FAQ DigiD assessment

FAQ versie: 2025.0 d.d. 25 november 2025

Naar aanleiding van de gestelde vragen aan de werkgroep DigiD over de update van de Handreiking ICT-beveiligingsassessment DigiD versie 2025 d.d. 29 augustus 2025 van NOREA, brengen we onderstaande nieuwe FAQ uit om de vragen van een eenduidig antwoord te voorzien. Deze FAQ prevaleert boven de Handreiking ICT-beveiligingsassessment DigiD.

Beveiligingsrichtlijn	Vraag	Antwoord
C.07	Wat is de exacte scope voor norm C.07, ook in samenhang met C.06 en U/NW.04?	Probleemschets In norm C.06 staat een duidelijke afbakening van de scope. Deze is niet als zodanig terug te vinden bij norm C.07. Argumentatie De scope is bij zowel C.06 als C.07 gelijk, namelijk: de infrastructuur voor het netwerksegment met de DigiD webapplicatie. De verduidelijking van C.06 is ook bij C.07 van toepassing. De scope is beperkt tot de detectiesystemen in de webapplicatie-infrastructuur, zijnde: Firewall, IDS, IPS en/of WAF.
C.07	Hoe om te gaan met een situatie waarbij een SOC is ingericht voor continue analyse van loginformatie?	Probleemschets Norm C.07 beschrijft een situatie waarin een periodieke loganalyse dient plaats te vinden. Hoe dient deze norm geïnterpreteerd te worden in een situatie waarin continue monitoring plaatsvindt door een SOC. Argumentatie Logius heeft na consultatie van de NOREA DigiD werkgroep besloten dat in het geval van alertafhandeling door een SOC ten minste use-cases dienen te zijn gedefinieerd voor: - Wijzigingen aan de configuratie van Firewall/IDS/IPS/WAF - Optreden verdachte gebeurtenissen en eventuele schendingen beveiligingseisen - Ongeautoriseerde toegang tot en wijzigen/verwijderen logbestanden - Toegangslogs Bij afhandeling door het SOC dient het SOC periodiek (minstens per kwartaal) een rapportage op te leveren aan de systeemeigenaren en/of het management waarin ook de afhandeling van alerts uit bovengenoemde use-cases een onderdeel vormt. Deze rapportage kan ook in de vorm van een dashboard zijn dat door de systeemeigenaar kan worden geraadpleegd. De populatie voor werking omvat alle alerts gegenereerd vanuit FW/IDS/IPS/WAF voor het netwerksegment met de DigiD webapplicatie.

U/WA.05	Is een dataclassificatie door de dienstverlener (aansluithouder) ook nodig bij gebruik van een RSO (voorheen: TPM)?	Probleemschets In het RSO wordt niet aangegeven dat de dienstverlener een dataclassificatie dient uit te voeren, terwijl een serviceorganisatie geen classificatie voor een dienstverlener kan uitvoeren. Argumentatie De classificatie van gegevens door de dienstverlener van de DigiD aansluiting op basis van een risicoanalyse is altijd noodzakelijk, ook als dit niet bij de verantwoordelijkheden voor de dienstverlener in het RSO is opgenomen. Een serviceorganisatie kan deze afweging niet maken voor de dienstverlener.
U/WA.05	Is de Handreiking strenger dan TLS richtlijn van het NCSC?	Probleemschets In de handreiking wordt gesteld dat gebruik moet worden gemaakt van "minimaal de TLS instellingen (TLS-versie en Algoritme) die het NCSC als 'Goed' of 'Voldoende' heeft aangemerkt". Hiermee mogen nu nog gangbare instellingen direct niet meer gebruikt worden. Dit is onwenselijk. Argumentatie Logius heeft na consultatie van de NOREA DigiD werkgroep besloten dat TLS-instellingen met beveiligingsniveau 'Uit te faseren' eveneens gebruikt mogen blijven worden. Hierbij attendeert de IT-auditor de dienstverlener (bij het gebruik van "uit te faseren" instellingen erop wijst dat deze op termijn, dan wel bij herziening van NCSC TLS-richtijn, als "onvoldoende" kunnen worden geclassificeerd, en daarmee niet meer geaccepteerd worden.
Non-occurrence op werking – Rapporttemplate, hoofdstuk 1.2 [2]	Hoe gebruik ik de tekst voor '[2] Werking – non-occurrence' in paragraaf '1.2 De basis voor onze oordelen'?	Probleemschets In de rapporttemplate is aangegeven welke tekst gebruikt kan worden als er sprake is van een non-occurrence waardoor de effectieve werking niet kan worden vastgesteld. In deze tekst moet een keuze worden gemaakt in de zin: "Wij zijn van oordeel dat de organisatie in opzet (**of**: opzet en bestaan) voldoet aan deze norm." De keus moet overeenkomen met het gegeven oordeel op opzet en bestaan voor de desbetreffende norm. Argumentatie De keuze "opzet (**of**: opzet en bestaan)" is hierin niet geel gearceerd waardoor niet duidelijk is gemaakt dat hier een keuze gemaakt moet worden. Bij een 'voldoet' op bestaan wordt de keus gemaakt voor "opzet en bestaan". Bij een non-occurrence op bestaan wordt de keuze gemaakt voor "opzet".