At Risk Advies

Overzicht wijzigingen Digid Control Framework 2020 t.o.v. 2019

De update betreft de testaanpak voor het DigiD assessment 2020. Het normenkader voor het DigiD assessment blijft ongewijzigd.

Naast een beperkt aantal tekstuele verbeteringen en verduidelijkingen zijn de belangrijkste wijzigingen:

- **U/WA.05:** minimaal de TLS instellingen die het NCSC als 'Goed' of 'Voldoende' heeft aangemerkt dienen te worden gebruikt.
- **U/PW.03:** de minimale configuratie en het gebruik van HSTS, X-Content-Type-Options, Content-Security-Policy (aangescherpt), en Referrer-Policy is verplicht.

Non-occurance bij de normen B.05, U/TV.01, U/WA.02 en C.08

Non-occurrence kan zich alleen voordoen bij de normen B.05, U/TV.01, U/WA.02 en C.08.

In die gevallen kan de situatie zich voordoen dat wel voldaan is aan de opzet van de interne beheersmaatregel, maar het bestaan niet vastgesteld kan worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode.

In die gevallen is het werkprogramma als volgt:

In situaties dat de relevante gebeurtenis zich niet heeft voorgedaan, kan relevante audit evidence voor het bestaan van de betreffende beheersmaatregel worden verzameld door een deelwaarneming te doen in een proces dat onderworpen is aan dezelfde control (i.c. dezelfde control owner, dezelfde tools, dezelfde registratie, dezelfde workflow, et cetera). In dat geval vermeldt de auditor 'Voldoet' voor de betreffende beheersmaatregel in de tabel oordelen zonder een voetnoot te plaatsen betreffende het toetsen op het bestaan van de beheersmaatregel.

Als er geen andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is waarmee het bestaan van de betreffende beheersmaatregel kan worden vastgesteld, dient de auditor 'Voldoet' voor de betreffende beheersmaatregel te vermelden in de tabel oordelen en daarbij met een voetnoot in het rapport aan te geven dat het bestaan van de beheersmaatregel niet kon worden getest omdat de relevante gebeurtenis zich niet heeft voorgedaan, noch er een andere deelpopulatie is waarop hetzelfde proces en dezelfde control van toepassing is.