Forum Standaardisatie

Verkennend onderzoek NEN-ISO/IEC 27001 en 27002

Datum 27 november 2014

Colofon

Projectnaam	Verkennend onderzoek NEN-ISO/IEC 27001 en 27002
Versienummer	0.9
Locatie	
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteurs	Drs. Norbert Kuiper CISA CISM

Inhoud

1 Inleiding op het onderzoek

1.1 Achtergrond

Op de 'pas toe of leg uit'-lijst (hierna: de lijst) staan de internationaal geaccepteerde normen voor informatiebeveiliging ISO/IEC 27001 en ISO/IEC 27002. ISO 27001 beschrijft de eisen aan het managementsysteem voor informatiebeveiliging. De bijbehorende ISO-norm 27002 bevat de maatregelen voor informatiebeveiliging.

Opname van een standaard op de lijst betekent dat bij het inkopen van ICT-producten boven de € 50.000,= overheidsorganisaties moeten vragen naar de (relevante) standaarden die op de lijst staan. Concreet houdt dit in dat overheidsorganisaties aan leveranciers vragen om te voldoen aan de 27001 en 27002-normen.

De versies die momenteel opgenomen zijn op de lijst dateren uit 2005 (NEN-ISO/IEC 27001) en 2007 (NEN-ISO/IEC 27002). Beide normen zijn echter in 2013 vernieuwd. Omdat bedrijven (leveranciers van de overheid) en auditoren volgens deze nieuwe versie gaan werken en toetsen, zal deze versie op de lijst moeten worden aangepast. Zodat er één taal voor informatiebeveiliging wordt gesproken.

De 27001 en 27002-normen zijn geschikt voor zowel bedrijfsleven als overheid. De Nederlandse overheid heeft echter ook haar eigen kaders voor informatiebeveiliging die zijn afgeleid van de 27001 en 27002-normen. Dit zijn de sectorale baselines informatiebeveiliging, oftewel de Baseline Informatiebeveiliging Rijksdienst (BIR), de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de Baseline Informatiebeveiliging Waterschappen (BIWA) en de Interprovinciale Baseline Informatiebeveiliging (IBI).

Deze baselines informatiebeveiliging zijn gebaseerd op de (oude) NEN-ISO/IEC 27002:2007 standaard en bevatten verder uitgewerkte beveiligingsmaatregelen. De standaarden en de sectorale baselines zijn beschreven in bijlage A van dit rapport.

1.2 Probleemstelling

Dit onderzoek gaat in op:

- De impact van de versiewijziging voor overheidsorganisaties en de ‘pas toe of leg uit’-lijst. Wanneer moet de versie op de lijst worden aangepast?
- De relatie tussen de standaarden en de baselines informatiebeveiliging en hoe deze relatie te verduidelijken op de ‘pas toe of leg uit’-lijst, dit met name ook in relatie tot leveranciers.

Binnen dit verkennende onderzoek worden de volgende hoofdvragen beantwoord. Een hoofdvraag bestaat uit één of meerdere subvragen. Deze vragen zijn in de overige hoofdstukken van dit rapport uitgewerkt.

Hoofdvraag 1
Wat zijn de wijzigingen van de nieuwe NEN-ISO/IEC 27001 en 27002-standaarden (versie 2013) ten opzichte van de oude en wat is de impact hiervan op overheidsorganisaties, de Baselines Informatiebeveiliging en leveranciers?

Hoofdvraag 2
Betekent dat het voldoen aan de Baselines Informatiebeveiliging door overheidsorganisaties ook dat wordt voldaan aan de NEN-ISO/IEC 27001 en 27002 standaarden?

De resultaten van dit verkennende onderzoekt helpt het Forum bij het besluit of, wanneer en hoe NEN-ISO/IEC 27001:2013 en 27002:2013 in procedure genomen moeten worden voor opname op de 'pas toe of leg uit'-lijst. Daarnaast helpt het onderzoek de relatie tot de baselines informatiebeveiliging beter te duiden, met name ook in relatie tot het inkopen van software bij leveranciers.

1.3 Scope

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. Het uitgevoerde onderzoek spitst zich toe op deze Nederlandse versies van de standaarden. Daarnaast wordt ook gekeken naar de relatie van de standaarden met de verschillende baselines informatiebeveiliging.

De NEN-ISO/IEC 27001 norm beschrijft de eisen die worden gesteld aan het managementsysteem voor informatiebeveiliging en waaraan een organisatie dient te voldoen wanneer zij conformiteit met deze norm claimt. De NEN/ISO 27002 beschrijft de implementatierichtlijnen voor beveiligingsmaatregelen.

1.4 Relatie met andere standaarden

Standaarden zijn cruciaal voor informatiebeveiliging en veilige gegevensuitwisseling. Er is alleen niet één bepaalde standaard die alle beveiligingsrisico's afdekt. Het gaat om een samenspel van meerdere standaarden. Op dit moment staat een zestal standaarden die betrekking hebben op informatiebeveiliging op de 'pas toe of leg uit'-lijst, namelijk:

1. NEN-ISO/IEC 27001/27002: beschrijft hoe informatiebeveiliging procesmatig in te richten en omvat implementatierichtlijnen voor informatiebeveiligingsmaatregelen.
2. DNSSEC: zorgt dat domeinnamen betrouwbaar worden vertaald naar ip-adressen.
3. DKIM: voorkomt misbruik van het afzendadres/domein en beschermt daarmee tegen phishing-mails.
4. SAML: beschrijft identiteitsattributen, uitwisselprotocollen en transport ten behoeve van authenticatie.
5. Digikoppeling: zorgt voor beveiligd berichtenverkeer.
6. TLS: zorgt voor een beveiligde internetverbinding en biedt zekerheid over de identiteit van beide communicerende partijen waardoor veilige communicatie mogelijk is.

Aanvullend hierop staan er ook verschillende standaarden voor informatiebeveiliging op de gangbare lijst (AES, IPSec, SHA2, HTTPS, SSH2, X509).

1.5 Ontwikkelingen

Naast dat er eind 2013 nieuwe versies van de standaarden NEN-ISO/IEC 27001 en 27002 zijn verschenen, zijn er diverse ontwikkelingen op het gebied van informatiebeveiliging binnen de overheid, namelijk:

1. Voor het aanpassen op de nieuwe 27001 standaard is er een overgangsperiode. 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 27001 standaard.
2. Overheidsinstellingen zijn de afgelopen jaren bewuster bezig met de onderwerpen informatiebeveiliging en cyber security. De initiatieven vanuit de overheid door bijvoorbeeld de Informatiebeveiligingsdienst voor gemeenten (IBD) [1] en de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) [2] spelen hierbij een belangrijke rol.
3. Overheidsinstellingen hebben zichzelf gecommitteerd aan de implementatie van diverse sectorale baselines informatiebeveiliging, zoals de BIR, BIG, BIWA en IBI. Diverse overheidsinstellingen zijn momenteel bezig om de beveiligingsmaatregelen, zoals beschreven in deze baselines, te implementeren.
   Momenteel vindt er een update plaats op het Besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR). Deze aanpassing is eind 2015 in concept gereed. In bijlage A van dit rapport is een toelichting te vinden op de VIR.
4. Tenslotte, is het de verwachting dat de BIR en de IBI worden aangepast aan de nieuwe ISO-normen. Dit proces start per 2015 en de planning is dat dit gereed is voor implementatie begin 2016.

