Forum Standaardisatie

Expertadvies NEN-ISO/IEC 27001:2013 en 27002:2013

Datum 9 februari 2015

Colofon

Projectnaam	Expertadvies NEN-ISO/IEC 27001:2013 en 27002:2013
Versienummer	1.0
Locatie	
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteurs	Paul Dam en Steven Debets

Inhoud

Forumadvies & Managementsamenvatting

Advies aan het Forum
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 respectievelijke versies 2005 en 2007 van deze standaarden.

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.

Als functioneel toepassingsgebied wordt geadviseerd:

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 de governance van informatiebeveiliging binnen een organisatie, de inrichting van leveranciersmanagement op het gebied van informatieveiligheid en technische beveiligingsmaatregelen.

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]

Als organisatorisch werkingsgebied wordt geadviseerd:

Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.

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 lijst voor 'pas toe of leg uit' 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.

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.

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.

Hoe is het proces verlopen?
In opdracht van het Bureau Forum Standaardisatie heeft een verkennend onderzoek plaatsgevonden naar de versie 2013 van de genoemde standaarden. Dit onderzoek was de aanleiding voor het Forum Standaardisatie om een expertonderzoek uit te laten voeren. De uitkomsten van de expertonderzoek, waaronder de vaststelling van het functioneel toepassingsgebied en organisatorisch werkingsgebied, zijn door de voorzitter en begeleider verwerkt in dit adviesrapport, dat ter publieke consultatie zal worden aangeboden.

Hoe scoort de standaard op de toetsingscriteria?

<u>Toegevoegde waarde</u>
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 schat in 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.

<u>Open standaardisatieproces</u>
De expertgroep concludeert dat het standaardisatieproces van NEN en ISO voldoende open is. Het standaardisatieproces kwalificeert positief op alle criteria. De expertgroep adviseert het Nationaal Beraad deze standaarden het predicaat 'uitstekend beheer' toe te kennen, waardoor voor nieuwe versies van de standaarden geen aanvullende toetsing meer nodig is.

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.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De expertgroep doet het Nationaal Beraad de aanbeveling om bij de opname op de 'pas toe of leg uit'-lijst de volgende oproepen ten aanzien van de adoptie van de standaarden NEN-ISO/IEC 27001:2013 en 27002:2013 te doen:

- 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;
- op de 'pas toe of leg uit'-lijst de verhouding tussen de standaarden en de baselines informatiebeveiliging op te nemen;
- de relatie tussen de normen en de baselines informatiebeveiliging met de beheerders van de baselines te bewaken via de Werkgroep Normatiek;
- 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
- 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.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2011-2015, de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Deze plannen onderstrepen de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met standaarden, die vallen onder het principe 'pas toe of leg uit'. Het Nationaal Beraad Digitale Overheid spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Doelstelling expertadvies

Onderwerp van dit expertadvies is NEN-ISO/IEC 27001:2013 en 27002:2013. De voorgaande versie van deze standaarden staat reeds op de 'pas toe of leg uit'-lijst.

Doel van dit advies is om, aan de hand van de criteria van het Forum en het Nationaal Beraad, vast te stellen:

- of de versie 2013 van de standaarden NEN-ISO/IEC 27001 en 27002 moet worden opgenomen op de 'pas toe of leg uit'-lijst, al dan niet onder bepaalde voorwaarden.

1.3 Doorlopen proces

Voor het opstellen van dit advies is de volgende procedure doorlopen:

- In opdracht van het Bureau Forum Standaardisatie heeft een verkennend onderzoek plaatsgevonden naar de versie 2013 van de genoemde standaarden. Het onderzoeksrapport is behandeld in de vergadering van het Forum op 16 december 2014. Het Forum besloot de versie 2013 van beide standaarden in procedure te nemen voor plaatsing op de 'pas toe of leg uit'-lijst ter vervanging van de respectievelijke versies NEN-ISO/IEC 27001:2005 en NEN-ISO/IEC 27002:2007.
- Op basis van dit besluit is een expertgroep samengesteld en een voorzitter aangesteld. Op basis van het verkennend onderzoek is een voorbereidingsdossier opgesteld voor de leden van de expertgroep.
- De expertgroep is op 19 januari 2015 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van het expertonderzoek zijn door de voorzitter en begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met het verzoek om een reactie. Na verwerking van deze reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend bij het Bureau Forum Standaardisatie ten behoeve van de publieke consultatieronde.

