

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

Voor gemeenten geldt vanaf 1 januari 2020 de Baseline Informatiebeveiliging Overheid (BIO). Als gevolg daarvan heeft het Ketenoverleg besloten dat vanaf 2020 de Verantwoordingsrichtlijn Gemeenschappelijke Voorziening Suwinet (hierna: Verantwoordingsrichtlijn GeVS) gebaseerd wordt op het normenkader van de BIO en verantwoording op basis daarvan moet plaatsvinden, in plaats van de Baseline Informatiebeveiliging Gemeenten (BIG) die tot 2019 de basis voor het Suwinet Control Framework vormde.

In Bijlage 1 van de Verantwoordingsrichtlijn GeVS is beschreven aan welke BIO normen inclusief de bijbehorende sub normen) de interne beheersmaatregelen voor de GeVS worden getoetst.

Vorenstaande heeft gevolgen voor de ENSIA IT-audit Suwinet. In de onderstaande tabel is in beknopte vorm aangegeven wat de belangrijke wijzigingen voor het controlejaar 2020 zullen zijn, ten opzichte van het controlejaar 2019. Voor detailinformatie wordt verwezen naar het Suwinet Control Framework 2020 elders in de Handreiking.

BIO control	Criterium BIO	SCF 2019	Wijziging
5. Informatiebeveiligingsbeleid			
5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	C.01	De termijn van 3 jaar is aangepast naar 4 jaar (cf. de raadsperiode).
6. Organiseren van informatiebeveiliging			
6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	B.04	Nieuw is het beschrijven van de rol en verantwoordelijkheden in een functieprofiel voor de CISO en het aanstellen van deze functionaris.
10. Cryptografie			
10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	U.11	Nieuw is de classificatie van gegevens en daaraan gerelateerde risicoanalyse.
12. Beveiliging bedrijfsvoering			
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Nieuw	Geheel nieuwe norm: betreft de beschikbaarheid van bedieningsprocedures/handleidingen voor gebruikers en/of beheerders.
18. Naleving			
18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Nieuw	Geheel nieuwe norm: betreft de aanstelling van een Functionaris Gegevensbescherming (FG) en het regelmatig controleren van de naleving van de privacyregels en informatieverwerking en -procedures.