

## **Baseline Informatiebeveiliging Overheid (BIO) en GGI-Veilig**

Uit bericht op IBD-website:

*“De kogel is door de kerk: de baseline informatiebeveiliging overheid (BIO) 1.0 is klaar en nu kunnen de diverse overheidslagen de bestuurlijke besluitvorming inrichten.*

*[...]*

*Vanaf 2016 is door vertegenwoordigers van de rijksoverheid, de provincies, waterschappen, gemeenten (VNG) en het Centrum voor Informatiebeveiliging en Privacy (CIP), gewerkt aan een gezamenlijke baseline die alle bestaande losse overheidsbaselines zal gaan vervangen. Diverse gemeenten hebben in de afgelopen tijd meegewerkt aan de review van deze BIO, alle commentaar is gewogen en verwerkt in de versie 1.0.*

*De BIO verschilt op een aantal punten van de BIG. De grootste verschillen zijn:*

- 1. Minder maatregelen (bijna 60% minder)*
- 2. Maatregelen zijn altijd verplicht*
- 3. Meer risicomanagement (het begint met een QuickScan, de QIS)*
- 4. 3 Basisbeveiligingsniveaus (BBN)*
- 5. Selectie van ontbrekende maatregelen vooraf*
- 6. Toewijzing van maatregelen op eindverantwoordelijke*
- 7. Een baselinetoets die nu QIS heet en die rekening houdt met die 3 niveaus*

*De grootste verandering zal zijn dat ook bijvoorbeeld ENSIA compleet opnieuw zal moeten worden ingericht en daar is heel wat werk te verzetten. Ook een grote verandering is dat de aanpak anders is dan bij de BIG en dat betekent ook een wijziging in het ondersteuningsaanbod van de IBD door middel van operationele BIO-producten voor gemeenten.*

### **Wanneer gaat de BIO er echt zijn voor gemeenten?**

*De verwachting is dat de BIO zal worden voorgelegd aan de besluitvormende gremia van de VNG en het [Overheidsbreed Beleidsoverleg Digitale Overheid \(OBDO\)-overleg](#). Wanneer de BIO wordt aangenomen in 2018 zal, met ingang van 1-1-2019, de BIO nieuwe normenkader worden voor alle gemeenten en gemeentelijke samenwerkingsverbanden. Het jaar 2019 zal dan gelden als overgangsjaar zodat pas vanaf 1-1-2020 daadwerkelijk volgens de BIO gewerkt en verantwoord moet worden.”*

### **De BIO en GGI-Veilig**

Zoals bovenstaand aangegeven is één van de wijzigingen t.o.v. de BIG dat maatregelen altijd verplicht zullen zijn. Onderstaand is aangegeven welke maatregelen vanuit de BIO verplicht zullen worden gesteld en waarin GGI-Veilig de gemeenten ondersteunt met voornamelijk technische maatregelen en voorzieningen.

### BIO en GGI-Veilig perceel 1

- BIO: de nieuwe normenkaders voor "Verslaglegging en monitoring" stelt het gebruik van SIEM/SOC verplicht.
- GGI-Veilig: Perceel 1 voorziet in deze dienstverlening.

### BIO en GGI-Veilig perceel 2

- BIO: de nieuwe normenkaders voor:
  - "Mobiele apparatuur en telewerken" en "Bedrijfseisen voor toegangsbeveiliging" stellen het gebruik van EMM (MDM/MAM) verplicht,
  - "Beheer van netwerkbeveiliging" stellen het gebruik van firewall, mailfiltering en IDS/IPS verplicht,
  - "Bedieningsprocedures en verantwoordelijkheden" onderdeel capaciteitsbeheer het gebruik van Anti DDos verplicht.
- GGI-Veilig: Perceel 2 voorziet in deze product/dienstverlening
  
- BIO: de nieuwe normenkaders voor:
  - "Mobiele apparatuur en telewerken" en "Bedrijfseisen voor toegangsbeveiliging" stellen meer passende maatregelen verplicht.
- GGI-Veilig: de producten/diensten "Mailfiltering" en "Endpoint protection" uit perceel 2 van GGI-Veilig zijn hiervoor geschikt en stellen u in staat om volledig aan deze normen te voldoen.

Voorts ondersteunt GGI-Veilig perceel 2 op onderstaande wijze het voldoen aan de BIO:

- BIO: het voldoen aan nieuwe normenkaders voor "Mobiele apparatuur en telewerken" en "Informatietransport" worden ondersteund door VPN management services
- BIO: het voldoen aan nieuwe normenkaders voor "Naleving van wettelijke en contractuele eisen" worden ondersteund door VPN management services en DLP services
- BIO: het voldoen aan nieuwe normenkaders voor "Bescherming tegen malware" worden ondersteund door CASB en ATP services
- BIO: het voldoen aan nieuwe normenkaders voor "Beheer van netwerkbeveiliging" worden ondersteund door CASB en ATP services

Bij de ondersteunende GGI-Veilig producten/diensten wordt opgemerkt dat de noodzaak tot inzet ervan afhankelijk is van de eigen "ICT-situatie" en in sommige gevallen ook een verplichtend karakter kunnen hebben.

### BIO en GGI-Veilig perceel 3

- BIO: de nieuwe normenkaders voor:
  - "Beheer van technische kwetsbaarheden" en "Beveiliging in ontwikkelings- en ondersteunende processen" stellen het uitvoeren van pentesten verplicht,
- GGI-Veilig: Perceel 3 voorziet in deze dienstverlening
- De expertise dienst "SIEM proces ondersteuning" biedt deelnemers ondersteuning bij het op een goede wijze ingericht en geborgd hebben van het SIEM proces om controleerbaar te kunnen voldoen aan de BIO normenkaders voor "Verslag en monitoring"
- De expertise diensten "Compliance scanning" en "Vulnerability scanning" bieden ondersteuning bij het aantoonbaar kunnen voldoen aan wet- en regelgeving op het gebied van informatiebeveiliging en privacy bescherming