1.4 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of de nieuwe versie van de standaard op de 'pas toe of leg uit'-lijst komt.

1.5 Samenstelling expertgroep

Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere kennishebbers. Daarnaast wordt een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden Steven Debets, partner bij Verdonck, Klooster & Associates. Paul Dam, adviseur bij Verdonck, Klooster & Associates, heeft de expertgroep in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:
- Wiekram Tewarie, CIP
- René Terbijhe, IPO/CIBO
- Koen Wortmann, VNG
- Jan Rietveld, NEN
- Tony van der Togt, ministerie van BZK
- Jule Hintzbergen, KING
- Tobias Schaap, ministerie van Financiën/ADR
- Robert Flinterman, gemeente Den Haag
- Erik de Groot, gemeente Den Haag
- Wilbert Vrouwenvelder, Logius
- Henk Keijzer, DEKRA
- Ruud de Bruijn, CIP
- Carl Adamse, ministerie van BZK/DGOBR
- Arjan de Jong, ministerie van BZK/DGBK
- Peter van Dijk, Taskforce BID

Lancelot Schellevis van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Leeswijzer

In hoofdstuk 2 wordt beschreven wat de standaard inhoudt, in welke gevallen de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de nieuwe versie van de standaard opgenomen moet worden op de lijst met standaarden voor 'pas toe of leg uit', is deze getoetst aan een viertal vastgestelde criteria. In hoofdstuk 3 staat het

resultaat van deze toetsing. Ook zijn er adviezen ter bevordering van de adoptie van de standaard gegeven.

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het 'pas toe of leg uit'-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruikt moet worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Toelichting[2] NEN-ISO/IEC 27001:2013 en 27002:2013

NEN-ISO/IEC 27001:2013
Deze standaard specificeert 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 van een organisatie. Het ISMS, het managementsysteem voor informatiebeveiliging, is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatievoorziening afdoende beveiligen en vertrouwen bieden.

De NEN-ISO/IEC 27001 norm bevat eisen waar het management systeem voor informatiebeveiliging aan dient te voldoen. Het is deze norm waartegen wordt geaudit bij certificering. Organisaties die gecertificeerd zijn, zijn dus gecertificeerd op de 27001 standaard.

Op dit moment is er een overgangsperiode voor het aanpassen op de nieuwe 27001 standaard. Tijdens deze overgangsperiode is het gebruik van zowel de oude als de nieuwe standaard toegestaan. Deze periode loopt tot en met september 2015 daarna toetsen auditoren alleen nog maar tegen de nieuwe standaard. Vanaf 1 oktober 2015 worden alleen nog maar certificaten op basis van de nieuwe 27001:2013 norm afgegeven. Dit geldt dus voor alle organisatie zowel overheidsinstellingen als de private sector.

NEN-ISO/IEC 27002:2013
Deze 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. De NEN-ISO/IEC 27002 standaard omvat best practices op het gebied van de governance van informatiebeveiliging binnen een organisatie, de inrichting van leveranciersmanagement op het gebied van informatieveiligheid en een aantal best practices op het gebied van technische beveiligingsmaatregelen (zoals o.a. het gebruik van firewalls, demilitarized zones, encryptie en operationeel beheer).

[2] Bron: *Verkennend onderzoek NEN-ISO/IEC 27001 en 27002*, Forum Standaardisatie, december 2014. Te raadplegen op https://www.forumstandaardisatie.nl/fileadmin/os/Vergaderstukken/FS_141216.5E_Onderzoek_NEN-ISO_IEC_27001_27002_v0.9c.pdf.

