BIO | Baseline Informatiebeveiliging Overheid

voor een veilige digitale overheid

Veelgestelde vragen Baseline Informatiebeveiliging Overheid

Versie 1.13 definitief, 21 juli 2023

Rijksoverheid

Interprovinciaal Overleg ipo

VNG Vereniging van Nederlandse Gemeenten

UNIE VAN WATERSCHAPPEN

Inhoudsopgave

De vragen en antwoorden zijn ingedeeld in de volgende hoofdonderwerpen:

De onderstaande inhoudsopgave bevat alle vragen met directe links naar de antwoorden hierop.

Algemeen

1. Wat is een baseline?

Naar vragenlijst

In de context van de Baseline Informatiebeveiliging Overheid (BIO) is een baseline het basisniveau voor informatiebeveiliging waaraan minimaal moet worden voldaan, uiteraard als de controls van toepassing zijn, zie antwoord 40.

2. Wat houdt de BIO in?

Naar vragenlijst

De BIO is een normenkader voor informatiebeveiliging en geeft het basisniveau weer voor informatiebeveiliging waaraan alle overheidspartijen moeten voldoen. Door dit normenkader wordt een stevige basis gelegd voor de verdere optimalisering van informatiebeveiliging binnen de overheid. Er 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 eigen baseline voor 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 waren daardoor niet actueel. Ook waren er verschillen tussen deze baselines, terwijl door ketensamenwerking zeer veel informatie-uitwisseling tussen overheidslagen plaatsvindt. Een gezamenlijk normenkader maakt ketensamenwerking makkelijker en efficiënter. Ook voor leveranciers is dit prettig, want zij hebben bij alle overheidsorganisaties te maken met dezelfde informatiebeveiligingseisen.

4. Welke voordelen biedt de BIO?

Naar vragenlijst

De BIO als een baseline voor alle overheidsorganisaties biedt vele voordelen. Het zorgt voor:

- een eenduidig en helder basisniveau van informatiebeveiliging voor alle overheidsorganisaties;
- één schema (meetlat), de schadescenario's, waardoor het belang van informatie door alle gebruikers op dezelfde manier gewogen wordt;
- een betere en makkelijkere samenwerking tussen diverse overheidsorganisaties en partners;
- het verlichten van de administratieve lasten;
- dat partijen makkelijker kunnen communiceren en effectiever opereren door een gemeenschappelijke taal;
- het stimuleren van de onderlinge kennisuitwisseling; professionals kunnen van elkaar leren en verbeteren.

5. Voor wie is de BIO bedoeld?

Naar vragenlijst

De BIO is voor alle Nederlandse overheidsorganisaties en overheidsgelieerde organisaties.

6. Is de BIO verplicht?

Naar vragenlijst

De BIO is verplicht voor alle bestuurslagen. 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 een wettelijke verankering van de BIO, vermoedelijk in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) en/of de Wet digitale overheid (Wdo). Voor meer informatie zie digitaleoverheid.nl. Rond oktober 2024 zal de herziene versie van de Wbni in werking treden.

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

Naar vragenlijst

Artikel 41 van de kaderwet ZBO's van 1 juli 2022 geeft aan dat de voor de rijksdienst geldende voorschriften voor gegevensbeveiliging ook van toepassing zijn op de (kaderwet-)ZBO's:

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 er anders in de BIO dan de BIR, BIG, BIWA en IBI?

Naar vragenlijst

Anders in de BIO is:

- De BIO is gebaseerd op de NEN-EN-ISO/IEC 27001:2017 en de NEN-EN-ISO/IEC 27002:2017, terwijl de baselines van de koepels, uitgezonderd de BIR, nog gebaseerd waren op de 2013-versies van deze ISO-normen.
- In de BIO ligt meer nadruk 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, gebaseerd op de richtlijnen uit de NEN-EN-ISO/IEC 27002:2017.
- De basisbeveiligingsniveaus (BBN's) zijn nieuw, met uitzondering voor de organisaties die eerder de BIR 2017 hanteerden.
- Er is meer aandacht voor handreikingen en thematische uitwerkingen.
- Er is een duidelijke onderhoudscyclus ingericht.

