

COURSEWARE

# Certified BIO2 (CBP) Practitioner Courseware

Voor de toepassing van de **Baseline  
Informatiebeveiliging Overheid (BIO2)**

Stefan van der Leede

**Certified BIO2 (CBP)  
Practitioner  
Courseware**

Voor de toepassing van  
de Baseline Informatiebeveiliging Overheid (BIO2)

## Colofon

|                 |                                                                          |
|-----------------|--------------------------------------------------------------------------|
| Titel:          | Certified BIO2 (CBP) Practitioner Courseware                             |
| Subtitel:       | Voor de toepassing van de Baseline Informatiebeveiliging Overheid (BIO2) |
| Auteur:         | Stefan van der Leede                                                     |
| Uitgever:       | Van Haren Publishing, 's-Hertogenbosch                                   |
| ISBN Hard Copy: | 978 94 018 1514 7                                                        |
| Druk:           | Eerste editie, Oktober, 2026                                             |
| Vormgeving:     | Van Haren Publishing, 's-Hertogenbosch                                   |
| Copyright:      | © Van Haren Publishing 2026                                              |

Voor verdere informatie over Van Haren Publishing, e-mail naar: [info@vanharen.net](mailto:info@vanharen.net)

Geen enkel deel van deze publicatie mag worden gereproduceerd, opgeslagen in een geautomatiseerd gegevensbestand, of verzonden in welke vorm of op welke wijze dan ook elektronisch, mechanisch, door fotokopieën, opnamen of anderszins zonder voorafgaande toestemming van de auteursrechthebbenden.

Specifiek geldt dat, zonder dergelijke schriftelijke toestemming, het gebruik of de opname van deze publicatie, geheel of gedeeltelijk, niet is toegestaan voor het trainen of ontwikkelen van Large Language Models (LLM) of andere generatieve kunstmatige-intelligentiesystemen. Evenmin is het toegestaan deze publicatie te gebruiken in, of in verband met, dergelijke technologieën, hulpmiddelen of modellen om gegevens of inhoud te genereren en/of deze te synthetiseren of te combineren met andere gegevens of inhoud.

## **Uitgever over de courseware**

De courseware is ontwikkeld door experts uit de praktijk, die als auteur(s) van deze publicatie hebben gefungeerd. De inhoud is gebaseerd op bestaande publicaties en op de ervaring en expertise van de auteur(s). Trainers die zelf met het materiaal werken, hebben het herzien. Daarbij is ook nauwkeurig gekeken naar de belangrijkste leerpunten, zodat duidelijk is wat de cursist moet beheersen.

Het doel van de courseware is de trainer en de cursist tijdens de training zo goed mogelijk te ondersteunen. Het materiaal is modulair opgebouwd. Volgens de auteur(s) geeft het de grootste kans op succes als de cursist ervoor kiest examen te doen. Daarom is de courseware, waar van toepassing, ook geaccrediteerd.

Voor accreditatie moet het materiaal aan bepaalde kwaliteitseisen voldoen. De opbouw, het gebruik van bepaalde termen, diagrammen en verwijzingen maken allemaal deel uit van deze accreditatie. Voor volledige accreditatie moet het materiaal bovendien aan elke cursist ter beschikking worden gesteld. Om de trainer en de deelnemer zo goed mogelijk te ondersteunen, worden bij het materiaal opdrachten, oefenexamens en de uitwerkingen daarvan meegeleverd.

Op de slides wordt ook regelmatig direct verwezen naar aanbevolen literatuur. Zo kunnen cursisten meer informatie over een bepaald onderwerp vinden. Er is bewust gekozen om geen notitiepagina's in de courseware op te nemen. Zo worden cursisten aangemoedigd om door het hele materiaal heen aantekeningen te maken. De courseware is volledig, maar het kan gebeuren dat de trainer afwijkt van de opbouw van de sheets of niet alle sheets of opdrachten behandelt. De cursist kan deze onderwerpen dan altijd zelf, in eigen tijd, doornemen. Voor de beste examenvorbereiding raden we aan de opbouw van de courseware en de publicaties te volgen.

De courseware en de aanbevolen literatuur vormen samen de ideale combinatie om de theorie te leren en te begrijpen.

— Van Haren Publishing

## Andere uitgaven bij Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven over best practices, methodes, frameworks en standaarden op het gebied van de volgende domeinen:

- IT-management;
- Enterprise-architectuur;
- Projectmanagement;
- Businessmanagement.

Deze uitgaven zijn beschikbaar in meerdere talen en maken deel uit van toonaangevende series, zoals Best Practice series en The Open Group series.