Relatie NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:2013
Tussen de NEN-ISO/IEC 27001 en 27002 standaarden is een duidelijke relatie. NEN-ISO/IEC 27001 beschrijft de eisen die worden gesteld aan het managementsysteem voor informatiebeveiliging. De maatregelen die hiervoor getroffen kunnen worden zijn samengevat in Annex A van de NEN-ISO/IEC 27001 norm. Het zijn deze maatregelen uit Annex A die vervolgens in de NEN-ISO/IEC 27002 standaard verder zijn uitgewerkt en voorzien van implementatierichtlijnen.

Verschillen NEN-ISO/IEC 27001:2005 en 27001:2013
Op hoofdlijnen zijn hieronder de verschillen tussen de NEN-ISO/IEC 27001:2005 en de NEN-ISO/IEC 27001:2013 norm weergegeven:

- De 2013 versie heeft een volledig andere structuur dan de oude norm. De nieuwe norm is in lijn met het vanuit ISO voorgeschreven template voor normen voor managementsystemen. Met deze nieuwe structuur is het makkelijker om verschillende normen voor managementsystemen (zoals ISO 27001, ISO 9001, ISO 22301) met elkaar te integreren.
- De eisen die de nieuwe versie stelt aan een risicoanalyse zijn meer generiek van aard en zijn in lijn met de ISO 31000 norm (Risk Management, Principles and Guidelines). Dit biedt overheidsinstellingen meer keuzevrijheid in het uitvoeren van de risicoanalyse.
- In de nieuwe versie is meer expliciet aandacht voor de context (omgeving) van de organisatie. Het uitvoeren van een stakeholderanalyse vormt een belangrijke aanvulling op de risicoanalyse.
- In de nieuwe versie is geen sprake meer van een dwingende lijst met verplichte documenten. Overal waar in de norm een proces beschreven wordt, staat nu dat er bewijs moet zijn van een werkend proces in de vorm van 'documented information'. Bijvoorbeeld in de nieuwe norm is de procedure voor preventieve acties komen te vervallen.
- Ten slotte bevat de nieuwe versie geen dubbele beveiligingsmaatregelen meer en zijn diverse maatregelen qua formulering herzien.

Verschillen NEN-ISO/IEC 27002:2007 en 27002:2013
Op hoofdlijnen zijn hieronder de verschillen tussen de NEN-ISO/IEC 27002:2007 en de NEN-ISO/IEC 27002:2013 standaard weergegeven:

- In de nieuwe versie zijn vier hoofdstukken toegevoegd. De nieuwe hoofdstukken behandelen de volgende onderwerpen:
  - Cryptografie (hoofdstuk 10)
  - Leveranciersrelaties (hoofdstuk 15)
  - Hoofdstuk 10 in de oude versie 'Beheer van communicatie- en bedieningsprocessen' is in de nieuwe versie uitgesplitst naar twee hoofdstukken Beveiliging bedrijfsvoering (hoofdstuk 12) en Communicatiebeveiliging (hoofdstuk 13).

  Door deze herschikking van hoofdstukken en het verdiepen van de bijbehorende beveiligingsmaatregelen schenkt de nieuwe standaard extra aandacht aan bovenstaande onderwerpen.
- In het hoofdstuk over bedrijfscontinuïteitsbeheer in de nieuwe versie wordt een beter onderscheid gemaakt tussen informatiebeveiligingscontinuïteit en beschikbaarheid. Dit is inclusief nieuwe maatregelen voor het gebruik van redundante uitvoering van de informatievoorziening om te voldoen aan vastgestelde beschikbaarheidseisen.

- In de nieuwe standaard worden specifieke maatregelen genoemd om informatiebeveiligingsincidenten te beoordelen en hierop adequaat te reageren.
- Ten slotte is de beschrijving van de beveiligingsmaatregelen in de nieuwe versie van NEN-ISO/IEC 27002 aangescherpt. Een aantal algemene maatregelen is vervangen door meer specifieke beveiligingsmaatregelen.

