BIO | Baseline Informatiebeveiliging Overheid

voor een veilige digitale overheid

FAQ’s Baseline Informatiebeveiliging Overheid

v1.12 definitief (publicatiedatum 20 januari 2023)

Rijksoverheid

Interprovinciaal Overleg ipo

VNG Vereniging van Nederlandse Gemeenten

UNIE VAN WATERSCHAPPEN

Inhoudsopgave

De vragen en antwoorden zijn ingedeeld in de volgende hoofdonderwerpen.

Onderaan dit document is de lijst met alle vragen met directe links naar de antwoorden opgenomen.

Algemeen

1. Wat is een baseline?

Naar vragenlijst

Een baseline voor informatiebeveiliging geeft het basisniveau van informatiebeveiliging weer waar elke overheidspartij minimaal aan moet voldoen.

2. Wat houdt de BIO precies in?

Naar vragenlijst

De Baseline Informatiebeveiliging Overheid (BIO) is een normenkader voor informatiebeveiliging en geeft het basisniveau weer voor informatiebeveiliging waar alle overheidspartijen aan moeten voldoen. Het is gebaseerd op de internationale standaarden voor informatiebeveiliging: NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017. Door dit eenduidige normenkader binnen de overheid, wordt een stevige basis gelegd voor de verdere optimalisering van informatiebeveiliging binnen de gehele overheid en ontstaat een gemeenschappelijke taal die bijdraagt aan veilige samenwerking in ketens binnen de overheid.

3. Waarom is de BIO nodig?

Naar vragenlijst

Voorheen had elke overheidslaag een baseline op het gebied van informatiebeveiliging: BIR (Rijksoverheid), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Met uitzondering van de BIR 2017, waren deze baselines gebaseerd op eerdere versies van de NEN-EN-ISO/IEC 27001: 2013 en NEN-EN-ISO 27002: 2013 en moesten nog geactualiseerd worden. Ook waren er verschillen tussen de baselines van de diverse overheidslagen, terwijl door ketensamenwerking zeer veel informatie-uitwisseling tussen overheidslagen plaatsvindt. Een gezamenlijk normenkader maakt ketensamenwerking veel makkelijker en efficiënter. Ook voor leveranciers is dit prettig. Zij hebben bij alle overheidsorganisaties te maken met dezelfde eisen op het gebied van informatiebeveiliging.

4. Welke voordelen zijn er verbonden aan de BIO?

Naar vragenlijst

Eén gezamenlijke baseline voor alle overheidsorganisaties biedt vele voordelen. Het draagt bij aan informatieveiligheid, zorgt voor eenduidigheid en leidt bovendien tot kostenbesparing. Verder:

- eenduidig en helder basisniveau van informatiebeveiliging voor alle overheidsorganisaties;

- betere en makkelijkere samenwerking tussen diverse overheidsorganisaties en partners;
- verlichten van administratieve lasten, omdat er nu aan één beveiligingsnorm moet worden voldaan;
- door gemeenschappelijke taal kunnen partijen makkelijker communiceren en effectiever opereren;
- één overheidsbrede baseline stimuleert onderlinge kennisuitwisseling, professionals kunnen van elkaar leren en verbeteren.

5. Voor wie is de BIO bedoeld?

Naar vragenlijst

Voor alle Nederlandse overheidsorganisaties en aan overheidsgelieerde organisaties.

6. Is de BIO verplicht?

Naar vragenlijst

De BIO moet verplicht door alle bestuurslagen worden nageleefd. Dit is vastgelegd in de circulaire Toepassen van de Baseline Informatiebeveiliging Overheid versie 1.04 in het digitale verkeer met het Rijk van 19 december 2019 (2019-0000684575). Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt gewerkt aan wettelijke verankering van de BIO in de Wet digitale overheid. Voor meer informatie zie digitaleoverheid.nl.

7. Is de BIO ook verplicht voor ZBO's als zij met het moederdepartement communiceren?

Naar vragenlijst

Artikel 41 van de kaderwet ZBO's geeft aan dat de voor de rijksdienst geldende voorschriften op het gebied van gegevensbeveiliging ook van toepassing zijn op de (kaderwet-)ZBO's:

Kaderwet ZBO's geldend van 01-07-2022 t/m heden, Artikel 41:

1. *Een zelfstandig bestuursorgaan draagt op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorg voor de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.*
2. *Onze Minister kan bepalen dat het eerste lid niet van toepassing is op een zelfstandig bestuursorgaan.*

Daarnaast heeft de Ministerraad op 14 december 2018 besloten om de BIO te hanteren in de informatie-uitwisseling tussen het Rijk en alle bestuurslagen. Dit is bevestigd in de circulaire van 9 januari 2020 waarmee de BIO van toepassing wordt verklaard, zie antwoord 6. Los van de specifieke afspraken die een departement met haar ZBO's maakt, is elke overheidspartij verplicht in het digitale verkeer met het Rijk verplicht de BIO te hanteren.

8. Wat is de relatie tussen de BIO en de BIR, BIG, BIWA en IBI?

Naar vragenlijst

De BIR (Rijksoverheid), BIG (gemeenten), BIWA (waterschappen) en de IBI (provincies) waren de baselines per overheidslaag voor de invoering van de BIO. De BIO vervangt deze baselines. Dit betekent overigens niet dat alle organisaties nu compleet andere normen hebben om aan te voldoen. De BIR 2017 was bijvoorbeeld al gebaseerd op de destijds actuele ISO 27001- en 27002-normen. Daarnaast zijn er voor de BIO-keuzes gemaakt in welke maatregelen verplicht gesteld worden (dit verschilde eerder ook per baseline). Het grootste gedeelte van de BIO is op inhoud gelijk aan de eerdere baselines.

9. Wat is er gebeurd met de BIR, BIG, BIWA en IBI?

Naar vragenlijst

De baselines BIR, BIG, BIWA en IBI zijn komen te vervallen. De BIO is hiervoor in de plaats gekomen.

10. Wat is er anders in de BIO dan de BIR, BIG, BIWA en IBI?

Naar vragenlijst

De BIO is gebaseerd op de NEN-EN-ISO/IEC 27001:2017 en de NEN-EN-ISO/IEC 27002:2017. Er is meer nadruk komen te liggen op risicomanagement. Hierdoor zal, ten opzichte van de meeste voorlopende baselines, het aantal verplicht gestelde maatregelen zijn afgenomen. Organisaties moeten zelf wel maatregelen definiëren om aan de controls te voldoen. Ook de basisbeveiligingsniveaus (BBN's) zijn nieuw, met uitzondering voor de organisaties die eerder de BIR 2017 hanteerde. Daarnaast is er meer aandacht voor handreikingen en thematische uitwerkingen en is er een duidelijke onderhoudscyclus ingericht.

