NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Ministerie van BZK,
t.a.v. de Staatssecretaris
Koninkrijksrelaties en Digitalisering

Gezonden via Internetconsultatie
Overheid.nl

Datum : 12 mei 2023
Kenmerk : NOREA / AB23-47/WO
Betreft : Consultatie Regeling dienstverleners informatieveiligheidsaudits Wdo

Geachte Staatssecretaris,

NOREA, de beroepsorganisatie van IT-auditors in Nederland, maakt graag gebruik van de geboden gelegenheid om te reageren op de consultatieversie van de Regeling dienstverleners informatieveiligheidsaudits Wdo.

Onze leden zijn nauw betrokken bij het uitvoeren van informatieveiligheidsaudits bij dienstverleners en verstrekken rechtstreeks zekerheid (assurance) en advies aan organisaties over informatietechnologie en informatiesystemen in de elektronische dienstenomgeving.

Wij onderschrijven de noodzaak om tot een Ministeriële regeling onder de Wdo te komen voor auditverklaringen (in ons vakgebied spreken wij over assurance-rapporten) om meer zekerheid te verkrijgen over de beveiliging van de toegang tot een elektronische dienstenomgeving door middel van een webapplicatie.

In ons werkveld zien we dat als IT onvoldoende beheerst wordt door organisaties, dit leidt tot materiële risico's voor de organisaties die in enkele gevallen ook de integriteit van de dienstverlening raken (denk o.a. aan cyberrisico's en outsourcingsrisico's). Wij zien ook een steeds toenemende cyberdreiging en grotere afhankelijkheid van nieuwe technologische ontwikkelingen, zoals het gebruik van mobiele apps en clouddiensten.

Dit is temeer een reden om in de Regeling te wijzen op deze risico's en continu in te spelen op deze risico's en de beheersing daarvan door hoogwaardige beveiligingsmaatregelen te implementeren.

In deze brief hebben wij onze belangrijkste opmerkingen bij de Regeling opgenomen. In de bijlage zijn aanvullende aandachtspunten opgenomen welke de Regeling inhoudelijk kunnen versterken.

1. De Regeling is voor een groot deel de codificering van de huidige DigiD-auditpraktijk, zoals deze op de sites van Logius en NOREA is beschreven en sluit daar goed bij aan. De Regeling is niet meer beperkt tot DigiD en webdiensten aan burgers. *'Onder het regime van de Wet digitale overheid wordt niet langer aangesloten op DigiD, maar op een stelsel voor toegang'.* De toelichting spreekt over burgers en bedrijven. Wij onderschrijven deze uitbreiding omdat de webdiensten voor bedrijven dezelfde cyberrisico's kennen als de webdiensten aan burgers. Onze vraag hierbij is wel of deze uitbreiding daadwerkelijk beoogd is. Indien dit zo is verdient dit nadere toelichting in de Regeling en dient tevens bezien te worden of de in de Regeling opgenomen codificering van de huidige DigiD-auditpraktijk 1 op 1 van toepassing is op het bredere werkingsgebied. De hierna opgenomen opmerkingen hebben in het bijzonder betrekking op het werkingsgebied DigiD audits.

2. Dat de Regeling voor een groot deel de codificering is van de huidige praktijk roept ook de vraag op in welke mate rekening is gehouden met het snel kunnen inspelen op de steeds groter wordende cyberdreigingen en nieuwe technologische ontwikkelingen, zoals deze onder meer in de NIS 2 directive worden beschreven. De Regeling specificeert een selectie van de ICT-beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum[1] die op dit moment als een normenset gebruikt wordt bij DigiD assessments. Bekend is dat enkele van deze richtlijnen binnenkort vernieuwd worden. Wij verwachten dat door nieuwe cyberdreigingen en nieuwe technologie de vernieuwing een permanent proces zal zijn. Graag zien wij dat de Regeling ruimte biedt voor het periodiek heroverwegen van de normenset, zodat a tempo ingespeeld kan worden op nieuwe dreigingen en technologische ontwikkelingen. Daarbij hoeven niet alleen de NCSC richtlijnen leidend te zijn. Ook andere (internationaal) richtlijnen en normenkaders voor cybersecurity kunnen hierbij in ogenschouw genomen worden. Naar analogie geldt dit ook voor het door IT-auditors kunnen inspelen op (internationale) ontwikkelingen in (audit-)regelgeving. Ook deze regelgeving is, gelet op de belangen van stakeholders, doorlopend in ontwikkeling.

