FS-20140204.03A

notitie

Forum Standaardisatie

Wilhelmina v Pruisenweg 52
2595 AN Den Haag
Postbus 96810
2509 EJ Den Haag
www.forumstandaardisatie.nl

Forum Standaardisatie

Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	04 februari 2014	**Versie**	1.0
Betreft:	Voorstel verwerking opmerkingen College Standaardisatie mbt bevordering adoptie ISO27001/27002		

I. Relevante passage verslag College (vergadering 28-11-2013)

4B - Advies adoptie normen voor informatiebeveiliging NEN-ISO 27001/2
Het College Standaardisatie stemt in met de adviespunten om de adoptie van de normen voor informatiebeveiliging NEN-ISO27001/27002 verder te bevorderen, met de aantekening dat ten aanzien van punt:

- 5. (drempelloos beschikbaar krijgen norm/baselines) wordt afgesproken dat BZK en EZ eerst samen een probleem analyse en aanpak uitwerken (actiepunt BZK/B&I en EZ);
- 9. (evalueren baselines en onderzoeken haalbaarheid harmonisatie baselines) wordt opgemerkt dat 2014 te vroeg is voor een evaluatie van de adoptie van baselines; daarnaast zou evaluatie via de desbetreffende koepelorganisaties plaats moeten vinden; punt wordt terugverwezen naar het Forum (actiepunt Forum);
- 10. (nieuwe versie NEN-ISO27001/2) wordt aangegeven dat een nieuwe versie van de norm brede impact heeft, bijvoorbeeld zowel op de Baselines, als op de vraag hoe om te gaan met de huidige versie staat op de past-toe-of-leg-uit lijst; dit punt wordt terugverwezen naar het Forum, zodat kan worden afgesproken hoe – en door wie – de bijbehorende acties worden opgepakt (actiepunt Forum).

II. Voorstel verwerking opmerkingen College tbv Forum

Ad 5. (drempelloos beschikbaar krijgen norm/baselines):

Oorspronkelijk advies:

College Standaardisatie roept BZK/DGBK/B&I i.s.m. Bureau Forum Standaardisatie op om namens de gehele overheid met NEN in gesprek te gaan over auteursrechten en kosten die een drempel vormen voor de verspreiding en kenbaarheid van NEN-ISO 27001/27002 en eventueel van de daarop gebaseerde Baselines Informatiebeveiliging;

Aangepast advies:

BZK/DGBK/B&I en EZ gaan namens de gehele overheid met NEN in gesprek over auteursrechten en kosten die een drempel vormen voor de verspreiding en kenbaarheid van NEN-ISO 27001/27002 en eventueel van de daarop gebaseerde Baselines Informatiebeveiliging. BFS zal hierbij op verzoek ondersteuning ('fact finding') bieden;

Eerste resultaten nadere 'fact finding':

- De overheid heeft zich via de 'pas toe of leg uit'-lijst maar ook politiek richting de Tweede Kamer gecommitteerd aan het toepassen van NEN-ISO27001/27002 en de daarop gebaseerde baselines.[1]
- Op de 'pas toe of leg uit'-lijst staan, naast NEN-ISO27001/27002, drie Nederlandstalige NEN-standaarden (NEN3610 als onderdeel Geo-standaarden, NTA 9040 ihkv Ondernemingsdossier, NTA 2035 ePortfolio). De drie bijbehorende specificatiedocumenten zijn kosteloos verkrijgbaar, omdat deze zijn afgekocht door respectievelijk Geonovum, EZ en Kennisnet.
- ISO27001/27002 zijn internationale normen. NEN publiceert een officiële Nederlandse vertaling die is opgenomen op de 'pas toe of leg uit'-lijst.
- In wet- en regelgeving wordt op verschillende plaatsen gerefereerd aan NEN-ISO27001/27002 (en aan de voorloper "Code voor Informatiebeveiliging").[2]
- NEN-ISO27001/27002 zijn niet kosteloos en vrij beschikbaar. De kosten voor beide normen bedragen EUR 510,-. Dit is conform het business model van NEN, dat op deze wijze de (auteurs)rechten op de normen exploiteert.[3]
- Alle overheidslagen hebben baselines informatiebeveiliging ontwikkeld die zijn gebaseerd op deze normen. Deze baselines zijn niet geheel vrij beschikbaar, omdat de rechten van NEN hieraan in de weg (lijken te) staan.
- Door expertgroep is aangegeven dat de kosten in de praktijk een drempel vormen voor de kenbaarheid van de normen en de baselines en daarmee ook voor de adoptie. Door Forum/College is dit onderschreven.