Van Haren Publishing is de uitgever voor toonaangevende instellingen en bedrijven, waaronder Agile Consortium, World Commerce and Contracting, IAOP, IPMA World, KNVI, PMI-NL, NLAIC en The Open Group.

Van Haren Publishing maakt deel uit van de Van Haren Group, die naast publicaties ook trainingsmaterialen en e-learning aanbiedt via Van Haren Learning Solutions, evenals professionele certificering via examens onder Van Haren Certify.

Onderwerpen per domein zijn:

|                                |                               |                                                                               |
|--------------------------------|-------------------------------|-------------------------------------------------------------------------------|
| <b>IT-Management</b>           | IT-servicemanagement          | FitSM, ISM®, ISO/IEC20000, IT4IT®, ITIL®, VerISM®, SAF, TRIM, XLA®            |
|                                | Datamanagement                | Data literacy, Data visualization, DMBOK                                      |
|                                | IT-assetmanagement            | HAM, ITAM, SAM                                                                |
|                                | IT-securitymanagement         | BIO, ISO/IEC27001, NIS2                                                       |
|                                | Testmanagement                | CTAP                                                                          |
|                                | Applicatiemanagement          | ASL                                                                           |
|                                | Overig                        | eCF, IT-CMF, Scrum                                                            |
| <b>Projectmanagement</b>       | Projectmanagement             | Half Double, ICB, ISO/IEC21500, P3.express, PM2, PMBOK Guide, Praxis, PRINCE2 |
|                                | Agile                         | Agile, Agile PM                                                               |
|                                | Overig                        | PMO                                                                           |
| <b>Businessmanagement</b>      | Operationsmanagement          | Lean, Lean Six Sigma, OBM, OMC, RASCI                                         |
|                                | Contractmanagement            | CATS CM, CATS RVM,                                                            |
|                                | IACCM World                   | BiSL, DID                                                                     |
|                                | Business informatiemanagement | BiSL, DID                                                                     |
|                                | Artificial intelligence       | AI, Generative AI                                                             |
| <b>Enterprise-architectuur</b> | Enterprise-architectuur       | BIAN, TOGAF                                                                   |
|                                | Modeling                      | ArchiMate, BPMN                                                               |
|                                | Softwarearchitectuur          | ISAQB                                                                         |
|                                | Overig                        | Open Agile Architecture                                                       |

Voor een compleet overzicht van alle uitgaven, ga naar onze website: [www.vanharen.net](http://www.vanharen.net)

## Inhoudsopgave

|                                                   | -- Slidenummer | -- Paginanummer |
|---------------------------------------------------|----------------|-----------------|
| Zelfreflectie                                     |                | 6               |
| Syllabus                                          |                | 8               |
| Module 0 - Kennismaken, Verwachtingen, Voorkennis | (2)            | 15              |
| Module 1 - Inleiding                              | (7)            | 17              |
| Module 2 - Governance deel 1                      | (50)           | 32              |
| Module 3 - Waar staan we?                         | (85)           | 49              |
| Module 4 - Wat gaan we doen?                      | (131)          | 70              |
| Module 5 - Governance deel 2                      | (147)          | 77              |
| Werkboek                                          |                | 85              |
| Checklist                                         |                | 111             |

## Diagram Zelfreflectie op begrip

Met dit diagram kun je je kennis en begrip van het materiaal evalueren. Vul hem in om te kijken hoe je ervoor staat. Om voor het examen te slagen zou je ernaar moeten streven om in het bovenste gedeelte van niveau 3 uit te komen. Wil je echt een pro worden? Richt je pijlen dan op niveau 4. Je algemene niveau van begrip zal natuurlijk de leercurve volgen. Daarom is het belangrijk dat je op ieder moment van de training weet waar je zit in het diagram en dat je aandacht besteedt aan de knelpunten. Op basis van je positie in het diagram Zelfreflectie op begrip, kun je de voortgang van je eigen training evalueren.