9. 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.

10. Op welke wetgeving is de BIO gebaseerd?

Naar vragenlijst

De BIO is niet op wetgeving gebaseerd. Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt gewerkt aan wettelijke verankering van de BIO. De BIO is gebaseerd op de internationale normen: NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017. Ze zijn als verplicht te gebruiken normen opgenomen in de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie, zie antwoord 6.

11. Waar vind je de BIO?

Naar vragenlijst

De volledige tekst van de BIO-versie 1.0.4 is op 11 februari 2020 in de Staatscourant gepubliceerd. De meest actuele versie, versie 1.0.4zv, de versie zonder verwijzingen, is te downloaden via de informatiepagina's van de koepels en op de BIO-website.

De BIO-website ontsluit ook de BIO in spreadsheet-formaat (bevat alleen controls en overheidsmaatregelen) en de handreiking BIO2.0-opmaat. De controls en maatregelen uit deze laatste handreiking volgen de nummering van de Europese versie van ISO 27002 (NEN-EN-ISO/IEC 27002:2022). Ook zijn alle goedgekeurde BIO-wijzigingsverzoeken in deze handreiking verwerkt. Bovendien zijn een aantal overheidsmaatregelen versterkt vanwege veranderende dreigingen.

12. 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 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:

- ISO/IEC 27000-serie (waarop de BIO is gebaseerd)
- 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

13. Wat is de inhoudelijke visie over de richting van de BIO-ontwikkeling?

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 is 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.'.

14. Is de BIO ook beschikbaar in het Engels?

De BIO is niet beschikbaar in het Engels. De BIO is voor een groot deel gebaseerd op de Nederlandse vertaling van de ISO 27002. Deze internationale norm is in het Engels opgesteld. Zowel de Nederlandse als de Engelse versie zijn beschikbaar op de website van de NEN. Om vrij gebruik te kunnen maken van ISO 27001 en ISO 27002 kan je terecht in NEN Connect - Home.

15. Waarom komt er geen actualisatie van de BIO in 2023?

Bij de vaststelling van de BIO is afgesproken dat hij in 2023 wordt geëvalueerd. Dat is inmiddels gebeurd. De evaluatie zal leiden tot een BIO2.0. Aanpassing van de BIO2.0 loopt parallel met de aanpassing van de Wbni en/of de Wdo, dit naar aanleiding van de komst van de NIB2. Rond oktober 2024 moet de NIB2 in Nederlandse wetgeving verankerd zijn. De BIO2.0 is dan ook beschikbaar.

16. Wachten we tot 2024 op een BIO2.0?

Gezien de huidige dreigingen, de goedgekeurde BIO-wijzigingsverzoeken en de in 2022 gepubliceerde ISO/IEC 27002, is het onverstandig om te wachten op een BIO2.0. Daarom is handreiking BIO2.0-opmaat opgesteld als opmaat naar een BIO2.0, zie ook antwoord 11. Hiermee is deels inzichtelijk welke kant de BIO opgaat. Deze handreiking kent een dringend implementatie-advies.

17. Is er een strategie voor het ontwikkelen en hanteren van de BIO?

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.

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

Naar vragenlijst

In paragraaf 1.5 van de BIO staat beschreven hoe de overheid met de standaarden van het Forum Standaardisatie omgaat.

ISO 27001/27002

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

Naar vragenlijst

De NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017 vormen de basis van de BIO. Het grootste gedeelte van de BIO is feitelijk deze ISO-normen. Aan de BIO zijn specifieke maatregelen toegevoegd die de overheid relevant acht in de bescherming van haar informatie. Ook is er onderscheid gemaakt in BBN's in de BIO.

20. 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 BBN 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-implementatie-aanwijzingen 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.