11. Hoe is de BIO tot stand gekomen?

Naar vragenlijst

Iedere overheidslaag heeft besloten de bestaande baseline informatiebeveiliging voor hun bestuurslaag te vervangen door de BIO. De besluitvorming hiertoe heeft per bestuurslaag plaatsgevonden.

12. Op welke wetgeving is de BIO gebaseerd?

Naar vragenlijst

De BIO is (nog) niet op wetgeving gebaseerd, wel op internationale standaarden, de NEN-EN-ISO/IEC 27001:2017 en de NEN-EN-ISO/IEC 27002:2017. Deze zijn als verplicht te gebruiken standaarden opgenomen op de pas-toe-of-leg-uit-lijst van het forum standaardisatie, zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit.

Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt gewerkt aan wettelijke verankering van de BIO, zie antwoord 6.

13. Waar kan je de tekst van de BIO vinden?

Naar vragenlijst

De volledige tekst van de BIO versie 1.04 is op 11 februari 2020 in de Staatscourant gepubliceerd. De meest actuele versie, versie 1.04zv, dat is de versie zonder verwijzingen, kun je downloaden via de informatiepagina's van de koepels en op https://bio-overheid.nl/media/1400/70463-rapport-bio-versie-104_digi.pdfhttps://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf.

14. Wat is de NIST en wat is de relatie met de BIO?

Naar vragenlijst

De NIST (National Institute of Standards en Technolgy) is een organisatie die onder de Amerikaanse federale overheid valt. De NIST heeft ook een methode voor informatiebeveiliging ontwikkeld. Er zijn wereldwijd diverse standaarden en methoden ontwikkeld, variërend van standaarden die het volledige proces beschrijven tot standaarden en methoden die een specifiek onderdeel ondersteunen.

Voorbeelden van standaarden die het volledige proces van informatiebeveiliging beschrijven:

- de ISO/IEC 27000-serie (waar de BIO op is gebaseerd)
- de NEN 7510-serie voor de medische sector (is een sectorspecifieke uitwerking van de ISO/IEC 27001)
- NIST special publications 800-serie
- BSI 100-2- tot 100-4-serie

Kijk voor meer informatie over de NIST op de website https://www.nist.gov/.

15. Is er een inhoudelijke visie over de richting van de ontwikkeling van de BIO? Zo ja, waar is dit vastgelegd?

Naar vragenlijst

In paragraaf 1.4 van de BIO staat beschreven hoe evaluatie en bijstelling van de BIO plaatsvindt. Bij de vaststelling van de BIO over het bijstellen het volgende besloten: 'De BIO is door de algemene opzet beoogd onderhoudsarm te zijn. Het onderhoud van de BIO, na vaststelling, vindt cyclisch plaats in de BIO Werkgroep, vanuit

samenwerking tussen DGOO/DIO, gemeenten, waterschappen, CIO rijk en provincies.'.

16. Is er een strategie gedefinieerd en afgestemd met de beleidsopdrachtgever hoe de norm verder ontwikkeld en gehanteerd dient te worden?

Naar vragenlijst

Er is een beheer- en onderhoudsplan opgesteld voor de BIO. Per overheidslaag is 0,1 fte beschikbaar gesteld om het onderhoud gestalte te geven. Het is de verantwoordelijkheid van de lijnmanagers binnen de overheidslagen om de BIO feitelijk te implementeren. Om de implementatie te bevorderen, is een ondersteuningsprogramma opgezet om de invoering van de BIO te stimuleren. Kijk daarvoor op www.bio-overheid.nl of op de website van jouw koepel.

17. Is er beleid over het gebruik van standaarden? Zo ja, wordt er in samenspraak met de beleidsopdrachtgevers hieraan invulling gegeven?

Naar vragenlijst

Ja, in paragraaf 1.5 van de BIO staat hoe de overheid met de standaarden van het Forum Standaardisatie omgaat.

ISO 27001/27002

18. Wat is de relatie tussen de BIO en ISO 27001/27002?

Naar vragenlijst

De NEN-EN-ISO/IEC 27002:2017 en NEN-EN-ISO:2017 vormen de basis van de BIO. Het grootste gedeelte van de BIO is feitelijk ISO. Daaraan zijn toegevoegd specifieke maatregelen die de overheid relevant acht in de bescherming van haar informatie. Ook is er onderscheid gemaakt in basisbeveiligingsniveaus in de BIO.

19. Waarom gebruiken we de ISO 27002 niet als baseline?

Naar vragenlijst

Er is gekeken naar de te beschermen belangen en risico's binnen de overheid. Op basis daarvan is bepaald welke controls bij welk basisbeveiligingsniveau van toepassing zijn. Daarnaast zijn als verdieping nog verplichte maatregelen gedefinieerd die noodzakelijk worden geacht voor een goede bescherming van overheidsinformatie. Het verschil tussen de BIO en de ISO 27002 is dat de ISO implementatieaanwijzigingen bevat en de BIO bevat concrete overheidsmaatregelen. De BIO zorgt daarmee voor twee zaken die de ISO 27002 niet doet:

- Het helpt organisaties in het bepalen van welke controls er nodig zijn op basis van het te beschermen belang (TBB), dat weer vertaald is naar een BBN.

- Het stelt een aantal overheidsmaatregelen verplicht die noodzakelijk zijn voor een goede beveiliging van informatie binnen de overheid.

20. Op welke versie van de ISO 27001 en 27002 is de BIO gebaseerd?

Naar vragenlijst

Versie 1.04zv van de BIO is gebaseerd op de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. In 2023 verschijnt versie 2.0 van de BIO die gebaseerd wordt op de meest actuele versie van deze twee standaarden.

21. Zijn de implementatierichtlijnen uit de ISO 27002 verplicht?

Naar vragenlijst

Nee, de implementatierichtlijnen uit de ISO 27002 zijn niet verplicht, maar ze kunnen zeker helpen bij het bepalen van maatregelen om invulling te geven aan de controls van de BIO. Je kunt de implementatierichtlijnen uit de ISO zien als best practices.

22. Wat gebeurt er als er een nieuwe versie van de ISO uitkomt?

Naar vragenlijst

Conform de onderhoudscyclus op de BIO volgt er een nieuwe versie van de BIO. Versie 2.0 van de BIO zal gebaseerd worden op de ISO/IEC 27001:2022 en de NEN-EN/IEC 27002:2022, die al verwerkt is in de handreiking Indeling BIO v1.0.4zv aan ISO/IEC 27002:2022.

