BIO | Baseline Informatiebeveiliging Overheid

voor een veilige digitale overheid

FAQ’s Baseline Informatiebeveiliging Overheid

v1.4 (publicatiedatum 21 januari 2020)

Rijksoverheid

Interprovinciaal Overleg ipo

VNG Vereniging van Nederlandse Gemeenten

UNIE VAN WATERSCHAPPEN

Inhoudsopgave

Algemeen

1. Wat is een baseline?

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

2. Wat houdt de BIO precies in?

De Baseline Informatiebeveiliging Overheid (BIO) is een normenkader voor informatiebeveiliging en geeft het basisniveau voor informatiebeveiliging waar alle overheidspartijen aan moeten voldoen. Het is gebaseerd op de actuele, internationale standaarden voor informatiebeveiliging, de ISO 27001 en 27002. 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?

Tot nu toe hadden we per overheidslaag een baseline op het gebied van informatiebeveiliging: de BIR (Rijksoverheid), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Echter, met uitzondering van de BIR 2017, waren deze baselines nog gebaseerd op eerdere versies van de ISO 27001 en 27002 en moesten dus 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 én efficiënter. We hebben immers allemaal dezelfde normen waar we aan moeten voldoen. Ook voor leveranciers is dit prettig, zij hebben bij alle overheidsorganisaties nu te maken met dezelfde eisen op het gebied van informatiebeveiliging.

4. Welke voordelen zijn er verbonden aan de BIO?

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

- Eén overheidsbrede baseline stimuleert onderlinge kennisuitwisseling, professionals kunnen van elkaar leren en verbeteren

5. Voor wie is de BIO bedoeld?

Voor alle Nederlandse overheidsorganisaties en aan de overheid gelieerde organisaties.

6. Is de BIO verplicht?

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

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

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 01-01-2015 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 versie 1.04 van toepassing wordt verklaard. 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?

De BIR (Rijksoverheid), BIG (gemeenten), BIWA (waterschappen) en de IBI (provincies) waren de vorige baselines per overheidslaag. De BIO vervangt deze baselines. Dit betekent overigens niet dat alle organisaties nu compleet andere normen hebben om aan te voldoen. De BIR2017 was bijvoorbeeld al gebaseerd op de 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 gebeurt er met de BIR, BIG, BIWA en IBI?

Deze zijn komen te vervallen. De BIO komt in plaats van deze baselines.

10. Wat is er veranderd in de BIO?

De BIO is gebaseerd op de nieuwste versies van de ISO 27001 en 27002. 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 hanteren. 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?

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?

De BIO is (nog) niet op wetgeving gebaseerd. Wel op internationale standaarden, de ISO-normen 27001 en 27002. Deze zijn als verplicht te gebruiken standaarden opgenomen op de pas-toe-of-leg-uit-lijst op 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 nu gewerkt aan wettelijke verankering van de BIO.

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

De volledige tekst van de BIO is op 23 mei via de Staatscourant gepubliceerd. U kunt de tekst downloaden via de informatiepagina's van de koepels en op **https://bio-overheid.nl/media/1324/bio-v103.pdf**.

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

De NIST is een organisatie die onder de Amerikaanse federale overheid valt (National Institute of Standards en Technolgy). 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 sector specifieke 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?

In paragraaf 1.4 van de BIO staat beschreven hoe evaluatie en bijstelling van de BIO plaatsvindt. Bij de vaststelling van de BIO is ten aanzien van 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 Werkgroep Normatiek, 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?

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 uw koepel.

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

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?

De ISO-standaarden vormen de basis van de BIO. Het grootste gedeelte van de BIO is dus feitelijk ISO. Daaraan toegevoegd zijn specifieke maatregelen die we als overheid relevant achten in de bescherming van onze informatie. Ook is er onderscheid gemaakt in basisbeveiligingsniveaus in de BIO.

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

Er is gekeken naar de te beschermen belangen en risico's binnen de overheid. Op basis daarvan is bepaald welke controls bij welk BasisBeveiligingsNiveau (BBN) van toepassing zijn. Daarnaast zijn als verdieping nog verplichte maatregelen gedefinieerd die noodzakelijk worden geacht voor een goede bescherming van overheidsinformatie. 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 maatregelen verplicht die noodzakelijk zijn voor een goede beveiliging van informatie binnen de overheid.

