FAQ DigiD assessment

FAQ versie: 4.0 d.d. 24 april 2024

Naar aanleiding van de invoering van de controle op werking en de vele gestelde vragen hierover aan het meldpunt DigiD assessments (bereikbaar voor auditors en hun opdrachtgevers via meldpunt@norea.nl), brengen we onderstaande nieuwe FAQ uit om de gestelde vragen van een eenduidig antwoord te voorzien.

Deze FAQ is gebaseerd op normenkader 3.0 van Logius en op de in de NOREA Handreiking ICT-beveiligingsassessment DigiD 4.0 (2023) versie 1.0 (definitief) d.d. 17 juli 2023 gepubliceerde testaanpak. Daarnaast is rekening gehouden met de resultaten van het proefjaar en met de mededelingen van Logius over de controle op werking: zie hiervoor https://www.logius.nl/domeinen/toegang/digid/ict-beveiligingsassessments-digid/mededelingen-ict-beveiligingsassessment-digid

Beveiliging richtlijn	Vraag	Antwoord
Toetsing op werking - verplicht	Vanaf wanneer is de toets op werking verplicht?	Vanaf de inleverperiode 1 januari -1 mei 2025 (over het voorgaande jaar 2024) moeten DigiD-aansluithouders de normen U/TV.01; U/WA.02; C.07; C.08 en C.09 laten toetsen op werking. Dit geldt ook voor het DigiD deel van het ENSIA assessment voor gemeenten. Het is belangrijk om vast te stellen dat de toets op werking betekent dat aansluithouder en serviceorganisatie hun processen en systemen goed op orde moeten hebben, zodat de IT-auditor de toets op werking kan uitvoeren en kan beoordelen.
Toetsing op werking - controletermijn	Wat is de periode waarover de effectiviteit van de controle op werking moet worden vastgesteld?	Deze periode noemen we de controleperiode. De controleperiode voor de inleverperiode 1 januari - 1 mei 2025 is door Logius bepaald op 6 maanden. Dit is minimaal 6 maanden *aaneengesloten* voorafgaand aan de audit waarbij de laatste dag van de controleperiode wordt gezien als de gespecificeerde datum waarop de opzet en het bestaan is getoetst (= de oordeelsdatum). Voor ENSIA assessments is en blijft de oordeelsdatum 31 december. Dat betekent automatisch dat de controleperiode voor het DigiD deel van de ENSIA de periode *1 juli – 31 december* van het verantwoordingsjaar wordt. De controleperiode voor serviceorganisaties (en sub-serviceorganisaties) is uiteraard ook minimaal 6 maanden. Rekening houdend met de wensen van gemeentelijke aansluithouders om voldoende

Beveiliging richtlijn	Vraag	Antwoord
		gelegenheid te hebben om de ENSIA tooling in te vullen, zal het assurancerapport voor deze groep aansluithouders uiterlijk 15 oktober gereed moeten zijn. Dit betekent voor serviceorganisaties die DigiD webapplicaties leveren aan gemeenten dat de controle periode in de praktijk *1 april- 30 september* zal zijn.
Toetsing op werking – welke beveiligingsrichtlijnen?	Welke normen worden in geval van een SaaS audit bij de aansluithouder op werking gecontroleerd?	Het beeld is dat aansluithouders steeds meer steunen op de beheersingsmaatregelen van de serviceorganisatie. Bij de controle bij de aansluithouder worden in principe alleen die beveiligingsrichtlijnen gecontroleerd die de IT-auditor van de serviceorganisatie als 'user control' aangeeft. User controls kunnen uiteraard ook beveiligingsrichtlijnen betreffen die niet bij de geselecteerde 5 normen behoren. Die zouden dan logischerwijs ook buiten de scope van de toets op werking vallen en enkel op opzet/bestaan worden getoetst.
Toetsing op werking – verschil tussen IT-auditor van de service-organisatie en de IT-auditor van de aansluithouder	Wat als de IT-auditor van de aansluithouder bij de controle op werking afwijkt van de user controls in het rapport van de serviceorganisatie?	De IT-auditor van de aansluithouder kan op basis van zijn/haar onderzoek afwijken van hetgeen in het hoofdstuk 2 (user controls) door de IT-auditor van de serviceorganisatie in zijn/haar assurancerapport is aangegeven. Dit kan ongeacht of het te maken heeft met opzet, bestaan of werking. De IT-auditor van de aansluithouder vermeldt deze afwijking als opmerking in paragraaf '1.2 De basis voor onze oordelen' in het assurancerapport. In de opmerking wordt expliciet opgenomen dat tot de afwijking is gekomen in overleg met IT-auditor van de serviceorganisatie.
Toetsing op werking – verbijzonderde interne controle	Is de verbijzonderde interne controle een verplichting of betreft het een groeipad?	De verbijzonderde interne (2e lijns) controle is vooralsnog een wenselijkheid en geen verplichting. Het DigiD assessment blijft vooralsnog een directe opdracht[1] waarbij de IT-auditor het onderzoeksobject meet of evalueert ten opzichte van de criteria. De auditee kan ook zelf meten, waarbij dan de IT-auditor zoveel mogelijk aan zal sluiten op en gebruik maken van de resultaten van de werkzaamheden in het kader van verbijzonderde interne controle en / of management bewering van de auditee.
Toetsing op werking – non-occurence regeling	Wat gebeurt er als binnen de beperkte scope van het DigiD assessment tijdens de controleperiode geen enkele gebeurtenis plaats heeft	Het is de bedoeling van de controle op werking om de effectiviteit van de beheersingsmaatregelen vast te stellen. In de praktijk kan het voorkomen dat er, als voorbeeld, tijdens de controleperiode geen beveiligingsincidenten voor de controle op U/WA.02 hebben plaatsgevonden binnen scope of geen gebruikersmutaties bij U/TV.01. Dit noemen we een non-occurence.

