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

Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen (Geconsolideerde versie ISO/IEC 27001:2013 inclusief Cor 1:2014 en Cor 2:2015)

Geldig vanaf 22-03-2017

Vervangt NBN ISO/IEC 27001:2014, NBN ISO/IEC 27001 NL:2014 en NBN ISO/IEC 27001 NL:2014/AC:2015

De geconsolideerde Nederlandstalige versie is uitgegeven onder de verantwoordelijkheid van het NBN en heeft dezelfde status als de officiële versies. Dit document is identiek aan de NBN EN ISO/IEC 27001:2017, waarin het technisch corrigendum ISO/IEC 27001:2013/COR 1:2014 en het technisch corrigendum ISO/IEC 27001:2013/COR 2:2015 zijn verwerkt. Hij heeft dezelfde status als de officiële versies.

ICS: 03.100.70, 35.030

Bureau voor Normalisatie
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

Nationaal voorwoord

Deze norm is opgesteld door de internationale Technische Commissie ISO/IEC JTC 1, Information technology, SC 27, IT Security techniques. Verdere details wat dat betreft worden verstrekt in het Voorwoord bij deze norm. De tekst van ISO/IEC 27001:2013, inclusief Cor 1:2014 en Cor 2:2015, is overgenomen als EN ISO/IEC 27001:2017.

De Europese norm werd door het Bureau voor Normalisatie (NBN) ongewijzigd geregistreerd en gepubliceerd als Belgische norm.

De Nederlandstalige versie van deze norm is opgesteld door het NEN.

Nederlands voorwoord (NEN)

Dit document bevat de vertaling in het Nederlands van de Europese norm EN-ISO/IEC 27001:2017. De Europese norm EN-ISO/IEC 27001:2017 heeft de status van Nederlandse norm.

Op NEN-ISO/IEC 27001:2013 zijn correcties verschenen (in de correctiebladen C11, C1 en C2), die in deze geconsolideerde versie zijn verwerkt. De correcties zijn op de volgende plaatsen aangebracht:

[C11] 8.1: Aan het eind van de paragraaf is toegevoegd: " De organisatie moet bewerkstelligen dat uitbestede processen worden vastgesteld en beheerst."

[C1] A.8.1.1: "Bedrijfsmiddelen die samenhangen" is vervangen door "informatie, andere bedrijfsmiddelen die samenhangen".

[C2] 6.1.3: punt d) van de opsomming is vervangen door:

"d) een verklaring van toepasselijkheid op te stellen die bevat:

— de benodigde beheersmaatregelen (zie 6.1.3 b) en c));

— een rechtvaardiging voor het opnemen ervan;

— de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet, en

— de rechtvaardiging voor het uitsluiten van in bijlage A genoemde beheersmaatregelen."

[C1] is de vertaling in het Nederlands van het technisch corrigendum ISO/IEC 27001:2013/COR 1:2014.

[C2] is de vertaling in het Nederlands van het technisch corrigendum ISO/IEC 27001:2013/COR 1:2015.

Dit document is dus identiek aan de NBN EN ISO/IEC 27001:2017, waarin het technisch corrigendum ISO/IEC 27001:2013/COR 1:2014 en het technisch corrigendum ISO/IEC 27001:2013/COR 2:2015 zijn verwerkt.

Deze NBN-versie is grotendeels gebaseerd op de NEN-versie, maar houdt tegelijk rekening met een aantal verschillen op het vlak van terminologie tussen Nederland en Vlaanderen. De onderstaande synoniemenlijst vermeldt de termen waarvoor het NBN een afwijkende keuze heeft gemaakt.

Synoniemenlijst

Engelse term	*Nederlandse term in de NEN-versie*	*Nederlandse term in de NBN-versie*
address <risks, opportunities>	oppakken <risico's, kansen>	aanpakken <risico's, kansen>
adequately protected	afdoend beveiligd	voldoende beveiligd
amendments	wijzigings- en correctiebladen	amendementen
contracting	het contracteren	het aannemen
feedback	feedback	terugkoppeling
retain (documented information)	bijhouden of bewaren	bewaren
valid <results>	valide	geldig

EUROPESE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27001

februari 2017

ICS 03.100.70; 35.030

Nederlandstalige versie

Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen (ISO/IEC 27001:2013 inclusief Cor 1:2014 en Cor 2:2015)

Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und 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)

Deze Europese norm is door CEN aangenomen op 26 januari 2017. De Nederlandstalige versie is uitgegeven onder verantwoordelijkheid van het NBN en heeft dezelfde status als de officiële versies.

