Toolkit Implementatie BIO

IFV | versie 2.0 | 20210805

Deze toolkit biedt de Veiligheidsregio's handreikingen om de eigen basis op orde te krijgen en te voldoen aan de BIO. Dit is een ondersteuningspakket dat randvoorwaarden biedt om als veiligheidsregio's cyberweerbaar te worden en te blijven.
Dit is een levend document dat continue in doorontwikkeling is naar aanleiding van de vragen die het landelijk implementatieloket zal ontvangen door regio's gedurende de regionale implementatie van de BIO.

Alle tools in de toolbox hebben e
TLP:wit = openbaar
TLP:amber= het document bevat vertrouwelijke informatie dat relevant is voor u als gebruiker en niet verder verspreid mag worden zonder toestemming van de betreffende organisatie/auteur.

Hulpmiddel	Toelichting	Doelgroep	Waarvoor te gebruiken?	Bron	Waar te vinden?	Classificatie (wordt bepaald door opsteller/eigenaar)	Toelichting classificatie
BIO Zelftoets		Directeuren Bedrijfsvoering / Veiligheidsregio's / CISO	Hulpmiddel bij aantoonbaar maken dat er voldaan wordt aan de maatregelen uit de verplichte norm Baseline Informatiebeveiliging Overheid (BIO)	Saxion Hogeschool / VR-ISAC		**Classificatie n.t.b.**	
BIO Self-Assessment	De BIO-Self Assessment van het CIP	Algemeen	BIO-SA is een krachtig doe-het-zelf instrument om te meten hoe volwassen de organisatie omgaat met informatiebeveiliging. Het is ook een stuurinstrument voor stapsgewijze planmatige verbetering en een krachtig middel voor het vergroten van bewustwording bij management en medewerkers.	CIP	https://cip-overheid.nl/productcategorie%c3%abn-en-worshops/producten/bio-en-thema-uitwerkingen/#BIO-SA	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
ISOR (Information Security and Object Repository)	De ISOR is een verzameling themagerichte normenkaders die hulp bieden bij de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Zij geven gedetailleerd aan hoe een organisatie kan voldoen aan de BIO. De ISOR wordt beheerd door het Centrum Informatiebeveiliging en Privacybescherming (CIP).	CISO / Architect	Hulp implementatie BIO	NORA	https://www.noraonline.nl/wiki/ISOR	**Openbaar (TLP:wit)**	Openbaar