| Niveau van begrip                                                                         | Voor de training<br>(voorkennis) | Training<br>Deel 1 (1ste helft) | Training<br>Deel 2 (2de helft) | Nadat je het boek hebt<br>doorgenomen en hebt<br>gestudeerd | Nadat je de oefeningen<br>en het proefexamen<br>gemaakt hebt |
|-------------------------------------------------------------------------------------------|----------------------------------|---------------------------------|--------------------------------|-------------------------------------------------------------|--------------------------------------------------------------|
| <b>Niveau 4</b><br><i>Ik kan de inhoud begrijpen en toepassen.</i>                        |                                  |                                 |                                |                                                             |                                                              |
| <b>Niveau 3</b><br><i>Ik snap het! Ik zit op de goede weg</i>                             |                                  |                                 |                                |                                                             | Klaar voor het examen                                        |
| <b>Niveau 2</b><br><i>Ik begrijp het bijna. Ik zou nog wat oefening kunnen gebruiken.</i> |                                  |                                 |                                |                                                             |                                                              |
| <b>Niveau 1</b><br><i>Ik leer, maar begrijp het nog niet echt.</i>                        |                                  |                                 |                                |                                                             |                                                              |

(Diagram Zelfreflectie op begrip)

Noteer welke knelpunten je nog tegenkomt zodat je ze zelf of met je trainer kunt oplossen.  
Evalueer daarna met behulp van het diagram of je beter begrijpt waar je staat op de leercurve.

### Probleemoplossing

***Knelpunt:***

***Onderwerp:***

**Deel 1**

**Deel 2**

**Nadat je het boek  
hebt doorgenomen  
en hebt gestudeerd**

**Nadat je  
oefeningen en het  
proefexamen hebt  
gemaakt**

# Syllabus

## Certified BIO2 Professional - Practitioner (CBP-P)

Versie 1.0



Alle rechten voorbehouden. Niets uit deze publicatie mag worden verveelvoudigd, gedistribueerd, opgeslagen in een gegevensverwerkingssysteem of openbaar gemaakt worden door middel van druk, fotokopie of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van de uitgever.

Dit materiaal bevat diagrammen en teksten gebaseerd op:  
Foundation training Baseline Informatiebeveiliging Overheid  
Certified BIO Professional - Foundation (CBP-F)

Alle namen van merken, bedrijven en producten worden uitsluitend gebruikt voor identificatiedoeleinden. Het kunnen handelsmerken zijn die het exclusieve eigendom zijn van hun respectieve eigenaars.

## Inhoudsopgave

|                                                            |    |
|------------------------------------------------------------|----|
| Beschrijving .....                                         | 10 |
| Samenvatting.....                                          | 10 |
| Belangrijke voordelen van certificering.....               | 10 |
| Doelgroep.....                                             | 10 |
| Over BIO en CBP-P certificering.....                       | 10 |
| Achtergrond BIO.....                                       | 10 |
| CBP-P Certificering .....                                  | 10 |
| Certificeringseisen .....                                  | 10 |
| Training en praktijk.....                                  | 11 |
| Studie inspanning (ECTS) .....                             | 11 |
| Leerdoel classificatie .....                               | 11 |
| Examen .....                                               | 11 |
| Literatuur .....                                           | 12 |
| Regelgeving en beleid.....                                 | 12 |
| Leerdoelen Certified BIO Professional - Practitioner ..... | 13 |
| Exameneisen en Specificatie .....                          | 14 |

## Beschrijving

Deze syllabus beschrijft de examinering voor de Certified BIO2 Professional - Practitioner (CBP-P). Dit betreft de certificering voor het kunnen toepassen van de Baseline Informatiebeveiliging Overheid (BIO). De BIO beschrijft een gemeenschappelijk basisniveau voor informatiebeveiliging voor alle overheidsorganisaties. Met een CBP-P certificering is het kunnen implementeren en toetsen van informatiebeveiliging binnen de overheid aantoonbaar.

## Samenvatting

De CBP-P certificering bestaat uit training, een praktijktoets en een examen. In de training wordt het noodzakelijke begrip en de noodzakelijke vaardigheden aangeleerd. Met de praktijktoets en het examen worden begrip en vaardigheden over de implementatie van de BIO getoetst.

## Belangrijke voordelen van certificering

- Aantoonbare kennis, inzicht en begrip van de BIO
- Aantoonbare vaardigheden in het kunnen toepassen van de BIO in de praktijk

## Doelgroep

De CBP-P certificering is voor iedereen die werkt bij het Rijk, Gemeenten, Waterschappen of Provincies en betrokken is bij de implementatie of voortzetting van de Baseline Informatiebeveiliging Overheid. De certificering is ook geschikt voor partijen die samenwerken met de overheid (ketenpartners), in die samenwerking ook verantwoordelijkheid dragen voor de informatieveiligheid en om die reden meer inzicht willen krijgen in de BIO.

Het instroomniveau van de CBP-P is de Certified BIO Professional - Foundation (CBP-F) of vergelijkbaar kennis niveau. De CBP-P borduurt voort op de kennis en het inzicht dat in CBP-F of een vergelijkbare andere BIO training is aangeleerd.

