Nederlandse norm

NEN-ISO/IEC 27001+C11+C1+C2
(nl)

Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen

Information technology - Security techniques - Information security management systems - Requirements

Vervangt NEN-ISO/IEC 27001+C11:2014+C1:2014 nl

ICS 35.040

december 2015

Nederlands voorwoord

Dit document bevat de vertaling in het Nederlands van de internationale norm ISO/IEC 27001:2013. De internationale norm ISO/IEC 27001:2013 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.”

Voor de in deze norm vermelde normatieve verwijzingen bestaan in Nederland de volgende equivalenten:

vermelde norm	Nederlandse norm	titel
ISO/IEC 27000	NEN-ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary

Normcommissie 381 027 "IT-Beveiligingstechnieken"

NEN

©2015 Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, Fax (015) 2 690 190

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.

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 wijzigings- en correctiebladen) 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 verkrijgen in de organisatie en haar context

De organisatie moet externe en interne onderwerpen 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 verkrijgen 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.

4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen

De organisatie moet de grenzen en toepasselijkheid van het managementsysteem voor informatiebeveiliging bepalen om het toepassingsgebied ervan vast te stellen.

Bij het vaststellen van dit toepassingsgebied moet de organisatie:

a) de in 4.1 genoemde externe en interne onderwerpen overwegen, evenals;

b) de in 4.2 genoemde eisen, en

c) raakvlakken en afhankelijkheden tussen de activiteiten die door de organisatie en de activiteiten die door andere organisaties worden verricht.

Het toepassingsgebied moet als gedocumenteerde informatie beschikbaar zijn.

4.4 Managementsysteem voor informatiebeveiliging

De organisatie moet een managementsysteem voor informatiebeveiliging inrichten, implementeren, onderhouden en continu verbeteren, in overeenstemming met de eisen van deze Internationale Norm.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

De directie moet leiderschap en betrokkenheid tonen met betrekking tot het managementsysteem voor informatiebeveiliging door:

a) te bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en aansluiten bij de strategische richting van de organisatie;

b) te bewerkstelligen dat de eisen van het managementsysteem voor informatiebeveiliging in de processen van de organisatie worden geïntegreerd;

c) te bewerkstelligen dat de voor het managementsysteem voor informatiebeveiliging benodigde middelen beschikbaar zijn;

d) het belang van een doeltreffend informatiebeveiligingsmanagement en van het voldoen aan de eisen van het managementsysteem voor informatiebeveiliging te communiceren;

e) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt;

f) mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging;

g) continue verbetering te bevorderen; en

h) andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

5.2 Beleid

De directie moet een informatiebeveiligingsbeleid vaststellen dat:

a) passend is voor het doel van de organisatie;

b) informatiebeveiligingsdoelstellingen bevat (zie 6.2) of het kader biedt voor het vaststellen van informatiebeveiligingsdoelstellingen;

c) een verbintenis bevat om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging; en

d) een verbintenis bevat tot continue verbetering van het managementsysteem voor informatiebeveiliging.

Het beleid voor informatiebeveiliging moet:

e) beschikbaar zijn als gedocumenteerde informatie;

f) worden gecommuniceerd binnen de organisatie, en

g) beschikbaar zijn voor belanghebbenden, voor zover van toepassing.

5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging worden toegekend en gecommuniceerd.

De directie moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot:

a) het bewerkstelligen dat het managementsysteem voor informatiebeveiliging voldoet aan de eisen van deze Internationale Norm; en

b) het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging aan de directie.

OPMERKING De directie kan ook verantwoordelijkheden en bevoegdheden toekennen met betrekking tot het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging binnen de organisatie.

6 Planning

6.1 Maatregelen om risico's te beperken en kansen te benutten

6.1.1 Algemeen

Bij het plannen voor het managementsysteem voor informatiebeveiliging moet de organisatie de in 4.1 genoemde onderwerpen en de in 4.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden aangepakt om:

a) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt;

b) ongewenste effecten te voorkomen of te beperken; en

c) continue verbetering te bereiken.

De organisatie moet:

d) maatregelen plannen om deze risico's te beperken en kansen te benutten;

e) plannen op welke wijze:

1) de maatregelen in haar managementsysteemprocessen voor informatiebeveiliging worden geïntegreerd en geïmplementeerd; en

2) de doeltreffendheid van deze maatregelen moet worden geëvalueerd.

6.1.2 Risicobeoordeling van informatiebeveiliging

De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die:

a) risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder:

1) de risicoacceptatiecriteria; en

2) criteria voor het verrichten van risicobeoordelingen van informatiebeveiliging;

b) waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, geldige en vergelijkbare resultaten opleveren;

c) de informatiebeveiligingsrisico's identificeert:

1) het risicobeoordelingsproces voor informatiebeveiliging toepassen om de risico's in verband met het verlies van vertrouwen in, integriteit van en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren; en

2) de risico-eigenaren identificeren;

d) de informatiebeveiligingsrisico's analyseert:

1) de potentiële gevolgen beoordelen indien de risico's die in 6.1.2 c) 1) zijn vastgesteld, zich zouden voordoen;

2) de realistische waarschijnlijkheid beoordelen van het voorkomen van de risico's die zijn vastgesteld in 6.1.2 c) 1); en

3) de risiconiveaus vaststellen;

e) de informatiebeveiligingsrisico's evalueert:

1) de resultaten vergelijken van risicoanalyses met de risicocriteria die zijn vastgesteld in 6.1.2 a); en

2) de geanalyseerde risico's prioriteren voor risicobehandeling.

De organisatie moet gedocumenteerde informatie bewaren over het risicobeoordelingsproces van informatiebeveiliging.

6.1.3 Behandeling van informatiebeveiligingsrisico's

De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen om:

a) passende opties voor het behandelen van informatiebeveiligingsrisico's te kiezen, rekening houdend met de resultaten van de risicobeoordeling;

b) alle beheersmaatregelen vast te stellen die nodig zijn om de gekozen optie(s) voor het behandelen van informatiebeveiligingsrisico's te implementeren;

OPMERKING Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen.

c) de beheersmaatregelen die hiervoor in 6.1.3 b) zijn vastgesteld te vergelijken met die in bijlage A, en om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten;

Bestelformulier

Stuur naar:

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft

NEN Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop

Ja, ik bestel

__ ex. NEN-ISO/IEC 27001+C11:2014+C1:2014+C2:2015 nl € 162.00
Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

Gegevens

Bedrijf / Instelling

T.a.v. O M O V

E-mail

Klantnummer NEN

Uw ordernummer BTW nummer

Postbus / Adres

Postcode Plaats

Telefoon Fax

Factuuradres (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode Plaats

Datum Handtekening

Retourneren

Fax: 015 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services,
t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft
(geen postzegel nodig).

Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typefouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.