



Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

17 oktober 2019

**Betreft: Consultatie Besluit beveiligde verbinding met overheidswebsites en -webapplicaties**

Wij danken u voor de mogelijkheid om als Instituut van Internal Auditors (IIA) te reageren.  
Het IIA onderschrijft het nut van een dergelijke richtlijn.  
Wij willen graag de volgende opmerkingen meegeven.

**Vraag 1**

Wij stellen voor bij de keuze van de standaard niet statisch te verwijzen naar een versie (versie 2015) van ICT beveiligingsrichtlijnen van het NCSC, maar juist naar de dynamische versie, waarbij de 2015 versie het startpunt is ten tijde van het besluit. Vooral bij dit soort zaken moet je snel handelen en zou je je beveiligingsstandaarden ook conform de stand der techniek moeten inrichten. Wij bevelen dus aan het detail, de invulling (die je bij het NCSC zou moeten kunnen vinden) meer te scheiden van het beleid.

T.a.v. het toezicht op de beveiliging van overheidswebsites zien wij deze in het verlengde liggen van BIO (v/h BIR) onderzoeken. Wij geven u in overweging om aan te haken op de taken t.a.v. de handhaving van de Baseline Informatiebeveiliging Overheid (BIO); BIO-maatregel 13.2.3 wordt met de beveiliging overheidswebsites nader ingevuld, en daarmee ook 9.4.

Daarbij doen wij de suggestie om in de daadwerkelijke uitvoering van het toezicht af te stemmen met de mogelijk aanwezige Internal Auditfunctie, die ook reeds werkzaamheden in dit kader kan uitvoeren. Voor meer toelichting over internal audit en het IIA wordt verwezen naar onderstaande alinea's).

**Vraag 2**

Het toepassingsbereik lijkt passend, gegeven de setting.

**Vraag 3**

We geven graag de suggestie mee om een consistente markering aan te houden, bijvoorbeeld: "uit te faseren" → "uitgefaseerd" → verwijderen en archiveren. Op die manier is het na de uiterlijke deadline heel zichtbaar dat een bepaalde instelling uit den boze is.

**Over het IIA**

*Het Instituut van Internal Auditors Nederland (IIA) is de grootste beroepsvereniging van internal auditors in Nederland. De missie van het IIA is om het beroep en vak internal audit in Nederland te ontwikkelen en te promoten. Op deze manier ondersteunt het IIA internal auditors, management en andere belanghebbenden bij een succesvolle invulling van de internal auditfunctie. De hoofdtaken van het IIA bestaan uit het profileren van het vak, kwaliteitsbewaking, belangenbehartiging en het delen van kennis.*

**Over internal audit**

*De internal auditor beoordeelt in welke mate zijn organisatie erin slaagt om het bedrijfsproces en de daarmee samenhangende risico's te beheersen. Dit gebeurt in de volle breedte van systemen, productie, techniek, marketing en human resources van de organisatie. De internal auditor zal in de regel naar aanleiding van zijn bevindingen aanbevelingen geven over het terugdringen van risico's. Een goed functionerende internal auditfunctie helpt het management om een organisatie met een goed stelsel van normen te beheersen.*