ICS: 35.040

Geregistreerde Belgische norm

NBN ISO/IEC 27002 NL

1e uitg., juli 2014

Normklasse: Z 07

Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (ISO/IEC 27002:2013)

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013)

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013)

Toelating tot publicatie: 25 juli 2014

Deze norm ISO/IEC 27002:2013 heeft de status van een Belgische norm.

Deze norm bestaat in twee officiële versies (Engels, Frans).

De Nederlandstalige versie is uitgegeven onder de verantwoordelijkheid van het NBN. Deze NBN ISO/IEC 27002 NL is identiek aan de NBN ISO/IEC 27002, 1e uitg. juni 2014 en heeft dezelfde status als de officiële versies.

Hoewel de grootste zorg is besteed aan deze Nederlandstalige uitgave, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het NBN kan dan ook niet aansprakelijk worden gesteld voor rechtstreekse en/of onrechtstreekse schade, ontstaan door of verband houdend met de toepassing van deze uitgave.

standards for .be

Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België
Tel: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Bank 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB BTW BE0880857592

Prijsgroep: 36

ICS: 35.040

norme belge enregistrée

NBN ISO/IEC 27002 NL

1e éd., juillet 2014

Indice de classement: Z 07

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information (ISO/IEC 27002:2013)

Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (ISO/IEC 27002:2013)

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013)

Autorisation de publication: 25 juillet 2014

La présente norme ISO/IEC 27002:2013 a le statut d'une norme belge.

La présente norme existe en deux versions officielles (anglais, français).

La version en néerlandais est publiée sous la responsabilité du NBN. Cette norme NBN ISO/IEC 27002 NL est identique à la NBN ISO/IEC 27002, 1e éd. juin 2014 et a le même statut que les versions officielles.

Bien que le plus grand soin ait été apporté à la réalisation de cette édition néerlandaise, des erreurs ou omission ne peuvent être totalement exclues. Par conséquent, le NBN décline toute responsabilité pour les dommages directs et/ou indirects dus ou liés à l'application de la présente norme.

standards for .be

Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique
Tél: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Banque 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB TVA BE0880857592

Prix: groupe 36

Nationaal voorwoord

De internationale norm ISO/IEC 27002:2013 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.

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***
amendments	wijzigings- en correctiebladen	corrigenda en amendementen
awareness program	bewustzijnsprogramma	bewustmakingsprogramma
back-up	back-uppen	een back-up maken van
bar	afsluitboom	slagboom
graduated response	gegradueerd antwoord	stapsgewijze reactie
logging	verslaglegging	registreren (het -)
operations security	beveiliging bedrijfsvoering	beveiliging van bedrijfsactiviteiten
record <of all privileges allocated>	verslaglegging	registratie
staging environment	gefaseerde omgeving	‘staging’-omgeving
user access provisioning process	gebruikerstoegangsverlenings-procedure	procedure voor het verlenen van toegang aan gebruikers

(blanco)

INTERNATIONALE NORM

ISO/IEC 27002

2e uitgave
2013-10-01

Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging

Information technology - Security techniques - Code of practice for information security controls

Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information

Referentienummer
ISO/IEC 27002:2013 (N)

(blanco)

Inhoud

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.

ISO/IEC 27002 is opgesteld door ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

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

Deze tweede versie herroept en vervangt de eerste versie (ISO/IEC 27002:2005), die technisch en structureel is herzien.

0 Inleiding

0.1 Achtergrond en context

Deze Internationale Norm is ontworpen voor organisaties om te worden gebruikt als referentie voor het selecteren van beheersmaatregelen binnen het implementatieproces van een managementsysteem voor informatiebeveiliging (ISMS) gebaseerd op ISO/IEC 27001 [10] of als een leidraad voor organisaties die algemeen aanvaarde beheersmaatregelen op het gebied van informatiebeveiliging implementeren. Deze norm is ook bedoeld om te worden gebruikt voor het ontwikkelen van industrie- en organisatiespecifieke richtlijnen voor informatiebeveiligingsbeheer die rekening houden met hun specifieke informatiebeveiligingsrisico's.