[1] 'ICT-Beveiligingsrichtlijnen voor Webapplicaties', Nationaal Cyber Security Centrum, September 2015

3. In Artikel 3.2 van de Regeling wordt aangegeven dat aan artikel 24, derde lid, van het Besluit digitale overheid in ieder geval voldaan wordt indien een audit wordt uitgevoerd door een auditor die is ingeschreven in het register van de Nederlandse Orde van Register EDP-Auditors. Vanzelfsprekend onderschrijven wij deze bepaling. In de toelichting op pagina 17 staat echter: 'Wanneer de audit niet is uitgevoerd door een EDP-auditor zal moeten worden gemotiveerd dat de uitvoerende auditor voldoet aan de geldende algemene eisen van onafhankelijkheid en deskundigheid die op grond van artikel 24 van het Besluit digitale overheid van kracht zijn.' Daarbij worden geen verdere kwaliteitseisen aangegeven. In onze visie zou minimaal bepaald moeten worden dat de auditor aangesloten dient te zijn bij een beroepsorganisatie waarvoor formeel kwaliteitsonderzoek en tuchtrecht geldt en dat de auditor aantoonbaar vakbekwaam is[2]. De hier geboden ruimte voor niet-EDP-auditors wijkt af van het audit regime bij Suwinet en Wpg audits, waarvoor de een inzet van een Register EDP-auditor vereist is.

4. Wij lezen in de nadere regels over de auditverklaring in de Regeling een beperking tot een directe-opdracht, waarbij de auditor het onderzoeksobject meet of evalueert ten opzichte van de criteria (zie hiervoor de NOREA standaard 3000D). (Inter-)nationaal is er sprake van het ontwikkelen van verantwoordingssystematieken waarbij de auditverklaring een attest-opdracht is, waarbij een andere partij dan de auditor het onderzoeksobject meet of evalueert ten opzichte van de criteria en daarover verantwoording aflegt (zie hiervoor de NOREA Standaard 3000A).

   Directe-opdrachten hebben veel gemeenschappelijke kenmerken met attest-opdrachten. Fundamentele concepten gerelateerd aan aangelegenheden zoals het niveau van assurance, risico en materialiteit zijn hetzelfde. Directe-opdrachten hebben ook kenmerken die duidelijk verschillen van die van attest-opdrachten. Voorbeelden hiervan zijn:

[2] In onze visie zou minimaal bepaald moeten worden dat de auditor onderworpen is aan professionele vereisten en kwaliteitsbeheersingsvereisten die ten minste gelijkwaardig is met het Reglement Gedragscode ('Code of Ethics') respectievelijk Reglement Kwaliteitsbeheersing NOREA (RKBN).

a. de verantwoordelijke partij voor het onderzoeksobject stelt geen verantwoording op of de prestaties van de entiteit voldeden aan de criteria;
b. de auditor kan besluiten over de van toepassing zijnde criteria voor de opdracht;
c. de auditor voert de evaluatie aan de hand van criteria zelf uit.

NOREA heeft een sterke voorkeur voor de attest-opdracht, omdat daarmee de eigen verantwoordelijkheid van de organisatie voor de beheersing van de informatieveiligheid tot uitdrukking komt. Daarmee wordt ook aangesloten op de hiervoor aangehaalde (inter-)nationale ontwikkelingen op het gebied van verantwoorden en het daarbij verstrekken van assurance.

5. Voor de goede orde wijzen wij erop dat het hanteren van Standaard 3000D afwijkt van de werkwijze die gehanteerd wordt bij ENSIA[3]. Hierbij vinden de afgesproken audits plaats op basis van de Standaard 3000A.
   Indien de auditverklaring conform de Regeling beperkt blijft tot een directe opdracht zal dit tot ingrijpende wijzigingen in het ENSIA stelsel moeten leiden.

