notitie

FORUM STANDAARDISATIE 22 april 2015
Agendapunt 2: Open standaarden, lijsten
Stuk 2B: Advies opname NEN-ISO/IEX 27001:2013 en 27002:2013 op de 'pas toe of leg uit'-lijst ter vervanging van de respectievelijke versies 2005 en 2007 van deze standaarden

Aanleiding en achtergrond
De standaarden NEN-ISO/IEC 27001 en 27002 zijn een vertaling van de internationale normen ISO/IEC 27001 en 27002. Op de 'pas toe of leg uit'-lijst staan de Nederlandse versies uit respectievelijk 2005 en 2007. Inmiddels zijn nieuwe versies van deze standaarden beschikbaar die zijn vastgesteld in 2013.

Ondanks dat de structuur van de nieuwe NEN-ISO/IEC 27001 aanzienlijk is veranderd en er een aantal nieuwe normen is toegevoegd, is de nieuwe 27001 standaard (2013) niet strijdig met de oude. De nieuwe NEN-ISO/IEC 27002 standaard omvat een aantal nieuwe normen en bestaande normen zijn geüpdatet naar de huidige stand der techniek.

De NEN-ISO/IEC 27001 standaard bevat eisen waar het management systeem voor informatiebeveiliging aan dient te voldoen. Tegen deze norm wordt geaudit bij certificering. De NEN-ISO/IEC 27002 standaard is een "best practice" van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. Deze standaard is een adviserend document en geen formele specificatie zoals NEN-ISO/IEC 27001:2013.

Betrokkenen en proces
Het Forum Standaardisatie heeft in samenwerking met de beheerders van de Baselines Informatiebeveiliging een verkennend onderzoek uitgevoerd naar de versie 2013 van de genoemde standaarden. Dit onderzoek was de aanleiding om het expertonderzoek uit te laten voeren. De uitkomsten van het expertonderzoek zijn ter publieke consultatie aangeboden. Aan het expertonderzoek hebben (toekomstig) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen.

De conclusie uit de expertgroep is om de standaarden NEN-ISO/IEC 27001:2013 en 27002:2013 op te nemen op de 'pas toe of leg uit'-lijst, ter vervanging van de versies 2005 en 2007 van deze standaarden. Naar aanleiding van de publieke

consultatie zijn een aantal aandachtspunten naar voren gekomen. Deze reacties zijn in overleg met de betrokken partijen verwerkt in dit forumadvies. Daarnaast gaf de expertgroep een aantal adoptieadviezen.

Consequenties en vervolgstappen
De expertgroep concludeert dat er geen specifieke risico's verbonden zijn aan de keuze. Ook uit de openbare consultatie blijken geen specifieke risico's. Verder zal op de lijst goed de verhouding tot de Baselines Informatiebeveiliging moeten worden weergegeven.

Certificaten afgegeven op basis van de oude norm NEN-ISO/IEC 27001:2005 verliezen hun geldigheid per 1 oktober 2015. Leveranciers hebben tot 1 oktober 2015 de tijd om zich te (her)certificeren tegen de nieuwe NEN-ISO/IEC 27001:2013. Tot slot zijn er enkele adviezen om de adoptie van de standaard te bevorderen, na opname van de standaard is het advies om hier uitvoering aan te geven.

Gevraagd besluit
Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om in te stemmen met:
1. de opname van NEN-ISO/IEC 27001:2013 en 27002:2013 op de 'pas toe of leg uit'-lijst, ter vervanging van de respectievelijke versies 2005 en 2007 van deze standaarden;
2. de adviezen ten aanzien van de adoptie van NEN-ISO/IEC 27001 en 27002.