Organisaties van elk type en elke omvang (met inbegrip van openbare en particuliere, commerciële en non-profitorganisaties) verzamelen, verwerken, bewaren en brengen informatie in vele vormen over, waaronder elektronisch, fysiek en mondeling (bijv. via gesprekken en presentaties).

De waarde van informatie is niet beperkt tot het geschreven woord, getallen en figuren: kennis, concepten, ideeën en merken zijn voorbeelden van immateriële vormen van informatie. In een onderling verbonden wereld zijn informatie- en gerelateerde processen, systemen, netwerken en medewerkers die betrokken zijn bij het uitvoeren, behandelen en beschermen ervan, bedrijfsmiddelen die, evenals andere belangrijke bedrijfsmiddelen, waardevol zijn voor de bedrijfsvoering van een organisatie en daarom bescherming tegen diverse risico's verdienen of vereisen.

Bedrijfsmiddelen zijn onderhevig aan opzettelijke en onopzettelijke bedreigingen, terwijl de gerelateerde processen, systemen, netwerken en personen inherente kwetsbaarheden. Wijzigingen in bedrijfsprocessen en -systemen, of andere externe wijzigingen (zoals nieuwe wetten en regelgeving) kunnen nieuwe informatiebeveiligingsrisico's met zich mee brengen. Daardoor en gezien de veelheid van manieren waarop bedreigingen kwetsbaarheden kunnen benutten om de organisatie schade toe te brengen, zijn informatiebeveiligingsrisico's altijd aanwezig. Doeltreffende informatiebeveiliging vermindert deze risico's door de organisatie te beschermen tegen bedreigingen en kwetsbaarheden, en verkleint de impact op haar bedrijfsmiddelen.

Informatiebeveiliging wordt bereikt door een passende reeks beheersmaatregelen te implementeren met inbegrip van beleid, processen, procedures, organisatiestructuren en software- en hardwarefuncties. Om te bewerkstelligen dat de specifieke veiligheids- en bedrijfsdoelstellingen van de organisatie worden gehaald, is het noodzakelijk dat deze beheersmaatregelen worden vastgesteld, geïmplementeerd, gemonitord, beoordeeld en verbeterd, waar nodig. Een ISMS zoals omschreven in ISO/IEC 27001 [10] benadert de informatiebeveiligingsrisico's van de organisatie holistisch en gecoördineerd met het doel om een allesomvattende reeks beheersmaatregelen voor informatiebeveiliging te implementeren onder het algehele kader van een samenhangend managementsysteem.

Veel informatiesystemen zijn niet ontworpen om te zijn beveiligd in de zin van ISO/IEC 27001 [10] en de voorliggende norm. De beveiliging die kan worden bereikt via technische middelen is beperkt en behoort te worden ondersteund door passend beheer en passende procedures. Het bepalen van de passende beheersmaatregelen vereist zorgvuldige planning en aandacht voor details. Een succesvol ISMS vereist de inzet van alle medewerkers binnen de organisatie. Ook participatie van aandeelhouders, leveranciers of andere externe partijen kan vereist zijn. Ook kan specialistisch advies van externe partijen nodig zijn.

In algemenere zin geeft doeltreffende informatiebeveiliging de directie en andere belanghebbenden de zekerheid dat de bedrijfsmiddelen van de organisatie redelijk veilig en tegen schade beschermd zijn, waardoor de beveiliging de bedrijfsuitvoering bevordert.