1.6 Onderzoeksprocedure

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

- Door het Bureau Forum Standaardisatie (BFS) is een intakegesprek gevoerd met Verdonck, Klooster & Associates (VKA) op 8 mei 2014. Tijdens de intake is een onderzoeksgroep samengesteld en een vragenlijst opgesteld.
- Op basis van de intake is tijdens de Forum vergadering van 17 juni besloten dit onderzoek uit te voeren met de in paragraaf 1.2 genoemde vraagstelling.
- Alle betrokkenen van de onderzoeksgroep zijn persoonlijk benaderd om te vragen of en in welke mate zij konden deelnemen aan dit onderzoek. Vervolgens zijn de vragenlijsten digitaal toegestuurd aan betrokkenen.
- De betrokkenen hebben de vragenlijsten beantwoord en digitaal geretourneerd.

1 https://www.ibdgemeenten.nl/
2 http://www.taskforcebid.nl/

- Daarnaast is er een additionele documentatiestudie uitgevoerd om de verschillen tussen de nieuwe en de oude NEN-ISO/IEC 27001 en 27002 normen vast te stellen en om de verschillen tussen de sectorale baselines en de oude NEN-ISO/IEC 27001 en 27002 normen vast te stellen.
- De resultaten van de vragenlijsten en de uitgevoerde documentatiestudie zijn verwerkt tot een conceptversie van dit onderzoeksrapport.
- De conceptversie is vervolgens ter review aangeboden aan de onderzoeksgroep. De input vanuit deze review is meegenomen in het eindrapport.
- Parallel hieraan zijn de concept resultaten en een gedeelte van de vraagstelling op 15 september 2014 gepresenteerd en besproken in de Werkgroep Normatiek van de Taskforce BID [3]. De input vanuit deze werkgroep is meegenomen in dit eindrapport en afgestemd met de onderzoeksgroep.
- Het definitieve onderzoeksrapport inclusief advies, is opgeleverd voor de Forumvergadering van 16 december.

1.7 Onderzoeksgroep

In totaal zijn achttien betrokkenen samengebracht in de onderzoeksgroep, die de twee hoofdvragen hebben beantwoord aan de hand van diverse subvragen.

Voor de onderzoeksgroep zijn personen uitgenodigd die vanuit hun persoonlijke betrokkenheid of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaarden en / of sectorale baselines. Zowel technisch deskundigen als betrokkenen die inzicht hebben in de functionele en organisatorische impact zijn uitgenodigd. Bijlage B geeft een overzicht van alle leden van de onderzoeksgroep.

Het onderzoek is in opdracht van het Forum Standaardisatie uitgevoerd door Norbert Kuiper, adviseur informatiebeveiliging en bedrijfscontinuïteit bij Verdonck, Klooster en Associates (VKA).

1.8 Vervolg

Op basis van de resultaten en het advies van dit verkennende onderzoek kan het Forum Standaardisatie besluiten hoe met de nieuwe versies van de Nederlandse normen NEN-ISO/IEC 27001 en 27002 om te gaan. Het vervolg is dat de toetsingsprocedure voor opname van de nieuwe versie wordt gestart. Daarnaast dient de informatie op de ‘pas toe of leg uit’-lijst te worden aangepast zodat het voor inkopers duidelijker wordt hoe om te gaan bij het vragen naar de normen en/of de sectorale baselines in aanbestedingen.

3 http://www.taskforcebid.nl/overheidslagen/stelsel-van-informatieveiligheid/normatiek-informatieveiligheid/

1.9 Leeswijzer

In hoofdstuk 2 staat beschreven wat de verschillen zijn tussen de oude en de nieuwe NEN-ISO/IEC 27001 en 27002 standaarden. Hoofdstuk 3 gaat in op de impact van de nieuwe standaarden op het gebruik van de lijst in de praktijk. Hoofdstuk 4 beschrijft de verschillende sectorale baselines en legt een link met de lijst en de oude NEN-ISO/IEC 27001 en 27002 standaarden. Hoofdstuk 5 bevat de conclusies van het verkennende onderzoek en het advies van de onderzoeksgroep aan het Forum Standaardisatie.

2 Verschillen tussen de oude en nieuwe standaarden

2.1 Samenvatting

Dit hoofdstuk geeft een antwoord op de subvraag:
1a. Wat zijn op hoofdlijnen de verschillen tussen de oude en de nieuwe versie van de NEN-ISO/IEC 27001 en 27002-standaarden?

Conclusie:
Ondanks dat de structuur van de nieuwe NEN-ISO/IEC 27001 aanzienlijk is veranderd en er een aantal nieuwe eisen en hoofdstukken zijn toegevoegd, conflicteert de nieuwe 27001 standaard (2013) niet met de oude versie. Zo is in de nieuwe versie meer expliciet aandacht voor de context (omgeving) van de organisatie.

De nieuwe NEN-ISO/IEC 27002 standaard omvat een aantal nieuwe hoofdstukken en maatregelen, daarnaast zijn deze geüpdatet naar de huidige stand der techniek. Zo is in de nieuwe versie meer aandacht voor leveranciersrelaties.

De onderzoeksgroep schat in dat wanneer overheidsinstellingen de oude 27001 en 27002 standaarden hebben geimplementeerd, het met beperkte inspanning en middelen mogelijk moet zijn de nieuwe standaarden te implementeren.

2.2 Kwantitatieve analyse

In onderstaande tabel is kwantitatief het verschil aangegeven tussen de oude en nieuwe versies van de NEN-ISO/IEC 27001 en 27002. De verschillen die hieronder zijn aangegeven richten zich op de aantallen hoofdstukken, de eisen ten aanzien van het managementsysteem voor informatiebeveiliging, de beveiligingsdoelstellingen en de beheersmaatregelen.

Standaard		Versie 2005/2007 (Oud)	Versie 2013 (Nieuw)
ISO27001	Hoofdstukken	5	7
	Eisen (control objective)	11	22
	Eisen (controls)	102	130
ISO27002*	Hoofdstukken	11	13
	Beveiligingsdoelstellingen (control objective)	39	35
	Beheersmaatregelen (controls)	113	114

* In ISO 27001 is de Annex A opgenomen. Deze Annex heeft precies dezelfde indeling als ISO 27002.