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

NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017.

21. Zijn de implementatierichtlijnen uit de ISO verplicht?

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

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

Conform de onderhoudscyclus op de BIO volgt er dan ook een nieuwe versie van de BIO.

BasisBeveiligingsNiveaus (BBN's)

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

Risicoafweging is de juiste bewoording.

24. Wat houden de BBN's in?

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 houden de drie BBN's in?

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 hier 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. BBN2 is het minimale niveau waarop met persoonsgegevens gewerkt wordt. BBN2 ligt qua zwaarte op hetzelfde niveau als de oude baselines. Bij BBN2 ligt voor statelijke actoren en vergelijkbare dreigers de nadruk op 'detectie'.

BBN3 is een set van maatregelen gebaseerd op relevante NAVO-regelgeving en specifiek ontwikkeld voor processen waarbinnen weerstand tegen statelijke of criminele actoren (of gelijksoortige dreigers) gewenst is of waar informatie wordt verwerkt die door de bronhouder een bepaalde classificatie heeft mee gekregen.

26. Wat is het nut van BBN1?

Bij de oude baselines 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?

BBN3 biedt bescherming tegen statelijke actoren, criminele actoren en gelijksoortige dreigers. De eisen aan vertrouwelijkheid liggen hier hoger dan op niveau 2.

Binnen de BIO context kan het hogere beschermingsniveau van BBN3 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 1 doel: weerstand tegen statelijke of vergelijkbare actoren

28. Hoe kies ik de juiste BBN's?

Hiervoor is een baselinetoets beschikbaar. Op basis van een aantal vragen, wordt hiermee duidelijk welk BBN van toepassing is. De proceseigenaar bepaalt op basis van de toets welk BBN gevolgd dient te worden.

29. Wanneer wordt er voor BBN3 gekozen?

Ongeacht wat de uitkomst van een analyse is, of deze nou BIV=LLL of BIV=MMM of BIV=HHL of kies zelf een combinatie uit, er zijn maar 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 meegekregen van de (externe) bronhouder?
3. Is er weerstand nodig tegen georganiseerde misdaad en zware criminaliteit?

Als één van deze vragen met JA kan worden beantwoord, dan 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.

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

In alle gevallen moet de proceseigenaar een risicoafweging maken want hij is immers verantwoordelijk voor het proces en hij moet dan dus ook 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 proces eigenaar geen keuze kan maken als het risico zijn afdeling of proces overstijgt en de gemeente raakt. Iedere BBN heeft zijn eigen verantwoordelijkheidsniveau en dat is uitgewerkt in de BIO binnen hoofdstuk 4.1.

31. Is de nieuwe BBN een vervanging van de TBB?

Nee, een TBB (Te Beschermen Belang) is het belang dat beschermd moet worden. Dit komt overeen met wat in de ISO 27001 wordt beoogd met 4.1 en 4.2 (Scope en doelstellingen). Een BBN is een classificatieniveau dat vervolgens op het TBB van toepassing is.

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

Risicomanagement gaat in feite over het bepalen welke risico's uw organisatie mogelijk loopt en welke risico's u 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 risk appetite wordt bekeken hoe deze risico's kunnen worden beheerst.

33. Hoe gebruikt u risicomanagement om tot maatregelselectie te komen?

Door risico's te inventariseren kunt u 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 de maatregelen die u neemt passen bij de daadwerkelijke risico's. Immers, 100% beveiligen 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 uw organisatie, kunt u ook bepalen hoe ver u wilt gaan in de maatregelen die u treft en welke maatregelen ook daadwerkelijk een risico kunnen verkleinen.

34. Wat houden de BBN-toets en de Quickscan precies in?

De BNN-toest en de Quickscan zijn vergelijkbaar. De BBN-toets is ontwikkeld door de IBD, bij het rijk heet deze toets de QIS (oorsprong BIR2017). Aan de hand van deze toetsen kunt u bepalen welk BBN u dient te kiezen. U beantwoordt een aantal vragen die uiteindelijk een antwoord geven op de BBN die nodig is voor uw informatiesysteem of proces.

