Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

Aan:	Forum Standaardisatie		
Van:	Bureau Forum Standaardisatie		
Datum:	26-03-2015	**Versie**	1.0
Betreft:	Overzicht reacties openbare consultatieronde NEN-ISO/IEC 27001 en 27002		
Bijlagen:	1. Reactie DHPA 2. Reactie CROW 3. Reactie DICTU 4. Reactie DUO, Kennisnet en ministerie van OCW 5. Reactie Kamer van Koophandel		

1. Reactie DHPA

Datum
24-03-2015

Van: Michiel Steltman
Verzonden: maandag 16 maart 2015 22:53
Aan: Schellevis, H.L. (Lancelot) - Logius
Onderwerp: RE: Openbare consultatie NEN-ISO/IEC 27001/2:2013

Beste Lancelot,
In verband met vakanties is onze reactie enigszins in het gedrang gekomen. De tijd ontbreekt om in detail te onderzoeken hoe de consultatie moet worden vormgegeven in de begeleidende documenten.
Op de adviezen DMARC/SPF, SKOS en digikoppeling hebben we geen feedback ; aam DMARC hebben we zelf als DHPA inhoudelijk meegewerkt en het expertadvies heeft onze volledige instemming.
Iets anders ligt dat met de ISO27001, daar zijn enkele kanttekingen te plaatsen. we hebben als leidraad het consultatiedocument
gebruikt: https://www.forumstandaardisatie.nl/fileadmin/os/Consultatiedocumenten/Consultatiedocument_ISO_27001_en_27002_-_v1.0.docx

Ik geef je hier onze ruwe feedback op het expert advies, laat me weten of dat werkbaar is; zoniet dan improviseren we nog iets in de komen de dagen.

Mbt 3.4 bullet 2:
Het functioneel toepassingsgebied spreekt over het ISMS, governance en leveranciersmanagement, die scope is juist. Maar het noemen van technische beveiligingsmaatregelen in deze context verdient een nadere toelichting. Bij het gestelde functionele toepassingsgebied zou de indruk kunnen ontstaan dat een organisatie die in het kader van de ISO een generieke set van technische beveiligingsmaatregelen voorschrijft of implementeert, een afdoende beveiliging organiseert voor alle systemen en leveranciers onder haar regie. Wij stellen daarom voor om e tekst over “technische beveiligingsmaatregelen” te schrappen, en te noemen dat de organisatie beleid dient vast te stellen vaststelt waarmee per “systeem“ en/of per leverancier de juiste technische maatregelen worden vereist.

Tevens schiet naar onze mening het slechts noemen van “de leverancier” tekort. In de complexe werkelijkheid van met name online IT, is er vrijwel altijd sprake van meerdere leveranciers, en van technische of functionele ketens. De keten is net zo zwak als de zwakste schakel. Het borgen van informatieveiligheid in technisch complexe ketens wordt (nog) slechts ten dele door de ISO standaards geadresseerd. Aanvullend beleid is daarom vereist om te borgen dat governance van informatieveiligheid voor de gehele keten daadwerkelijk wordt geregeld.
Ter illustratie: in de keten van levering van PKI overheidscertificaten waren naast diginotar zelf meerdere partijen betrokken (hoster, datacenter, diginotar zelf, domein registrant/DNS provider) en niet zichtbaar en bekend was in hoeverre al deze organisaties een ISMS c.q. een ISO2700x framework hadden en gebruikten.
Wij stellen voor om hier te noemen dat, in aanvulling op de ISO, het ISMS (van de organisatie die het betreft) moet voorzien in het aantonen van governance en control voor alle leveranciers in de technische keten. Dat geldt met name voor de leveranciers die niet als onderaannemer / onder directe regie van de organisatie werken, maar leveranciers die een autonome dienstverlening inbrengen in de leveringsketen (voorbeeld: een hoster of co-locatie provider).

Met Vriendelijke Groet,
Michiel Steltman | Directeur
Dutch Hosting Provider Association

2. Reactie CROW

Datum
24-03-2015

Van: Jansen, P.Ph. [mailto:[/]]
Verzonden: dinsdag 10 maart 2015 12:08
Aan: Forum standaardisatie
Onderwerp: RE: Openbare consultatie Digikoppeling, DMARC, SKOS en ISO27001/2

Geacht Forum c.s.,
De openbare consultatie over de onderstaande standaarden is jl. vrijdag besproken in de VISI Technische Commissie. Namens de TC wil ik de volgende reactie aangeven op alle vier de standaarden tegelijk.
(het is wellicht een beetje met een 'vormfout' omdat ik niet het consultatiedocument gebruik, met mijn excuses daarvoor, maar ik vertrouw erop dat het commentaar niettemin serieus wordt genomen)
De TC acht het hoogstwaarschijnlijk dat de onderstaande standaarden (grote) raakvlakken of zelfs overlap hebben met de VISI Open Standaard. De TC vindt het belangrijk dat wordt nagegaan in hoeverre die raakvlakken/overlap bestaan. Wij denken dat Forum dat zou moeten initiëren. De TC wil vervolgens zelf ook wel energie steken in een eventuele afstemming of harmonisatie.
Aan Forum wordt ook gevraagd om na te (doen) gaan of en in hoeverre de beheerders van onderstaande standaarden VISI wellicht zouden kunnen adopteren in hun standaard. VISI is weliswaar ontwikkeld vanuit de bouw, maar niets staat in de weg om VISI ook in andere sectoren/industrieën te gebruiken.
Ten slotte vraagt de TC zich af of de nieuwe Digicommissaris een rol zou kunnen (misschien wel moeten?) spelen in de eventuele afstemming van al deze standaarden. In de TC is afgesproken dat de voorzitter, dr. Hans Mulder, dit zal aankaarten dat bij Bas Eenhoorn. De suggestie van de TC is dat Forum dat van haar kant ook doet. Dan wordt dit hopelijk met succes vervolgd.
Met vriendelijke groet,

namens de VISI Technische Commissie

Paul Jansen
projectmanager

3. Reactie DICTU

Datum
24-03-2015

From: "Kreeft, S.F. van der (Friso)" <[/]>
To: "
Date: Tue, 24 Feb 2015 16:21:17 +0100
Subject: RE: openbare consultatie standaarden