Geconcludeerd kan worden dat het aantal hoofdstukken, de eisen ten aanzien van het managementsysteem, de beveiligingsdoelstellingen (control objective) en de beheersmaatregelen (controls) is toegenomen met het verschijnen van de nieuwe versies van de standaarden.

2.3 Verschillen oude en nieuwe versie NEN-ISO/IEC 27001

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.
- In de nieuwe versie is er meer expliciet aandacht voor de context (omgeving) van de organisatie. Het uitvoeren van een stakeholderanalyse vormt een belangrijke aanvulling op de risicoanalyse.
- 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 er 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.

Ondanks dat de structuur van de nieuwe versie aanzienlijk is veranderd en er een aantal nieuwe normen is toegevoegd, conflicteert de nieuwe versie van de standaard niet met de oude versie. De nieuwe standaard biedt een organisatie meer flexibiliteit. De vrijheid ten aanzien van het uitvoeren van een risicoanalyse en de keuzevrijheid om beveiligingsmaatregelen te selecteren uit welke maatregelenset dan ook. Tot slot is deze versie beter toegerust op samenwerking binnen een keten en wordt rekening gehouden met de context en het speelveld van een organisatie.

De onderzoeksgroep schat in dat wanneer overheidsinstellingen al de oude versie hebben geimplementeerd, het met beperkte inspanning en middelen mogelijk moet zijn de nieuwe versie te implementeren.

2.4 Verschillen oude en nieuwe versie NEN-ISO/IEC 27002

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 er 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 'bedrijfscontinuïteitsbeheer' wordt een beter onderscheid gemaakt tussen informatiebeveiligingscontinuïteit en beschikbaarheid.
- 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 aangescherpt. Een aantal algemene maatregelen zijn vervangen door meer specifieke beveiligingsmaatregelen.

Ook voor deze 2013 versie van NEN-ISO/IEC 27002 geldt dat de onderzoeksgroep inschat dat wanneer overheidsinstellingen de oude versie hebben geimplementeerd, het met beperkte inspanning en middelen mogelijk is de nieuwe versie te implementeren.

In het kader van de verschillen tussen de oude (2005 en 2007) en nieuwe versies (2013) is het van belang te weten dat beide versies niet door elkaar gebruikt kunnen worden. Het is dus niet mogelijk van NEN-ISO/IEC 27001 de 2005 versie te gebruiken en van NEN-ISO/IEC 27002 de 2013 versie en vice versa. Dit in verband met de gewijzigde structuur en het aantal maatregelen van de standaarden. Voor een nadere toelichting op de verschillen tussen de oude en de nieuwe versie van de 27002 standaard, zie bijlage A van dit rapport, en zijn diverse vertaaltabellen beschikbaar [4], zie ook de referentielijst in hoofdstuk 6.

4 http://www.informationshield.com/papers/ISO27002-2013%20Version%20Change%20Summary.pdf en http://www.gammassl.co.uk/27001/27002ControlMap.html

3 Impact van de nieuwe standaarden

3.1 Samenvatting

Dit hoofdstuk geeft een antwoord op de volgende subvragen:

1b. Welke (typen) organisaties binnen de (semi-)overheid hanteren momenteel de (oude) standaarden bij aanschaf of (ver)bouw van ICT-systemen/-diensten of zouden dit moeten doen?
1c. Wat is de impact van deze wijzigingen voor overheidsorganisaties?
1d. Wat is de impact van deze wijzigingen voor de Baselines Informatiebeveiliging?
1e. Wat is de impact van deze wijzigingen voor leveranciers?
1f. In hoeverre zijn overheidsorganisaties bezig met implementatie van de 2013 versies en wat zijn hun plannen hieromtrent?

Conclusie:
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 is vastgesteld dat veel overheidsinstellingen zijn gefocust op het implementeren van de sectorale baselines informatiebeveiliging en zich in beperkte mate richten op de implementatie van de nieuwe 27001 en 27002 standaarden.

Certificeren tegen de oude 27001 norm is niet meer mogelijk en oude certificaten zijn uiterlijk geldig tot 1 oktober 2015, dit is afhankelijk van het moment van certificering. (Her)certificering door organisaties, overheidsinstellingen en leveranciers, kan alleen nog tegen de nieuwe NEN-ISO/IEC 27001:2013 norm.

Vanaf 1 oktober 2015 beschikken organisaties uitsluitend over certificaten op basis van de NEN-ISO/IEC 27001:2013. Voor inkoopafdelingen 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 norm uit te vragen bij leveranciers.

Tenslotte, wil men gebruik maken van gecertificeerd leveranciers dan is het daarvoor noodzakelijk dat de oude standaarden op de 'pas toe of leg uit'-lijst worden aangepast met de nieuwe 2013 standaarden.

3.2 ISO 27001/2 standaarden en de 'pas toe en leg uit'-lijst

Het Forum Standaardisatie richt zich op (open) standaarden voor elektronische gegevensuitwisseling tussen overheidsinstellingen onderling en tussen overheidsinstellingen, bedrijven en burgers. Hierbij gaat het om standaarden waarmee gegevensuitwisseling over organisatiegrenzen heen kan plaatsvinden.

Overheden en semi-overheden zijn verplicht om te kiezen voor de relevante standaarden op de 'pas toe of leg uit'-lijst, bij aanschaf of (ver)bouw van ICT-systemen/-diensten (*'pas toe'*). Afwijken mag alleen met zwaarwegende redenen en verantwoording hierover moet worden afgelegd in het jaarverslag (*'leg uit'*). De NEN-ISO/IEC 27001:2005 en NEN-ISO/IEC 27002:2007 zijn open standaarden en staan sinds 2008 op de 'pas toe of leg uit'-lijst.

De NEN-ISO/IEC 27001 norm beschrijft de eisen die worden gesteld aan het managementsysteem voor informatiebeveiliging en waaraan een organisatie dient te voldoen wanneer zij conformiteit met deze norm claimt. Tegen deze norm wordt geaudit bij certificering. Organisaties die gecertificeerd zijn, zijn dus gecertificeerd op de 27001 standaard. De NEN/ISO 27002 beschrijft de implementatierichtlijnen voor beveiligingsmaatregelen.

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. Maar geven ook aan dat als nu bij leveranciers naar de 27001 en 27002 standaarden wordt gevraagd, men naar de nieuwe versies moet vragen.

3.3 Status implementatie nieuwe standaarden

Bij veel overheidsinstellingen ligt de focus op het implementeren van de sectorale baselines informatiebeveiliging en dus in beperkte mate bij NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. Organisaties stellen overigens individueel een informatiebeveiligingsbeleid vast die is gebaseerd op de baselines. Er wordt dus altijd een vertaalslag gemaakt naar de eigen omgeving en eisen. Dit informatiebeveiligingsbeleid kan dus, afhankelijk van het type organisatie, verschillen.

