

Opvolger Baseline Informatiebeveiliging Overheid: BIO2

Portefeuillehouder: Vincent Lokin / Steller: Nicole de Keijzer

Bespreekstuk (oordeelvormend)

Gevraagd besluit

De CBCF wordt gevraagd in te stemmen met de opvolger van de Baseline Informatiebeveiliging Overheid, BIO2. BIO2 is het nieuwe kader voor de overheid voor informatiebeveiliging dat via de zorgplicht in de nieuwe Cyberbeveiligingswet wettelijk verplicht wordt gesteld.

De kern van het advies

Sinds 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO verving de afzonderlijke baselines informatieveiligheid voor gemeenten, Rijk, waterschappen en provincies. Met de komst van de BIO kwam er een eenduidige en herkenbare stevige basis voor een veilige digitale overheid.

Overheidsbreed wordt aan de opvolger van de BIO gewerkt, BIO2 genaamd. BIO2 volgt op de evaluatie van de huidige BIO en geeft tevens invulling aan eisen vanuit de nieuwe Europese Network and Information Security (NIS2) richtlijn. Het ontwerp voor de BIO2 is ontwikkeld in samenwerking met gemeenten, provincies, waterschappen en de Rijksoverheid. De actuele conceptversie van de BIO2 staat in Github¹, zie [Baseline-Informatiebeveiliging-Overheid/docs/ontwerp/index.md at main · MinBZK/Baseline-Informatiebeveiliging-Overheid · GitHub](https://github.com/MinBZK/Baseline-Informatiebeveiliging-Overheid/docs/ontwerp/index.md).

Twee experts vanuit de waterschappen hebben aan het ontwerp van BIO2 meegeschreven en hun ervaringen regelmatig gedeeld in het overleg van de Coördinatoren Informatieveiligheid Waterschappen (CIW). In de periode 8 mei tot 7 juni 2024 is de tekst van de BIO2 via een brede maatschappelijke consultatie bij alle waterschappen voorgelegd, waarop geen inhoudelijke reacties zijn gekomen. Overeenkomstig NIS2 is de BIO2 gebaseerd op een risico-gestuurde benadering bij organisaties en het sluiten van hun Plan-Do-Check-Act cyclus, iets wat de waterschappen al langere tijd nastreven door toe te werken naar volwassenheidsniveau 4. De externe audits van de waterschappen, die in 2025 weer zullen worden gehouden, worden hierop aangepast door het accent te verleggen van maatregelen naar het managementsysteem.

Argumenten

Risico-gestuurde benadering

In de Vaarkaat 'Digitaal op Koers' - de bestuurlijke visie op de digitale transformatie bij de waterschappen - staat informatieveiligheid benoemd als onderdeel van een betrouwbaar digitaal waterschap. Bestuurlijk is afgesproken om bestaande afspraken te bevestigen, waaronder het toewerken naar volwassenheidsniveau 4 en periodiek via een externe audit te toetsen waar iedereen staat in dit traject. Met volwassenheidsniveau 4 wordt bedoeld dat de waterschappen risico-gestuurd werken en handelen volgens een organisatiebreed gedragen Plan-Do-Check-Act (PDCA) cyclus. Met BIO2 wordt het accent verlegd van maatregelen naar risico-gestuurd werken en het toepassen van de PDCA-cyclus, wat uitstekend aansluit bij de ambities van de waterschappen.

¹ Om discussie over versies te voorkomen, is er bewust voor gekozen om via GitHub te werken en geen pdf-versie van BIO2 te verspreiden. In de GitHub-omgeving wordt tevens de samenhang met de NIS2/Cyberbeveiligingswet nader toegelicht.



Aansluiting NIS2/Cyberbeveiligingswet

BIO2 geeft mede invulling aan de Europese NIS2 richtlijn, die in Nederland wordt uitgewerkt in de nieuwe Cyberbeveiligingswet. Er wordt uitgegaan van risicomanagement en via BIO2 wordt onder andere invulling gegeven aan de meldplicht. Via de zorgplicht in de Cybersecuritywet zal BIO2 uiteindelijk wettelijk verplicht worden gesteld als kader.

Besproken in

Twee leden van het CIW overleg hebben meegeschreven aan BIO2 en de leden van het CIW overleg geïnformeerd over de ontwikkelingen. Op de consultatie zijn geen inhoudelijke reacties vanuit de waterschappen gekomen.

De Werkgroep Bedrijfsvoering Digitalisering en Dienstverlening d.d. 18 oktober 2024 heeft de CBCF positief geadviseerd over BIO2 als opvolger van de BIO.

Andere partijen

De VNG heeft onlangs via een [brief aan de staatssecretaris](#) op de BIO2 consultatie gereageerd. In deze brief geeft de VNG aan dat een duidelijke invoeringstermijn en voldoende financiële middelen noodzakelijk zijn voor een goede implementatie van BIO2. Verder wordt om verduidelijking van de positie van de Chief Information Security Officer (CISO) gevraagd en om versimpeling en harmonisatie van het toezichtstelsel. Ook pleit de VNG voor een gezamenlijke aanpak van inkoop en leveranciersmanagement.

Vervolg/Communicatie

BIO2 zal wettelijk verplicht worden gesteld via de NIS2 implementatie in de Cyberbeveiligingswet. De Unie zal het oordeel van de CBCF meenemen in het besluitvormingstraject van de Cyberbeveiligingswet.