Richard,

De ISO2700x onderbouwing heb ik bekeken en besproken met IB (Koos van Rijs).
Hierop hebben wij geen aanvullend commentaar of bezwaar.

DMARC heb ik bekeken en besproken met IB (Alex Caljouw).
Hierop hebben wij geen aanvullend commentaar of bezwaar.

4. Reactie DUO

Datum
24-03-2015

Van: Groot Roessink, Gerald
Verzonden: donderdag 12 maart 2015 20:32
Aan: Forum standaardisatie
Onderwerp: 'Consultatieprocedure NEN-ISO/IEC 27001:2013 en 27002:

Dag,
Hierbij na sectorale afstemming de reactie van het onderwijs
Groet
Gerald Groot Roessink
Dienst Uitvoering Onderwijs

Vraag 2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied? [paragraaf 2.2 van het expertadvies]?

➔ Reactie DUO/Kennisnet/OCW

"Governance" nergens goed gedefinieerd en is het een term met diverse betekenissen in diverse contexten. Ook gaat het niet alleen om Informatiebeveiliging "binnen" de organisatie maar juist ook tussen of buiten de organisatie in relatie tot ketens of netwerken.

Vraag 4. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]?

➔ Reactie DUO/Kennisnet/OCW
Versie 2013 is een verbetering ten opzichte van de huidige versies van 10 respectievelijk 8 jaar oud. Deze versie bevat betere handvatten voor ketens of netwerken. Onder meer door aandacht in de risico-analyse voor van externe stakeholders en ketenpartners. Het is zinvol dat alle organisaties synchroon lopen. Een algehele verplichting is extra zinvol.

Vraag 9. Bent u het eens met de adoptie-aanbevelingen van de expertgroep aan het Nationaal Beraad Digitale Overheid? [paragraaf 3.5 van het expertadvies]?

➔ Reactie DUO/Kennisnet/OCW
Bij tweede en derde bullit:
1. Hierin graag meenemen de baseline voor onderwijsinstellingen beschreven in het ROSA katern Privacy en Security (P&S).
2. Deze baselines werken feitelijk als een collectieve leg-uit. Zolang deze standaard niet is overgenomen door een baseline is het acceptabel dat de betrokken organisaties er geen gebruik van maken. Dat vergt niet alleen bewaking door een werkgroep Normatiek, maar ook een agenda.

5. Reactie Kamer van Koophandel

Datum
24-03-2015

Van: Rob Spoelstra
Verzonden: vrijdag 13 maart 2015 14:21
Aan: Forum standaardisatie
Onderwerp: Consultatiedocument_ISO_27001_en_27002 met antwoorden KvK.docx

Hallo,
Hierbij onze reactie op de nieuwe versie van de ISO27001/2 standaard.
Groeten,
Rob Spoelstra

1. Zijn er volgens u in deze toelichting aanvullingen of anderszins wijzigingen nodig in paragraaf 1.5 (‘samenstelling expertgroep’) bezien vanuit het doel van het document (het Forum en Nationaal Beraad Digitale Overheid voorzien van een inhoudelijk relevante toelichting)?
Antwoord: Nee

2. Bent u het eens met het door de expertgroep geadviseerde functionele toepassingsgebied? [paragraaf 2.2 van het expertadvies]?
Antwoord: Ja

3. Bent u het eens met het door de expertgroep geadviseerde organisatorische werkingsgebied? [paragraaf 2.3 van het expertadvies]?
Antwoord: Ja

4. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de toegevoegde waarde? [paragraaf 3.1 van het expertadvies]?
Antwoord: Ja

5. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het open standaardisatieproces? [paragraaf 3.2 van het expertadvies]?
Antwoord: Ja

6. Bent u het eens met de constateringen en conclusies van de expertgroep inzake het draagvlak? [paragraaf 3.3 van het expertadvies]?
Antwoord: Ja

7. Bent u het eens met de constateringen en conclusies van de expertgroep inzake de bevordering van de adoptie door opname op de lijst? [paragraaf 3.4 van het expertadvies]?
Antwoord: Ja

8. Bent u het eens met het advies van de expertgroep aan het Forum met betrekking tot opname van NEN-ISO/IEC 27001:2013 en 27002:2013 op de ‘pas toe of leg uit’-lijst? [Advies aan het Forum]
Antwoord: Ja

9. Bent u het eens met de adoptie-aanbevelingen van de expertgroep aan het Nationaal Beraad Digitale Overheid? [paragraaf 3.5 van het expertadvies]?
Antwoord: Ja

10. Is/zijn er volgens u nog andere informatie of overwegingen die aan het Forum en Nationaal Beraad Digitale Overheid zou moeten worden meegegeven voor een besluit over het opnemen van deze standaard op de lijst met standaarden?
Antwoord: Nee