Basisbeveiligingsniveaus (BBN's)

23. Spreken we in het kader van de BIO over risicoanalyse of risicoafweging?

Naar vragenlijst

Dat verschilt per maatregel. Een risicoanalyse is vaak gebaseerd op een expliciete formele methodische aanpak en een risicoafweging is meer free format en hoeft ook niet vastgelegd te worden. In de BIO kom je ook de term expliciete risicoafweging tegen, in feite wordt dan een risicoanalyse bedoeld.

24. Wat houden de BBN's in?

Naar vragenlijst

De basisbeveiligingsniveaus helpen om risicomanagement hanteerbaar en efficiënt te houden. Door te kijken naar de betrouwbaarheidseisen (beschikbaarheid, integriteit en vertrouwelijkheid) die gesteld worden aan de informatie die beveiligd moet worden en de dreigingen die er zijn, wordt bepaald welke set aan maatregelen relevant is voor een adequate beveiliging van die informatie.

25. Wat houdt elk BBN in?

Naar vragenlijst

Bij BBN1 gaat het om wat er minimaal verwacht mag worden van de overheid voor de bescherming van informatie. We hebben hier te maken met een laag betrouwbaarheidsniveau en daarom blijven complexe eisen achterwege. Het gaat puur om een minimale basis.

Bij BBN2 komen we op het niveau waar de meeste informatie van de overheid in valt. Het gaat hier om goed huisvaderschap voor informatie. BBN2 is het standaardniveau. Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV) (zoals gedefinieerd in het VIR-BI) /vergelijkbaar vertrouwelijk bij andere overheidslagen en privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau. Bij BBN2 ligt voor statelijke actoren en vergelijkbare dreigingen de nadruk op 'detectie'.

BBN3 vergt aanvullende maatregelen om weerstand te kunnen bieden tegen statelijke actoren of criminele organisaties (of gelijksoortige actoren) of waar informatie wordt verwerkt die door de bronhouder een bepaalde classificatie (boven BBN2) heeft meegekregen. De BIO schrijft voor BBN3 geen standaard maatregelen voor, aangezien op dit niveau vanwege de hoge complexiteit veelal maatwerk is vereist. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van NAVO- en EU-normen.

26. Wat is het nut van BBN1?

Naar vragenlijst

Bij de baselines BIR, BIG, BIWA en IBI moest elk systeem op een hoog basisniveau worden beveiligd. Met BBN1 is het mogelijk om voor eenvoudigere bedrijfsprocessen zonder vertrouwelijke informatie aan minder complexe risicomanagement en verantwoordingseisen te voldoen, waarbij nog altijd wel een minimum beveiligingsniveau wordt gewaarborgd.

27. Wat is het verschil tussen BBN2 en BBN3?

Naar vragenlijst

BBN3 beoogt actieve bescherming tegen statelijke actoren, criminele organisaties en gelijksoortige actoren. De eisen aan vertrouwelijkheid liggen hier hoger dan op BBN2.

Binnen de BIO-context kan het hogere beschermingsniveau van BBN3-maatregelen ook van toepassing zijn op BBN2-informatie, maar ook op BBN1-informatie. In feite is BBN3 niet het logische gevolg op BBN2, maar een heel eigen norm voor maar één doel: actieve weerstand bieden tegen statelijke actoren, criminele organisaties of vergelijkbare actoren.

28. Wordt BBN3 als complete set van maatregelen toegevoegd aan de BIO?

Naar vragenlijst

Met name waar het gaat om het hoogste basisbeveiligingsniveau, BBN3, dat actieve weerstand moet bieden tegen dreigingen van statelijke actoren, is geconstateerd dat maatwerk is vereist. Ministeries doen dit bijvoorbeeld door het implementeren van een geschikte set van beveiligingsmaatregelen uit de geldende EU- en NATO-kaders. Aangezien onvoldoende toegevoegde waarde wordt verwacht van een algemene overheidsbrede standaard voor BBN3 wordt afgezien van uitbreiding van de BIO op dit punt. Indien daar in een later stadium toch behoefte aan blijkt te bestaan bij de Rijksdienst of bij andere bestuurslagen, zal dit in het reguliere onderhoudsproces van de BIO worden meegenomen.

Zie: https://www.rijksoverheid.nl/documenten/rapporten/2020/05/01/strategische-i-agenda-rijksdienst-2019-2021-editie-2020.

29. Hoe kom je tot het juiste BBN?

Naar vragenlijst

Hiervoor is een baselinetoets beschikbaar en beschreven in de BIO. Op basis van een aantal vragen wordt duidelijk welk BBN van toepassing is. De proceseigenaar bepaalt op basis van de toets welk BBN gevolgd dient te worden. De Rijksoverheid heeft daarnaast een Quickscan (QIS) beschikbaar die meer in detail uitgewerkt is dan hetgeen in de BIO beschreven is.

30. Wanneer zijn BBN3-maatregelen nodig?

Naar vragenlijst

Ongeacht wat de uitkomst van de baselinetoets is, bijvoorbeeld BIV=LLL, BIV=MMM of BIV=HHL, zijn er 3 vragen die gesteld moeten worden om op het niveau van BBN3 uit te komen:

1. Is er weerstand vereist tegen statelijke actoren?

2. Heeft de informatie die ontvangen is een bepaalde classificatie (boven BBN2) meegekregen van de (externe) bronhouder?

3. Is er weerstand nodig tegen georganiseerde misdaad en zware criminaliteit?

Als één van deze vragen met Ja wordt beantwoord, is BBN3 van toepassing.

De basisgedachte achter de BIO is dat er minder overheidsmaatregelen zijn en dat de proceseigenaar op basis van een risicoafweging zelf de ontbrekende maatregelen moet selecteren, dan wel toevoegen aan de minimale en verplichte set die opgenomen is in de BIO. Dit geeft de proceseigenaar meer vrijheid en zorgt ervoor dat het proces van risicomanagement op die plaats kan worden uitgevoerd waar het risico daadwerkelijk optreedt en behandeld moet worden.

31. Wat als er meer nodig is dan BBN2 en hoe zit dat met ontbrekende maatregelen?

Naar vragenlijst

In alle gevallen moet de proceseigenaar een risicoafweging maken, want hij is verantwoordelijk voor het proces. Hij moet de risico's die zijn proces loopt accepteren, mitigeren, overdragen of vermijden. Hierbij geldt wel: hoe hoger het belang, hoe minder keuzevrijheid in het kiezen van maatregelen of het accepteren van risico. Daarbij geldt ook dat een proceseigenaar geen keuze kan maken als het risico zijn afdeling of proces overstijgt en de hele organisatie of ketens raakt. Iedere BBN heeft zijn eigen verantwoordelijkheidsniveau en dat is uitgewerkt in de BIO binnen hoofdstuk 4.1.