Afhankelijk van de desbetreffende baseline zijn overheidsinstellingen al enkele jaren bezig met de implementatie hiervan (geldt voor de BIR en IBI) of is men onlangs gestart met de implementatie (geldt voor BIG en BIWA). Ook tussen overheidsinstellingen binnen een sector bestaan verschillen in de mate waarin men voortgang boekt met de implementatie van de baselines.

Op basis van de antwoorden vanuit de onderzoekgroep is dan ook vast te stellen dat door overheidsinstellingen een hogere prioriteit wordt geschonken aan de implementatie van de sectorale baselines dan aan de implementatie van de 27001 en 27002 standaarden.

Zoals aangegeven in hoofdstuk 1, vindt vanuit de overheid een update plaats ten aanzien van de VIR, BIR en IBI. Leden van de onderzoeksgroep verwachten dat de wijzigingen van de nieuwe NEN-ISO/IEC 27002 standaard ook onderdeel uitmaakt van deze aangepaste sectorale baselines.

3.4 Impact nieuwe standaarden voor baselines

Zoals is aangegeven, beschrijft NEN/ISO 27001 de eisen die worden gesteld aan het managementsysteem voor informatiebeveiliging en NEN/ISO 27002 beschrijft de implementatierichtlijnen.
De sectorale baselines hebben slechts een relatie met de ISO 27002.

De sectorale baselines zijn gebaseerd op de oude NEN/ISO 27002 standaard. Overheidsinstellingen die bezig zijn met de implementatie van de sectorale baselines hanteren dus de oude NEN/ISO 27002 standaard.

Een praktische beschrijving hoe de ISO standaarden zich verhouden tot de sectorale baselines is opgenomen in bijlage A.

De impact van de nieuwe ISO 27002 standaard voor de baselines is dan ook dat de maatregelen zoals in de baselines benoemd zijn niet meer synchroon lopen met die van de nieuwe ISO 27002 standaard.

3.5 Impact nieuwe standaarden voor overheidsorganisaties

Zoals in het voorgaande hoofdstuk is aangegeven, zijn de verschillen tussen oude en de nieuwe standaarden te overzien. De nieuwe standaarden zijn niet fundamenteel anders dan de oude. De impact van de nieuwe standaarden is daarmee niet zo groot.

De leden van de onderzoeksgroep verwachten dan ook dat wanneer overheidsinstellingen al de oude standaarden hebben geimplementeerd, het met beperkte inspanning en middelen mogelijk moet zijn de nieuwe standaarden te implementeren.

3.6 Impact nieuwe standaarden voor interne leveranciers

Enkele interne ICT leveranciers van de overheid, waaronder shared service centers en interne beheersorganisaties, maar ook overheidsinstellingen zelf (zoals RDW en eHerkenning) zijn momenteel gecertificeerd of zijn dat op korte termijn. Deze organisaties kunnen niet blijven vasthouden aan de oude versie, NEN-ISO/IEC 27001:2005, maar moeten de nieuwe versie hanteren. Zoals eerder is aangegeven bestaat er momenteel een transitieperiode voor dergelijke 27001 certificeringen (op 27002 kan men zich niet certificeren).

Concreet houdt dit in dat certificeren tegen de oude norm niet meer mogelijk is en oude certificaten uiterlijk geldig zijn tot 1 oktober 2015, dit is afhankelijk van het moment van certificering. (Her)certificering door organisaties, overheidsinstellingen en leveranciers, kan alleen nog tegen de nieuwe NEN-ISO/IEC 27001:2013 norm. Per 1 oktober 2015 verliezen ISO27001:2005 certificaten hun geldigheid.

3.7 Impact nieuwe standaarden voor leveranciers

Overheidsinstellingen kunnen gebruik maken van diensten geleverd door externe leveranciers, bijvoorbeeld externe ICT leveranciers van de overheid, waaronder hostingsorganisaties en datacenters.

Ook voor externe leveranciers van de overheid geldt dat deze organisaties 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 oude ISO27001:2005 certificaten hun geldigheid verliezen.

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.

Als leveranciers gecertificeerd dienen te zijn bij het aannemen van opdrachten, kan dat zorgen voor een conflict. De 'pas toe of leg uit'-lijst dient hiervoor te worden aangepast.

4 Sectorale baselines

4.1 Samenvatting

Dit hoofdstuk geeft een antwoord op de volgende subvragen:
2a. Zijn de Baselines Informatiebeveiliging (BIR, BIG, IBI en BIWA) in lijn met de NEN-ISO/IEC 27001 en 27002 standaarden?
2b. Kan op de 'pas toe of leg uit'-lijst worden aangegeven dat het voldoen aan de baselines betekent dat ook wordt voldaan aan de NEN-ISO/IEC 27001 en 27002 standaarden en zo ja, hoe?

Conclusie:
De sectorale baselines hebben geen directe relatie met de oude of nieuwe versie van de ISO 27001. De relatie zit met name tussen de sectorale baselines en ISO 27002.

De huidige baselines zijn in lijn met de oude NEN-ISO/IEC 27002:2007 standaard. Ondanks dat de verschillen tussen de oude en de nieuwe versies van de 27002 zijn te overzien, zijn de sectorale baselines niet in lijn met deze nieuwe standaarden. Bij het updaten van de baselines is het aan te bevelen om deze in lijn te brengen met de 2013 versie van 27001 en 27002.

Op de 'pas toe of leg uit'-lijst kan dan ook slechts deze relatie nader toegelicht worden. Hierbij is het van belang om de verhouding tussen de ISO 27002 standaard en de sectorale baselines helder en eenduidig toe te lichten.

4.2 Baselines in lijn met de nieuwe ISO 27001/2 standaard

De sectorale baselines hebben geen directe relatie met de oude of nieuwe versie van de ISO 27001. De ISO 27001 standaard geeft wel aan dat een organisatie zelf beheersmaatregelen mag ontwerpen. Concreet houdt dit in dat een overheidsorganisatie kan kiezen voor het gebruiken van beveiligingsmaatregelen uit onder meer de desbetreffende sectorale baseline of hiervoor de beveiligingsmaatregelen uit de ISO 27002 overneemt.

De relatie tussen de baselines en de standaarden zit dan ook met name tussen de sectorale baselines en ISO 27002. De baselines zijn gebaseerd op de (oude) NEN-ISO/IEC 27002:2007 standaard en bevatten nader uitgewerkte maatregelen. De huidige baselines zijn in lijn met de oude NEN-ISO/IEC 27002:2007 standaard. Dit staat ook nadrukkelijk in de baselines vermeld. Met de opmerking dat er per baseline additionele eisen zijn opgenomen die aanvullend zijn op deze 27002 standaard.

