handhabung der Unparteilichkeit	8
5.2.1 IS 5.2 Interessenskonflikte	8
5.3 Haftung und Finanzierung	8
6 Strukturelle Anforderungen	8
7 Anforderungen an Ressourcen	8
7.1 Kompetenz des Personals	8
7.1.1 IS 7.1.1 Allgemeine Betrachtungen	9
7.1.2 IS 7.1.2 Bestimmung von Kompetenzkriterien	9
7.2 Personal, das in die Zertifizierungstätigkeiten einbezogen ist	13
7.2.1 IS 7.2 Nachweis des Wissens und der Erfahrung der Auditoren	13
7.3 Einsatz einzelner externer Auditoren und externer Fachexperten	14
7.3.1 IS 7.3 Einsatz einzelner externer Auditoren und externer Fachexperten als Teil des Auditteams	14
7.4 Aufzeichnungen über Personal	14
7.5 Ausgliederung	15
8 Anforderungen an Informationen	15
8.1 Öffentliche Informationen	15
8.2 Zertifizierungsdokumente	15
8.2.1 IS 8.2 ISMS-Zertifizierungsdokumente	15
8.3 Verweis auf Zertifizierung und Zeichennutzung	15
8.4 Vertraulichkeit	15
8.4.1 IS 8.4 Zugang zu den Aufzeichnungen der Organisation	15
8.5 Informationsaustausch zwischen einer Zertifizierungsstelle und ihren Kunden	15
9 Anforderungen an Prozesse	16
9.1 Tätigkeiten vor der Zertifizierung	16
9.1.1 Antrag	16
9.1.2 Antragsprüfung	16
9.1.3 Auditprogramm	16
9.1.4 Ermittlung des Auditzeitaufwandes	17
9.1.5 Stichprobenprüfung an mehreren Standorten	17
9.1.6 Mehrfach-Managementsysteme	19
9.2 Planung von Audits	19
9.2.1 Festlegung der Auditziele, des Auditumfangs und der Auditkriterien	19
9.2.2 Auswahl des Auditteams und Aufgabenzuordnung	19

9.2.3	Auditplan	20
9.3	Erstzertifizierung	20
9.3.1	IS 9.3.1 Erstzertifizierungsaudit	20
9.4	Durchführen von Audits.....	22
9.4.1	IS 9.4 Allgemeines	22
9.4.2	IS 9.4 Spezifische Elemente des ISMS-Audits.....	22
9.4.3	IS 9.4 Auditbericht	22
9.5	Zertifizierungsentscheidung.....	23
9.5.1	IS 9.5 Zertifizierungsentscheidung	23
9.6	Aufrechterhaltung der Zertifizierung.....	23
9.6.1	Allgemeines	23
9.6.2	Überwachungstätigkeiten	23
9.6.3	Re-Zertifizierung	24
9.6.4	Audits aus besonderem Anlass.....	25
9.6.5	Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung	25
9.7	Einsprüche	25
9.8	Beschwerden.....	25
9.8.1	IS 9.8 Beschwerden.....	25
9.9	Aufzeichnungen zu Kunden	25
10	Managementsystemanforderungen für Zertifizierungsstellen.....	25
10.1	Optionen	25
10.1.1	IS 10.1 ISMS-Umsetzung.....	25
10.2	Option A: Allgemeine Managementsystemanforderungen	25
10.3	Option B: Managementsystemanforderungen übereinstimmend mit ISO 9001	25
	Anhang A (informativ) Wissen und Fertigkeiten für ISMS-Audits und -Zertifizierung	26
	Anhang B (normativ) Auditzeitaufwand.....	28
	Anhang C (informativ) Methoden für Berechnungen des Auditzeitaufwands.....	34
	Anhang D (informativ) Anleitung für die Prüfung umgesetzter Maßnahmen nach ISO/IEC 27001:2013, Anhang A.....	40
	Literaturhinweise.....	51

Europäisches Vorwort

Der Text von ISO/IEC 27006:2015, inklusive Amd.1:2020 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als EN ISO/IEC 27006:2020 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 Mai 2021, und etwaige entgegenstehende nationale Normen müssen bis Mai 2021 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.

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 27006:2015, einschließlich Amd.1:2020 wurde von CEN als EN ISO/IEC 27006:2020 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.

Eine Erläuterung zum freiwilligen Charakter 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, enthält der folgende Link: 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.

ISO/IEC 27006 wurde vom Gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques* erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 27006:2011), die technisch überarbeitet wurde.

Einleitung

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

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

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

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

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