[1] *Bij een directe opdracht wordt volgens de 3000 Richtlijn direct over het onderzoeksobject en de van toepassing zijnde criteria door de IT-auditor gerapporteerd.*

Beveiliging richtlijn	Vraag	Antwoord
	gevonden waardoor de populatie leeg is?	Anders dan bij de bestaanscontrole kan bij een non-occurence voor het verkrijgen van voldoende zekerheid over de effectiviteit van de maatregelen NIET de scope van de test worden uitgebreid tot een ander systeem of proces of procedure waar wel relevante gebeurtenissen hebben plaatsgevonden. Daarmee zou de populatie wijzigen en wordt de effectiviteit van een andere procedure, proces of systeem gemeten; de populatie kan niet worden bepaald noch de omvang van de deelwaarneming. In de situatie dat de populatie leeg is maar de maatregelen in opzet en bestaan geen afwijkingen hebben laten zien, wordt de volgende tekst als opmerking in paragraaf 1.2 van het assurancerapport opgenomen: [1] Werking. Voor beveiligingsrichtlijn < vul in U/TV.01, U/WA.02 en of C.08> hebben wij na een controle vastgesteld dat de organisatie maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en wij hebben deze gevalideerd. Er zijn geen afwijkingen door ons geconstateerd. Wij zijn van oordeel dat de organisatie in opzet voldoet aan deze norm. Vanwege non-occurence kan de effectieve werking niet worden vastgesteld en daarom geven wij geen oordeel daarover.
Toetsing op werking – afwijkingen	Hoe wordt er omgegaan met afwijkingen binnen de controleperiode die zelf zijn opgemerkt en geadresseerd?	Afwijkingen die door de auditee zelf zijn opgemerkt, geadresseerd en van een risicobeperkende compenserende beheersingsmaatregel zijn voorzien, kunnen op basis van het professional judgement van de behandeld IT-auditor, niet als beperking worden behandeld. De situatie geeft aanleiding voor aanvullende werkzaamheden van de IT auditor omtrent de compenserende maatregelen omdat de interne beheersing op dit punt niet op orde lijkt te zijn. In deze situatie wordt de volgende tekst als opmerking in paragraaf 1.2 van het assurancerapport opgenomen: [1] Werking. Voor beveiligingsrichtlijn < vul in U/TV.01, U/WA.02, C.07, C.08 en/of C.09> hebben wij na een uitgebreide controle vastgesteld dat de organisatie effectieve maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en wij hebben deze gevalideerd. Er zijn afwijkingen door de organisatie zelf opgemerkt, tijdig geadresseerd en tijdig van risicobeperkende compenserende maatregelen voorzien. Wij zijn van oordeel dat de organisatie voldoet aan deze norm.
Toetsing op werking – templates	Hoe wordt de controle op werking verwoord in het assurancerapport?	In juni/juli 2024 zal een nieuwe Handreiking worden gepubliceerd met daarin aangepast templates voor het assurancerapport voor zowel de aansluithouder, de serviceorganisatie als de LMA, waarin ook de controle op de werking verwoord kan worden.

Beveiliging richtlijn	Vraag	Antwoord
		Hierbij wordt verschil gemaakt tussen een oordeel 'opzet/bestaan' en een oordeel 'werking' voor de vijf geselecteerde beveiligingsrichtlijnen.
Toetsing op werking – nieuwe aansluitingen	Hoe wordt controle op werking getoetst en verantwoord bij nieuwe DigiD aansluitingen?	Bij nieuwe DigiD aansluitingen vervalt de controle op werking voor de aansluithouder, aangezien de controleperiode pas kan starten bij de activatie van de aansluiting door Logius. Wanneer er van een bestaande uitbestede dienst gebruik wordt gemaakt moet de serviceorganisatie (en sub-serviceorganisatie) uiteraard wel voldoen aan de toets op werking voor de vijf geselecteerde beveiligingsrichtlijnen die voor de serviceorganisatie van toepassing zijn. Een nieuwe aansluiting die gebruik maakt van een verkregen uitstel vanwege een koppelvlakmigratie wordt - in dit opzicht- *niet* gezien als een nieuwe aansluiting en zal aan de toets op werking moeten voldoen.