Functies waarvoor de CBP-P certificering in ieder geval geschikt is:

- CISO's
- Informatiebeveiligingsfunctionarissen
- Medewerkers die een specifieke rol in informatiebeveiliging hebben
- Medewerkers bij toeleveranciers die kennis van de BIO nodig hebben
- Managers

## Over BIO en CBP-P certificering

De BIO is de verplichte standaard voor Informatiebeveiliging voor Rijk, Provincies, Waterschappen en Gemeenten. De BIO wordt aanbevolen voor onder andere overheidsorganisaties, publiek-private samenwerkingen en organisaties waarbij de overheid de enige aandeelhouder is.

## Achtergrond BIO

De BIO is gebaseerd op de internationale standaard voor informatiebeveiliging (ISO/IEC 27001) en de best practice (ISO/IEC 27002). De BIO is een baseline waarbij uitgegaan wordt van een minimaal (verplicht) niveau van beveiliging.

Zie meer over de BIO op: <https://bio-overheid.nl>

## CBP-P Certificering

Professionals die Certified BIO Professional – Practitioner zijn hebben niet alleen kennis over de BIO standaard maar zijn daarnaast ook in staat om deze te implementeren binnen organisaties.

## Certificeringseisen

Certificering bestaat uit drie vereiste onderdelen:

- Het volgen van de training
- Het behalen van het multiple-choice examen
- Het maken van de praktijkopdracht

## Training en praktijk

Training en praktijkopdracht zijn een verplicht onderdeel voor de CBP-P certificering. De praktijkopdracht bestaat uit vier onderdelen. In de verklaring van uitvoering praktijkopdracht Certified BIP Practitioner (CBP-Practitioner) worden de eisen hieromtrent gespecificeerd.

## Studie inspanning (ECTS)

De verwachte te leveren studie inspanning bedraagt 40 uur. Het aantal contacturen voor de CBP-P training bedraagt 24 uur en daarnaast 45 uur werken aan de huiswerkopdrachten en de praktijkopdracht. In verband met deze opdrachten is er ten aanzien van de lesdagen gekozen voor een frequentie van een lesdag per week.

Er wordt niet verwacht dat de cursist diepgaande kennis heeft betreffende informatiebeveiliging. Echter er moet wel een basis kennisniveau zijn op foundation-niveau van de BIO en de belangrijkste begrippen en best practices van informatiebeveiliging.

## Leerdoel classificatie

De Certified BIO Professional - Practitioner certificering volgt de Bloom levels 2 en 3.

Volgens de Bloom Taxonomie houdt dat het volgende in:

- 2 = Begrijpen: De cursist wordt getest op de volgende vaardigheden: het laten zien van begrip van feiten en ideeën, door te organiseren, te vergelijken of uitleg te geven.
- 3 = Toepassen: De cursist kan informatie in een andere context gebruiken, hetgeen betekent: bewerkstelligen, uitvoeren, gebruiken of toepassen.

## Examen

|                                                                                          |                                                                    |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Aantal multiple choice vragen examen:                                                    | 40                                                                 |
| Duur (minuten) van het examen:                                                           | 60 minuten                                                         |
| Minimaal te behalen score voor slagen:                                                   | 70%                                                                |
| Open/Gesloten boek:                                                                      | Gesloten                                                           |
| Taal:                                                                                    | Nederlands                                                         |
| Fysiek exemplaar en online beschikbaarheid:                                              | Alleen online beschikbaar                                          |
| Zijn negatieve vragen onderdeel van het examen:<br>(welke van de volgende is NIET juist) | Ja, leesvaardigheid wordt ook getest                               |
| Zijn er vragen waarbij meerdere antwoorden worden                                        | Ja, dit maakt een detail georiënteerd examen gevraagd:<br>mogelijk |

## Literatuur

Van Haren Publishing is leverancier van de officiële CBP-P literatuur.