Informatieplattegrond	De informatieplattegrond helpt veiligheidsregio's grip op hun gegevens(management) te houden. Het maakt bovendien kwetsbaarheden en risico's voor de interne informatievoorziening inzichtelijk. Zeer relevant dus, in tijden met meer cyberaanvallen en kans op datalekken dan ooit. Ricardo tekst aanleveren Inzicht in ICT-foto (applicatie- en informatielandschap) is noodzakelijk om fase II versnellingsprogramma te kunnen starten.	CISO / Architect	Inzichtelijk maken van kritieke infrastructuur (processen en informatie). voor meer informatie, zie: https://www.ifv.nl/nieuws/Paginas/Informatieplattegrond-beschikbaar-in-Ve.aspx	VeRa online	https://www.veraonline.nl/index.php/Bedrijfsinformatiemodel_Veiligheidsregio_(BIM)	**Classificatie n.t.b**	
Baseline Informatiebeveiliging Overheid (BIO) v1.04	Het gebruik van teksten uit normen in de BIO geschiedt met toestemming van het Nederlands Normalisatie Instituut.	Directie / mgt Bedrijfsvoering overheid	De Baseline Informatiebeveiliging Overheid (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector.	VNG	https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
FAQ Versnellingsplan	De FAQ is tot stand gekomen door de VR-ISAC en dient als hulpmiddel om de meest gestelde vragen en antwoorden in kaart te brengen.	Directeuren Bedrijfsvoering / Veiligheidsregio's / CISO	Hulpmiddel om de meest gestelde vragen en antwoorden die kunnen worden gesteld aan het implementatieloket rondom het versnellingsprogramma in kaart te brengen.	IFV	https://www.ifv.nl/kennisplein/Documents/20210720-VR-ISAC-FAQ-Versnellingsplan-Informatieveiligheid.pdf.pdf	**Openbaar (TLP:wit)**	Openbaar
Windows basisconfiguratie voor loggen	De JSCU (AIVD & MIVD) heeft een basisconfiguratie voor het loggen op Github geplaatst. Met de introductie van een basisconfiguratie willen de diensten zorgen voor een hoge(re) mate van weerbaarheid tegen aanvallen van geavanceerde (statelijke) actoren. Zo worden organisaties in staat gesteld om deze in een vroegtijdig stadium te detecteren.	ICT-specialisten	Hierdoor kunnen ICT-specialisten handelingen op Windows-computers binnen hun netwerk zodanig registreren dat zelfstandige detectie van kwaadwillenden beter kan plaatsvinden. Gebruikers kunnen deze basisconfiguratie implementeren en al dan niet met tussenkomst van een commerciële partij de detectie uitvoeren. De basisconfiguratie is voor iedereen beschikbaar en rechtenvrij over te nemen.	AIVD	https://www.aivd.nl/actueel/nieuws/2021/04/22/joint-sigint-cyber-unit-vanaf-nu-actief-op-github	**Openbaar (TLP:wit)**	Openbaar
Toolbox cyberincident	Wat betekent het voor uw organisatie als deze wordt geraakt door een cyberincident.	Directie / mgt Bedrijfsvoering gemeenten	Wat te doen bij een cyberincident. Iedere stap delen ervaringsdeskundigen – deelnemers en sprekers aan de overheidsbrede cyberoefening- hun tips en trucs.	Digitale Overheid	https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/oefenen-en-kennisdelen/toolbox-cyberincident/	**Openbaar (TLP:wit)**	
Handreiking bij Volwassenheidsmodel Informatiebeveiliging	Inhoudelijk stuk over de manier waarop gemeenten het volwassenheidsniveau kunnen verhogen	Directie / mgt Bedrijfsvoering gemeenten	Het volwassenheidsmodel heeft tot doel de interne audit afdelingen alsmede de directies van organisaties een leidraad en handvaten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging.	NBA	handreiking_volwassenheidsmodel_informatiebeveiliging.pdf	**Openbaar (TLP:wit)**	

Verhogen digitale weerbaarheid	Gemeenten groeien in volwassenheid van informatiebeveiliging. De focus verschuift van reageren op incidenten naar het herkennen en voorkomen van incidenten.	Directie / mgt Bedrijfsvoering gemeenten	Een digitaal weerbare gemeente kan potentiële incidenten vroegtijdig signaleren en de gevolgen ervan beperken, omdat de juiste maatregelen zijn getroffen.	VNG	https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
Introductie aanpak BIO	Introductie aanpak BIO. Het ondersteunen van proceseigenaar en de CISO bij het procesmatig omgaan met de BIO	CISO gemeenten	Hoe implementeren gemeenten de BIO en hoe ziet het proces er dan uit	VNG	https://www.informatiebeveiligingsdienst.nl/product/introductie-aanpak-bio/	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
Aanpak BIO voor kleine gemeenten	Aanvulling op Introductie aanpak BIO, voor kleine gemeenten	Directie / mgt Bedrijfsvoering / Veiligheidsregio's / CISO	Een operationeel kennisproduct ter ondersteuning van de implementatie van de (BIO)	VNG	https://www.informatiebeveiligingsdienst.nl/product/handreiking-bio-voor-kleine-gemeenten/	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
Aanpak Informatie-beveiligingsbeleid BIO gemeenten	Aanvulling informatiebeveiligingsbeleid om aan te geven welke doelen bestuurders en managers willen bereiken rond informatiebeveiliging.	Directie / mgt Bedrijfsvoering / Veiligheidsregio's / CISO	Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)	VNG	https://www.informatiebeveiligingsdienst.nl/product/handreiking-informatiebeveiligingsbeleid-bio/	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
Baseline Toets BBN BIO	Toets ten behoeve van verbeteren proces en/of als start voor project/informatiesysteem	Directie / mgt Bedrijfsvoering / Veiligheidsregio's / CISO	1. Bepalen of een proces, informatiesysteem en/of informatie een bepaald Basis Beveiligings Niveau (BBN) heeft binnen de BIO, of meer maatregelen nodig heeft en 2. Voor fase start project-/ informatiesysteem opstellen Baseline BIO door procesverantwoordelijke.	VNG	https://www.informatiebeveiligingsdienst.nl/product/baseline toets-bbn-bio/	**Openbaar (TLP:wit)**	Let op!! Veel van deze producten/handreikingen zijn Openbaar te vinden via de VNG Web site en hebben dus de classificatie Openbaar (TLP:wit). Op het moment dat een regio de handreiking invult op basis van regionale gegevens die beschikbaar zijn in de regio, verdient het de classificatie TLP:amber. de opsteller bepaalt het classificatieniveau.
GAP analyse BIO v2.3	Aangepast aan de versie GAP BIO 1.04	Directie / mgt Bedrijfsvoering / Veiligheidsregio's/ CISO	Update GAP analyse	VNG	https://www.informatiebeveiligingsdienst.nl/product/gap-analyse-1-2-alle-sheets/	**Openbaar (TLP:wit)**	