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

Naar vragenlijst

Versie 1.0.4zv van de BIO is gebaseerd op de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. In 2024 verschijnt versie 2.0 van de BIO die gebaseerd wordt op de meest actuele versie van deze twee normen. De handreiking BIO2.0-opmaat maakt inzichtelijk welke kant de BIO2.0 opgaat, zie antwoord 11.

22. Zijn de implementatierichtlijnen uit de ISO 27002 verplicht?

Naar vragenlijst

De richtlijnen 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, die in aanvulling op of naast de BIO-overheidsmaatregelen gebruikt kunnen worden.

23. Wat gebeurt er als er een nieuwe versie van de ISO 27001 of 27002 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-ISO/IEC 27002:2022. De handreiking BIO2.0-opmaat geeft aan welke kant versie 2.0 van de BIO opgaat, zie antwoord 11.

Basisbeveiligingsniveaus (BBN’s)

24. Is in het kader van de BIO het een 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 de term expliciete risicoafweging tegen. Daarmee wordt een risicoanalyse bedoeld. Er wordt verlangd dat aangetoond kan worden dat die risicoafweging plaatsgevonden heeft en dat het resultaat daarvan vastgelegd is.

25. Wat houden de BBN’s in?

Naar vragenlijst

De BBN’s 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.

26. 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. Het gaat om een laag betrouwbaarheidsniveau en om een minimale basis. Daarom blijven complexe eisen achterwege.

In BBN2 valt de meeste overheidsinformatie. Het gaat om goed huisvaderschap voor informatie. BBN2 is het standaardniveau. Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV), zoals gedefinieerd in het VIRBI)/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 maatwerk is vereist. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van NAVO- en EU-normenkaders. Gemeenten gebruiken in aanvulling op BBN2 voor vertrouwelijkheid = hoog een set van maatregelen die zij noemen BBN2+.

27. 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 (de vertrouwelijkheid is laag) aan minder complexe risicomanagement- en verantwoordingseisen te voldoen, waarbij een minimum beveiligingsniveau wordt gewaarborgd.

28. 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 (de vertrouwelijkheid is midden).

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.

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

Naar vragenlijst

Met name waar het gaat om het hoogste BBN, 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-normenkaders. Aangezien onvoldoende toegevoegde waarde wordt verwacht van een algemene overheidsbrede standaard voor BBN3 wordt afgezien van uitbreiding van de BIO op dit punt. Als daar behoefte aan is, wordt dit in het reguliere BIO-onderhoudsproces meegenomen.

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

30. Hoe kom je tot het juiste BBN?

Naar vragenlijst

Om het BBN uit de BIO te bepalen, is een baselinetoets beschikbaar. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties beschikt over de handreiking Quickscan Information Security (QIS) (oorsprong BIR 2017), een detailuitwerking van de BIO. De BBN-toets is ontwikkeld door de IBD. De BBN-toets en de Quickscan zijn vergelijkbaar. Op basis van een aantal vragen wordt duidelijk welk BBN voor een informatiesysteem of proces van toepassing is. De proceseigenaar bepaalt met de toets welk BBN gevolgd dient te worden. Zie ook de schadescenario's uit deel 2 Kader BIO, bijlage 2 Basisbeveiligingsniveaus van de BIO.

31. Wanneer zijn BBN3-maatregelen nodig?

Naar vragenlijst

Ongeacht wat de uitkomst van een analyse is, bijvoorbeeld BIV=LLL, BIV=MMM of BIV=HHL, zijn er 3 vragen, waarvan er minimaal 1 met Ja beantwoord moet worden, om op 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?

De basisgedachte achter de BIO is dat er minder overheidsmaatregelen zijn en dat de proceseigenaar met een risicoafweging zelf de ontbrekende maatregelen selecteert en toevoegt aan de minimale en verplichte set uit de BIO. Dit geeft de proceseigenaar meer vrijheid en zorgt ervoor dat het risicomanagementproces op die plaats kan worden uitgevoerd waar het risico daadwerkelijk optreedt en behandeld moet worden.