Met de introductie van de NEN-ISO/IEC 27002:2013 standaard vermindert dan ook de mate waarin de baselines zijn afgeleid van deze standaarden. Zoals eerder aangeven in hoofdstuk 2 zijn er wel verschillen tussen de oude en nieuwe standaarden, echter deze verschillen zijn te overzien.

Ten slotte, zoals ook eerder is aangegeven vinden (op korte termijn) updates plaats van een aantal sectorale baselines. De onderzoeksgroep verwacht dan ook op korte termijn dat een aantal baselines, namelijk BIR en IBI, en het VIR, weer in lijn wordt gebracht met de nieuwe ISO 27002 standaard. Dit proces start per 2015 en de planning is dat dit gereed is voor implementatie begin 2016. Als de andere baselines in de toekomst een update gaan uitvoeren is het aan te bevelen dit ook te doen aan de hand van de nieuwe ISO27001/2 versies.

4.3 Gebruik van de lijst en de baselines bij aanbestedingen

Ondanks het feit dat overheidsinstellingen momenteel prioriteit toekennen aan de implementatie van de baselines, heeft het Forum Standaardisatie van diverse overheidsinstellingen vragen ontvangen hoe om te gaan met de nieuwe versies van de standaarden en of ze moeten voldoen aan zowel de baselines als de 27001/2 standaarden.

Deze vragen richten zich vooral op de wijze waarop de oude en in de toekomst de nieuwe NEN-ISO/IEC 27001 en 27002 standaarden toegepast dienen te worden als onderdeel van een aanbestedingstraject (‘Pas toe of leg uit’-lijst). Gebruikers van de lijst, zoals inkopers, dienen dus geholpen te zijn met wat op de ‘pas toe of leg uit’-lijst staat aangegeven.

Een belangrijk aspect hierbij is de vraag of op de ‘pas toe of leg uit’-lijst kan worden aangegeven dat het voldoen door overheidsinstellingen aan de baselines betekent dat ook wordt voldaan aan de NEN-ISO/IEC 27001 en 27002 standaarden.

De sectorale baselines hebben uitsluitend een relatie met de ISO 27002. Op de ‘pas toe of leg uit’-lijst kan dan ook slechts deze relatie nader toegelicht worden. Hierbij is het van belang om de verhouding tussen de ISO 27002 standaard en de sectorale baselines helder en eenduidig toe te lichten. Een voorstel hiervoor is opgenomen in bijlage A van dit rapport.

Te hanteren principes bij inkoop
Geadviseerd wordt om de volgende principes te hanteren en deze ook als zodanig te communiceren naar inkopers en leveranciers:

- Overheidsinstellingen zijn zowel gebonden aan een adequate implementatie en toepassing van de sectorale baselines als aan het gebruik van relevante standaarden, waaronder NEN/ISO 27001 en 27002, van de 'pas toe of leg uit'-lijst.
- In geval van aanbesteding van ICT-producten, stelt de overheidsinstelling de volgende eisen aan haar leverancier:
    - Te voldoen aan het informatiebeveiligingsbeleid van de overheidsinstelling. De informatiebeveiliging moet zowel organisatorisch als technisch op een adequaat niveau zijn.
    - Leveranciers voldoen als zodanig niet aan de baselines, maar dienen daarentegen te voldoen aan ISO/IEC 27001 en de maatregelen uit de 27002 standaard. Dit conform de 'pas toe of leg uit'-lijst.
    - Additioneel kunnen aanvullende geformuleerde beveiligingseisen worden geëist. Deze additionele beveiligingseisen die voor de dienst of het betreffende systeem van belang zijn kunnen zijn afgeleid van de desbetreffende baseline.

    - Het voldoen aan de ISO/IEC 27001 en 27002 standaarden kan wanneer nodig worden aangetoond door een relevant 27001 of gelijkwaardig certificaat te overleggen, inclusief een toelichting op de getroffen beveiligingsmaatregelen conform de 27002 standaard.
      Aanvullende zou gevraagd kunnen worden naar ten minste één referentie uit de afgelopen X jaar waarin de leverancier aantoont ervaring te hebben met informatiebeveiligingsmaatregelen van ISO 27002 of daaraan gelijkwaardig.
    - De woorden 'of gelijkwaardig' dienen te worden vermeld. Dit betekent dat door aanbieders aangedragen alternatieve oplossingen die aan de specificaties voldoen niet mogen worden afgewezen. In de context van deze selectie-eis worden de baselines als gelijkwaardig aan ISO 27002:2005 beschouwd. Dit geldt ook voor de ISO 27002:2013 als opvolger van de ISO 27002:2005 standaard, ondanks dat deze niet op de 'pas toe of leg uit'-lijst staat.
- Op basis van het aangeleverde certificaat [5], door de leverancier, stelt de overheidsinstelling vast of de scope van het certificaat overeenkomt met de af te nemen ICT-producten en of de onderbouwing van de getroffen beveiligingsmaatregelen voldoende zekerheid biedt.
- Hiermee geeft de overheidsinstelling zichzelf zekerheid over de mate waarin de leverancier in control is van de uitgevoerde beveiligingsmaatregelen.
- Het kan gezien de marktsituatie te zwaar zijn om van alle gegadigden volledige certificatie te vragen. Een en ander is tevens afhankelijk van de risico-inschatting van de gegevensverwerking en de aard van de dienstverlening.

5 Daarnaast is het van belang dat de overheidsinstelling vaststelt of het certificaat is voorzien van een legitiem logo van de Raad van Accreditatie of een legitiem logo van een gelijkwaardige buitenlandse Accreditatie Instelling.

5 Conclusies en aanbevelingen

Dit hoofdstuk geeft een antwoord op de twee hoofdvragen:
1. Wat zijn de wijzigingen van de nieuwe NEN-ISO/IEC 27001 en 27002-standaarden (versie 2013) ten opzichte van de oude en wat is de impact hiervan op overheidsorganisaties, de Baselines Informatiebeveiliging en leveranciers?
2. Betekent dat het voldoen aan de Baselines Informatiebeveiliging door overheidsorganisaties ook dat wordt voldaan aan de NEN-ISO/IEC 27001 en 27002 standaarden?

Dit onderzoekt helpt het Forum bij het besluit of, en zo ja wanneer en hoe NEN-ISO/IEC 27001:2013 en 27002:2013 in procedure genomen moeten worden voor opname op 'pas toe of leg uit'-lijst. Daarnaast helpt het onderzoek de relatie tussen de nieuwe ISO-normen en de baselines informatiebeveiliging beter te duiden, met name ook in relatie tot inkoop bij leveranciers.

In dit verkennende onderzoek is enerzijds gekeken naar wat de versiewijziging betekent voor overheidsorganisaties en de 'pas toe of leg uit'-lijst. Anderzijds is gekeken naar de relatie van deze nieuwe ISO-normen met de baselines informatiebeveiliging en hoe dit is te verduidelijken in de 'pas toe of leg uit'-lijst.