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

Nee, een nieuwe versie van de handreiking QIS is niet gemaakt. De reeds bestaande BIR-versie van de QIS is ook 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/VNG.

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

De BBN is een meetlat op basis van schadescenario's en te beschermen belang. De BIV zijn de aspecten waarlangs informatiebeveiliging wordt ingericht.

Controls en maatregelen

37. Wat zijn controls?

Een control is een beheersmaatregel waarmee specifieke veiligheids- en bedrijfsdoelstellingen van de organisatie kunnen worden gehaald.

38. Waarom is er geen onderscheid tussen systeemspecifieke controls en organisatiebrede controls?

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

39. Hoe weet ik of een control helemaal is afgedekt?

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 rijksmaatregelen.

40. Wat moet ik doen als een control niet van toepassing is?

Als een control of een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt deze binnen de gegeven scope om verplicht te worden ingericht, maar dan moet 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.

41. Wat zijn maatregelen?

Maatregelen geven invulling aan het bereiken van de beveiligingsdoelstellingen (controls).

42. Zijn de maatregelen uit BIR2017 nog inhoudelijk veranderd in de BIO?

De huidige versie van de BIO is 1.03. Deze versie is in mei 2019 in de Staatscourant gepubliceerd. Inhoudelijk is deze versie nog steeds gelijk aan versie BIO 1.0 en aan de BIR2017. Er zijn wel tekstuele aanpassingen aangebracht, maar die doen dus geen afbreuk aan de beveiligingsniveaus die de BIO biedt.

43. Zijn alle maatregelen vanuit privacy regelgeving ook opgenomen in de BIO?

Nee, maar artikel 32 van de AVG wordt door de BIO afgedekt. Indien u persoonsgegevens beschermt, helpt de BIO wel bij het invulling geven aan passende organisatorische en technische beveiligingsmaatregelen.

44. Wat moet ik doen als bij een control geen maatregelen staan?

Zowel wanneer er geen maatregelen bij staan, als wanneer deze er wel bij staan, maakt u een risicoafweging. Op die manier bekijkt u welke maatregelen nodig zijn om de controls af te dekken. De ISO:27002 kan helpen bij het bepalen van maatregelen.

45. Moet ik voor BBN2 ook de maatregelen uit BBN1 implementeren?

Kort en goed gezegd: ja.

46. Waar vind ik de thematische uitwerkingen voor de BIO-maatregelen?

De thema-uitwerkingen zijn (voor zover beschikbaar) ook gepubliceerd in wiki-vorm op de website van NORA: **https://www.noraonline.nl/wiki/isor**.

47. Wat is de betekenis van de letter 'G' in het kader van de waarden G/B/I/V bij de maatregelen?

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

Specifieke maatregelen

48. Waarom is BIR2017-maatregel 16.1.7.1 in de BIO vervallen?

Door een fout is maatregel 16.1.6.1 ook op de plek van maatregel 16.1.7.1 terechtgekomen in de BIR2017. 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 dus schijnbaar een maatregel bijgekomen, maar feitelijk bestond die maatregel al. Het klopt nu dus wel.

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

Kort en goed gezegd: ja, 'beoordeeld' bevat ook 'verwijderen'.

50. Bij maatregelen 9.4.1.1 en 9.4.1.2 wordt gesproken over 'informatie met specifiek belang'. Wat wordt daarmee bedoeld?

Hier wordt bedoeld: het beschermen van informatie die niet openbaar is. De term specifiek belang moet hier breed worden geïnterpreteerd. Zodra de informatie niet voor iedereen is bedoeld, of dat nu is vanwege een rubricering, privacy of commercieel vertrouwelijke informatie, moet ervoor worden gezorgd dat de informatie goed afgeschermd is (fysiek dan wel logisch). Daarbij gaat maatregel 9.4.1.1 over het nemen van maatregelen om te voorkomen dat mensen te veel informatie kunnen zien ('least privallage') en maatregel 9.4.1.2 over het recht om iets te mogen zien (bijv. het inzien van informatie die nodig is voor het uitoefenen van een taak).

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

Ja, en dat wordt in paragraaf 12.4 van de BIO uitgewerkt.