Vanuit de Stuurgroep open standaarden
De expertgroep geeft aan dat het beheer voor de standaard goed is geregeld en dat het predicaat 'uitstekend beheerproces' toegekend kan worden. Het advies vanuit de stuurgroep open standaarden is echter om deze status niet toe te kennen. Dit vanwege de kosten voor het aanschaffen van de standaard en de mogelijke impact van nieuwe versies voor overheden. Ook voor een eventuele nieuwe versie blijft nadere toetsing nodig en zal de gehele procedure doorlopen moeten worden.

<u>Ad 1 Opname van NEN-ISO/IEC 27001:2013 en 27002:2013 op de 'pas toe of leg uit'-lijst</u>

Het functioneel toepassingsgebied van NEN-ISO/IEC 27001:2013 betreft:
Specificeren van eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

Het functioneel toepassingsgebied van NEN-ISO/IEC 27002:2013 betreft:
De standaard omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van

bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

Op de standaarden is de 'pas toe of leg uit'-verplichting van toepassing bij de inkoop (waaronder bij aanbestedingen) van die ICT-producten en –diensten, waarvoor met een risicotaxatie door de behoeftesteller wordt vastgesteld dat naleving van de standaarden door de leverancier vereist is. Deze 'pas toe of leg uit'-verplichting houdt niet in dat leveranciers gecertificeerd moeten zijn tegen NEN-ISO/IEC 27001:2013.[1] Voorts geldt voor NEN-ISO/IEC 27002:2013 dat de behoeftesteller beleid dient vast te stellen aan de hand waarvan de te vereisen beveiligingsmaatregelen worden bepaald uit de set van beveiligingsmaatregelen die NEN-ISO/IEC 27002:2013 beschrijft. Voor overheden kunnen dit de Baselines Informatiebeveiliging zijn.

Als organisatorisch werkingsgebied voor beide standaarden wordt geadviseerd: *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.*

Ad 2 Additionele adviezen ten aanzien van de adoptie van NEN-ISO/IEC 27001 en 27002

Ten aanzien van de adoptie van NEN-ISO/IEC 27001 en 27002 worden de volgende oproepen gedaan:

1. de lopende besprekingen tussen het ministerie van BZK en de NEN ten aanzien van de afkoop van het gebruik van de standaarden zo snel mogelijk af te ronden;
2. op de 'pas toe of leg uit'-lijst de verhouding tussen de standaarden en de baselines informatiebeveiliging op te nemen;
3. de relatie tussen de normen en de baselines informatiebeveiliging met de beheerders van de baselines te bewaken via de Werkgroep Normatiek;
4. inkopende organisaties dienen zelf, ten aanzien van een specifieke aanschaf, risicogebaseerd te bepalen of zij de naleving van deze standaarden van hun leverancier vereisen, mede op basis van de eigen intern geldende baseline informatiebeveiliging; er is geen algemeen vereiste om deze standaarden bij alle inkopen van ICT-producten en diensten te vereisen, en
5. in de communicatie rond opname van deze standaarden op de 'pas toe of leg uit'-lijst dient helder te zijn dat niet beoogd wordt om in alle gevallen van toepassing van deze standaarden certificering van de leverancier te eisen; in eerste instantie kan naleving van de standaarden vereist worden en daarna, voor zover opportuun voor de inkopende organisatie in het specifieke geval, kan certificering van de leverancier vereist worden.

De opgeroepen partijen worden gevraagd om zo spoedig mogelijk, maar in ieder geval uiterlijk na één jaar na opname van de standaard over de voortgang van deze punten te rapporteren aan het Forum Standaardisatie.

Toelichting

1. Waar gaat het inhoudelijk over?

De standaarden NEN-ISO/IEC 27001 en 27002 zijn een vertaling van de internationale normen ISO/IEC 27001 en 27002. Op de 'pas toe of leg uit'-lijst

[1] *Door de aard van de standaarden is certificering tegen NEN-ISO/IEC 27001:2013 wel mogelijk en certificering tegen NEN-ISO/IEC 27002:2013 niet mogelijk.*

staan de Nederlandse versies uit respectievelijk 2005 en 2007. Inmiddels zijn versies beschikbaar die zijn vastgesteld in 2013.

