Belgische Norm

ISO/IEC 27001:2013
ISO/IEC 27001:2013/Cor 1:2014
ISO/IEC 27001:2013/Cor 2:2015
EN ISO/IEC 27001:2017
NBN EN ISO/IEC 27001:2017

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014 + Cor. 2:2015)

Gültig ab 22-03-2017

Ersetzt NBN ISO/IEC 27001:2014, NBN ISO/IEC 27001 NL:2014 und NBN ISO/IEC 27001 NL:2014/AC:2015

ICS: 03.100.70, 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 27001

Februar 2017

ICS 03.100.70; 35.030

Deutsche Fassung

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014 + Cor. 2:2015)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

Diese Europäische Norm wurde vom CEN am 26. Januar 2017 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, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management Centre:
Avenue Marnix 17, B-1000 Brussels

Inhalt

Seite

Europäisches Vorwort ... **3**

Vorwort ... **4**

0 Einleitung ... **5**

1 Anwendungsbereich ... **6**

2 Normative Verweisungen ... **6**

3 Begriffe ... **6**

4 Kontext der Organisation ... **6**
4.1 Verstehen der Organisation und ihres Kontextes ... **6**
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien ... **6**
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems ... **7**
4.4 Informationssicherheitsmanagementsystem ... **7**

5 Führung ... **7**
5.1 Führung und Verpflichtung ... **7**
5.2 Politik ... **8**
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation ... **8**

6 Planung ... **8**
6.1 Maßnahmen zum Umgang mit Risiken und Chancen ... **8**
6.2 Informationssicherheitsziele und Planung zu deren Erreichung ... **10**

7 Unterstützung ... **11**
7.1 Ressourcen ... **11**
7.2 Kompetenz ... **11**
7.3 Bewusstsein ... **11**
7.4 Kommunikation ... **12**
7.5 Dokumentierte Information ... **12**

8 Betrieb ... **13**
8.1 Betriebliche Planung und Steuerung ... **13**
8.2 Informationssicherheitsrisikobeurteilung ... **13**
8.3 Informationssicherheitsrisikobehandlung ... **14**

9 Bewertung der Leistung ... **14**
9.1 Überwachung, Messung, Analyse und Bewertung ... **14**
9.2 Internes Audit ... **14**
9.3 Managementbewertung ... **15**

10 Verbesserung ... **16**
10.1 Nichtkonformität und Korrekturmaßnahmen ... **16**
10.2 Fortlaufende Verbesserung ... **16**

Anhang A (normativ) Referenzmaßnahmenziele und -maßnahmen ... **17**

Literaturhinweise ... **31**

Europäisches Vorwort

Der Text von ISO/IEC 27001:2013 + Cor. 1:2014 + Cor. 2:2015 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 EN ISO/IEC 27001:2017 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2017, und etwaige entgegenstehende nationale Normen müssen bis August 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind 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 ehemalige jugoslawische Republik Mazedonien, 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 27001:2013 + Cor. 1:2014 + Cor. 2:2015 wurde vom CEN als EN ISO/IEC 27001:2017 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. Internationale Organisationen, staatlich und nichtstaatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

Die Hauptaufgabe von Technischen Komitees ist es Internationale Normen zu erarbeiten. Internationale Norm-Entwürfe, die von Technischen Komitees verabschiedet wurden, werden den Mitgliedsorganisationen zur Abstimmung zur Verfügung gestellt. Für die Veröffentlichung als Internationale Norm werden mindestens 75 % Zustimmung der Mitgliedsorganisationen 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 27001 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 27001:2005), welche technisch überarbeitet wurde.

0 Einleitung

0.1 Allgemeines

Diese Internationale Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Umsetzung eines Informationssicherheitsmanagementsystems innerhalb einer Organisation richten sich nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern.

Das Informationssicherheitsmanagementsystem wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Information unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Es ist wichtig, dass das Informationssicherheitsmanagementsystem als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt wird. Es wird erwartet, dass die Umsetzung eines Informationssicherheitsmanagementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Diese Internationale Norm kann von internen und externen Parteien dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu beurteilen.

Die Reihenfolge, in der die Anforderungen in dieser Internationalen Norm aufgeführt sind, spiegelt nicht deren Bedeutung wider noch die Abfolge, in der sie umzusetzen sind. Die Einträge sind lediglich zu Referenzierungszwecken nummeriert.

ISO/IEC 27000 liefert einen Überblick und die Begrifflichkeiten von Informationssicherheitsmanagementsystemen und verweist auf die Informationssicherheitsmanagementsystem-Normenfamilie (einschließlich ISO/IEC 27003 [2], ISO/IEC 27004 [3] und ISO/IEC 27005 [4]), einschließlich deren Begriffe.

0.2 Kompatibilität mit anderen Normen für Managementsysteme

Diese Internationale Norm wendet die Grundstrukturen, den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen für den Gebrauch in Managementsystemnormen an, die jeweils im Anhang SL der ISO/IEC-Direktiven, Teil 1, „Consolidated ISO Supplement“ festgelegt sind, und stellt so die Übereinstimmung mit anderen Managementsystemnormen her, die ebenfalls den Anhang SL anwenden.

Die in Anhang SL festgelegte allgemeine Herangehensweise nützt jenen Organisationen, die sich für den Betrieb eines einzigen Managementsystems entscheiden, um die Anforderungen von zwei oder mehr Normen für Managementsysteme zu erfüllen.

1 Anwendungsbereich

Diese Internationale Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet diese Internationale Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen, ungeachtet ihrer Art und Größe, anwendbar sein. Wenn eine Organisation Konformität mit dieser Internationalen Norm für sich beansprucht, darf sie keine der Anforderungen in den Abschnitten 4 bis 10 ausschließen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung des Dokuments erforderlich. 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/IEC 27000, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die in ISO/IEC 27000 angegebenen Begriffe.

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagement-systems zu erreichen.

ANMERKUNG Die Bestimmung dieser Themen bezieht sich auf die Festlegung des externen und internen Kontexts des Unternehmens, wie in ISO 31000:2009 [5], 5.3, beschrieben.

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation muss:

a) die interessierten Parteien, die für ihr Informationssicherheitsmanagementsystem relevant sind; und

b) die Anforderungen dieser interessierten Parteien mit Bezug zur Informationssicherheit

bestimmen.

ANMERKUNG Die Anforderungen interessierter Parteien können gesetzliche und regulatorische Vorgaben sowie vertragliche Verpflichtungen beinhalten.