

DIN EN ISO/IEC 27000

ICS 01.040.03; 01.040.35; 03.100.70; 35.030

Ersatz für
DIN EN ISO/IEC 27000:2017-10

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

Information technology –
Security techniques –
Information security management systems –
Overview and vocabulary (ISO/IEC 27000:2018);
German version EN ISO/IEC 27000:2020

Technologies de l'information –
Techniques de sécurité –
Systèmes de management de sécurité de l'information –
Vue d'ensemble et vocabulaire (ISO/IEC 27000:2018);
Version allemande EN ISO/IEC 27000:2020

Gesamtumfang 43 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 27000:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27000:2020 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 Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

ISO 9000:2015	siehe	DIN EN ISO 9000:2015-11
ISO 19011:2011	siehe	DIN EN ISO 19011:2011-12
ISO 27799	siehe	DIN EN ISO 27799
ISO/IEC 17021:2011	siehe	DIN EN ISO/IEC 17021:2011-07-00
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001
ISO/IEC 27002	siehe	DIN EN ISO/IEC 27002
ISO/IEC 27009	siehe	DIN ISO/IEC 27009

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

Änderungen

Gegenüber DIN EN ISO/IEC 27000:2017-10 wurden folgende Änderungen vorgenommen:

- a) die Einleitung wurde umformuliert;
- b) einige Begriffe und Definitionen wurden entfernt;
- c) Abschnitt 3 wurde auf die High-Level-Struktur für MSS ausgerichtet;
- d) Abschnitt 5 wurde überarbeitet, um die Änderungen in den betrachteten Standards zu berücksichtigen;
- e) Anhang A und Anhang B wurden entfernt;
- f) redaktionelle Überarbeitung der Norm.

Frühere Ausgaben

DIN ISO/IEC 27000: 2011-07
DIN EN ISO/IEC 27000: 2017-10

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 9000:2015-11, *Qualitätsmanagementsysteme — Grundlagen und Begriffe (ISO 9000:2015); Deutsche und Englische Fassung EN ISO 9000:2015*

DIN EN ISO 19011:2011-12, *Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2011); Deutsche und Englische Fassung EN ISO 19011:2011*

DIN EN ISO 27799, *Medizinische Informatik — Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002*

DIN EN ISO/IEC 17021:2011-07-00, *Konformitätsbewertung — Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren (ISO/IEC 17021:2011); Deutsche und Englische Fassung EN ISO/IEC 17021:2011*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

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

DIN ISO/IEC 27009, *Informationstechnik — IT-Sicherheitsverfahren — Sektorspezifische Anwendung der ISO/IEC 27001 — Anforderungen*

— Leerseite —

Deutsche Fassung

Informationstechnik —
Sicherheitsverfahren —
Informationssicherheitsmanagementsysteme —
Überblick und Terminologie (ISO/IEC 27000:2018)

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

Technologies de l'information —
Techniques de sécurité —
Systèmes de management de la sécurité de
l'information —
Vue d'ensemble et vocabulaire (ISO/IEC 27000:2018)

Diese Europäische Norm wurde vom CEN am 20. Oktober 2019 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 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

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
0.1 Überblick	6
0.2 Zweck dieses Dokuments	6
0.3 Inhalt dieses Dokumentes	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Managementsysteme für Informationssicherheit (ISMS)	20
4.1 Allgemeines	20
4.2 Was ist ein ISMS?	21
4.2.1 Überblick und Grundsätze	21
4.2.2 Informationen	21
4.2.3 Informationssicherheit	22
4.2.4 Management	22
4.2.5 Managementsystem	22
4.3 Prozessorientierter Ansatz	23
4.4 Warum ein ISMS wichtig ist	23
4.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS	24
4.5.1 Übersicht	24
4.5.2 Identifizierung von Informationssicherheitsanforderungen	24
4.5.3 Beurteilung von Informationssicherheitsrisiken	25
4.5.4 Behandlung von Informationssicherheitsrisiken	25
4.5.5 Auswahl und Umsetzung von Maßnahmen	26
4.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS	27
4.5.7 Fortlaufende Verbesserung	27
4.6 Kritische Erfolgsfaktoren für das ISMS	27
4.7 Nutzen der ISMS-Normenfamilie	28
5 Die ISMS-Normenfamilie	29
5.1 Allgemeine Informationen	29
5.2 Norm, die einen Überblick und die Terminologie beschreibt: ISO/IEC 27000 (dieses Dokument)	30
5.3 Normen, die Anforderungen festlegen	30
5.3.1 ISO/IEC 27001	30
5.3.2 ISO/IEC 27006	30
5.3.3 ISO/IEC 27009	31
5.4 Normen, die allgemeine Leitfäden beschreiben	31
5.4.1 ISO/IEC 27002	31
5.4.2 ISO/IEC 27003	31
5.4.3 ISO/IEC 27004	32
5.4.4 ISO/IEC 27005	32
5.4.5 ISO/IEC 27007	32
5.4.6 ISO/IEC TR 27008	32
5.4.7 ISO/IEC 27013	33