52. 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?

Het beschermen van een control tegen bedreigingen van buitenaf moet worden gedaan of is handig om te doen voor alle bedrijfskritische processen. Dat betekent wel dat alle bedrijfskritische processen eerst moeten worden geanalyseerd.

Vervolgens kunnen maatregelen voor die kritische bedrijfsprocessen op basis van een expliciete risicoafweging worden doorgevoerd.

53. Hoe kan ik 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?

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.

54. 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?

Het betreft hier de standaarden die gangbaar zijn binnen een overheidslaag. Voor Rijkskantoren staat dit 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.

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

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

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

Een onvertrouwde zone is die zone waarover geen invloed kan worden uitgeoefend door de eigen partij. De meest voor de hand liggende onvertrouwde zone is het internet. Zie ook FAQ 55.

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

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 onderscheppen informatie niet zomaar toegankelijk is. Zie ook FAQ 54.

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

In communicatie met de overheid moet een leverancier hier aan voldoen. Een leverancier moet op onafhankelijke wijze kunnen aantonen dat de partij aan de geldende normen voldoen. Het gaat daarbij expliciet om onafhankelijke aantoonbaarheid. Een audit is niet nodig als de leverancier d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd, maar in alle andere gevallen is het noodzakelijk om hierover afspraken te maken.

59. 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?

In het rijtje ondersteunend, belangrijk, strategisch en kritisch strategisch is de laatst genoemde – 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 en visie van een organisatie. (missie = doelen, visie = waarom).

60. Bij maatregel 17.1.3.3.2 ("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?

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; subprocessen 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 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

61. 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 dan worden gehanteerd voor informatiebeveiliging?

De BIO is van toepassing op alle organisatieonderdelen van de overheid. Uitgangspunt is dat de proceseigenaar op basis van risicomanagement bepaalt welk basis beveiligingsniveau (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-standaarden 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 de ISO-standaarden, zal in de meeste gevallen de beveiligingseisen die een overheidsopdrachtgever stelt aan zijn of haar leverancier op z'n minst herkenbaar zijn en waarschijnlijk reeds geïmplementeerd.

62. Hoe moet ik de BIO aan externe dienstenleveranciers voorleggen?

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 gebonden aan de BIO. Een externe dienstenleverancier niet. Conform hoofdstuk 15 van de BIO zorgt u voor een contract met een externe leverancier waarin de afspraken rondom informatiebeveiliging zijn opgenomen. U kunt daarin aangeven waar de leverancier aan moet voldoen.

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

Ga het gesprek aan met uw leverancier om te kijken aan welke maatregelen de leverancier nog niet voldoet en maak op basis daarvan separate afspraken.

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

De medewerker is een breed begrip. Lang niet elke medewerker in een organisatie heeft direct met de BIO te maken. Van een IT-medewerker of HRM'er 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 ten aanzien van informatiebeveiliging is.

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

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

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

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

67. Als mijn leverancier een ISO27001-certificering heeft, is dat dan ook goed?

Het is mogelijk dat een (externe) diensten-leverancier beschikt over een ISO27001-certificering, ISAE3402 soc type 1 of 2 auditrapport of een ander kwaliteitskeurmerk. Een dergelijk keurmerk geeft een waarborg over het proces dat bij de dienstenleverancier is ingericht, maar geeft niet aan op welk niveau de beveiliging is gerealiseerd.

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

De eisen staan nu in hoofdstuk 4 'Verantwoording over de BIO' van de BIO in deel 1. Omdat deel 1 ('Achtergrond BIO') en 2 ('Kader BIO') van de BIO hebben hetzelfde gewicht, is een toevoeging in hoofdstuk 15 niet nodig.

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

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 crux het vinden van een vergelijkbaar instrument. Als je dat hebt, dan kun je een goede afweging maken en is er geen probleem. Let wel, als je een Nederlandse medewerkers wel om een VOG vraagt en buitenlandse medewerkers niet, is er sprake van discriminatie.

Verantwoording

70. Wat moet ik doen als ik niet aan een control of maatregel kan/wil voldoen?

Het niet invullen van een control moet intern kunnen worden toegelicht. 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.