Onze reactie kan tevens gepubliceerd worden. Indien gewenst geven wij graag een nadere (mondelinge) toelichting op deze brief aan de stelselverantwoordelijke.

Met vriendelijke groet,

Het NOREA-bestuur

[3] ENSIA – Eenduidige Normatiek Single Information Audit – stelsel gehanteerd door gemeenten om zich te verantwoorden over het beheer van een aantal onderdelen van de voor overheden belangrijke IT-applicaties.

Bijlage: Aanvullende aandachtspunten bij Regeling dienstverleners informatieveiligheidsaudits Wdo.

1. De Regeling gaat uit van een oordeel per norm, terwijl de NOREA-richtlijnen één totaal oordeel over het gehele object van onderzoek vereisen. Dit hoeft niet strijdig te zijn met het verkrijgen van zekerheid over het wel / niet voldoen aan individuele normen conform de wens van de stelselhouder / toezichthouder DigiD.
2. De Regeling geeft aan dat de toezichthouder eisen kan stellen aan het rapport van de auditor. Daarbij dient er op te worden toegezien dat deze eisen niet in strijd zijn met de NOREA-richtlijnen voor het assurance-rapport. Dit vereist voorgaand overleg met de NOREA.
3. NOREA ziet voor de normenset alleen een verwijzing naar NCSC-richtlijnen en geen aansluiting op andere standaarden zoals BIO en CSIR of internationale cybersecurity standaarden.
4. De Regeling besteedt geen aandacht aan periodieke bestuurlijke evaluatie en rapportage over de resultaten van de uitgevoerde audits. De NOREA hanteert één normenset voor alle dienstverleners in deze Regeling. In andere regelingen ziet NOREA regelmatig op basis van een risico-inschatting, afhankelijk van de grootte van de organisatie of de positie in de keten, verschillende niveaus van beveiligingseisen. Er wordt geen aandacht besteed aan een risicoanalyse op basis van de uitkomsten van de audits en het afwegen van alternatieve vormen van toezicht vormen of dynamisering van de audits (risicogebaseerd, doelgroep gericht, thema gericht, cyclisch, etc).
5. De Regeling beperkt de toetsing van de werking tot 5 met name genoemde normen. Er wordt geen ruimte geven voor een bredere toepassing van toetsing op werking.
6. Audits op leveranciers van identificatie en authenticatiediensten vallen niet onder deze regeling. In navolging van onze opmerking 3 over de inzet van RE's spreekt NOREA de wens uit dat ook voor audits op leveranciers van authenticatiediensten geldt dat deze worden uitgevoerd door een auditor die is ingeschreven in het register van de Nederlandse Orde van Register EDP-Auditors.

7. Wij zien toenemend gebruik van mobiele Apps. Hiervoor gelden op onderdelen afwijkende beveiligingseisen. In de Regeling wordt hier niet in voorzien.
8. Wij zien in de Regeling geen voornemens om periodiek de auditaanpak te bespreken met de NOREA.
9. Op één punt stellen wij een concrete aanpassing voor in de tekst: Artikel 4.1 punt a: De tekst over de software en processen dient niet te zijn 'die organisaties' maar de derde partij voor die organisaties. Vergelijkbaar met de LMA constructie bij DigiD.
10. Op twee punten is de regeling in strijd met geldende beroepsregels voor IT-auditors:

    - In art 3.4 lid 2 staat vermeld, als een norm uit art 3.1 lid 2 in werking niet voldoet, een conclusie moet worden gegeven over het bestaan. Dit is ons inziens een aanpassing van de scope van het onderzoek.
    - In art 3.6 wordt ingegaan op non-conformiteit werking van een maatregel. In dat geval dient een correctief actieplan te worden opgenomen. Dit is echter geen verantwoordelijkheid van de IT-auditor maar van de indiener van het auditrapport (de eigenaar van de aansluiting). Zoals nu geformuleerd, kan het worden geïnterpreteerd als een verantwoordelijkheid van de IT-auditor en dat is onwenselijk