Wijzigingen in DigiD-audits

Vanaf 2023: audit op werking

U heeft een DigiD-aansluiting, daarom bent u verplicht jaarlijks een audit te laten uitvoeren. Let op: vanwege wijzigingen zullen DigiD-audits vanaf 2023 uitgebreider worden.

Recent heeft het Ministerie van Binnenlandse Zaken (BZK) besloten dat in DigiD-assessments ook 'werking' van beheersmaatregelen moet worden getoetst. In dit document leggen wij uit wat deze verandering inhoudt en wat de gevolgen zijn voor uw organisatie.

Wat betekent opzet, bestaan en werking?

OPZET

De beschrijving van een maatregel in bijvoorbeeld beleidsdocumentatie, procedures, enz. Met andere woorden: Er is een procedure/maatregel op papier aanwezig.

BESTAAN

De maatregel is eenmalig aantoonbaar uitgevoerd. De auditor beoordeelt dit via een willekeurige sample of voorbeeld uit een lijst (van bijvoorbeeld wijzigingen). Met andere woorden: Er kan met minstens één voorbeeld worden aangetoond dat de procedure/maatregel wordt toegepast.

WERKING

De maatregel is aantoonbaar over een bepaalde periode uitgevoerd. Met andere woorden: De procedure/maatregel wordt **altijd** gevolgd. Eventuele afwijkingen hiervan worden gecorrigeerd.

Welke partijen zijn betrokken bij de audits?

Ministerie van Binnenlandse Zaken
Beleidsopdrachtgever voor DigiD als authenticatie-mechanisme

Logius
Levert DigiD-aansluiting, controleert naleving van de beveiligingsvereisten

NOREA werkgroep DigiD-assessments
Stelt handreiking voor het uitvoeren van DigiD-assessments op, met daarin aanpak en gedetailleerde uitwerking van normenkader.

RE-auditor en auditorganisatie
Voert DigiD-assessments uit volgens handreiking en NOREA vak- en beroepsregels en rapporteert hierover.

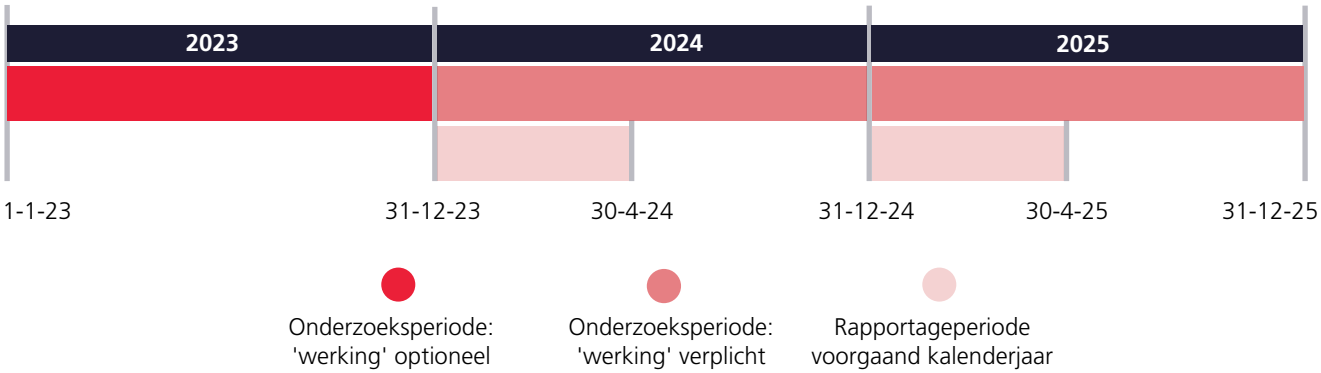
Wat verandert er en wat zijn de gevolgen?

Bij onderzoek naar de werking van beheersmaatregelen moet worden bepaald wat de populatie (het aantal van wijzigingen, patches, incidenten, enz.) is, op basis waarvan een steekproef/deelwaarneming gedaan kan worden. Het bepalen van de grootte van de populaties, het beoordelen van de betrouwbaarheid hiervan, het nemen van een representatieve steekproef en het beoordelen van de geselecteerde items betekenen: extra werk voor de auditors. Een audit wordt dus uitgebreider, duurt langer en de kosten ervan zullen hoger zijn.

Wat is het tijdpad?

- In kalenderjaar 2023, met deadline voor indienen van het rapport bij Logius op 30 april 2024, is het beoordelen van de werking **optioneel.**
- In kalenderjaar 2024, met deadline voor indienen van het rapport bij Logius op 30 april 2025, is het beoordelen van de werking **verplicht**.

Tijdens het aankomende DigiD-onderzoek is nog ruimte om zonder consequenties in het oordeel ons voor te bereiden op de toekomstige situatie. Zo kunnen wij de geleerde lessen meenemen naar het volgende jaar, als de verplichting van kracht wordt.



Over welke normen gaat het?

U/TV.01 – Toegangsbeveiliging
U/WA.02 – Beheer van de webapplicatie en incidentbeheer
C.07 – Logging en monitoring
C.08 – Wijzigingbeheer
C.09 – Patch Management

NOREA is inmiddels ten aanzien van de toetsing op de werking met nadere invulling gekomen. U vindt de handreiking hier: www.secura.com/norea-handreiking.

Heeft u meer vragen over wat deze DigiD-wijziging voor u betekent?

Neem contact met ons op via info@secura.com

Secura
A BUREAU VERITAS COMPANY

Over Secura

Secura is een gespecialiseerd security-bedrijf. Wij bieden organisaties inzicht in hun digitale beveiliging, met aandacht voor mens, proces en technologie. Secura biedt audit-, test- en certificeringsdiensten in de wereld van IT, IoT en OT. We voeren onze audits en tests uit volgens internationale standaarden. Secura is uw onafhankelijke, betrouwbare security-partner.