Gemeenten hebben vanuit hun ondersteuningsorganisatie Informatiebeveiligingsdienst (IBD) de beschikking over een set met maatregelen die zij BBN2+ noemen. Deze set is een aanvulling op BBN2 en is niet verplicht. Het is een aanvulling als tijdens een BBN-toets een score V=hoog gehaald wordt.

32. Is BBN een vervanging van de TBB?

Naar vragenlijst

Nee, een TBB (Te Beschermen Belang) is het belang dat beschermd moet worden. Dit komt overeen met wat in de NEN-EN-ISO/IEC 27001:2017 wordt beoogd met 4.1 (Inzicht in de organisatie en haar context) en 4.2 (Scope en doelstellingen). Een BBN is een classificatieniveau dat vervolgens op het TBB van toepassing is.

33. Wat is risicomanagement in het kader van de BIO?

Naar vragenlijst

Risicomanagement gaat in feite over het bepalen welke risico's jouw organisatie mogelijk loopt en welke risico's je op welke wijze kunt beheersen. Risicomanagement is een continu proces waarbij in kaart wordt gebracht welke risico's er zijn, hoe groot de kans is dat een risico manifest wordt en wat de gevolgen hiervan zijn. Op basis van risicobereidheid wordt bekeken hoe deze risico's worden beheerst.

34. Hoe gebruikt je risicomanagement om tot maatregelselectie te komen?

Naar vragenlijst

Door risico's te inventariseren, kun je kijken welke maatregel in afdoende mate kan voorkomen dat een specifiek risico manifest wordt, dan wel dat de schade ervan beperkt blijft. Het zorgt ervoor dat te nemen maatregelen, passen bij de daadwerkelijke risico's. Immers 100% veiligheid is nooit mogelijk en ook niet wenselijk, alleen al niet vanwege de hoge kosten die vaak komen kijken bij het implementeren van maatregelen. Door goed te kijken naar de risico's en te bepalen wat wel en niet acceptabel is voor jouw organisatie, kun je ook bepalen hoe ver je wilt gaan in de maatregelen die je treft en welke maatregelen ook daadwerkelijk een risico kunnen verkleinen.

35. Wat houden de BBN-toets en de Quickscan in?

Naar vragenlijst

De BNN-toets en de QuickScan zijn vergelijkbaar. De BBN-toets is ontwikkeld door de IBD. Bij het rijk heet deze toets de QIS (oorsprong BIR 2017). Aan de hand van deze toetsen is het BBN-niveau te bepalen. Je beantwoordt een aantal vragen die uiteindelijk een antwoord geven op het BBN die nodig is voor jouw informatiesysteem of proces.

36. Bestaat er een handreiking van de Quickscan (QIS) voor de BIO?

Naar vragenlijst

Nee, een nieuwe versie van de handreiking QIS is niet gemaakt. De reeds bestaande BIR-versie van de QIS is goed bruikbaar bij de BIO. Er bestaat wel een handreiking Quick Scan Information Security die het ministerie van Binnenlandse Zaken en Koninkrijksrelaties destijds bij de BIR heeft opgesteld. Daarnaast bestaat de BBN-toets van de IBD.

37. Wat is het verschil tussen het BBN en de BIV?

Naar vragenlijst

Het BBN is een meetlat op basis van schadescenario's en het te beschermen belang. De BIV zijn de betrouwbaarheidscriteria Beschikbaarheid, Integriteit en Vertrouwelijkheid waarlangs informatiebeveiliging wordt ingericht.

Controls en maatregelen

38. Wat zijn controls?

Naar vragenlijst

Een control is een beheersmaatregel waarmee specifieke veiligheids- en bedrijfsdoelstellingen van de organisatie kunnen worden gehaald. De NEN-EN-ISO/IEC 27002:2022 gebruikt de term beheersmaatregel, de BIO de term control. Verwar de overheidsmaatregel uit de BIO niet met een beheersmaatregel.

39. Waarom is er geen onderscheid tussen systeem-specifieke controls en organisatie-brede controls?

Naar vragenlijst

Dit onderscheid wordt gemaakt door de toewijzing van de controls aan de rollen (organisatie-breed), proceseigenaar (specifiek) en dienstenleverancier (specifiek). Als blijkt dat er behoefte is aan een dergelijke nadere uitsplitsing, dan zal hier een handreiking voor opgesteld worden.

40. Hoe weet je of een control helemaal is afgedekt?

Naar vragenlijst

De eigenaar van een informatiesysteem bepaalt op basis van een risicoafweging welke maatregelen per control moeten worden genomen om deze af te dekken. De implementatierichtlijnen uit de ISO 27002 kunnen daarbij als inspiratiebron worden gebruikt. De verzameling te nemen maatregelen per control omvat in ieder geval de bij die control behorende overheidsmaatregelen.

41. Wat moet je doen als een control niet van toepassing is?

Naar vragenlijst

Als een control of een overheidsmaatregel voor een specifiek geval niet van toepassing kan zijn, vervalt deze binnen de gegeven scope om verplicht te worden ingericht, maar dan moet er wel een verklaring worden gemaakt (NVTV). Dit geldt bijvoorbeeld bij een control die betrekking heeft op een externe koppeling, terwijl het betreffende systeem geen externe koppeling heeft.

42. Wat zijn overheidsmaatregelen?

Naar vragenlijst

Overheidsmaatregelen uit de BIO geven invulling aan het bereiken van de beveiligingsdoelstellingen en controls (beheersmaatregelen).

43. Zijn de maatregelen uit BIR 2017 inhoudelijk veranderd in de BIO?

Naar vragenlijst

De BIO is direct ontleend aan de BIR 2017. Verschillen zijn tekstueel van aard en betreffen vooral terminologie die veranderd is door de verbreding van het Rijk naar de gehele overheid. Bij de invoering van de BIO is deze inhoudelijk gelijk gehouden aan de BIR 2017.

NB Sinds de invoering van de BIO wordt alleen de BIO onderhouden en niet meer de BIR 2017. De BIR 2017 is vervallen.

44. Zijn alle maatregelen vanuit privacyregelgeving ook opgenomen in de BIO?

Naar vragenlijst

Nee, artikel 32 van de AVG wordt door de BIO afgedekt. Indien je persoonsgegevens beschermt, helpt de BIO bij het invulling geven aan passende organisatorische en technische beveiligingsmaatregelen. Voor een overzicht van belangrijkste AVG-verplichtingen raadpleeg de handreiking Privacy Baseline. Gemeenten hebben een vergelijkbare uitwerking: Privacy Normenkader Gemeenten (PNG).

