Belgische Norm

ISO/IEC 27017:2015
EN ISO/IEC 27017:2021
NBN EN ISO/IEC 27017:2021

Informationstechnik - Sicherheitsverfahren - Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015)

Gültig ab 25-02-2021

Ersetzt NBN ISO/IEC 27017:2016

ICS: 35.030

Bureau for Standarisation
Jozef II-straat 40 bus 6
1000 Brussel

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27017

Januar 2021

ICS 35.030

Deutsche Fassung

Informationstechnik - Sicherheitsverfahren - Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015)

Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)

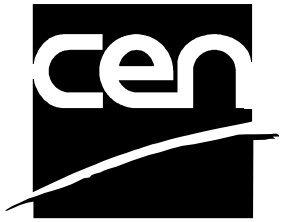
Technologies de l'information - Techniques de sécurité - Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage (ISO/IEC 27017:2015)

Diese Europäische Norm wurde vom CEN am 20. Dezember 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

EN ISO/IEC 27017:2021 (D)

Europäisches Vorwort

Der Text von ISO/IEC 27017:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 27017:2021 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 2021, und etwaige entgegenstehende nationale Normen müssen bis Juli 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 27017:2015 wurde von CEN als EN ISO/IEC 27017:2021 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.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe der gemeinsamen Technischen Komitees besteht in dem Erarbeiten von Internationalen Normen. Die von den gemeinsamen Technischen Komitees angenommenen Norm-Entwürfe werden den Mitgliedsorganisationen zur Umfrage zur Verfügung gestellt. Für eine Veröffentlichung als Internationale Norm wird eine Zustimmung von mindestens 75 % der Mitgliedsländer, die abgestimmt haben, benötigt.

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.

ISO/IEC 27017 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology,* Unterkomitee SC 27, *IT Security techniques*, in Zusammenarbeit mit ITU-T erarbeitet. Der identische Text wird veröffentlicht als ITU-T. X.1631 (07/2015).

Einleitung

Die Leitlinien in dieser Empfehlung | Internationalen Norm ergänzen die Leitlinien, die in ISO/IEC 27002 enthalten sind.

Insbesondere enthält diese Empfehlung | Internationale Norm Leitlinien, die die Umsetzung der Informationssicherheitsmaßnahmen durch Cloud-Dienstleistungskunden und Cloud-Dienstleister unterstützen. Einige Leitlinien sind für Cloud-Dienstleistungskunden bestimmt, die die Maßnahmen umsetzen, und andere Leitlinien für Cloud-Dienstleister, die die Umsetzung dieser Maßnahmen unterstützen. Die Auswahl der geeigneten Informationssicherheitsmaßnahmen und die Anwendung der bereitgestellten Anleitungen zur Umsetzung hängt von der Risikobeurteilung und sämtlichen rechtlichen, vertraglichen, behördlichen oder anderen für den Cloud-Sektor spezifischen Anforderungen an die Informationssicherheit ab.

1 Anwendungsbereich

Diese Empfehlung | Internationale Norm gibt Leitfäden zu Informationssicherheitsmaßnahmen, die für die Bereitstellung und Nutzung von Cloud-Diensten anwendbar sind, durch Bereitstellung von:

— zusätzlichen Anleitungen zur Umsetzung von relevanten in ISO/IEC 27002 festgelegten Maßnahmen;

— zusätzlichen Maßnahmen mit Anleitungen zur Umsetzung, die insbesondere Cloud-Dienste betreffen.

Diese Empfehlung | Internationale Norm bietet Maßnahmen und Anleitungen zur Umsetzung sowohl für Cloud-Dienstleister als auch für Cloud-Dienstleistungskunden.

2 Normative Verweisungen

Die folgenden Empfehlungen und Internationalen Normen enthalten Festlegungen, die durch Verweisung in diesem Text Festlegungen der vorliegenden Empfehlung | Internationalen Norm sind. Zum Zeitpunkt der Veröffentlichung dieser Empfehlung | Internationalen Norm waren die angegebenen Ausgaben gültig. Alle Empfehlungen und Normen unterliegen der Überarbeitung. Vertragspartner, deren Vereinbarungen auf dieser Empfehlung | Internationalen Norm basieren, werden gebeten, die Möglichkeit zu prüfen, ob die jeweils neuesten Ausgaben der im Folgenden genannten Empfehlungen und Normen angewendet werden können. Die Mitglieder von IEC und ISO führen Verzeichnisse der gegenwärtig gültigen Internationalen Normen. Das Telecommunication Standardization Bureau der ITU pflegt eine Liste der gegenwärtig gültigen ITU-T-Empfehlungen.

2.1 Identische Empfehlungen | Internationale Normen

— ITU-T-Empfehlung Y.3500 (in Kraft) | ISO/IEC 17788: (in Kraft), *Information technology — Cloud computing — Overview and vocabulary*.

— ITU-T-Empfehlung Y.3502 (in Kraft) | ISO/IEC 17789: (in Kraft), *Information technology — Cloud computing — Reference architecture*.

2.2 Zusätzliche Verweisungen

— ISO/IEC 27000: (in Kraft), *Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

— ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*.

3 Begriffe und Abkürzungen

3.1 An anderer Stelle definierte Begriffe

Für die Anwendung dieser Empfehlung | Internationale Norm gelten die Begriffe nach ISO/IEC 27000, ITU-T-Empfehlung Y.3500 | ISO/IEC 17788, ITU-T-Empfehlung Y.3502 | ISO/IEC 17789 und die folgenden Begriffe:

3.1.1 Folgender Begriff ist in ISO 19440 definiert:

— **Fähigkeit**: Eigenschaft, in der Lage zu sein, eine bestimmte Tätigkeit auszuführen.

3.1.2 Folgende Begriffe sind in ISO/IEC 27040 definiert:

— **Bruch der Vertraulichkeit**: Beeinträchtigung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unberechtigten Offenlegung von oder den Zugang zu geschützten Daten führt, die übertragen, gespeichert oder anderweitig verarbeitet werden.