5.4.8	ISO/IEC 27014.....	33
5.4.9	ISO/IEC TR 27016.....	34
5.4.10	ISO/IEC 27021.....	34
5.5	Normen, die branchenspezifische Leitfäden beschreiben	34
5.5.1	ISO/IEC 27010.....	34
5.5.2	ISO/IEC 27011.....	35
5.5.3	ISO/IEC 27017.....	35
5.5.4	ISO/IEC 27018.....	35
5.5.5	ISO/IEC 27019.....	36
5.5.6	ISO 27799	37
	Literaturhinweise.....	38

Europäisches Vorwort

Der Text von ISO/IEC 27000:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27000:2020 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 August 2020, und etwaige entgegenstehende nationale Normen müssen bis August 2020 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.

Dieses Dokument ersetzt EN ISO/IEC 27000:2017.

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 27000:2018 wurde von CEN als EN ISO/IEC 27000:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

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 ist 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 fünfte Ausgabe ersetzt die vierte Ausgabe (ISO/IEC 27000:2016), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- die Einleitung wurde umformuliert;
- einige Begriffe und Definitionen wurden entfernt;
- Abschnitt 3 wurde auf die High-Level-Struktur für MSS ausgerichtet;
- Abschnitt 5 wurde überarbeitet, um die Änderungen in den betrachteten Standards zu berücksichtigen;
- Anhang A und Anhang B wurden entfernt;

Einleitung

0.1 Überblick

Internationale Normen für Managementsysteme stellen ein Vorgehensmodell zum Einrichten und Betreiben eines Managementsystems zur Verfügung. Dieses Modell berücksichtigt die Merkmale, zu denen unter Experten auf dem Gebiet Konsens herrscht, dass diese Merkmale den internationalen Stand der Technik widerspiegeln. ISO/IEC JTC 1/SC 27 unterhält ein Expertengremium, dass sich der Entwicklung von Internationalen Managementsystemnormen für Informationssicherheit, auch bekannt als die Informationssicherheitsmanagementsystem(ISMS)-Normenfamilie.

Durch den Einsatz der ISMS-Normenfamilie können Organisationen ein Rahmenwerk zur Handhabung der Sicherheit ihrer Informationswerte, einschließlich Finanzinformationen, Rechte an geistigem Eigentum und Details zu Beschäftigten, oder der ihnen von Kunden oder Dritten anvertrauten Informationen entwickeln und umsetzen. Diese Standards können auch eingesetzt werden, um sich auf eine unabhängige Beurteilung ihres zum Schutz von Informationen eingesetzten ISMS vorzubereiten.

0.2 Zweck dieses Dokuments

Die ISMS-Normenfamilie beinhaltet Normen, die:

- a) Anforderungen an ein ISMS und an diejenigen, die solche Systeme zertifizieren, festlegen;
- b) direkte Unterstützung, detaillierte Anleitung und/oder Interpretationen für den Gesamtprozess zur Errichtung, Umsetzung, Aufrechterhaltung und Verbesserung eines ISMS anbieten;
- c) sektorspezifische Anleitungen für ISMS adressieren; und
- d) Konformitätsbewertung für ISMS adressieren.

0.3 Inhalt dieses Dokumentes

In diesem Dokument werden die folgenden Verbformen verwendet:

- „muss“ bezeichnet eine Anforderung;
- „sollte“ bezeichnet eine Empfehlung;
- „darf“ bezeichnet eine Erlaubnis;
- „kann“ bezeichnet eine Möglichkeit oder Fähigkeit.

Information, die als „Anmerkung“ gekennzeichnet ist, dient dem Verständnis oder der Klarstellung der dazugehörigen Anforderung. „Anmerkungen zum Begriff“, die in Abschnitt 3 verwendet werden, stellen zusätzliche Information bereit, welche die terminologische Information ergänzt und Maßnahmen in Bezug zur Verwendung eines Begriffes enthalten kann.

1 Anwendungsbereich

Dieses Dokument stellt einen Überblick über Informationssicherheitsmanagementsysteme (ISMS) bereit und enthält Begriffe, die in der ISMS-Normenfamilie üblicherweise verwendet werden. Dieses Dokument ist anwendbar für Organisationen aller Arten und Größe (z. B. gewerbliche Unternehmen, Behörden, nicht-gewinnorientierte Unternehmen).