Maatregelenset BBN2+	Een best practice set van maatregelen die passend is om informatie boven BBN2 adequaat te beschermen. Kan in plaats van een diepgaande risicoanalyse gebruikt worden.	Directie / mgt Bedrijfsvoering / Veiligheidsregio's / CISO	Een best practice set van maatregelen die passend is om informatie boven BBN2 adequaat te beschermen. Kan in plaats van een diepgaande risicoanalyse gebruikt worden. Er geldt een aanpak op basis van een eigen risicoinschatting en geen verplichting. De set kan vrijelijk gebruikt worden om (geheel of gedeeltelijk) te implementeren. De set is tevens te gebruiken bij afspraken binnen ketens en met leveranciers. Bij een score boven BBN2 moeten nog steeds alle verplichte maatregelen van BBN1 en BBN2 geimplementeerd worden, de BBN2+-set is nadrukkelijk een aanvulling. De set is aangevuld met een suggestie voor het aanwijzen van de verantwoordelijke functionaris, maar dit is een suggestie, zie ook BIO 2.7. Daarnaast zijn de maatregelen ingedeeld naar BIV en voorzien van een MAPGOOD-aspect (Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten).	VNG	https://www.informatiebeveiligingsdienst.nl/product/maatregelenset-bbn2/	**Openbaar (TLP:wit)**	
Diepgaande risico analyse methode gemeenten	Versie 2.1 Aangepast naar aanleiding van BBN3 anders waarderen	Directie / mgt Bedrijfsvoering gemeenten	Het bieden van een instrument om risicoanalyses uit te voeren indien de uitkomst van de baselinetoets dit als resultaat geeft.	VNG	https://www.informatiebeveiligingsdienst.nl/product/diepgaande-risicoanalyse-methode-excel/	**Openbaar (TLP:wit)**	
NEN/ISO 27001 / 2	NEN-NL-ISO/IEC 27001 en NEN-NL-ISO/IEC 27002, voor de implementatie van een goede BIO.	Directie / mgt Bedrijfsvoering gemeenten	Bij de implementatie van de Baseline Informatiebeveiliging Overheid (BIO) kunt u gebruik maken van de NEN/ISO-normen.	VNG	https://www.informatiebeveiligingsdienst.nl/nen-iso-27001-2/	**Openbaar (TLP:groen)**	
Handreiking Dataclassificatie	Deze classificatie is een basis voor de maatregelselectie of een aanvullende risicoanalyse	Directie / mgt Bedrijfsvoering gemeenten	Inzicht krijgen in de waarde van informatie over de assen Beschikbaarheid, Integriteit en Vertrouwelijkheid d.m.v. classificatie.	VNG	https://www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/	**Openbaar (TLP:wit)**	
Handreiking Cybersecurity maatregelen	Kort stappenplan en richting om optimale cyberweerbare organisatie in te richten.	Directie / mgt Bedrijfsvoering gemeenten	De maatregelen in de handleiding helpen bij cyberincidenten.	NCSC MinJenV	https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen	**Openbaar (TLP:wit)**	