45. Wat moet je doen als bij een control geen maatregelen staan?

Naar vragenlijst

Zowel wanneer er geen maatregelen bij staan, als wanneer deze er wel bij staan, maak je een risicoafweging. Op die manier bekijk je welke maatregelen nodig zijn om de controls af te dekken. De implementatierichtlijnen in de ISO 27002 helpen bij het bepalen van (aanvullende) maatregelen.

46. Moet je voor BBN2 ook de maatregelen uit BBN1 implementeren?

Naar vragenlijst

Ja, zowel de overheidsmaatregelen van BNN1 als van BBN2 zijn van toepassing.

47. Waar vind je de thematische uitwerkingen voor de BIO-maatregelen?

Naar vragenlijst

De BIO Thema-uitwerkingen zijn te vinden op de volgende plaatsen:

1. Op de website van het CIP staan de complete versies in PDF: BIO en Thema-uitwerkingen - cip-overheid.
2. In de NORA-online zijn ze gepubliceerd in wiki-vorm: https://www.noraonline.nl/wiki/isor.
3. Op de website van de IBD vind je daarnaast zeer veel handreikingen die ook op themagebied uitgewerkt zijn: https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/.

48. Wat is de betekenis van de letter ‘G’ in het kader van de waarden G/B/I/V bij de maatregelen?

Naar vragenlijst

De G staat voor Generiek. Generieke maatregelen hebben effect op zowel de Beschikbaarheid, Integriteit als Vertrouwelijkheid. Voorbeelden zijn beleidsmaatregelen en controlemaatregelen.

Specifieke maatregelen

49. Waarom is BIR 2017-maatregel 16.1.7.1 in de BIO vervallen?

Naar vragenlijst

Door een onvolkomenheid is maatregel 16.1.6.1 ook op de plek van maatregel 16.1.7.1 terechtgekomen in de BIR 2017. Hierdoor is de oorspronkelijke maatregel weggevallen, dat is 16.1.7.1: In geval van een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.

In de BIO is deze dubbele maatregel verwijderd en is maatregel 16.1.7.1 hersteld. Er is schijnbaar een maatregel bijgekomen, maar feitelijk bestond die maatregel al. Het klopt nu wel.

50. Maatregel 9.2.3.1 luidt 'De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.' Wordt onder beoordeeld eventueel ook ingetrokken of verwijderen verstaan?

Naar vragenlijst

Ja, 'beoordeeld' bevat ook 'verwijderen'.

51. Wat wordt in maatregel 9.4.1.1 en 9.4.1.2 bedoeld met 'informatie met specifiek belang'?

Naar vragenlijst

Informatie met specifiek belang is breed te interpreteren. Dit gaat over informatie die een bepaalde waarde heeft (niet openbare informatie). Dit komt voort uit de wet (bijvoorbeeld privacybescherming) of een risicoafweging (vanwege een rubricering/classificatie). Het is informatie waar een ander een voordeel mee kan behalen/misbruik van kan maken, als die onbedoeld bij een niet gerechtigde bekend wordt.

52. Bij maatregel 9.4.2.2 wordt preventief een risico-afweging gemaakt. Moet logging ook achteraf worden gecontroleerd?

Naar vragenlijst

Ja, dat is in paragraaf 12.4 van de BIO uitgewerkt.

53. Bij maatregel 11.1.4.1 ('De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging') wordt gesproken over risicoafweging. Gaat het om bedrijfskritisch zijn van apparatuur of archieven of gaat het om informatieveiligheid/rubricering?

Naar vragenlijst

Het beschermen tegen bedreigingen van buitenaf moet worden gedaan of is zinvol om te doen voor alle bedrijfskritische processen. Dat betekent dat alle bedrijfskritische processen eerst moeten worden geanalyseerd. Vervolgens kunnen maatregelen voor die kritische bedrijfsprocessen op basis van een expliciete risicoafweging worden doorgevoerd.

54. Hoe kan je maatregel 11.1.4.2 ('Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.') toespitsen op informatieveiligheid?

Naar vragenlijst

Informatieveiligheid draait om beschikbaarheid, integriteit en vertrouwelijkheid. Om IT beschikbaar te houden, dient rekening gehouden te worden met dergelijke rampen in de huisvesting van de IT-apparatuur. Immers, wanneer de fysieke apparatuur geraakt wordt door een ramp, zal ook de informatie die de IT levert, niet meer beschikbaar zijn. Daarmee is de fysieke bescherming onderdeel van informatieveiligheid.

55. Bij maatregel 11.1.1.1 wordt er verwezen naar standaarden ('Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.'). Aan welke standaarden wordt hier gerefereerd?

Naar vragenlijst

Het betreft hier de standaarden die gangbaar zijn binnen een overheidslaag. Voor Rijkskantoren staat dit bijvoorbeeld verwoord in het addendum in deel 3 van de BIO. Daarnaast kan gebruikt gemaakt worden van de Handreiking Toegangsbeleid die is uitgegeven door de IBD voor gemeenten.

56. Bij maatregel 11.2.9.4: Hoe en wie maakt de risicoafweging en hoe wordt deze vastgelegd?

Naar vragenlijst

De procesverantwoordelijke zal moeten aangeven of en hoe aan de BIO wordt voldaan.

57. Bij maatregel 12.1.3.1 wordt gesproken over een 'onvertrouwde zone'. Wat wordt hiermee bedoeld?

Naar vragenlijst

Een onvertrouwde zone is die zone waarover geen invloed kan worden uitgeoefend door de eigen organisatie. De meest voor de hand liggende onvertrouwde zone is het internet. Zie ook FAQ 58.

58. Bij maatregel 13.1.2.3 wordt gesproken over 'buiten het gecontroleerd gebied'. Wat is in dit verband de definitie van ongecontroleerd gebied?

Naar vragenlijst

Ongecontroleerd gebied is gebied waarover de verantwoordelijke manager geen beheersing heeft over de vraag wie zichzelf er toegang toe kan verschaffen. Draadloze verbindingen zijn ook te onderscheppen in gecontroleerd gebied; het is namelijk afhankelijk van de apparatuur van de kwaadwillende of deze contact kan krijgen, signaal kan opvangen en verzenden. Bij een bedrade verbinding gaat het om onderscheppen door fysieke toegang tot de bekabeling en derhalve buiten gecontroleerd gebied. In de BIO is daarom opgenomen dat bij zowel draadloze verbindingen als bij bedrade verbindingen buiten het gecontroleerd gebied bij BBN2-encryptie moet worden toegepast, zodat bij onderschepping informatie niet zomaar toegankelijk is. Zie ook antwoord 57.

59. Bij maatregel 15.1.2.6 wordt gesproken over het opnemen van het 'right to audit' in contracten. Wordt dit altijd door leveranciers geaccepteerd?