De CEN- en CENELEC-leden zijn verplicht zich te houden aan het huishoudelijk reglement van de CEN/CENELEC waarin is vastgelegd onder welke voorwaarden aan deze Europese norm, zonder veranderingen, de status van nationale norm moet worden gegeven. Bijgewerkte lijsten van en bibliografische gegevens betreffende zulke nationale normen kunnen op aanvraag worden verkregen bij het centrale secretariaat en bij elk CEN- en CENELEC-lid.

Deze Europese norm bestaat in drie officiële versies (Duits, Engels en Frans). Een versie in een andere taal, die onder verantwoordelijkheid van een CEN- en CENELEC-lid in zijn landstaal is gemaakt en die is aangemeld bij het centrale secretariaat, heeft dezelfde status als de officiële versies.

Leden van de CEN en de CENELEC zijn de nationale normalisatie-organisaties van België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Macedonië, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Servië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

Managementcentrum CEN-CENELEC:
Wetenschapsstraat 23, B-1040 Brussel

Inhoud

Contents

Europees voorwoord

De tekst van ISO/IEC 27001:2013, inclusief Cor 1:2014 en Cor 2:2015, is opgesteld door Technische Commissie ISO/IEC/JTC 1 'Information technology' van de Internationale Organisatie voor Standaardisatie (ISO) en het Internationaal Elektrotechnisch Comité (IEC), en is overgenomen als EN ISO/IEC 27001:2017.

Aan deze Europese norm moet uiterlijk in augustus 2017 de status van nationale norm worden gegeven, door publicatie van een identieke tekst of door bekrachtiging, en strijdige nationale normen moeten uiterlijk in augustus 2017 worden ingetrokken.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. CEN (en/of CENELEC) is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

Volgens het huishoudelijk reglement van CEN-CENELEC zijn de normalisatieorganisaties van de volgende landen verplicht deze Europese norm in te voeren: België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Macedonië, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Servië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het Verenigd Koninkrijk, Zweden en Zwitserland.

Verklaring van bekrachtiging

De tekst van ISO/IEC 27001:2013, inclusief Cor 1:2014 en Cor 2:2015, is zonder wijzigingen door CEN als EN ISO/IEC 27001:2017 aanvaard.

ISO/IEC-voorwoord

ISO (International Organization for Standardization) en IEC (International Electrotechnical Commission) vormen tezamen een stelsel dat gespecialiseerd is in wereldwijde normalisatie. Nationale organisaties die lid zijn van ISO of IEC participeren in het ontwikkelen van internationale normen via technische commissies die door de desbetreffende organisatie zijn ingesteld ten behoeve van de normalisatie in specifieke technische werkvelden. Technische commissies van ISO en IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als ngo's nemen, in samenwerking met ISO en IEC, ook deel aan deze werkzaamheden. Op het gebied van informatietechnologie hebben ISO en IEC een gezamenlijke technische commissie opgericht, ISO/IEC JTC 1.

Internationale normen worden opgesteld in overeenstemming met de voorschriften die zijn opgenomen in de ISO/IEC-richtlijnen, deel 2.

De belangrijkste taak van de gezamenlijke technische commissie (JTC) is het opstellen van internationale normen. Ontwerpversies van internationale normen die zijn aangenomen door de gezamenlijke technische commissie, worden ter stemming voorgelegd aan de normalisatie-instellingen. Publicatie als internationale norm vereist goedkeuring van ten minste 75 % van de door nationale normalisatie-instellingen uitgebrachte stemmen.

Er wordt op gewezen dat sommige delen van dit document mogelijk beschermd zijn door patentrechten. ISO en IEC zijn niet verantwoordelijk voor identificatie van dergelijke patentrechten.

ISO/IEC 27001 is opgesteld door ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

Deze tweede versie herroept en vervangt de eerste versie (ISO/IEC 27001:2005), die technisch is herzien.