Ondanks dat de structuur van de nieuwe NEN-ISO/IEC 27001 aanzienlijk is veranderd en er een aantal nieuwe normen is toegevoegd, is de nieuwe 27001 standaard (2013) niet strijdig met de oude. De nieuwe NEN-ISO/IEC 27002-standaard omvat een aantal nieuwe normen en bestaande normen zijn geüpdatet naar de huidige stand der techniek.

De NEN-ISO/IEC 27001-standaard bevat eisen waar het management systeem voor informatiebeveiliging aan dient te voldoen. Het is deze norm waartegen wordt geaudit bij certificering. De NEN-ISO/IEC 27002-standaard is een "best practice" van beveiligingsmaatregelen. Deze standaard is een adviserend document en geen formele specificatie zoals NEN-ISO/IEC 27001:2013. De NEN-ISO/IEC 27002 standaard is een set met beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening.

2. Hoe is het proces verlopen?

In opdracht van het Bureau Forum Standaardisatie heeft in 2014 een verkennend onderzoek (zie Forumvergadering 16 december 2014) plaatsgevonden naar de versie 2013 van de genoemde standaarden. Dit onderzoek is onder ander uitgevoerd in afstemming met de beheerders van de verschillende Baselines (BIG, BIR, IBI, BIWA) en de Werkgroep Normatiek van de Taskforce BID.

Het verkennend onderzoek was de aanleiding voor het Forum Standaardisatie om een expertonderzoek uit te laten voeren. De uitkomsten van het expertonderzoek zijn ter publieke consultatie aangeboden. Aan het expertonderzoek hebben (toekomstig) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen. Naar aanleiding van de publieke consultatie zijn een aantal aandachtspunten naar voren gekomen. Deze reacties zijn in overleg met de betrokken partijen verwerkt in dit advies.

3. Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

De expertgroep concludeert dat het standaardisatieproces van NEN en ISO voldoende open is. Het standaardisatieproces kwalificeert positief op alle criteria. De expertgroep geeft aan dat het predicaat 'uitstekend beheer' toegekend kan worden. Dit betekent dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaarden. Gezien de kosten die gemaakt moeten worden voor de standaard en de impact van eventuele wijzigingen is het advies van de stuurgroep open standaarden om dit advies niet over te nemen en het predicaat 'uitstekend beheer' niet toe te kennen.

Toegevoegde waarde

De standaarden NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:2013 zijn internationaal de *de facto* standaarden voor informatiebeveiliging. De huidige sectorale baselines BIR, BIG, BIWA en IBI zijn afgeleid van de vorige versie NEN-ISO/IEC 27001:2005 en NEN-ISO/IEC 27002:2007.

De standaarden werken uniformerend ten aanzien van het informatiebeveiligingsbeleid, het managementsysteem voor informatiebeveiliging en de beveiligingsmaatregelen. Dit zorgt voor duidelijkheid in de relatie tussen

(overheids-)opdrachtgever en leveranciers van ICT-producten en -diensten. Het is met de standaarden voor leveranciers eenduidiger aantoonbaar dat zij aan de vereiste informatiebeveiligingsnormen voldoen.

De vorige versie van de standaarden ISO 27001 en 27002 staan reeds op de 'pas toe of leg uit'-lijst. De expertgroep is van mening dat wanneer overheidsinstellingen al de oude standaarden uitvragen bij leveranciers, het met beperkte inspanning en middelen mogelijk moet zijn de nieuwe standaarden uit te vragen bij leveranciers.

De expertgroep concludeert dat NEN-ISO/IEC 27001:2013 en 27002:2013 voldoende toegevoegde waarde hebben binnen het gekozen functioneel toepassingsgebied en organisatorisch werkingsgebied.