71. Moet ik een explain indienen als ik ergens niet aan voldoe?

Nee, in principe niet, tenzij hiermee de veiligheid van andere partijen wordt geraakt. In dat geval moet u de situatie bespreken binnen uw 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.

72. Moet ik over alle controls en maatregelen verantwoording afleggen?

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 (BBN) onderscheid in de striktheid van de verantwoording.

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

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.

74. Zijn alle maatregelen vanuit privacy regelgeving ook opgenomen in de BIO?

Nee, maar een aantal relevante maatregelen is wel opgenomen. Wanneer u persoonsgegevens beschermt, helpt de BIO wel bij het invulling geven aan passende beveiligingsmaatregelen.

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

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

76. Bij wie worden incidenten gemeld?

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

77. Wanneer leggen leveranciers verantwoording af?

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?

Wanneer de organisatie op basis van risicomanagement invulling heeft gegeven aan alle controls en maatregelen van de BIO die van toepassing zijn, én 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?

Nee, het zonder meer certificeren tegen de BIO is niet mogelijk. 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 bij 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 normenset bij het vaststellen van de controls die van toepassing zijn op de scope van een management systeem (ISMS) in het traject van een certificering in het kader van de ISO27001. De maatregelen waarmee de beveiligingsdoelstelling

Transitie naar de BIO

80. Wat houdt de transitieperiode in?

Op 1 januari 2019 is de BIO van kracht geworden. Om organisaties de tijd te geven om de omslag van de oude baseline naar de nieuwe BIO te maken, is er afgesproken dat er een overgangsperiode is die organisaties gebruiken om de BIO te implementeren. Het tijdspad hierbij is door elke overheidslaag zelf bepaald. Meer informatie hierover vindt u op de websites van de bestuurslagen.

81. Wanneer moeten overheden verantwoorden volgens de BIO?

Vanaf 1 januari 2019 is de BIO het algemeen geldend normenkader voor de Nederlandse overheid. 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 BIR2017 niet wordt verstoord met goedkeuring van BIO 1.0. Zodra een rijksoverheidsorganisatie de BIR2017 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 BIR2017 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?

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

83. Wat houdt het ondersteuningsprogramma precies in?

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 implementatiepad. Daarnaast is een interbestuurlijk ondersteuningsprogramma opgezet waarin alle overheidslagen betrokken zijn. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is

daarbij de opdrachtgever. Het ondersteuningsprogramma is de komende twee jaar bedoeld als stimulans voor een overheidsbrede implementatie van de BIO.

84. Welke ondersteuningsmaterialen komen er beschikbaar?

Vanuit het ondersteuningsprogramma worden diverse middelen en activiteiten ontwikkeld om bestuurders en professionals te ondersteunen bij de implementatie van de BIO, waaronder: thematische workshops, handreikingen en thema-uitwerkingen. Kijk op: **https://bio-overheid.nl/category/workshops** en **https://bio-overheid.nl/category/kennis**.

85. Wat zijn handreikingen?

De handreikingen helpen met het geven van invulling van controls en maatregelen. Ze bieden een basis die kan worden gebruikt in uw organisatie. U bent niet verplicht om deze handreikingen te gebruiken. U vindt meer informatie over de handreikingen op de websites van de koepels van de bestuurslagen.

86. De BIV-maatregelen ontbreken in de BIO, hoe kan ik hier toch mee aan de slag?

VNG-IBD heeft de schadescenario's reeds 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 komen er beschikbaar?

Reeds beschikbaar zijn de uitwerkingen voor de thema's: Applicatieontwikkeling, Communicatievoorzieningen, Huisvesting, Serverplatform en Toegangsbeveiliging. In de loop van 2019 zullen daar nog uitwerking bijkomen van de thema's Beheersprocessen, Beleidsthema's, Cloud, Database & Opslag en Softwarepakketten.

88. Waar kan ik de BIO thema-uitwerkingen vinden?

De thema-uitwerkingen zijn (voor zover beschikbaar) ook gepubliceerd in wiki-vorm op de website van NORA: **https://www.noraonline.nl/wiki/isor**.

89. Waar kan ik terecht met mijn inhoudelijke vragen?

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