CBP-P courseware: Certified BIO Practitioner – Baseline Informatiebeveiliging Overheid - Courseware – Nederlands: ISBN (9789401815130)

Aanvullende documentatie:

|                                                     |                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Baseline Informatiebeveiliging Overheid             | <a href="https://bio-overheid.nl">https://bio-overheid.nl</a>                                                                                                                                                                                                                                           |
| NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002           | <a href="https://www.nen.nl">https://www.nen.nl</a>                                                                                                                                                                                                                                                     |
| Informatiebeveiligingsdienst                        | <a href="https://www.informatiebeveiligingsdienst.nl">https://www.informatiebeveiligingsdienst.nl</a><br>Handreiking-GAP-analyse-v2.01.docx<br>GAP-analyse-BIO-v2.3-ISO27701.xlsx<br>IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf<br>handreiking-indeling-bio-v104zv-aan-iso-iec-27002-2022-v11-def.xlsx |
| Centrum Informatiebeveiliging en Privacybescherming | <a href="https://www.cip-overheid.nl">https://www.cip-overheid.nl</a><br>BIO Self-Assessment:<br>- bio-sa-factsheet-095.pdf<br>- CIP_BIO_SA_individueel_v1_03-def.xlsx<br>de-16-criteria-van-de-bio-sa-v10.pdf<br>handreiking-sturen-op-informatieveiligheid.pdf<br>quickscan-bir2017.pdf               |
| Nationaal Cyber Security Centrum                    | Meest actuele dreigingsbeeld CSBN                                                                                                                                                                                                                                                                       |
| RAVIB                                               | Meest actuele dreigingsbeeld van Ravib                                                                                                                                                                                                                                                                  |

## Regelgeving en beleid

Certified BIO Professional - Practitioner is een begrip dat kwaliteit en een hoge mate van kennis en kunde aantoont. Fraude wordt in geen enkele situatie toegestaan. Als fraude wordt gedetecteerd via het CertN platform (smart examen platform), dan zal de cursist direct zakken voor het examen en geen certificaat ontvangen. De gemaakte kosten voor het examen en/of de cursus worden niet vergoed.

Wanneer iemand niet slaagt voor het examen omdat er niet genoeg goede antwoorden zijn gegeven en er niet voldaan wordt aan het minimale aantal om te slagen (70%) dan zal die persoon ook niet slagen in het behalen van de certificering. Een cursist kan eenmaal het examen afnemen per keer dat het examen besteld is, er is dus één kans om voor het examen te slagen. Wanneer de persoon niet slaagt voor het examen, moet er een nieuw examen worden besteld en succesvol afgenomen om alsnog gecertificeerd te raken.

## Leerdoelen Certified BIO Professional - Practitioner

De leerdoelen geven weer wat deelnemers begrijpen en kunnen wanneer zij Certified BIO Professional - Practitioner zijn.

Deelnemers moeten de BIO begrijpen en kunnen implementeren in de praktijk. Het certificaat dat deelnemers na het slagen voor het examen krijgen dient als bewijs dat de deelnemer:

- Weet welk doel de BIO dient en welke plek de BIO inneemt in het totale palet van informatieveiligheidsmaatregelen;
- De stakeholders kan identificeren die binnen haar/zijn organisatie betrokken zijn bij de implementatie van de BIO en deze kan betrekken bij de implementatie;
- In staat is om het gewenste niveau van informatieveiligheid binnen haar/zijn organisatie te definiëren;
- Een inschatting kan maken op welk volwassenheidsniveau de informatieveiligheid van haar/zijn organisatie zich bevindt;
- Met behulp van de BIO een stapsgewijze aanpak kan definiëren naar een hoger informatieveiligheid volwassenheidsniveau voor haar/zijn organisatie;
- Organisatie breed een BIO GAP analyse kan (laten) uitvoeren;
- Een BIO Quick Scan kan uitvoeren op een bedrijfsproces uit de eigen organisatie;
- Een diepgaande risicoanalyse kan uitvoeren bij afwijkende betrouwbaarheidseisen;
- Op basis van de gekozen beheerdoelstellingen bijbehorende maatregelen kan kiezen én de manier waarop deze maatregelen moeten worden geïmplementeerd.
- In de tijd op basis van voortschrijdend inzicht een GAP analyse kan uitvoeren op de gekozen beheerdoelstellingen én maatregelen om deze indien noodzakelijk aan te passen;
- Een besturingsstructuur kan bedenken én implementeren die garandeert dat er een continu proces van verbetering plaatsvindt op BIO/informatieveiligheid gebied.