Draagvlak
Deze standaarden zijn de *de facto* standaarden voor informatiebeveiliging. Vrijwel alle leveranciers waar informatiebeveiliging een rol speelt in de geleverde producten en diensten, hanteren deze standaarden.

Leveranciers hebben tot 1 oktober 2015 de tijd om zich te (her)certificeren tegen de nieuwe NEN-ISO/IEC 27001:2013. Vanaf 1 oktober 2015 kunnen externe leveranciers van de overheid uitsluitend over certificaten op basis van de NEN-ISO/IEC 27001:2013 beschikken aangezien per die datum de ISO27001:2005 certificaten hun geldigheid verliezen.

De expertgroep concludeert dat het draagvlak voor NEN-ISO/IEC 27001:2013 en 27002:2013 voldoende is.

Opname bevordert de adoptie
De expertgroep concludeert dat de ‘pas toe of leg uit’-lijst het passende middel is om de adoptie van de standaarden binnen de (semi-) overheid te bevorderen.

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad om de standaarden NEN-ISO/IEC 27001:2013 en 27002:2013 op te nemen op de ‘pas toe of leg uit’-lijst, ter vervanging van de versies 2005 en 2007 van deze standaarden. De expertgroep adviseert tevens de relatie met de Baselines Informatiebeveiliging op de lijst te verduidelijken zoals vastgesteld in het verkennend onderzoek.

Daarnaast adviseert de expertgroep het Forum Standaardisatie en het Nationaal Beraad de standaarden het predicaat ‘uitstekend beheerproces’ toe te kennen, waardoor voor nieuwe versies van de standaarden niet de gehele toetsingsprocedure doorlopen hoeft te worden. Het advies van de stuurgroep open standaarden is om dit laatste advies niet over te nemen.

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies zijn reacties ontvangen van DHPA, CROW, DICTU, DUO en de Kamer van Koophandel. Deze partijen hebben positief gereageerd op het expertadvies en onderschrijven het belang van de standaarden en opname op de ‘pas toe of leg uit-lijst. Hieronder volgt het commentaar van de genoemde partijen. DICTU en de Kamer van Koophandel hadden geen inhoudelijk commentaar.

DHPA
DHPA heeft opmerkingen gemaakt over:
1. Het functioneel toepassingsgebied van NEN-ISO/IEC 27002: hieraan zou moeten worden toegevoegd dat een behoeftesteller bij inkoop van ICT beleid dient vast te stellen waarmee per "systeem" en/of per leverancier de juiste technische maatregelen worden vereist.
   Reactie: De opmerking is overgenomen in de toelichting op het functioneel toepassingsgebied van NEN-ISO/IEC 27002.

2. Overheden dienen te voorzien in het aantonen van governance en control voor alle leveranciers in de technische leveringsketen. Dat geldt met name voor de leveranciers die een autonome dienstverlening inbrengen.
   Reactie: Dit is een belangrijk aspect en wordt in het algemeen geadresseerd in NEN-ISO/IEC 27001:2013 (met name door de holistische en gecoördineerde benadering van informatiebeveiligingsrisico's van de organisatie) en specifiek geadresseerd in NEN-ISO/IEC 27002:2013 (met name paragraaf 15.1.3 *Toeleveringsketen van informatie- en communicatietechnologie*).

CROW
CROW heeft opmerkingen gemaakt over:
3. Het mogelijke raakvlak en/of overlap van NEN-ISO/IEC 27001 en 27002 met de VISI-standaard.
   Toelichting op de vraag: VISI staat op de 'pas toe of leg uit'-lijst en richt zich op digitale communicatie tussen partijen in een bouwproject. VISI wordt gebruikt in de bouw bij het geven van opdrachten, het aanleveren van tijdschema's, het opleveren van resultaten en het melden van afwijkingen.
   Reactie: In nader overleg met CROW is geconcludeerd dat er geen raakvlak of overlap is tussen NEN-ISO/IEC 27001 en 27002 en de VISI-standaard in relatie tot het werkingsgebied van de standaarden.