Naar vragenlijst

In afstemming met de overheid moet een leverancier hier in principe altijd aan voldoen. De 'right to audit' wordt echter niet in alle gevallen geaccepteerd. In dat geval moet een leverancier op onafhankelijke wijze kunnen aantonen dat hij aan de geldende normen voldoet. Het gaat daarbij expliciet om een onafhankelijke aantoonbaarheid. Een audit is niet nodig als de leverancier met een relevante certificering of een (geldende) auditverklaring aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd. In alle andere gevallen is het noodzakelijk om hierover afspraken te maken. Overigens is het right to audit ook bedoeld om in bepaalde gevallen (los van de contractuele jaarlijkse verplichting) een onderzoek uit te kunnen laten voeren bij een leverancier. Bijvoorbeeld bij of na een incident.

60. Bij maatregel 17.1.3.3.2 ('de dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld') wordt gesproken over bedrijfskritisch. Wat is hierbij de duiding voor bedrijfskritisch?

Naar vragenlijst

In het rijtje ondersteunend, belangrijk, strategisch en kritisch strategisch is de laatstgenoemde - kritisch strategisch - een synoniem voor bedrijfskritisch. Bedrijfskritische onderdelen zijn die organisatiedelen die direct bijdragen aan het ondersteunen van de strategische doelstellingen van een organisatie. Daarbij geldt ook dat deze doelstellingen vertaald dan wel aangevuld kunnen worden uit (verplichtende) wetgeving. Een goede vuistregel is dat strategische doelstellingen gehaald kunnen worden uit de missie (doelen) en visie (waarom) van een organisatie.

61. Bij maatregel 17.1.3.3 ('de dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld') wordt ook gesproken over een minimaal herstel binnen een week. Is dit een haalbaar tijdspad?

Naar vragenlijst

Een maximale hersteltijd van een week in geval van een calamiteit is realistisch. Het gaat tenslotte om bedrijfskritische processen. Je kunt het ook omdraaien door te stellen dat als een hersteltijd van minder dan een week als te zwaar wordt gezien, het waarschijnlijk niet om een bedrijfskritisch proces gaat. Binnen een bedrijfskritisch proces kan weer gediversifieerd worden; sub-processen kunnen in belang verschillen. Het herstellen van een minimale dienstverlening in geval van een calamiteit kan ook invulling geven aan de norm. De risicoanalyse en de Bedrijfs- (of Business) Impact Analyse (BIA) geeft daar input voor. Overigens is de dienstverlening van de meeste shared service-organisaties zodanig ingericht dat bij incidenten herstel binnen 2 werkdagen (85% van de gevallen) moet zijn gerealiseerd.

Rollen

62. In hoeverre is de BIO 2019 ook van toepassing op opdrachtnemers, zoals aannemers bouwwerken van de Rijksoverheid? Indien de BIO 2019 niet van toepassing is, welke richtlijn kan worden gehanteerd voor informatiebeveiliging?

Naar vragenlijst

De BIO is van toepassing op alle organisatieonderdelen van de overheid. Uitgangspunt is dat de proceseigenaar op basis van risicomanagement bepaalt welk basisbeveiligingsniveau (BBN) van toepassing is. Vervolgens bepaalt de manager aan de hand van de toepasselijke controls hoe de gestelde beveiligingsdoelstellingen moeten worden ingevuld. De invulling van de beveiligingsdoelstellingen met vereiste beveiligingsmaatregelen vindt plaats aan de hand van een risicoafweging.

In paragraaf 4.4 van de BIO wordt uitgelegd hoe met leveranciers moet worden opgegaan. Leveranciers die geen onderdeel zijn van de overheid zijn niet rechtstreeks gebonden aan de BIO. Een opdrachtgever bepaalt aan welke informatiebeveiligingseisen een (externe) leverancier moet voldoen. Deze eisen zullen in het contract met de leverancier moeten worden vastgelegd. In de BIO zijn in hoofdstuk 15 over leveranciersrelaties controls en overheidsmaatregelen opgenomen die moeten zorgen voor een goede borging van informatiebeveiliging in contracten.

De BIO is gebaseerd op de ISO 27001 en 27002. Deze standaarden worden wereldwijd gebruikt als basis voor de informatiebeveiliging. Verwacht mag worden dat ook externe leveranciers hun diensten en producten adequaat hebben beveiligd. Als zij dat hebben gedaan op basis van deze ISO-standaarden, dan zal alleen nog het verschil tussen de gebruikte standaard en de BIO moeten worden aangetoond en zal een verbeterplan moeten worden gemaakt door de leverancier om compliant te worden op die overheidsmaatregelen die op hem van toepassing zijn. Het verschil tussen de standaard en de BIO-subset kan worden onderzocht met een GAP-analyse.

63. Hoe moet je de BIO aan externe dienstenleveranciers voorleggen?

Naar vragenlijst

In de BIO staat bij elke control vermeld wie verantwoordelijk is voor de maatregel. Eén van de mogelijke verantwoordelijken is de dienstenleverancier. Dit kan zowel een interne als een externe dienstenleverancier zijn. Een interne dienstenleverancier is zelf ook gehouden aan de BIO. Een externe dienstenleverancier niet. Conform hoofdstuk 15 van de BIO zorg je voor een contract met een externe leverancier waarin de afspraken rondom informatiebeveiliging zijn opgenomen. Je kunt daarin aangeven waar de leverancier aan moet voldoen. Met het mede op de BIO gebaseerde tool ICO-Wizard kun je een specifiek eisenpakket samenstellen om mee te geven aan de leverancier bij inkopen/aanbestedingen, waarbij geldt dat alleen de overheidsmaatregelen verplicht zijn.

64. Wat moet je doen bij bestaande contracten die nog niet op de BIO zijn afgesloten?

Naar vragenlijst

Ga het gesprek aan met jouw leverancier om te kijken aan welke maatregelen de leverancier nog niet voldoet. Maak op basis daarvan separate (verbeter)afspraken. Laat de leverancier een GAP-analyse opleveren om concreet te maken waaraan de leverancier mogelijk nog niet voldoet.

65. Wat moet de medewerker doen met de BIO-maatregelen?

Naar vragenlijst

De medewerker is een breed begrip. Lang niet elke medewerker in een organisatie heeft direct met de BIO te maken. Van een IT- of HRM-medewerker mag verwacht worden dat zij, al dan niet met behulp van een informatiebeveiliger, zich verdiepen in de maatregelen die voor hun vakgebied gelden. Een inkoper moet weten welke eisen de BIO aan leveranciers stelt. Per saldo moeten gemiddelde medewerkers vooral op de hoogte zijn van het informatiebeveiligingsbeleid en meegenomen worden in bewustwordingsprogramma's om te begrijpen wat zijn of haar verantwoordelijkheid voor informatiebeveiliging is.