## Examineisen en Specificatie

Om de leerdoelen af te dekken is de certificering opgedeeld in verschillende examenvoorwaarden. Deze examenvoorwaarden bestaan weer uit gespecificeerde examineisen. Onderstaande tabel beschrijft de verschillende modules (examenvoorwaarden) en subonderwerpen (examenspecificaties). Daarnaast geeft het ook de zwaarte van telling aan, wat een indicatie is voor de verhouding van de vragen die in het examen worden gesteld.

| Dag | Module | Examen eisen                             | Specificatie                                                                                                              | Niveau (Bloom-level) | Weging % |
|-----|--------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------|----------|
| 1   | 0      | Kennismaken, verwachtingen en voorkennis |                                                                                                                           |                      |          |
|     | 1      | Inleiding                                |                                                                                                                           | 1+2                  | 10%      |
|     | 1.1    |                                          | Doel, achtergrond, context, etc. opfrissen                                                                                |                      |          |
|     | 1.2    |                                          | Relatie met ISO 27001/2, vooruitblik naar 2022 versie.                                                                    |                      |          |
|     | 2      | Governance deel 1                        |                                                                                                                           | 2+3                  | 20%      |
|     | 2.1    |                                          | Stakeholderanalyse                                                                                                        |                      |          |
|     | 2.2    |                                          | Bewustwording stakeholders en gewenst niveau informatieveiligheid                                                         |                      |          |
| 2   | 3      | Waar staan we?                           |                                                                                                                           | 3                    | 25%      |
|     | 3.1    |                                          | Huidige volwassenheidsniveau informatieveiligheid van organisatie                                                         |                      |          |
|     | 3.2    |                                          | Huidige beveiligingsniveau organisatie breed in kaart brengen                                                             |                      |          |
|     | 3.3    |                                          | Huidige beveiligingsniveau per proces / systeem in kaart brengen en BBN niveau bepalen                                    |                      |          |
|     | 3.4    |                                          | Risicoanalyse uitvoeren                                                                                                   |                      |          |
| 3   | 4      | Wat gaan we doen?                        |                                                                                                                           | 3                    | 25%      |
|     | 4.1    |                                          | Welke maatregelen moeten er genomen worden?                                                                               |                      |          |
|     | 4.2    |                                          | De gekozen maatregelen implementeren                                                                                      |                      |          |
|     | 5      | Governance deel 2                        |                                                                                                                           | 2+3                  | 20%      |
|     | 5.1    |                                          | Het monitoren van het beveiligingsniveau en indien noodzakelijk aanpassen van beheerdoelstellingen en gekozen maatregelen |                      |          |
|     | 5.2    |                                          | Het borgen van het continue proces van verbeteren van de informatieveiligheid                                             |                      |          |
|     |        |                                          |                                                                                                                           |                      |          |

# CBP-P dag 1

Certified Baseline Informatiebeveiliging Overheid Professional -  
Practitioner



© Van Haren Publishing

1

## MODULE 0

### KENNISMAKEN VERWACHTINGEN VOORKENNIS

#### Doelstelling

1. Bevestiging dat jullie voldoende voorkennis hebben van de BIO.

COURSEWARE

©2023 - All training materials are sole property of Van Haren Publishing BV  
and are not to be reproduced in any form or shape without written permission.

## Kennismaken

Wie ben ik (docent)?

- Wat zijn mijn verwachtingen.



© Van Haren Publishing

3

## Kennismaken

- Kennismakingsopdracht 0: Wie zijn jullie?
- Security pitches
  - Naam
  - Werkt bij organisatie...
  - Functie / rol
  - Achtergrond / opleiding / ervaring
  - Parate kennis en/of ervaring van/met de BIO
  - Volwassenheidsniveau informatiebeveiliging in organisatie en welke rol speelt de BIO daarin
  - Status informatiebeveiliging binnen de organisatie
  - Wat zijn je verwachtingen?



© Van Haren Publishing

4

## Programma

| Dag | Module | Specificatie                                                                                                               |
|-----|--------|----------------------------------------------------------------------------------------------------------------------------|
| 1   | 0      | Kennismaken, verwachtingen en voorkennis                                                                                   |
|     | 1      | Inleiding                                                                                                                  |
|     | 1.1    | Doel, achtergrond, context, etc. opfrissen                                                                                 |
|     | 1.2    | Relatie met ISO 27001/2, vooruitblik naar 2022 versie.                                                                     |
|     | 2      | Governance deel 1                                                                                                          |
|     | 2.1    | Stakeholderanalyse                                                                                                         |
|     | 2.2    | Bewustwording stakeholders en gewenst niveau informatieveiligheid                                                          |
| 2   | 3      | Waar staan we?                                                                                                             |
|     | 3.1    | Huidige volwassenheidsniveau informatieveiligheid van organisatie                                                          |
|     | 3.2    | Huidige beveiligingsniveau organisatie breed in kaart brengen                                                              |
|     | 3.3    | Huidige beveiligingsniveau per proces / systeem in kaart brengen en BBN niveau bepalen                                     |
|     | 3.4    | Risicoanalyse uitvoeren                                                                                                    |
| 3   | 4      | Wat gaan we doen?                                                                                                          |
|     | 4.1    | Welke maatregelen moeten er genomen worden?                                                                                |
|     | 4.2    | De gekozen maatregelen implementeren                                                                                       |
|     | 5      | Governance deel 2                                                                                                          |
|     | 5.1    | Het monitoren van het beveiligingsniveau en indien noodzakelijk aanpassen van beheersdoelstellingen en gekozen maatregelen |
|     | 5.2    | Het borgen van het continue proces van verbeteren van de informatieveiligheid                                              |
|     |        |                                                                                                                            |