DUO
DUO heeft opmerkingen gemaakt over:
4. Het gebruik van de term *governance* in het functioneel toepassingsgebied van NEN-ISO/IEC 27002.
   Reactie: De term *governance* komt niet voor in NEN-ISO/IEC 27002. De beschrijving van het functioneel toepassingsgebied is gewijzigd en komt nu woordelijk overeen met de lijst van onderwerpen in NEN-ISO/IEC 27002.
5. Het functioneel toepassingsgebied van NEN-ISO/IEC 27002 reikt verder dan informatiebeveiliging "binnen" de organisatie. Het betreft ook informatiebeveiliging tussen of buiten de organisatie in relatie tot ketens of netwerken.
   Reactie: De standaard maakt de inperking tot informatiebeveiliging "binnen" organisaties niet. Het functioneel toepassingsgebied is aangepast en sluit nu aan op de omschrijving die de standaard zelf geeft. Het functioneel toepassingsgebied betreft richtlijnen voor informatiebeveiligingsnormen voor organisaties.
6. Onderschrijft dat het zinvol is de standaarden te verplichten.
   Reactie: Behoeft geen reactie.
7. De vraag om bij de adoptieadviezen die betrekking hebben op sectorale baselines ook de baseline van de onderwijssector te betrekken, beschreven in het ROSA-katern Privacy en Security.
   Reactie: Waar in de adoptieadviezen specifieke sectorale baselines genoemd worden, is toegevoegd dat daaronder ook sectorale baselines, zoals die in het onderwijs, verstaan moeten worden.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaarden?

Ten aanzien van de adoptie van NEN-ISO/IEC 27001 en 27002 worden de volgende oproepen gedaan:

1. de lopende besprekingen tussen het ministerie van BZK en de NEN ten aanzien van de afkoop van het gebruik van de standaarden zo snel mogelijk af te ronden;
2. op de 'pas toe of leg uit'-lijst de verhouding tussen de standaarden en de baselines informatiebeveiliging (zoals de BIR, BIG, BIWA, IBI en sectorale baselines zoals die in het onderwijs[2]) op te nemen;
3. de relatie tussen de normen en de baselines informatiebeveiliging met de beheerders van de baselines te bewaken via de Werkgroep Normatiek;
4. inkopende organisaties dienen zelf, ten aanzien van een specifieke aanschaf, risicogebaseerd te bepalen of zij de naleving van deze standaarden van hun leverancier vereisen, mede op basis van de eigen intern geldende baseline informatiebeveiliging; er is geen algemeen vereiste om deze standaarden bij alle inkopen van ICT-producten en diensten te vereisen, en
5. in de communicatie rond opname van deze standaarden op de 'pas toe of leg uit'-lijst dient helder te zijn dat niet beoogd wordt om in alle gevallen van toepassing van deze standaarden certificering van de leverancier te eisen; in eerste instantie kan naleving van de standaarden vereist worden en daarna, voor zover opportuun voor de inkopende organisatie in het specifieke geval, kan certificering van de leverancier vereist worden.

De opgeroepen partijen worden gevraagd om zo spoedig mogelijk, maar in ieder geval uiterlijk na één jaar na opname van de standaard over de voortgang van deze punten te rapporteren aan het Forum Standaardisatie.

Aanvullende informatie

- Expertadvies ISO27001/2: https://www.forumstandaardisatie.nl/sites/default/files/FS/2015/0422/Expertadvies-ISO-27001-en-27002-v1-0.pdf

- Overzicht reacties consultatieronde: https://www.forumstandaardisatie.nl/sites/default/files/FS/2015/0422/Reacties-uit-openbare-consultatie-NEN-ISO-IEC-27001-en-27002.pdf

[2] *Zoals vastgelegd in het Edustandaard ROSA-katern Privacy en Security.*