0.2 Informatiebeveiligingseisen

Het is essentieel dat een organisatie haar beveiligingseisen bepaalt. Er zijn drie belangrijke bronnen voor beveiligingseisen:

a) de beoordeling van de risico's waar de organisatie aan blootgesteld is, rekening houdend met de algehele bedrijfsstrategie en -doelstellingen. Via een risicobeoordeling worden bedreigingen voor

bedrijfsmiddelen vastgesteld, de kwetsbaarheid voor en de waarschijnlijkheid dat een bepaalde bedreiging zich voordoet, geëvalueerd en wordt de potentiële impact ingeschat;

b) de wettelijke, statutaire, regelgevende en contractuele eisen waaraan een organisatie, haar handelspartners, leveranciers en dienstverleners, en hun sociaal-culturele omgeving, moeten voldoen;

c) de reeks van principes, doelstellingen en bedrijfseisen die gelden voor het hanteren, verwerken, bewaren, communiceren en archiveren van informatie die een organisatie heeft ontwikkeld om haar bedrijfsvoering te ondersteunen.

Hulpmiddelen die worden gebruikt voor het implementeren van beheersmaatregelen behoren te worden afgewogen tegen de bedrijfsschade die waarschijnlijk ontstaat door beveiligingsproblemen als dergelijke beheersmaatregelen niet worden genomen. De resultaten van een risicobeoordeling dienen als richtlijn en helpen de directie bij het bepalen van de passende actie en de prioriteiten voor het beheer van informatiebeveiligingsrisico's en voor het implementeren van beheersmaatregelen die zijn gekozen ter bescherming tegen deze risico's.

ISO/IEC 27005 [11] biedt een richtlijn voor het risicobeheer van informatiebeveiliging, met inbegrip van advies over risicobeoordeling, -aanpak, accepteren van risico's, communiceren over risico's, monitoren en opnieuw beoordelen van risico.

0.3 Beheersmaatregelen selecteren

Beheersmaatregelen kunnen worden geselecteerd uit deze norm of uit andere overzichten van beheersmaatregelen. Ook kunnen nieuwe beheersmaatregelen worden ontworpen die voldoen aan specifieke behoeften indien nodig.

De selectie van beheersmaatregelen hangt af van de beslissingen van de organisatie die zijn gebaseerd op de criteria voor het accepteren van risico's, de opties voor het omgaan met risico's en de algemene benadering van risicobeheer die in de organisatie wordt toegepast, en behoort ook in overeenstemming te zijn met alle relevante nationale en internationale wet- en regelgeving. De selectie van beheersmaatregelen hangt ook samen met de manier waarop deze beheersmaatregelen op elkaar inwerken om een diepteverdediging te bewerkstelligen.

Een aantal van de beheersmaatregelen in deze norm kan worden beschouwd als richtlijn voor informatiebeveiligingsbeheer die voor de meeste organisaties van toepassing is. De beheersmaatregelen worden hierna gedetailleerder uiteengezet samen met richtlijnen voor implementatie. Meer informatie over het selecteren van beheersmaatregelen en andere opties voor het omgaan met risico's is te vinden in ISO/IEC 27005 [11].

0.4 Eigen richtlijnen ontwikkelen

Deze Internationale Norm kan worden beschouwd als uitgangspunt voor het ontwikkelen van organisatiespecifieke richtlijnen. Mogelijk zijn niet alle beheersmaatregelen en richtlijnen in deze praktijkrichtlijn van toepassing. Voorts zijn mogelijk aanvullende beheersmaatregelen en richtlijnen vereist die niet in deze norm zijn opgenomen. Als er documenten zijn ontwikkeld die aanvullende richtlijnen of beheersmaatregelen bevatten, kan het, voor zover van toepassing, nuttig zijn kruisverwijzingen op te nemen naar hoofdstukken in deze norm om het voor auditoren en zakenpartners gemakkelijker te maken om op naleving te controleren.