5.1 Conclusies

In de voorafgaande drie hoofdstukken zijn de subvragen die centraal staan in dit verkennende onderzoek beantwoord. Op basis van het uitgevoerde onderzoek kunnen de volgende conclusies worden getrokken.

Met betrekking tot de nieuwe versies

1. Ondanks dat de structuur van de nieuwe NEN-ISO/IEC 27001 aanzienlijk is veranderd en er een aantal nieuwe eisen is toegevoegd, conflicteert de nieuwe 27001 standaard (2013) niet met de oude versie. De nieuwe NEN-ISO/IEC 27002 standaard omvat een aantal nieuwe hoofdstukken en bestaande maatregelen zijn geüpdatet naar de huidige stand der techniek. Een verbetering van de nieuwe versie is dat het rekening houdt met de context van een organisatie. Hierdoor zijn de normen niet alleen intern, maar juist gericht op informatiebeveiliging over de organisatiegrenzen heen.

2. De onderzoeksgroep schat in dat wanneer overheidsinstellingen de oude 27001 en 27002 standaarden hebben geimplementeerd, het met beperkte inspanning en middelen mogelijk moet zijn de nieuwe standaarden te implementeren.

3. Daarnaast is vastgesteld dat veel overheidsinstellingen zijn gefocust op het implementeren van de sectorale baselines informatiebeveiliging en zich in beperkte mate richten op de implementatie van de 27001 en 27002 standaarden.

   Inkoopafdelingen van overheidsinstellingen vragen op dit moment veelal, onder verwijzing naar 'pas toe of leg uit'-lijst, de 27001 en 27002 standaarden uit bij hun leveranciers bij de aanschaf of (ver)bouw van ICT-systemen/-diensten.

4. Certificeren tegen de oude ISO-norm is niet meer mogelijk en oude 27001 certificaten zijn uiterlijk geldig tot 1 oktober 2015, dit is afhankelijk van het moment van certificering. (Her)certificering door organisaties, overheidsinstellingen en leveranciers, kan alleen nog tegen de nieuwe NEN-ISO/IEC 27001:2013 norm. Vanaf 1 oktober 2015 kunnen organisaties uitsluitend over certificaten op basis van de NEN-ISO/IEC 27001:2013 beschikken aangezien per die datum de ISO27001:2005 certificaten hun geldigheid verliezen.

5. In het geval van aanbestedingen die onder het regime van de 'pas toe of leg uit'-lijst vallen is het aan te raden dat de inkoopafdeling gedurende de transititieperiode vraagt naar het ISO 27001 certificaat (of gelijkwaardig) en in de beoordeling rekening houdt met het feit dat de certificering gebaseerd kan zijn op de oude of de nieuwe norm. In het geval het een certificering betreft op de oude 27001 norm is het aan te bevelen om aan de leverancier te vragen of en op welke termijn hij verwacht te voldoen aan de nieuwe 27001 certificering.

6. Om de nieuwe versie te kunnen uit vragen is het echter nodig dat de oude ISO-normen op de 'pas toe of leg uit'-lijst worden aangepast met de nieuwe 2013 normen.

Met betrekking tot de relatie tussen de Baselines en de lijst

Door het implementeren van de baselines hoeven overheidsorganisatie niet alsnog te voldoen aan de ISO27002 standaard. De baselines informatiebeveiliging zijn namelijk een nadere uitwerking van ISO27002/2005.
Dit gaat niet op voor ISO27001 en overheidsorganisaties zouden dan ook nadrukkelijker aandacht moeten besteden aan de beveiligingsprincipes omtrent het managementsysteem van informatiebeveiliging.

Op de 'pas toe of leg uit'-lijst zal de relatie tussen de ISO 27002 standaard en de sectorale baselines moeten worden toegelicht. Uitgangspunt is dat aan leveranciers wordt gevraagd te voldoen aan de ISO27001 norm voor het informatiebeveiligingsmanagement en zich afhankelijk van de gewenste zekerheid ook laat certificeren. Voor concrete beveiligingsmaatregelen dient naar de ISO27002 norm of gelijkwaardig te worden gevraagd. Additioneel kunnen door een overheidsorganisatie aanvullend geformuleerde beveiligingseisen worden geëist. Deze additionele beveiligingseisen kunnen zijn afgeleid van het in de organisatie geldende informatiebeveiligingsbeleid gebaseerd op de desbetreffende baseline.

5.2 Advies

Op basis van bovenstaande conclusies, wordt het volgende advies aan het Forum Standaardisatie gegeven.

1. De nieuwe versie en de toetsingsprocedure

In ogenschouw nemende dat:

- De geldigheid van geaudite certificaten van de oude 27001 norm uiterlijk per 1 oktober 2015 verlopen;
- De doorlooptijd van de toetsingsprocedure minimaal 6 maanden is;
- De nieuwe versie 2013 een verbetering zijn, onder andere met betrekking tot de context van een organisatie;
- De nieuwe 2013 versie voortbouwt op de oude versie en de nieuwe versie niet strijdig is met de baselines.

Is het advies om per direct de nieuwe versies van de standaarden in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst.

Om te voorkomen dat de toetsingsprocedure van de nieuwe 27001 en 27002 standaarden, de adoptie van de sectorale baselines informatiebeveiliging belemmert, is het belangrijk om een onderscheid te maken tussen de baselines, de nieuwe ISO-normen en de implementatie van dezen. Het is dus van belang om de communicatie rondom de procedure af te stemmen met belanghebbenden, zoals de Werkgroep Normatiek. Bij het updaten van de diverse baselines is het advies deze in lijn te brengen met de 2013 versie van 27001 en 27002.

2. De normen, de Baselines en de 'pas toe of leg uit'-lijst

Het is belangrijk dat er voor overheidsinstellingen en leveranciers een aanvullende toelichting komt op de 'pas toe of leg uit'-lijst hoe met de verschillende baselines en ISO standaarden dient te worden omgegaan.

Voor overheidsorganisatie:

- 1. Schenk meer nadrukkelijk aandacht aan de implementatie van de beveiligingsprincipes omtrent het managementsysteem van informatiebeveiliging zoals is vastgelegd in NEN-ISO/IEC 27001 norm (of gelijkwaardig) en het Voorschrift Informatiebeveiliging Rijksdienst (VIR).
- 2. Implementeer de beveiligingsmaatregelen zoals vastgelegd in het informatiebeveiligingsbeleid van de overheidsorganisatie.
- 3. Deze beveiligingsmaatregelen dienen gebaseerd te zijn op de eigen sectorale baseline. Deze baselines zijn een invulling van de NEN-ISO/IEC 27002 norm. Door implementatie van de baselines wordt ook voldaan aan de adoptie van deze norm.