0 Inleiding

0.1 Algemeen

Deze internationale norm is opgesteld om te voorzien in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. Het invoeren van een managementsysteem voor informatiebeveiliging is voor een organisatie een strategische beslissing. Het vaststellen en implementeren van een managementsysteem voor informatiebeveiliging wordt beïnvloed door de behoeften en doelstellingen van de organisatie, de beveiligingseisen, de procedures die de organisatie toepast en de omvang en structuur van de organisatie. Er wordt van uitgegaan dat al deze beïnvloedende factoren mettertijd wijzigen.

Het managementsysteem voor informatiebeveiliging beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie door een risicobeheerproces toe te passen, en geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de organisatie en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen. Er wordt van uitgegaan dat de implementatie van een managementsysteem voor informatiebeveiliging in omvang wordt afgestemd op de behoeften van de organisatie.

Deze internationale norm kan worden gebruikt door interne en externe partijen om het vermogen van de organisatie te beoordelen om te voldoen aan de eigen informatiebeveiligingseisen.

De volgorde waarin de eisen in deze internationale norm worden gepresenteerd geeft niet de volgorde van belangrijkheid aan en impliceert niet de volgorde waarin ze moeten worden geïmplementeerd. De nummering van de lijstitems dient alleen voor referentiedoeleinden.

ISO/IEC 27000 beschrijft het overzicht en de terminologie van managementsystemen voor informatiebeveiliging, en verwijst naar de normenfamilie betreffende managementsystemen voor informatiebeveiliging (met inbegrip van ISO/IEC 27003 [2], ISO/IEC 27004 [3] en ISO/IEC 27005 [4]), met gerelateerde termen en definities.

0.2 Compatibiliteit met andere managementsysteemnormen

Deze internationale norm past de hoofdstructuur (HLS) toe, identieke paragraaftitels, identieke tekst, gemeenschappelijke termen en kerndefinities zoals gedefinieerd in bijlage SL van ISO/IEC Directives, deel 1, geconsolideerd ISO-supplement, en is daardoor compatibel met andere managementsysteemnormen die bijlage SL hebben aangenomen.

Deze gemeenschappelijke benadering zoals gedefinieerd in bijlage SL is nuttig voor organisaties die ervoor kiezen een enkel managementsysteem uit te voeren dat voldoet aan de eisen van twee of meer managementsysteemnormen.

Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen

1 Onderwerp en toepassingsgebied

Deze internationale norm noemt de eisen voor het binnen de context van de organisatie vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. In deze internationale norm zijn ook eisen opgenomen voor het beoordelen en behandelen van informatiebeveiligingsrisico's afgestemd op de behoeften van de organisatie. De eisen die in deze internationale norm zijn vermeld zijn algemeen en bedoeld toepasselijk te zijn voor alle organisaties, ongeacht type, omvang of aard. Als een organisatie conformiteit met deze internationale norm claimt, is uitsluiting van een van de eisen genoemd in de hoofdstukken 4 tot en met 10 niet acceptabel.

2 Normatieve verwijzingen

De volgende documenten, waarnaar als geheel of voor een onderdeel, in dit document normatief is verwezen, zijn onmisbaar voor de toepassing ervan. Bij gedateerde verwijzingen is alleen de aangehaalde uitgave van toepassing. Bij ongedateerde verwijzingen is de laatste uitgave van het document (met inbegrip van eventuele amendementen) waarnaar is verwezen van toepassing

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

3 Termen en definities

Voor de toepassing van dit document gelden de termen en definities zoals vermeld in ISO/IEC 27000.

4 Context van de organisatie

4.1 Inzicht in de organisatie en haar context

De organisatie moet externe en interne belangrijke punten (issues) vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen.

OPMERKING Het vaststellen van deze onderwerpen verwijst naar het vaststellen van de externe en interne context van de organisatie zoals behandeld in 5.3 van ISO 31000:2009 [5].

4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

De organisatie moet vaststellen:

a) welke belanghebbenden relevant zijn voor het managementsysteem voor informatiebeveiliging, en

b) welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging.

OPMERKING De eisen van belanghebbenden kunnen eisen op het gebied van wet- en regelgeving en contractuele verplichtingen inhouden.