Die Begriffe, die mit diesem Dokument bereitgestellt werden,

- decken die gebräuchlichen Begriffe ab, die in der ISMS-Normenfamilie verwendet werden;
- decken nicht sämtliche verwendete Begriffe innerhalb der ISMS-Normenfamilie ab; und
- schränken die Normen aus der ISMS-Normenfamilie nicht darin ein, neue Begriffe für die Anwendung zu definieren.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

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/>

3.1

Zugangssteuerung

(en: access control)

Mittel um sicherzustellen, dass der Zugang zu Werten aufgrund von Geschäfts- und Sicherheitsanforderungen (3.56) befugt und eingeschränkt ist

3.2

Angriff

(en: attack)

Versuch, einen Wert zu zerstören, aufzudecken, zu verändern, außer Funktion zu setzen, zu stehlen, zu diesem unbefugten Zugang zu erhalten oder diesen unbefugt zu verwenden

3.3

Audit

(en: audit)

systematischer, unabhängiger und dokumentierter *Prozess* (3.54) zum Erlangen von Auditnachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit die Auditkriterien erfüllt sind

Anmerkung 1 zum Begriff: Ein Audit kann ein internes (Erstparteien-Audit) oder ein externes (Zweitparteien- oder Drittparteien-Audit) Audit sein und es kann ein kombiniertes Audit sein (Verbindung zweier oder mehrerer Disziplinen).

Anmerkung 2 zum Begriff: Ein internes Audit wird von der Organisation selbst durchgeführt oder durch eine externe Partei in ihrem Auftrag.

Anmerkung 3 zum Begriff: „Auditnachweise“ und „Auditkriterien“ sind in ISO 19011 definiert.

3.4

Auditumfang

(en: audit scope)

Ausmaß und Grenzen eines *Audits* (3.3)

[QUELLE: ISO 19011:2011, 3.14, modifiziert — Anmerkung 1 zum Begriff wurde gestrichen.]

3.5

Authentisierung

(en: authentication)

Sicherstellung, dass die von einer Entität behaupteten Eigenschaften richtig sind

3.6

Authentizität

(en: authenticity)

Eigenschaft, dass eine Entität das ist, was sie angibt zu sein

3.7

Verfügbarkeit

(en: availability)

Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

3.8

Elementarmessgröße

(en: base measure)

Messgröße (3.42), die mittels eines Attributs und der Methode ihrer Quantifizierung definiert ist

Anmerkung 1 zum Begriff: Eine Elementarmessgröße ist funktional unabhängig von anderen *Messgrößen*.

[QUELLE: ISO/IEC/IEEE 15939:2017, 3.3, modifiziert — Anmerkung 2 zum Begriff wurde gestrichen.]

3.9

Kompetenz

(en: competence)

Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen

3.10

Vertraulichkeit

(en: confidentiality)

Eigenschaft, dass Information unbefugten Personen, Entitäten oder *Prozessen* (3.54) nicht verfügbar gemacht oder offengelegt wird

3.11

Konformität

(en: conformity)

Erfüllung einer *Anforderung* (3.56)

3.12

Folge

(en: consequence)

Ergebnis eines *Ereignisses* (3.21), welches *Ziele* (3.49) beeinflusst

Anmerkung 1 zum Begriff: Ein Ereignis kann eine Reihe von Folgen haben.

Anmerkung 2 zum Begriff: Eine Folge kann gewiss oder ungewiss sein und ist im Kontext von Informationssicherheit in der Regel negativ.

Anmerkung 3 zum Begriff: Folgen können qualitativ oder quantitativ beschrieben werden.

Anmerkung 4 zum Begriff: Primäre Folgen können sich durch Dominoeffekte verstärken.

[QUELLE: ISO Guide 73:2009, 3.6.1.3, modifiziert – Anmerkung 2 zum Begriff wurde nach dem „und“ geändert]

3.13

fortlaufende Verbesserung

(en: continual improvement)

wiederkehrende Tätigkeit zum Steigern der *Leistung* (3.52)

3.14

Maßnahme

(en: control)

Mittel zur Veränderung von *Risiken* (3.61)

Anmerkung 1 zum Begriff: Maßnahmen umfassen *Prozesse* (3.54), Richtlinien, Geräte, Methoden oder anderweitige Handlungen, die *Risiken* (3.61) verändern.

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

[QUELLE: ISO Guide 73:2009 3.8.1.1 — Anmerkung 2 zum Begriff wurde geändert.]

3.15

Maßnahmenziel

(en: control objective)

Beschreibung dessen, was als Ergebnis umgesetzter *Maßnahmen* (3.14) erzielt werden soll

3.16

Korrektur

(en: correction)

Maßnahme zum Beseitigen einer erkannten *Nichtkonformität* (3.47)

3.17

Korrekturmaßnahme

(en: corrective action)

Maßnahme zum Beseitigen der Ursache einer *Nichtkonformität* (3.47) und zum Verhindern des erneuten Auftretens

3.18

abgeleitete Messgröße

(en: derived measure)

Messgröße (3.42), die als Funktion von zwei oder mehr Werten von *Elementarmessgrößen* (3.8) definiert ist

[QUELLE: ISO/IEC/IEEE 15939:2017, 2.8 modifiziert — Anmerkung 1 zum Begriff wurde gestrichen.]