2.2 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:

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 de governance van informatiebeveiliging binnen een organisatie, de inrichting van leveranciersmanagement op het gebied van informatieveiligheid en technische beveiligingsmaatregelen.

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.[3]

2.3 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaarden NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:2013 overeen te laten komen met het algemene werkingsgebied waarop het 'pas toe of leg uit' principe van toepassing is, te weten:

Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

3 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.

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor indieners en experts"* en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

3.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

3.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.2.

3.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.3.

3.1.1.3 Is de standaard generiek toepasbaar en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke voorzieningen? (toelichtende vraag)
Ja, de standaard is algemeen toepasbaar. De standaard is generiek van toepassing op overheidsorganisaties. De toepassing is niet sectoraal bepaald en is niet beperkt tot specifieke vormen van gegevensuitwisseling. De normen zijn geschikt voor zowel overheid als bedrijfsleven. De standaard levert geen belemmering op voor het van toepassing zijn van andere (meer specifieke) normen.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?
Ja, op de 'pas toe of leg uit'-lijst staan de volgende standaarden die betrekking hebben op informatiebeveiliging: DNSSEC, DKIM, SAML, Digikoppeling en TLS. Daarnaast staan op lijst met gangbare standaarden: AES, IPSec, SHA2, HTTPS, SSH2 en X509. Geen van deze standaarden conflicteert met NEN-ISO/IEC 27001:2013 of NEN-ISO/IEC 27002:2013.

3.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan)
Ja, de standaarden zijn geactualiseerd en in lijn gebracht met huidige inzichten op het gebied van informatiebeveiliging en de stand der techniek.

Voor zover organisaties vereisen dat een leverancier gecertificeerd is, is van belang dat alle certificaten op basis van de oude versie van de standaard NEN-ISO/IEC 27001:2005 zullen vervallen per 1 oktober 2015. Audits en hercertificering zijn vanaf 1 oktober 2015 uitsluitend mogelijk tegen de nieuwe versie van de standaard NEN-ISO/IEC 27001:2013.

3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)
Ja, 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).

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)
Ja, de standaarden NEN-ISO/IEC 27001 en 27002 zijn een vertaling van de internationale normen ISO/IEC 27001 en 27002.

3.1.2.5 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)
Ja. De NEN-ISO/IEC 27001:2013 standaard geeft, in een voetnoot, aan dat een organisatie zelf de beheersmaatregelen hiervoor mag ontwerpen of hiervoor gebruik mag maken van een bepaalde bron. Concreet houdt dit in dat organisaties kunnen kiezen voor het ontwerp van de noodzakelijke beveiligingsmaatregelen uit onder meer de desbetreffende sectorale baseline of hiervoor de beveiligingsmaatregelen uit de NEN-ISO/IEC 27002:2013 te nemen.[4]

Ongeacht de set van maatregelen die de organisatie kiest is het noodzakelijk om de gekozen maatregelenset te vergelijken met de beveiligingsmaatregelen zoals deze is vastgesteld in Annex A van de ISO 27001 standaard. Hiervoor is het gebruikelijk om een verklaring van toepasselijkheid op te stellen.

Er is geen sprake van (lokale) profielen die randvoorwaardelijk zijn voor interoperabiliteit. Wel moeten organisaties zelf bepalen welke normen uit ISO 27001 Annex A van toepassing zijn.

Bij opname van de nieuwe versie van de standaarden op de 'pas toe of leg uit'-lijst zal nadrukkelijk aandacht moeten worden besteed aan de relatie tussen de standaarden en de baselines.

3.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de

[4] *Zie het eerder genoemde verkennend onderzoek voor een beschrijving van de relatie tussen ISO 27001 en 27002 en de sectorale baselines.*

standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

3.1.3.1 Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?
Ja. 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.