## MODULE 1 INLEIDING

### Doelstelling:

1. Weten welk doel de BIO dient en welke plek de BIO inneemt in het totale palet van informatieveiligheids-maatregelen.



## 27002 versie 2022

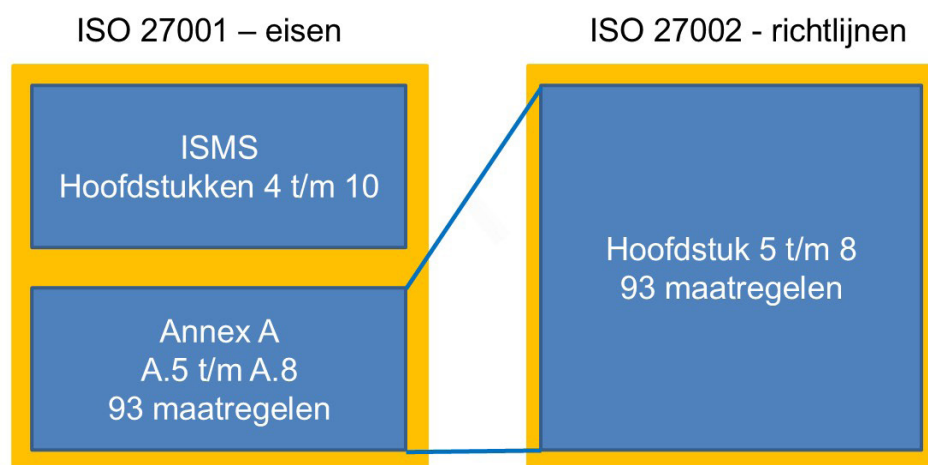


## De samenhang tussen 27001 en 27002

- ISO 27001
  - Hoofdstuk 4 t/m 10: vereisten voor het ISMS
  - Annex A: 114 maatregelen
- ISO 27002
  - Richtlijnen: geen informatie m.b.t. het ISMS
  - Richtlijnen: 114 maatregelen



## De samenhang tussen 27001 en 27002



## ISO 27002: 2013 opbouw

Hoofdstuk

Doelstelling

Maatregel

Maatregel tekst

Implementatie richtlijn

Overige informatie

Maatregel ...

Doelstelling ...



## ISO 27002: 2022 opbouw

Maatregelen verwijderd, samengevoegd en toegevoegd

Maatregelen onderverdeeld in vier hoofdstukken:

1. Organisatorische beheersmaatregelen
2. Mensgerichte beheersmaatregelen
3. Fysieke beheersmaatregelen
4. Technologische beheersmaatregelen



## ISO 27002: 2022

Elke maatregel:

- kent attributen en attriboot eigenschappen;
- bevat informatie over het doel, de richtlijnen en overige aanvullende informatie.

Annex A: biedt een tabel aan om te kunnen werken met attributen

Annex B: referentie tussen 2013 en 2022 versies



## Attributen, attriboot perspectieven

Type beheersmaatregel

- Preventief, Detectief, Correctief

Informatiebeveiligingseigenschappen

- Beschikbaarheid, Integriteit, Vertrouwelijkheid

Cybersecurity concepten

- Identificeren, Beschermen, Detecteren, Reageren, Herstellen

Operationele vaardigheden

Beveiligingsdomeinen



## Operationele capaciteiten

*Operationele capaciteiten zijn een attribuut om interne beheersingsmaatregelen te bekijken vanuit het perspectief van de beoefenaar van informatiebeveiligingscapaciteiten*

- Governance
- Beheer van bedrijfsmiddelen
- Informatiebescherming
- Personeelsbeveiliging
- Fysieke beveiliging
- Systeem en netwerkbeveiliging
- Toepassingsbeveiliging
- Veilige configuratie
- Identiteits- en toegangsbeheer
- Beheer van dreigingen en kwetsbaarheden
- Continuïteit
- Beveiliging in leveranciersrelaties
- Juridisch en compliance
- Beheer van informatiebeveiligings gebeurtenissen
- Borging van informatiebeveiliging