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

Naar vragenlijst

In alle gevallen moet de proceseigenaar, als verantwoordelijke, een risicoafweging maken. Hij moet de risico's die zijn proces loopt, accepteren, mitigeren, overdragen of vermijden. Hierbij geldt: hoe hoger het belang, hoe minder keuzevrijheid in het kiezen van maatregelen of het accepteren van een risico. Ook geldt dat de proceseigenaar geen keuze kan maken als het risico zijn afdeling of proces overstijgt en de hele organisatie of ketens raakt. Ieder BBN heeft zijn eigen verantwoordelijkheidsniveau. Dit is uitgewerkt in paragraaf 4.1 van de BIO.

Gemeenten beschikken vanuit hun ondersteuningsorganisatie Informatiebeveiligingsdienst (IBD) over een maatregelenset BBN2+ (niet verplicht). Het is een aanvulling op BBN2 als tijdens een BBN-toets een score V=hoog gehaald wordt.

33. Is het BBN een vervanging van het TBB?

Naar vragenlijst

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 paragraaf 4.1 (Inzicht in de organisatie en haar context) en paragraaf 4.2 (Scope en doelstellingen). Een BBN is een classificatieniveau dat op het TBB van toepassing is.

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

Naar vragenlijst

Risicomanagement gaat over het bepalen van welke risico's jouw organisatie/de keten mogelijk loopt en hoe je deze risico's 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.

35. 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 niet mogelijk en niet wenselijk, vanwege de vaak hoge kosten 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/de keten, kun je ook bepalen hoe ver je wilt gaan in de te treffen maatregelen en welke maatregelen ook daadwerkelijk een risico kunnen verkleinen.

36. 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

37. Wat zijn controls?

Naar vragenlijst

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

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

Naar vragenlijst

Dit onderscheid wordt gemaakt door de toewijzing van controls aan rollen (organisatie-breed), proceseigenaar (specifiek) en dienstenleverancier (specifiek). Omdat overheidsorganisaties pluriform zijn ingericht, is de toewijzing van maatregelen in een meer gedetailleerd niveau voor de BIO niet wenselijk. De toewijzing aan bijvoorbeeld 'PIOFACH'-actoren kan op lokaal niveau zelf bepaald worden.

39. 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.

40. Wat doe je als een control/overheidsmaatregel 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. Dit geldt bijvoorbeeld bij een control die betrekking heeft op een externe koppeling, terwijl het betreffende systeem geen externe koppeling heeft. Er moet dan wel een 'niet van toepassingsverklaring' worden gemaakt.

41. Wat zijn overheidsmaatregelen?

Naar vragenlijst

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

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

Naar vragenlijst

Alleen 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).

43. Wat doe je als bij een control geen maatregelen staan?

Naar vragenlijst

Maak altijd een risicoafweging, ook als een control wel overheidsmaatregelen kent. 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.

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

Naar vragenlijst

Bij BBN2 zijn zowel de overheidsmaatregelen behorende bij BNN1 als bij BBN2 van toepassing.

45. Waar staat de letter 'G' voor in de maatregelwaarden G/B/I/V?

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

46. Heeft de beoordeling in maatregel 9.2.3.1 ook betrekking op ingetrokken of verwijderde bevoegdheden?

Naar vragenlijst

Beoordeeld betreft ook het intrekken en verwijderen van bevoegdheden.

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

Naar vragenlijst

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

48. In maatregel 9.4.2.2 staat dat er preventief een risico-afweging wordt gemaakt. Moet logging ook achteraf worden gecontroleerd?

Naar vragenlijst

In paragraaf 12.4 Verslaglegging en monitoren van de BIO is dit uitgewerkt.

49. Gaat het in maatregel 11.1.4.1 om bedrijfskritisch zijn van apparatuur of archieven of 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 deze kritische bedrijfsprocessen op basis van een expliciete risicoafweging worden doorgevoerd.

50. Hoe kan je maatregel 11.1.4.2 toespitsen op informatieveiligheid?

Naar vragenlijst

Informatieveiligheid draait om beschikbaarheid, integriteit en vertrouwelijkheid. Om de IT beschikbaar te houden, dient rekening gehouden te worden met dergelijke rampen in de huisvesting van de IT-apparatuur. Als 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.