66. Houdt de BIO er rekening mee dat veel organisaties hun ICT-dienstverlening geheel of gedeeltelijk hebben uitbesteed?

Naar vragenlijst

Ja, de BIO geeft expliciet aan welke maatregelen voor de dienstenleverancier zijn. De BIO maakt daarbij geen onderscheid tussen interne en externe dienstenleveranciers.

67. Waarom is er geen onderscheid tussen interne en externe dienstleveranciers?

Naar vragenlijst

Interne en externe leveranciers leveren producten en diensten die aan dezelfde betrouwbaarheidseisen moeten voldoen.

68. Als mijn leverancier een ISO 27001-certificering heeft, is dat dan ook goed?

Naar vragenlijst

Het is mogelijk dat een (externe) dienstenleverancier beschikt over een ISO 27001-certificering of enig ander kwaliteitskeurmerk. Dergelijke keurmerken kunnen zekere waarborgen geven over de opzet, bestaan en soms ook werking van het proces dat bij de dienstenleverancier is ingericht, maar geven niet aan op welk niveau de beveiliging is gerealiseerd. Veiligheid van uitbestede producten en diensten van leveranciers moet worden geborgd in de inkoop-, contract- en leveranciersmanagementprocessen. Voor de ondersteuning daarvan, zie de ICO-producten. Zie ook het antwoord bij vraag 62.

69. Waarom komen de eisen aan leveranciers (paragraaf 4.4) niet terug in hoofdstuk 15 van de BIO?

Naar vragenlijst

De eisen staan in hoofdstuk 4 'Verantwoording over de BIO' van de BIO in deel 1 Achtergrond BIO. Omdat deel 1 'Achtergrond BIO' en deel 2 'Kader BIO' van de BIO hetzelfde gewicht hebben, is een toevoeging aan hoofdstuk 15 van deel 2 niet nodig. Voorts is het zo dat de veiligheid van uitbestede producten en diensten van leveranciers moet worden geborgd in de inkoop-, contract- en leveranciersmanagementprocessen van de organisatie. Voor de ondersteuning daarvan, zie de ICO-producten. Zie ook het antwoord bij vraag 62.

70. Hoofdstuk 7 van de BIO gaat over 'Veilig personeel'. Hoe kan de opdrachtgever bepalen of een potentiële buitenlandse medewerker geschikt of bekwaam is als je niet over een VOG kan beschikken?

Naar vragenlijst

Het beveiligingsdoel is het kunnen vaststellen of een potentiële (buitenlandse) medewerker geschikt/bekwaam is voor de functie. Als de VOG geen optie is, is de oplossing het vinden van een vergelijkbaar instrument. Als je dat hebt, kun je een goede afweging maken.

Verantwoording

71. Wat doen je als je niet aan een control of maatregel kan/wil voldoen?

Naar vragenlijst

Het niet invullen van een control moet intern kunnen worden toegelicht ('comply or explain': pas toe of leg uit). Wanneer een overheidsmaatregel wel van toepassing is, maar een organisatie er niet of op een andere manier invulling aan geeft, wordt dit door de organisatie in een registratie van explains bijgehouden. Wanneer er samengewerkt wordt, bijvoorbeeld in een keten, en de explain heeft invloed op de bescherming van de informatie die tussen organisaties wordt uitgewisseld, dan moet de explain ook met de partners binnen die samenwerking gedeeld worden. In gezamenlijkheid kan dan worden bekeken of er tijdelijke maatregelen genomen kunnen worden ter mitigatie of verkleining van het risico dat is ontstaan.

Voor de Rijksoverheid geldt dat explains die de veiligheid van andere delen van de Rijksoverheid raken, worden voorzien van een advies van de Security Accreditation Authority (SAA, ingevuld door het CISO-overleg) en door het ministerie worden voorgelegd aan het CIO-beraad.

72. Moet je een explain indienen als je ergens niet aan voldoet?

Naar vragenlijst

Nee, in principe niet, tenzij hiermee de veiligheid van andere partijen wordt geraakt. In dat geval moet je de situatie bespreken binnen jouw samenwerkingsverband (bijvoorbeeld een ketensamenwerking). Voor de Rijksoverheid geldt dat de explain voorzien van advies van de SAA wordt voorgelegd aan het CIO-beraad wanneer de veiligheid van andere organisaties van de Rijksoverheid in het geding is. Voor lagere overheden geldt dat explains moeten worden voorgelegd ter besluitvorming aan de eindverantwoordelijke voor de bedrijfsvoering, omdat een explain mogelijk van invloed is op de risicobereidheid van de organisatie.

73. Moet je over alle controls en maatregelen verantwoording afleggen?

Naar vragenlijst

De BIO maakt in zijn geheel onderdeel uit van de bestuurlijke verantwoording over informatieveiligheid. Hoe dit precies is vormgegeven, verschilt per overheidslaag en per organisatie. Ook maakt het basisbeveiligingsniveau onderscheid in de striktheid van de verantwoording.

74. Is de huidige comply or explain-afspraak ook van toepassing op BBN1?

Naar vragenlijst

Ja, deze is van toepassing op alle BBN's. De risicoafweging en het effect op andere partijen is echter waarschijnlijk geringer en daarmee zal het grotendeels bij een interne explain blijven.

75. Moet je ook explains indienen als een maatregel niet van toepassing is?

Naar vragenlijst

Nee, een explain geldt alleen wanneer een maatregel ook daadwerkelijk van toepassing is.

76. Bij wie worden incidenten gemeld?

Naar vragenlijst

Belangrijkste incidenten moeten worden gemeld aan het hoogste management binnen de organisatie. De opvolging van incidenten wordt maandelijks gerapporteerd aan het managementteam.

77. Wanneer leggen leveranciers verantwoording af?

Naar vragenlijst

Leveranciers moeten altijd op onafhankelijke wijze aantonen dat aan de normen wordt voldaan. Daarbij gaat het nadrukkelijk om onafhankelijke aantoonbaarheid. Maak altijd afspraken over het 'right to audit'.

78. Wanneer voldoet een organisatie aan de BIO?

Naar vragenlijst

Wanneer de organisatie op basis van risicomanagement invulling heeft gegeven aan alle controls en maatregelen van de BIO die van toepassing zijn, en de organisatie hiervoor een goede PDCA-cyclus heeft ingeregeld om blijvend te voldoen, kan in elk geval geconcludeerd worden dat de organisatie voldoet aan de BIO.

Wanneer een organisatie nog niet volledig voldoet, maar wel een goed verbeterplan heeft en eventuele tijdelijke maatregelen heeft genomen om risico's te beperken, is een organisatie ook goed op weg naar voldoen aan de BIO.

