Position statement

BBN's in 2026

vhic bron van vernieuwing

Colofon

Uitgever:	VHIC, Einsteinlaan 26a, 2289 CC Rijswijk, www.vhic.nl
Auteur:	Gertjan van Heijst, Donna Schumacher
Versie:	1.1
Publicatiedatum:	19 januari 2026

Versiebeheer:

versie 1.1	19 januari 2026

BBN’s in 2026

Inleiding

De introductie van de Baseline Informatiebeveiliging Overheid 2 (BIO2) brengt een verandering met zich mee in de manier waarop overheidsorganisaties invulling moeten geven aan informatiebeveiliging. Waar de oorspronkelijke BIO een systematiek bood voor het classificeren van informatie en het bepalen van de basisbeveiligingsniveaus (de BBN-niveaus), richt de BIO2 zich primair op risicogestuurd werken en verwijst zij voor verdere uitwerking naar standaarden zoals de ISO 27001.

Deze benadering heeft als gevolg dat organisaties meer vrijheid krijgen om hun eigen risicobeoordelingsmethodiek vorm te geven. Tegelijkertijd ontstaat hierdoor ook onzekerheid: welke systematiek hanteer je wanneer de BIO2 zelf geen concrete handreikingen meer bevat? En hoe ga je om met het feit dat de vertrouwde BBN-niveaus niet langer worden benoemd, terwijl veel organisaties deze nog altijd gebruiken als basis voor hun beveiligingsmaatregelen en beleidskeuzes?

Wij krijgen regelmatig de vraag wat wij adviseren te doen met het vervallen van de BBN-niveaus in de BIO2 en met de Cyberbeveiligingswet. In dit position statement beantwoorden we deze vraag.

Huidige situatie

In de voorganger van de BIO2, de BIO, was een gedetailleerde methodiek opgenomen om organisatieonderdelen, informatieobjecten en informatiesystemen te beoordelen op de risicodimensies ‘beschikbaarheid’, ‘integriteit’ en ‘vertrouwelijkheid’ en om deze beoordelingen vervolgens samen te vatten in een algemene risicoclassificatie, het BBN-niveau. In de BIO2 wordt weliswaar het belang van risicoanalyses benadrukt, maar de wijze waarop dit moet worden ingevuld wordt alleen in algemene termen beschreven, door middel van verwijzingen naar de ISO 27001. Hierdoor wordt de verantwoordelijkheid voor het kiezen van een risicobeoordelingsmethodiek bij de organisatie zelf gelegd. Omdat veel organisaties de wijze waarop zij informatie beheren en beveiligen deels baseren op de inhoud van door VHIC ontwikkelde en beheerde modellen (model-DSP en PIV-framework), is het logisch dat wij ook om advies worden gevraagd.

Standpunt

Wanneer we kijken naar elementen van de risicobeoordelingsmethodiek die je zowel binnen als tussen organisaties zou willen standaardiseren, gaat het in essentie om twee onderdelen.

Ten eerste: de waardeset.

In de BIO wordt gewerkt met een driewaardige waardeset ‘hoog’, ‘midden’ en ‘laag’. Het valt echter ook te verdedigen om met vier-, vijf- of zelfs zevenwaardige waardesets te werken. Hoe meer waardes je hebt, hoe meer finetuning mogelijk is bij het kiezen van je beveiligingsmaatregelen.

Ten tweede: de betekenis van die waardes.

Hoe zorg je er nu voor dat wanneer twee verschillende domeindeskundigen allebei de waarde 'hoog’ hanteren, ze ook hetzelfde bedoelen? Dit kan alleen door de waardes – welke waardeset je ook kiest – heel precies te definiëren.

Het kiezen van een risicobeoordelingsmethodiek komt neer op het beantwoorden van de bovenstaande vragen. De in de BIO gehanteerde/beschreven methodiek geeft deze antwoorden. Alhoewel er zeker kanttekeningen te plaatsen zijn bij de kwaliteit van de gehanteerde definities, is deze methodiek de afgelopen jaren redelijk werkbaar gebleken. De BIO2 stelt hiervoor, zoals eerder aangegeven, geen (beter) alternatief beschikbaar.

Advies

Zolang er geen gestandaardiseerd beter alternatief beschikbaar is, adviseren wij organisaties de waardeset en de definities van de oorspronkelijke BIO te blijven hanteren. Een gezamenlijk gedragen vervangende risicoclassificatiemethode ontbreekt momenteel, waardoor het risico bestaat dat organisaties verschillende methoden zullen toepassen, er interpretatieverschillen zullen zijn, minder volwassen organisaties er zelf niet mee uit de voeten kunnen, en er versnippering ontstaat.

We begrijpen de overweging die in de BIO2 is gemaakt om het gebruik van BBN-niveaus los te laten. De risicobeoordeling waarop de BBN-niveaus zijn gebaseerd m.b.t.. beschikbaarheid, integriteit en vertrouwelijkheid geven namelijk betere handvatten om beveiligingsmaatregelen te selecteren dan de hiervan afgeleide BBN-niveaus. Daarnaast worden de BBN-niveaus in de BIO2 niet meer gebruikt voor de selectie van overheidsmaatregelen. De toegevoegde waarde van het gebruik van de BBN-niveaus is dus gering.

Tegelijkertijd kunnen we constateren dat de BBN-niveaus in het verleden breed zijn toegepast en dat het gebruik ervan ook geen extra complicaties met zich meebrengt. Dus mocht u in het verleden BBN-niveaus gebruikt hebben, dan is er ook geen dwingende reden om hier direct vanaf te stappen.

Conclusie

Ons advies luidt als volgt:

- **Blijf de waardeset en de definities gebruiken van de BIO1** tot er een overheidsbrede geaccepteerde betere methodiek voorhanden is.
- **Hanteert u momenteel BBN-niveaus in uw informatiebeveiligingsmethodiek**? Blijf dit dan doen tot er een breed geaccepteerd alternatief beschikbaar is.
- **Maakt u geen gebruik van BBN-niveaus**? Dan is er geen aanleiding om deze alsnog in te voeren.

Om dezelfde reden zullen de BBN-niveaus ook voorlopig nog zichtbaar blijven in de i-Navigator.

We staan open voor vragen en nadere uitwisseling over dit onderwerp. Wij volgen de ontwikkelingen rondom risicobeoordelingsmethodieken, de BIO2 en de Cyberbeveiligingswet nauwgezet. Op het moment dat er vernieuwde kaders of breed geaccepteerde methoden verschijnen, zal de redactie onze modellen en instrumenten altijd daaraan toetsen en zo nodig tijdig en zorgvuldig aanpassen, zodat u blijft beschikken over een actueel en goed toepasbaar product. Zo blijven wij u ondersteunen.

Meer informatie

Wil je meer weten over VIND Informatiemanagement en het PIV Framework?

Neem dan contact op met VHIC, via 088 053 5400 of info@vhic.nl. Wij vertellen je er graag meer over.