3.1.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?
Ja. Het is met de standaarden voor leveranciers eenduidiger aantoonbaar dat zij aan de vereiste informatiebeveiligingsnormen voldoen.

3.1.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?
De onderzoeksgroep schat in 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.

3.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Ja, er zijn geen beveiligingsrisico's aan overheidsbrede adoptie van deze standaarden.

3.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Ja, er zijn geen privacyrisico's aan overheidsbrede adoptie van deze standaarden.

3.1.4 Conclusie criteria '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 staat reeds op de 'pas toe of leg uit'-lijst. De expertgroep schat in 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.

3.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?
Ja, de specificatiedocumenten van de standaarden zijn tegen betaling bij de NEN verkrijgbaar. De kosten bedragen respectievelijk € 156,48 en € 224,52 excl. BTW per gebruiker voor de standaarden ISO 27001 en 27002 (tarieven geraadpleegd in januari 2015). Op dit moment lopen er gesprekken tussen de rijksoverheid en NEN over een mogelijke afkoop van de standaarden. De uitkomst van deze gesprekken staat nog niet vast. De expertgroep geeft aan dat het belangrijk is dat hier snel duidelijkheid over komt.

3.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?
Ja, inspraak op en kennisneming van de internationale ontwikkeling van de normen is laagdrempelig en (vrijwel) kosteloos. De Nederlandse versies zijn vertalingen van de internationale norm en wijken niet materieel af.

3.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

3.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten onherroepelijk royalty-free voor eenieder beschikbaar?
Ja, het intellectueel eigendom op de normen blijft bij de standaardisatie organisatie (NEN, respectievelijk ISO). De standaardisatie organisatie stelt de norm tegen betaling beschikbaar aan organisaties voor eigen gebruik.

3.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?
Ja, op de normen rusten geen intellectuele eigendomsrechten van anderen (dan de standaardisatieorganisatie).

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?
Ja, zowel bij ISO als NEN is de besluitvorming toegankelijk voor alle belanghebbenden.

3.2.3.2 *Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?*
Ja, bij de ontwikkeling van de normen gaat ISO uit van besluitvorming bij consensus.

3.2.3.3 *Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?*
Ja, bezwaar dient tijdens (voorafgaand aan) de besluitvorming kenbaar te worden gemaakt.

3.2.3.4 *Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard? (geen harde voorwaarde)*
Ja, zowel NEN als ISO organiseren regelmatig de samenkomst van de standaardisatiecommissie/technische commissie ten behoeve van de doorontwikkeling van de standaarden.

3.2.3.5 *Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld? (geen harde voorwaarde)*
Er vindt consultatie plaats bij de leden van ISO.

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 *Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?*
Ja, NEN als ISO zijn onafhankelijke organisaties zonder winstoogmerk.

3.2.4.2 *Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
Ja, de expertgroep acht de financiering voor die termijn geborgd.

3.2.5 Is het (versie) beheer van de standaard goed geregeld?

3.2.5.1 *Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)*
Voor de standaarden zijn verschillende handreikingen verkrijgbaar ten behoeve van implementatie en migratie naar nieuwere versies.

3.2.5.2 *Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?*
Ja, de expertgroep acht het standaardisatieproces bij NEN en ISO aan deze voorwaarde te voldoen.

3.2.5.3 *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*
Ja, NEN is een "participating member" van de technische commissie van ISO die deze standaarden behandelt. De Nederlandse overheid neemt sinds kort deel aan de normcommissie van NEN.

3.2.5.4 *Is de vertyegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?*
Ja, zie 3.2.5.3.

3.2.6 Conclusie criteria 'Open standaardisatieproces'
De expertgroep concludeert dat het standaardisatieproces van NEN en ISO voldoende open is. Het standaardisatieproces kwalificeert positief op alle criteria. De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad deze standaarden het predicaat 'uitstekend beheerproces' toe te kennen, waardoor voor nieuwe versies van de standaarden geen aanvullende toetsing meer nodig is.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?
Leveranciers hebben tot 1 oktober 2015 de tijd hebben 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.