0.5 Overwegingen betreffende de levenscyclus

Informatie heeft een natuurlijke levenscyclus, van aanmaken en ontstaan, via opslag, verwerking, gebruik en verzending tot uiteindelijk vernietiging of waardeverlies. De waarde van en risico's voor bedrijfsmiddelen kunnen tijdens hun levenscyclus variëren (bijvoorbeeld ongeoorloofde bekendmaking of diefstal van de financiële rekeningen van een bedrijf is veel minder belangrijk nadat deze officieel zijn gepubliceerd), maar informatiebeveiliging blijft tot op zekere hoogte in alle stadia belangrijk.

Informatiesystemen hebben levenscycli waarbinnen ze worden gemaakt, gespecificeerd, ontworpen, ontwikkeld, getest, geïmplementeerd, gebruikt, onderhouden en ten slotte buiten bedrijf worden gesteld en

verwijderd. In elk stadium behoort rekening te worden gehouden met informatiebeveiliging. Nieuwe systeemontwikkelingen en wijzigingen aan bestaande systemen bieden organisaties kansen om beheersmaatregelen te actualiseren en te verbeteren, rekening houdend met feitelijke incidenten en huidige en verwachte informatiebeveiligingsrisico's.

0.6 Gerelateerde normen

Terwijl deze norm richtlijnen biedt voor een brede waaier aan beheersmaatregelen voor informatiebeveiliging die in veel verschillende organisaties gangbaar zijn, bieden de overige normen in de ISO/IEC 27000-familie aanvullende eisen of advies met betrekking tot andere aspecten van het algehele proces van informatiebeveiligingsbeheer.

Zie ISO/IEC 27000 voor een algemene introductie van beide ISMS'en en de normenfamilie. ISO/IEC 27000 biedt een glossarium dat de meeste in de ISO/IEC 27000-normenfamilie gebruikte termen formeel definieert, en het onderwerp, toepassingsgebied en de doelstellingen voor elk onderdeel van de familie beschrijft.

Informatietechnologie – Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging

1 Onderwerp en toepassingsgebied

Deze Internationale Norm geeft richtlijnen voor informatiebeveiligingsnormen voor organisaties en toepassingen inzake informatiebeveiligingsbeheer, waaronder de selectie, implementatie en het beheer van beheersmaatregelen die rekening houden met de omgeving(en) waarin de informatiebeveiligingsrisico's van de organisatie gelden.

Deze Internationale Norm is ontworpen om te worden gebruikt door organisaties die voornemens zijn om:

a) beheersmaatregelen te selecteren binnen het implementatieproces van een managementsysteem voor informatiebeveiliging gebaseerd op ISO/IEC 27001 [10];

b) algemeen aanvaarde beheersmaatregelen inzake informatiebeveiliging te implementeren;

c) hun eigen richtlijnen voor informatiebeveiligingsbeheer te ontwikkelen.

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 corrigenda en 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 opgenomen in ISO/IEC 27000.

4 Structuur van deze norm

Deze norm bevat 14 clausules over beheersmaatregelen die tezamen totaal 35 hoofdbeveiligingscategorieën en 114 beheersmaatregelen bevatten.

4.1 Hoofdstukken

Elk hoofdstuk dat beheersmaatregelen inzake beveiliging definieert, bevat een of meer hoofdbeveiligingscategorieën.

De volgorde van de hoofdstukken in deze norm zegt niets over hun belang. Afhankelijk van de omstandigheden kunnen beheersmaatregelen uit een of uit alle hoofdstukken belangrijk zijn. Daarom behoort elke organisatie die deze norm toepast geschikte beheersmaatregelen, hun belang en hun toepassing voor individuele bedrijfsprocessen te bepalen. Verder staan opsommingen in deze norm niet in volgorde van prioriteit.

4.2 Categorieën beheersmaatregelen

Elke hoofdbeveiligingscategorie beheersmaatregelen bevat:

a) een beheersdoelstelling die aangeeft wat moet worden bereikt;

b) een of meer beheersmaatregelen die kunnen worden toegepast om de beheersdoelstelling te realiseren.