FS-20140617.03C

Forum Standaardisatie

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

notitie

FORUM STANDAARDISATI E

Bijlagen:	geen		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	5 juni 2014	**Versie**	1.0
Betreft:	onderzoek NEN-ISO/IEC 27001/27002		

Gevraagd besluit

Aan het Forum wordt gevraagd om in te stemmen met de in deze notitie geschetste onderzoeksaanpak en een inventariserend onderzoek te doen naar de volgende twee vragen.

1. W*at zijn de wijzigingen van de nieuwe NEN-ISO27001 en 27002-standaarden (versie 2013) ten opzichte van de oude en wat is de impact hiervan op overheidsorganisaties en de Baselines Informatiebeveiliging?*

2. *Betekent dat het voldoen aan de Baselines Informatiebeveiliging door overheidsorganisaties ook dat wordt voldaan aan de NEN-ISO27001/2 standaarden?*

Op basis hiervan kan het Forum Standaardisatie besluiten hoe met de nieuwe versie van de NEN-ISO27001/2 standaarden en de Baselines Informatiebeveiliging om te gaan in relatie tot de 'pas toe of leg uit'-lijst en zo nodig aanvullend onderzoek en/of acties te bepalen.

Doel van het onderzoek
Oktober 2013 zijn de standaarden NEN-ISO/IEC 27001:2013 en 27002:2013 gepubliceerd. Deze standaarden zijn een update van NEN-ISO/IEC 27001:2005 en 27002:2007, die op de 'pas toe of leg uit'-lijst staan. De Baselines Informatiebeveiliging, die belangrijk zijn voor de adoptie van 27001/2 standaard, zijn op deze oude normen gebaseerd.

In een verkennend onderzoek willen wij kijken naar wat deze versiewijziging betekent voor de overheid en daarmee voor de 'pas toe of leg uit'-lijst. Centraal staat de vraag: wat zijn wijzigingen van de nieuwe 27001/2 versie ten opzichte van de oude en wat is de impact hiervan op de Baselines Informatiebeveiliging? Op basis van het onderzoek kan worden beoordeeld of het nodig is om de nieuwe versies in te dienen voor de toetsingsprocedure en op welk termijn.

Datum
5 juni 2014

Het tweede deel van het verkennend onderzoek gaat in op de vraag of de Baselines Informatiebeveiliging volledig in lijn zijn met de NEN-ISO27001/2 standaarden. Het doel hiervan is om op de 'pas toe of leg uit'- lijst aan te geven dat het voldoen aan de baselines ook het voldoen aan de ISO27001/2 standaard betekent. Als zodanig kan dit dan ook worden meegenomen in de adoptiemonitor. Dit betekent dus niet dat de baselines als losse standaard opgenomen worden op de lijst.

Op basis van het onderzoek kan het Forum Standaardisatie besluiten hoe met de nieuwe versies van NEN-ISO27001/2 en n de Baselines Informatiebeveiliging om te gaan in relatie tot de 'pas toe of leg uit'-lijst en zo nodig aanvullend onderzoek en/of acties te bepalen. Het onderzoek zal worden uitgevoerd in samenspraak met de beheerders van deze baselines.

Vraagstelling
De hoofdvragen bestaat uit twee onderdelen:
1. W*at zijn de wijzigingen van de nieuwe NEN-ISO27001 en 27002-standaarden (versie 2013) ten opzichte van de oude en wat is de impact hiervan op overheidsorganisaties en de Baselines Informatiebeveiliging?*

Deze vraag kan worden onderverdeeld in de volgende subvragen:
- Wat zijn op hoofdlijnen de verschillen tussen de oude en de nieuwe versie van de 27001 en 27002-standaarden?
- 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?
- Wat is de impact van deze wijzigingen voor overheidsorganisaties, de Baselines Informatiebeveiliging en leveranciers?
- In hoeverre zijn overheidsorganisaties bezig zijn met implementatie van de 2013 versies en wat zijn hun plannen hieromtrent?
- Wat moeten (gebruikers)organisaties en leveranciers extra uitvoeren om conform de nieuwe 27001 en 27002-standaarden te werken?

2. *Betekent dat het voldoen aan de Baselines Informatiebeveiliging door overheidsorganisaties ook dat wordt voldaan aan de NEN-ISO27001/2 standaarden?*

Deze vraag kan worden onderverdeeld in de volgende subvragen:
- Zijn de Baselines Informatiebeveiliging (BIR, BIG, IBI en BIWa) in lijn met de NEN-ISO27001/2 standaarden?
- Hoe kan op de 'pas toe of leg uit'-lijst op een inzichtelijke wijze worden aangegeven dat het voldoen aan de baselines betekent dat ook wordt voldaan aan de INENSO27001/2 standaard?

<u>Onderzoeksaanpak</u>
Het onderzoek zal worden gedaan aan de hand van (telefonische) interviews met de hieronder genoemde partijen. Aan de hand van deze interviews zal een rapport worden opgesteld waarin bovenstaande onderzoeksvragen worden beantwoord. Dit document wordt eenmalig per e-mail ter review voorgelegd aan de betrokken partijen. Op- en aanmerkingen zullen, waar nodig, worden verwerkt, waarna het document in het Forum wordt voorgelegd.

Bij het onderzoek worden in ieder geval de volgende organisaties betrokken:
- NEN
- NCSC
- Baselinebeheerders BZK/DGOBR, KING/IBD, IPO, UvW
- Taskforce BID

- SURFnet
- BZK/DGBK/B&I
- CPB
- Auditors (ADR, Raad voor Accreditatie etc.)
- (Gecertificeerde) gebruikers (eHerkenning, RDW etc.)
- Leverancierorganisaties

Resultaat
Het resultaat van deze opdracht is één document (advies), waarin bovengenoemde onderzoeksvragen worden beantwoord. Op basis hiervan kan het Forum besluiten hoe met de nieuwe versie van de NEN-ISO27001/2 en Baselines Informatiebeveiliging om te gaan. Een volgende stap kan bijvoorbeeld zijn om de nieuwe versie van de standaard in procedure te nemen of besluiten dat dit vooralsnog niet nodig is. Het inventariserend onderzoek dient uiterlijk 16 september 2014 gereed te zijn.