Voor leveranciers:

- 1. Voldoe aan de NEN-ISO/IEC 27001 norm en laat hierop een certificering uitvoeren.
- 2. Implementeer beveiligingsmaatregelen, hierbij dient de 27002 norm (of gelijkwaardig) als referentie.
- 3. Aanvullend kunnen er beveiligingsmaatregelen worden geëist door overheidsorganisatie. Deze aanvullende maatregelen zijn beschreven in hun informatiebeveiligingsbeleid die zijn gebaseerd op de baselines.

Het Forum Standaardisatie wordt geadviseerd om aan de conclusie uit het onderzoek en bovenstaande opsomming nader invulling te geven op de 'pas toe of leg uit'-lijst. Daarbij is het van belang om de exacte teksten af te stemmen met de diverse vertegenwoordigers van de sectorale baselines en de Werkgroep Normatiek.

6 Referenties

1. NEN-ISO/IEC 27001 (nl) Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen, 2005
2. NEN-ISO/IEC 27002 (nl) Informatietechnologie – Beveiligingstechnieken – Code voor informatiebeveiliging, 2007
3. NEN-ISO/IEC 27001 (nl) Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen, 2013
4. NEN-ISO/IEC 27002 (nl) Informatietechnologie – Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging, 2013
5. Baseline Informatiebeveiliging Rijksdienst (BIR), Tactisch normenkader, versie 1.0, 2012;
6. Baseline Informatiebeveiliging Rijksdienst (BIR), Operationele Handreiking, versie 1.0, 2013;
7. Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), Strategisch en Tactisch normenkader, 2013;
8. Baseline Informatiebeveiliging Waterschappen (BIWA), Strategisch en Tactisch normenkader, WS versie 1.0, 2013;
9. Interprovinciale Baseline Informatiebeveiliging (IBI), versie 1.0, 2010.
10. "ISO 27001-2013 Transition Guide", November 2013, Henk Keijzer DEKRA
11. "ISO27001 Herzien", InformatieBeveiliging Magazine, Ernst Oud
12. http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/
13. http://www.gammassl.co.uk/27001/revision.php
14. http://www.gammassl.co.uk/27001/27002ControlMap.html
15. "Revision ISO-IEC 27002", Nieuwe versie ISO/IEC 27002, Code of practice for information security controls, 24 september 2013, Frank Fransen, TNO
16. http://www.informationshield.com/papers/ISO27002-2013%20Version%20Change%20Summary.pdf

Bijlage A – Standaarden en Baselines

Introductie

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. Het uitgevoerde onderzoek spitst zich toe op deze Nederlandse versies van de standaarden. Daarnaast is ook gekeken naar de relatie van de standaarden met de verschillende sectorale baselines informatiebeveiliging.

In deze bijlage zijn de volgende standaarden en sectorale baselines beschreven:
a. NEN-ISO/IEC 27001:2013;
b. NEN-ISO/IEC 27002:2013;
c. Baseline Informatiebeveiliging Rijksdienst (BIR);
d. Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
e. Baseline Informatiebeveiliging Waterschappen (BIWA);
f. Interprovinciale Baseline Informatiebeveiliging (IBI);
g. Voorschrift Informatiebeveiliging Rijksdienst (VIR).

Standaarden

a. NEN-ISO/IEC 27001:2013
NEN-ISO/IEC 27001:2013 specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het een 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. Tegen deze norm 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.

b. NEN-ISO/IEC 27002:2013

De NEN-ISO 27002:2013 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).

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.

In het kader van de verschillen tussen de oude (2005 en 2007) en nieuwe versies (2013) is het van belang te weten dat beide versies niet door elkaar gebruikt kunnen worden. Het is dus niet mogelijk van NEN-ISO/IEC 27001 de 2005 versie te gebruiken en van NEN-ISO/IEC 27002 de 2013 versie en vice versa. Dit in verband met de gewijzigde structuur en het aantal maatregelen van de standaarden.

Verhouding ISO standaarden tot de sectorale baselines

De ISO 27001 standaard eist (paragraaf 6.1.3) dat beveiligingsmaatregelen (controls) moeten worden vastgesteld die nodig zijn om de geïdentificeerde beveiligingsrisico's (paragraaf 6.1.2) af te dekken.

De ISO 27001 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 een overheidsorganisatie kan kiezen voor het ontwerp van de noodzakelijke beveiligingsmaatregelen uit onder meer de desbetreffende sectorale baseline of hiervoor de beveiligingsmaatregelen uit de ISO 27002 te nemen.

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 27001 standaard Annex A. Hiervoor is het gebruikelijk om een verklaring van toepasselijkheid op te stellen.

Sectorale Baselines Informatiebeveiliging

Een baseline informatiebeveiliging is een instrument waarmee bestuur en management in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatieveiligheid. Er wordt zo een indruk opgedaan of informatieveiligheid als zodanig aantoonbaar beheerst wordt tot op een niveau dat van de organisatie verwacht mag worden.

De diverse overheidslagen hebben een eigen, sectorale, baseline informatiebeveiliging ontwikkeld:
- Rijksoverheid, de Baseline Informatiebeveiliging Rijksdienst (BIR);
- Gemeenten, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG);
- Waterschappen, de Baseline Informatiebeveiliging Waterschappen (BIWA);
- Provinciën, de Interprovinciale Baseline Informatiebeveiliging (IBI).

De sectorale baselines hebben geen relatie met de oud of nieuwe versie van de ISO 27001. Er is alleen een relatie tussen de sectorale baselines en ISO 27002.

Deze baselines zijn gebaseerd op de (oude) NEN-ISO/IEC 27002:2007 standaard en bevatten verder uitgewerkte maatregelen. Deze aanvullende beveiligingsmaatregelen die gelden voor de betreffende overheidslaag, zijn in deze baselines gemerkt. In de BIR zijn specifieke rijksnormen bijvoorbeeld gemerkt met een [R].

Voor alle sectorale baselines geldt dat zij geheel gestructureerd zijn volgens NEN-ISO/IEC 27002. Dit houdt in dat de structuur van de sectorale baselines in lijn is met de beheersdoelstellingen en beheersmaatregelen van NEN-ISO/IEC 27002.
Echter, de eisen zoals benoemd binnen NEN-ISO/IEC 27001, het managementsystemen voor informatiebeveiliging, is onderbelicht binnen de baselines. Dit vergroot de kans dat bij het voldoen aan de diverse baselines de focus uitsluitend ligt op de implementatie van de beveiligingsmaatregelen en dat er onvoldoende aandacht is voor de implementatie van het managementsysteem voor informatiebeveiliging.

c. <u>Baseline Informatiebeveiliging Rijksdienst</u>
De Baseline Informatiebeveiliging Rijksdienst (BIR) is een toepassingshandleiding van NEN-ISO/IEC 27001 en 27002 voor de rijksoverheid.