---

[1] *Zie: https://zoek.officielebekendmakingen.nl/kst-26643-275.html en https://zoek.officielebekendmakingen.nl/blg-193173.html*

[2] *Zie: http://wetten.overheid.nl/zoeken_op/regeling_type_wetten+AMVB+ministeries/tekst_bevat_27001/, http://wetten.overheid.nl/zoeken_op/regeling_type_wetten+AMVB+ministeries/tekst_bevat_27002/, http://wetten.overheid.nl/zoeken_op/regeling_type_wetten+AMVB+ministeries/tekst_bevat_%2522code%2Bvoor%2Binformatiebeveiliging%2522/*

[3] *Namelijk (€ 171,47 + € 249,40) x 1,21 = €509,25*
Zie: http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012005-nl.htm en http://www.nen.nl/NEN-shop/Norm/NENISOIEC-270022007-nl.htm

Ad 9. (evalueren baselines en onderzoeken haalbaarheid harmonisatie baselines):

Oorspronkelijk advies:

College Standaardisatie roept Taskforce BID en BZK/DGBK/B&I op om, in overleg met de baselinebeheerders en andere stakeholders, voor eind 2014 de adoptie van de Baselines te evalueren en de haalbaarheid te onderzoeken van harmonisatie van de verschillende Baselines Informatiebeveiliging (richting één Baseline Informatie Beveiliging Overheid);

Aangepast advies:

De baselinebeheerders (of te wel de koepels) evalueren, in overleg met BZK/DGBK/B&I, in 2015 de adoptie van de eigen Baselines en richten een gezaghebbende, duurzame dialoog in om de baselines, waar mogelijk, te harmoniseren en de onderlinge samenhang te borgen;

Ad 10. (nieuwe versie NEN-ISO27001/2):

Oorspronkelijk advies:

College Standaardisatie roept Taskforce BID en BZK/DGBK/B&I om voor eind 2014 de impact van de nieuwe versie van NEN-ISO 27001/27002 te bepalen en deze eventueel aan te melden voor opname op de 'pas toe of leg uit'-lijst bij Forum Standaardisatie.

Aangepast advies:

Forum Standaardisatie neemt (liefst na aanmelding door BZK/DGBK/B&I) voor eind 2014 de nieuwe versie van NEN-ISO 27001/27002 in behandeling voor opname op de 'pas toe of leg uit'-lijst en bepaalt met stakeholders de impact daarvan voor de diverse baselines, gebruikmakend van de hiervoor genoemde dialoog tussen de verschillende baselinebeheerders.

Eerste resultaten nadere 'fact finding':

- Uit navraag bij NEN is gebleken dat ISO27001-certificaten tegen de oude norm (die nu op 'pas toe of leg uit'-lijst staat) nog geldig zijn tot 1 oktober 2015. Daarnaast heeft het International Accreditation Forum (IAF) bepaald dat certificerende instellingen vanaf 1 oktober 2014 niet meer tegen de oude norm mogen auditen. Dat betekent dat in de loop van de periode tot 1 okt 2014 certificaten ge-upgrade KUNNEN worden en in de periode van 1 okt 2014 tot 1 okt 2015 de certificaten MOETEN worden ge-upgrade.