51. Aan welke standaarden wordt in maatregel 11.1.1.1 gerefereerd?

Naar vragenlijst

Het betreft de standaarden die gangbaar zijn binnen een overheidslaag. Voor Rijkskantoren staat dit bijvoorbeeld verwoord in het addendum in deel 3 van de BIO. Daarnaast kunnen gemeenten gebruik maken van de Handreiking Toegangsbeleid van de IBD.

52. Hoe en wie maakt de risicoafweging uit maatregel 11.2.9.4 en hoe wordt deze vastgelegd?

Naar vragenlijst

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

53. Wat wordt in maatregel 12.1.3.1 bedoeld met een onvertrouwde zone?

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 antwoord 54.

54. Wat betekent in maatregel 13.1.2.3 ongecontroleerd gebied?

Naar vragenlijst

Ongecontroleerd gebied is het 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 53.

55. Wordt 'right to audit' uit maatregel 15.1.2.6 altijd door leveranciers geaccepteerd?

Naar vragenlijst

In afstemming met de overheid moet een leverancier in principe altijd aan 'right to audit' voldoen. '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 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 '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.

56. Wat is in maatregel 17.1.3.3.2 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/primaire doelstellingen van een organisatie. Daarbij geldt ook dat deze doelstellingen vertaald of 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.

57. Is in maatregel 17.1.3.3 herstel binnen een week een haalbaar?

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 Bedrijfsimpactanalyse (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.

58. Waar 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.

Rollen

59. In hoeverre is de BIO ook van toepassing op opdrachtnemers, zoals aannemers bouwwerken van de Rijksoverheid? Indien de BIO 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 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 omgegaan. 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 moeten in het contract met de leverancier 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 normen worden wereldwijd gebruikt als basis voor informatiebeveiliging. Verwacht mag worden dat ook externe leveranciers hun diensten en producten adequaat beveiligen. Doen zij dat op basis van deze ISO-normen, dan zal alleen nog het verschil tussen de gebruikte standaard en de BIO moeten worden aangetoond. Een verbeterplan moet 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.

60. 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. Met 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 inkoop/aanbestedingen, waarbij geldt dat alleen de overheidsmaatregelen verplicht zijn.

61. 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.

62. 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.

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

Naar vragenlijst

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

64. 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.

65. Mijn leverancier heeft een ISO 27001-certificering, is dat 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, het bestaan en soms ook de 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. Binnen de verschillende overheidslagen is dat uitgewerkt in de generieke inkoopvoorwaarden. Voor het vinden van aanvullende maatregelen, zie de ICO-producten. Zie ook antwoord 59.

66. 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. Verder 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 antwoord 59.

67. Hoe bepaal je 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 om een goede afweging te kunnen maken.

Verantwoording

68. Vanaf wanneer verantwoorden overheden 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'. Dit betekent dat de implementatieafspraken voor BIR 2017 blijven gehandhaafd.
- **Gemeenten, provincies en waterschappen**: Voor hen was 2019 een overgangsjaar en geldt de BIO in 2020.

69. Wat doe 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. Wanneer een overheidsmaatregel wel van toepassing is, maar een organisatie er geen 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.

70. 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.

71. 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 BBN onderscheid in de striktheid van de verantwoording.

72. Is de 'pas toe of leg uit'-afspraak ook van toepassing op BBN1?

Naar vragenlijst

Pas toe of leg uit is van toepassing op alle BBN's. De risicoafweging en het effect op andere partijen is waarschijnlijk geringer. Daarmee zal het grotendeels bij een interne explain blijven.

73. Moet je een explain indienen als een maatregel niet aan de orde is?

Naar vragenlijst

Een explain geldt alleen wanneer een maatregel daadwerkelijk van toepassing is.

74. Wanneer leggen leveranciers verantwoording af?

Naar vragenlijst

Leveranciers moeten altijd op een onafhankelijke wijze aantonen dat aan de normen wordt voldaan. Daarbij gaat het nadrukkelijk om onafhankelijke aantoonbaarheid. Maak altijd afspraken over het uitvoeren van audits, zie antwoord 55.