De BIR:2012 bestaat uit een Tactisch Normenkader (TNK) [6] en een Operationele Handreiking (OH) [7].
De baseline beschrijft de aanvullingen op NEN-ISO/IEC 27001 en 27002 voor de overheid. In de Tactische Baseline zijn die aanvullingen gemerkt met een [R]. Het tactisch normenkader is verplicht ('comply or explain'). De operationele handreiking is niet verplicht en bestaat uit voorbeelden, "best practices". Het volgen van deze best practices leidt wel tot een goede manier van invullen van de BIR TNK.

De BIR refereert en beschrijft zeer beperkt het managementsysteem voor informatiebeveiliging, zoals dat in ISO 27001 is beschreven.

6 http://www.wikixl.nl/wiki/ear/images/ear/6/6f/BIR_TNK_1_0_definitief.pdf
7 http://www.wikixl.nl/wiki/ear/images/ear/5/5c/BIR_Operationele_Handreiking_v1_0.pdf

d. Baseline Informatiebeveiliging Nederlandse Gemeenten

De integrale Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) bestaat uit twee delen, een strategische baseline en een tactische baseline. De Strategische Baseline [8] beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline [9] beschrijft aan de hand van dezelfde indeling als de beveiligingsnorm NEN-ISO/IEC 27002:2007 de controls/maatregelen die als baseline gelden voor de gemeenten.

Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn diverse producten ontwikkeld op operationeel niveau.

De BIG refereert en beschrijft zeer beperkt het managementsysteem voor informatiebeveiliging, zoals dat in NEN-ISO/IEC 27001 is beschreven.

e. Baseline Informatiebeveiliging Waterschappen

De Baseline Informatiebeveiliging Waterschappen (BIWA) [10] bestaat uit twee delen, een strategische baseline en een tactische baseline en is gebaseerd en afgestemd op de baselines van de gemeenten (BIG) en het Rijk (BIR). Het eerste deel is een strategisch normenkader en het tweede deel een tactisch normenkader.

De BIWA is gebaseerd op de NEN-ISO/IEC 27001 en 27002 en is opgebouwd rondom deze normen. In het tactisch normenkader worden de maatregelen uit de NEN-ISO/IEC 27002 gebruikt en is de hoofdstukindeling gelijk.

De BIWA refereert en beschrijft zeer beperkt het managementsysteem voor informatiebeveiliging, zoals dat in NEN-ISO/IEC 27001 is beschreven.

f. Interprovinciale Baseline Informatiebeveiliging

De inhoud van de Interprovinciale Baseline Informatiebeveiliging (IBI) [11] is gebaseerd op de NEN-ISO/IEC 27001:2005 en NEN-ISO/IEC 27002:2007 en is aangepast voor gebruik door de provincies.

Voor gebruik door de provincies zijn de volgende aanpassingen gedaan:

- Sommige maatregelen uit de NEN-ISO/IEC 27002 standaard zijn niet van toepassing voor de provincies: deze zijn weggelaten in de Interprovinciale Baseline Informatiebeveiliging.
- Andere maatregelen uit de NEN-ISO/IEC 27002 standaard zijn onveranderd van toepassing voor de provincies: naar de betreffende passage in de standaard wordt verwezen vanuit de Interprovinciale Baseline Informatiebeveiliging.
- Weer andere maatregelen uit de NEN-ISO/IEC 27002 standaard zijn niet geheel of anders van toepassing op de provincies: de aanpassing is vermeld in de Interprovinciale Baseline Informatiebeveiliging.
- Niet elke maatregel is altijd van toepassing, maar slechts bij of vanaf een bepaald beveiligingsniveau. Het bijbehorende beveiligingsniveau is vermeld in de Interprovinciale Baseline Informatiebeveiliging.

8 https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-0506-Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.0.pdf

9 https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-0506-Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.0.pdf

10 http://www.uvw.nl/index.php?laatste-nieuws&newsdetail=20131001-1_baseline-informatiebeveiliging-waterschappen

11 http://www.ipo.nl/files/7013/5722/9178/interprovinciale_baseline_informatiebeveiliging_v1_0_2010-09_definitief.pdf

Daarnaast is gebruik gemaakt van de zogenaamde NORA aanpak (best practices) [12].

De IBI refereert en beschrijft zeer beperkt het managementsysteem voor informatiebeveiliging, zoals dat in NEN-ISO/IEC 27001 is beschreven.

g. Voorschrift Informatiebeveiliging Rijksdienst

De huidige baselines zijn allen gebaseerd en in lijn met de oude NEN-ISO/IEC 27002:2007 standaard. In deze baselines zijn de eisen zoals beschreven in de ISO/IEC 27001:2005 onderbelicht. De 2007 versie van het Voorschrift Informatiebeveiliging Rijksdienst (VIR), welke uitsluitend van toepassing is op overheidsinstellingen, is het enige document dat slechts een beperkt aantal eisen stelt aan het ontwerpen, implementeren en continue verbeteren van beveiligingsmaatregelen middels een managementsysteem, zoals beschreven in de NEN-ISO/IEC 27001:2005.

Het VIR:2007 benoemt de noodzaak van een informatiebeveiligingsbeleid en de verantwoordelijkheden van het lijnmanagement. Het VIR is een doelstellende regeling, die veel overlaat aan de verantwoordelijke overheidsinstelling. De regeling stelt minimumeisen aan het te ontwikkelen informatiebeveiligingsbeleid. Daarnaast worden eisen gesteld aan het stelsel van maatregelen dat dit beleid in de praktijk moet brengen.

12 http://www.noraonline.nl/wiki/Beveiliging

Bijlage B – Betrokkenen uit onderzoeksgroep

Aan de onderzoeksgroep hebben deelgenomen:

1. Jan Rietveld (Nederlandse Normalisatie-instituut)
2. Michiel Oosterwijk (National Cyber Security Centrum)
3. Carl Adamse (Directoraat-Generaal Organisatie en Bedrijfsvoering Rijk (DGOBR), Ministerie van Binnenlandse Zaken en Koninkrijkrelaties)
4. Tony van der Togt (TGBI, Ministerie van Binnenlandse Zaken en Koninkrijkrelaties)
5. Kees Hintzbergen (Informatiebeveiligingsdienst (IBD), KING)
6. Rene Terbijhe (Provincie Flevoland)
7. Marianne Krug (Unie van Waterschappen)
8. Freddie Muller (Het Waterschapshuis)
9. Peter van Dijk (Taskforce Bestuur en Informatieveiligheid Dienstverlening)
10. Alf Moens (SURFnet)
11. Olivier Tielen (Auditdienst Rijk)
12. Frank van Vonderen (Raad voor Accreditatie)
13. Peter van der Enden (eHerkenning)
14. Gert Maneschijn (Rijksdienst voor het Wegverkeer)
15. Bart Pegge (Nederland ICT)
16. Henk Keijzer (DEKRA)
17. Jaap van der Veen (NORA)
18. Renato Kuiper (NORA)