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. Een groot aantal leveranciers van ICT-diensten is ook gecertificeerd conform ISO 27001. Daarnaast zijn er meerdere ondernemingen (advies- en auditorganisaties) die hulp bieden bij de implementatie van de standaarden.

3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?
Op dit moment is er een overgangsperiode voor het aanpassen op de nieuwe NEN-ISO/IEC 27001:2013 standaard. Tijdens deze overgangsperiode is het gebruik van zowel de oude als de nieuwe standaard toegestaan. Deze periode loopt tot en met september 2015 daarna toetsen auditoren alleen nog maar tegen de nieuwe standaard.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
Een aantal overheidsorganisaties hanteert al de nieuwe standaard bij de inkoop van ICT-producten en diensten. Zij specificeren de norm voor leveranciers om aan te voldoen.

Doordat overheidsorganisaties de sectorale baselines implementeren voldoen zij zelf al (deels) aan ISO 27002:2013, ondanks dat de baselines op de oude versie gebaseerd zijn.

3.3.2.2 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?
De onderzoeksgroep geeft aan dat conform de 'pas toe of leg uit' lijst, de inkoopafdelingen van overheidsinstellingen de oude versies van de 27001

en 27002 standaarden uitvragen bij hun leveranciers bij aanschaf of (ver)bouw van ICT-systemen/-diensten.
Daarnaast zijn de overheidsorganisaties druk bezig met het in eigen organisatie implementeren van hun baselines, die gebaseerd zijn op de ISO 27002:2007.

3.3.2.3 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
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.

3.3.2.4 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
Zie 3.3.2.1.

3.3.3 Conclusie criteria '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 hebben 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.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:
1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

3.4.1 Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja. Conform de 'pas toe of leg uit' lijst, vragen de inkoopafdelingen van overheidsinstellingen de oude versies van de 27001 en 27002

standaarden uit bij hun leveranciers bij aanschaf of (ver)bouw van ICT-systemen/-diensten. Voor inkoopafdeling van overheidsinstellingen is het dan ook aan te raden dat in geval van aanbestedingen die onder het regime van de 'past toe of leg uit'-lijst vallen, vanaf 1 oktober 2015 uitsluitend certificaten op basis van de nieuwe ISO 27001 (2013) norm uit te vragen bij leveranciers. Opname van de standaarden op de lijst voor 'pas toe of leg uit' stimuleert de snelle overgang naar de nieuwe standaarden.

3.4.2 Is de lijst met gangbare open standaarden het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee. Het gebruik van de standaarden ISO 27001 en 27002 bij de inkoop van ICT-producten en –diensten heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen.
Het opnemen van deze standaarden op de "pas toe of leg uit' lijst heeft de adoptie bij Rijk, gemeenten, provincies en waterschappen wel al sterk bevorderd, o.a. door het verwerken in de betreffende baselines. Bij een aantal ZBO's en andere (semi)publieke organisaties behoeft de adoptie van deze standaarden nog de nodige aandacht.

3.4.3 Conclusie criteria 'Opname bevordert 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.

3.5 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum Standaardisatie en het Nationaal Beraad. Plaatsing op de lijsten is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan het Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

De expertgroep doet het Nationaal Beraad de aanbeveling om bij de opname op de 'pas toe of leg uit'-lijst de volgende oproepen ten aanzien van de adoptie van de standaarden NEN-ISO/IEC 27001:2013 en 27002:2013 te doen:

- 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;
- op de 'pas toe of leg uit'-lijst de verhouding tussen de standaarden en de baselines informatiebeveiliging op te nemen;
- de relatie tussen de normen en de baselines informatiebeveiliging met de beheerders van de baselines te bewaken via de Werkgroep Normatiek;
- 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

- 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 Bureau Forum Standaardisatie.