75. Wanneer voldoet een organisatie aan de BIO?

Naar vragenlijst

Geeft de organisatie met risicomanagement invulling aan alle van toepassing zijnde controls en maatregelen, en regelt zij hiervoor een goede PDCA-cyclus in om blijvend te voldoen, kan 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 op weg naar voldoen aan de BIO.

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

Naar vragenlijst

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 ISO 27001-certificering.

Ondersteuning bij de BIO-implementatie

77. Is ervoor de BIO-implementatieondersteuning?

Naar vragenlijst

Vanaf 1 januari 2019 zijn alle overheidslagen gestart met de implementatie van de BIO volgens een door elke overheidslaag zelf opgesteld pad. Uiteraard moet iedere overheidsorganisatie de BIO zelf implementeren. Voor de overgang naar de BIO is in 2019 het ondersteuningsprogramma opgezet met betrokkenheid van alle overheidslagen. Het ondersteuningsprogramma, wat nu heet 'Basis op orde', is bedoeld als stimulans voor een overheidsbrede implementatie van de BIO.

78. Wat houdt het programma Basis op orde in?

Naar vragenlijst

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is de opdrachtgever en CIP de opdrachtnemer. CIP organiseert kennissessies, webinars e.d. Alle overheidslagen zijn betrokken.

79. Welke ondersteuningsmaterialen zijn er beschikbaar?

Naar vragenlijst

Vanuit het programma Basis op orde worden diverse hulpmiddelen en activiteiten ontwikkeld/onderhouden om bestuurders en professionals te ondersteunen bij de implementatie van de BIO. Dit zijn: webinars, thematische workshops, handreikingen, BIO Thema-uitwerkingen, een zoekfunctie voor handreikingen, een tool voor het selecteren en opmaken van informatiebeveiligingseisen bij inkopen (ICO-Wizard) etc.

Op https://bio-overheid.nl/ zijn hulpmiddelen van de IBD, het CIP, het NCSC en meer ontsloten.

80. Welke BIO Thema-uitwerkingen bestaan er?

Naar vragenlijst

Beschikbaar zijn de BIO Thema-uitwerkingen: Applicatieontwikkeling, Clouddiensten, Communicatievoorzieningen, Huisvesting Informatievoorzieningen, Serverplatform, Toegangsbeveiliging, Softwarepakketten, Grip op Secure Software Development (SSD) en Middleware. De BIO Thema-uitwerkingen zijn te vinden op de volgende plaatsen:

- de BIO-website in PDF-formaat;
- de CIP-website in PDF-formaat;
- de NORA-online in wiki-vorm.

Op de IBD-website vind je ook thematische handreikingen.

81. Wat zijn handreikingen?

Naar vragenlijst

Handreikingen zijn praktische richtlijnen of aanbevelingen om te helpen bij de invulling van controls en overheidsmaatregelen. Ze bieden een basis voor gebruik in jouw organisatie. Ze zijn een handig hulpmiddel en voorkomen dat je alles zelf moet uitvinden.

Je vindt handreikingen op de websites van de koepels van de bestuurslagen. Met de zoekfunctie Verwijzingsmatrix BIO - BIO-practices op de BIO-website vind je handreikingen bij hoofdstukken en paragrafen van de BIO.

82. 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).

83. Waar kan je terecht met inhoudelijke vragen?

Naar vragenlijst

Je kunt met inhoudelijke vragen op meerdere plekken terecht:

- Je kunt allereerst terecht bij de CIO, CISO of andere informatiebeveiligingsfunctionaris van jouw organisatie of bij jouw koepel.
- Veel informatie is te vinden op of via de BIO-website. Ook kun je kijken op de BIO-community op CIP.Pleio (via de BIO-website).
- Het CIP organiseert een IB&P-spreekuur om te sparren met een ervaren vakgenoot van een andere organisatie over een beveiligingsvraagstuk.