79. Is het mogelijk om op de BIO te certificeren?

Naar vragenlijst

Nee, zoals ook de ISO 27002 - de basis waarop de BIO steunt - zich niet leent voor certificering, is ook geen certificering mogelijk tegen de BIO. De BIO geeft aan dat door middel van een risicoafweging moet worden bepaald hoe aan de beveiligingsdoelstelling van de individuele controls moet worden voldaan (zie ook het voorwoord in de BIO), waarbij de BIO in een aantal gevallen zelf verplichte overheidsmaatregelen vastgesteld heeft als minimale norm. De BIO als normenkader kan wel ingebracht worden als minimale set van normen bij het vaststellen van de controls die van toepassing zijn op de scope van een managementsysteem (ISMS) in het traject van een certificering in het kader van de ISO 27001.

Transitie naar de BIO

80. Wat houdt de transitieperiode in?

Naar vragenlijst

Hiermee wordt bedoeld de periode van 1 januari 2019, waarop de BIO van kracht werd, tot 1 januari 2020, waarop de BIO als uitgangpunt voor de overheid ging gelden. Deze periode is ingesteld om organisaties de tijd te geven de omslag van de oude baseline naar de nieuwe BIO te maken. Het tijdspad daarbij is door elke overheidslaag zelf bepaald.

81. Vanaf wanneer moeten overheden verantwoorden volgens de BIO?

Naar vragenlijst

Per overheidslaag heeft besluitvorming plaatsgevonden en zijn bindende afspraken gemaakt. Daarnaast zijn ook per overheidslaag afspraken gemaakt voor de overgangsperiodes. Er is geen sprake van een algemeen geldende verantwoordingsplicht. Per overheidslaag is onderstaande van toepassing en gelden afspraken over de wijze van verantwoording:

- **Rijk**: In de besluitvorming over BIO is door het OBDO (29 november 2018) onder meer het volgende vastgesteld: 'Voor de rijksoverheid geldt dat het implementatieproces van de BIR 2017 niet wordt verstoord met goedkeuring van BIO 1.0. Zodra een rijksoverheidsorganisatie de BIR 2017 conform de PDCA-cyclus heeft ingevoerd, heeft zij daarmee ook de BIO 1.0 ingevoerd en is daarmee de facto over naar de BIO.'. Dat betekent dat de implementatieafspraken voor BIR 2017 blijven gehandhaafd.

- **Gemeenten, provincies en waterschappen**: voor gemeenten en waterschappen was 2019 een overgangsjaar en geldt in 2020 de BIO als normenkader.

82. Is er ondersteuning beschikbaar voor de overgang naar de BIO?

Naar vragenlijst

Ja, hiervoor werd het ondersteuningsprogramma opgezet waarin alle overheidslagen betrokken zijn. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is daarbij de opdrachtgever. Het ondersteuningsprogramma loopt vanaf 2019 en is bedoeld als stimulans voor een overheidsbrede implementatie van de BIO.

83. Wat houdt het ondersteuningsprogramma precies in?

Naar vragenlijst

Uiteraard moet iedere overheidsorganisatie de BIO zelf implementeren. Vanaf 1 januari 2019 zijn alle overheidslagen gestart met de implementatie van de BIO volgens een door elke overheidslaag zelf opgesteld pad. Het interbestuurlijk ondersteuningsprogramma brengt een veelheid van ondersteunde hulpmiddelen bijeen en ontsluit deze via de site www.bio-overheid.nl. Daarnaast worden kennissessies, webinars e.d. georganiseerd. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is daarbij de opdrachtgever en het Centrum Informatiebeveiliging en Privacybescherming opdrachtnemer. Alle overheidslagen zijn betrokken.

84. Welke ondersteuningsmaterialen zijn er beschikbaar?

Naar vragenlijst

Vanuit het ondersteuningsprogramma worden diverse middelen en activiteiten ontwikkeld om bestuurders en professionals te ondersteunen bij de implementatie van de BIO, waaronder: webinars, thematische workshops, handreikingen, BIO Thema-uitwerkingen, een handige zoekfunctie voor practices, een tool voor het selecteren en opmaken van securityeisen bij inkopen (ICO-Wizard) etc. Kijk op: https://bio-overheid.nl/ waar deze hulpmiddelen van de IBD, het CIP, het NCSC en meer worden ontsloten.

Met de Verwijzingsmatrix BIO - BIO-practices vind je relevante practices bij de verschillende onderdelen van de BIO.

85. Wat zijn handreikingen?

Naar vragenlijst

Handreikingen helpen met het geven van de invulling van controls en overheidsmaatregelen. Ze bieden een basis die kan worden gebruikt in jouw organisatie. Je bent niet verplicht om deze handreikingen te gebruiken, maar ze zijn wel heel handig en voorkomen dat je alles zelf moet uitvinden. Je vindt meer informatie over de handreikingen op de websites van de koepels van de bestuurslagen. Met deze zoekfunctie Verwijzingsmatrix BIO - BIO-practices kun je vinden wat te relateren is aan onderdelen van de BIO.

86. Hoe kan je aan de slag als BIV-maatregelen ontbreken in de BIO?

Naar vragenlijst

De IBD heeft schadescenario's gemaakt. Dit maakt het mogelijk om maatregelen te selecteren of bedenken. Daarmee wordt duidelijk welk effect betreffende maatregelen hebben (B, I of V).

87. Welke Thema-uitwerkingen zijn er beschikbaar?

Naar vragenlijst

Beschikbaar zijn de Thema-uitwerkingen: Applicatieontwikkeling, Clouddiensten, Communicatievoorzieningen, Huisvesting Informatievoorzieningen, Serverplatform, Toegangsbeveiliging, Softwarepakketten, de Privacy Baseline en Grip op Secure Software Development (SSD) en Middleware.

88. Waar kan je BIO Thema-uitwerkingen vinden?

Naar vragenlijst

BIO Thema-uitwerkingen zijn gepubliceerd in wiki-vorm op de website van NORA: https://www.noraonline.nl/wiki/isor. Op de pagina BIO en Thema-uitwerkingen van het CIP zijn PDF-versies te downloaden.

89. Waar kan je terecht met inhoudelijke vragen?

Naar vragenlijst

Je kunt allereerst terecht bij de CIO of CISO van jouw organisatie of bij jouw koepel. Daarnaast kun je veel informatie vinden op of via de website van de BIO www.bio-overheid.nl. Ook kun je kijken op het BIO-forum op Pleio (via de BIO-website).

Overzicht vragen

Klik in onderstaand overzicht op een vraag om direct naar het antwoord te gaan.