BIO Baseline Informatiebeveiliging Overheid

voor een veilige digitale overheid

FAQ’s Baseline Informatiebeveiliging Overheid

v1.02

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. 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.

8. Wat gebeurt er met de BIR, BIG, BIWA en IBI?

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

9. 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.

10. 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.

11. 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.

12. 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**.

ISO 27001/27002

13. 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.

14. 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.

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

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

16. 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.

17. 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)

18. 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.

19. 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 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'.

Bij BBN3 gaat het om informatie waar weerstand tegen statelijke of criminele actoren (of gelijksoortige dreigers) nodig is. De vertrouwelijkheid heeft hier een hogere score, de andere eisen kunnen nog altijd op midden zitten.

20. 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 systemen zonder vertrouwelijke informatie aan minder complexe risicomanagement en verantwoordingseisen te voldoen, waarbij nog altijd wel een minimum beveiligingsniveau wordt gewaarborgd.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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

28. Wat zijn controls?

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

29. 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.

30. 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.

31. 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.

32. Wat zijn maatregelen?

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

33. 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.

34. 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.

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

Kort en goed gezegd: ja.

Rollen

36. 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.

37. 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.

38. 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.

39. 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.

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

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

41. 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.

Verantwoording

42. 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 de Subcommissie Informatiebeveiliging) en door het ministerie worden voorgelegd aan het CIO-Beraad.

43. 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.

44. 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.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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'.

50. 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.

Transitie naar de BIO

51. 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.

52. Wanneer moeten overheden verantwoorden volgens de BIO?

Vanaf 1 januari 2020 zijn alle bestuurslagen en bestuursorganen krachtens de richtlijn verplicht om volledig conform de BIO te werken.

53. 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.

54. 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.

55. 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**.

56. 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.

57. 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).

58. 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.

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

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

60. 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).