## Domeinen

*Veiligheidsdomeinen is een attribuut om controles vanuit vier informatiebeveiligingsdomeinen te bekijken*

- Governance en ecosysteem
- Bescherming
- Verdediging
- Veerkracht



## Voorbeeld

Tabel A.1 — Matrix van beheersmaatregelen en attribuutwaarden

| Identificatie-code beheersmaatregel<br>ISO/IEC 27002: 2022 | Naam beheersmaatregel                                     | Type beheersmaatregel | Informatiebeveiligings-eigenschappen                   | Cybersecurity-concepten | Operationele capaciteiten | Beveiligingsdomeinen                                         |
|------------------------------------------------------------|-----------------------------------------------------------|-----------------------|--------------------------------------------------------|-------------------------|---------------------------|--------------------------------------------------------------|
| 5.1                                                        | Beleidsregels voor informatiebeveiliging                  | #Preventief           | #Vertrouwelijkheid<br>#Integriteit<br>#Beschikbaarheid | #Identificeren          | #Governance               | #Governance_en<br>_Ecosysteem<br>#Veerkracht                 |
| 5.2                                                        | Rollen en verantwoordelijkheden bij informatiebeveiliging | #Preventief           | #Vertrouwelijkheid<br>#Integriteit<br>#Beschikbaarheid | #Identificeren          | #Governance               | #Governance_en<br>_Ecosysteem<br>#Bescherming<br>#Veerkracht |



## A5 Organisatorische beheersmaatregelen (1v4)

- A.5.1 Beleidsregels voor informatiebeveiliging Rood = nieuw !
- A.5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging
- A.5.3 Functiescheiding
- A.5.4 Managementverantwoordelijkheden
- A.5.5 Contact met overheidsinstanties
- A.5.6 Contact met speciale belangengroepen
- A.5.7 Informatie en analyses over dreigingen: Informatie met betrekking tot informatiebeveiligingsdreigingen behoort te worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.
- A.5.8 Informatiebeveiliging in projectmanagement
- A.5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen
- A.5.10 Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen



## A5 Organisatorische beheersmaatregelen (2v4)

- A.5.11 Retourneren van bedrijfsmiddelen
- A.5.12 Classificeren van informatie
- A.5.13 Labelen van informatie
- A.5.14 Overdragen van informatie
- A.5.15 Toegangsbeveiliging
- A.5.16 Identiteitsbeheer
- A.5.17 Beheren van authenticatie-informatie
- A.5.18 Toegangsrechten
- A.5.19 Informatiebeveiliging in leveranciersrelaties
- A.5.20 Adresseren van informatiebeveiliging in leveranciersdiensten



## A5 Organisatorische beheersmaatregelen (3v4)

- A.5.21 Beheren van informatiebeveiliging in de ICT-keten
- A.5.22 Monitoren, beoordelen en beheren van wijzigingen van leveranciersdiensten
- A.5.23 *Informatiebeveiliging voor het gebruik van clouddiensten: Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten behoren overeenkomstig de informatiebeveiligingseisen van de organisatie te worden opgesteld.*
- A.5.24 Plannen en voorbereiden van het Beheer van informatiebeveiligingsincidenten
- A.5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen
- A.5.26 Reageren op informatiebeveiligingsincidenten
- A.5.27 Leren van informatiebeveiligingsincidenten
- A.5.28 Verzamelen van bewijsmateriaal



## A5 Organisatorische beheersmaatregelen (4v4)

- A.5.29 Informatiebeveiliging tijdens een verstoring
- A.5.30 ICT-gereedheid voor bedrijfscontinuïteit
- A.5.31 Wettelijke, statutaire, regelgevende en contractuele eisen
- A.5.32 Intellectuele-eigendomsrechten
- A.5.33 Beschermen van registraties
- A.5.34 Privacy en bescherming van persoonsgegevens
- A.5.35 Onafhankelijke beoordeling van informatiebeveiliging
- A.5.36 Naleving van beleid, regels en normen voor informatiebeveiliging
- A.5.37 Gedocumenteerde bedieningsprocedures



## A.6 Mensgerichte beheersmaatregelen

- A.6.1 Screening
- A.6.2 Arbeidsovereenkomst
- A.6.3 Bewustwording van, opleiding en training in informatiebeveiliging
- A.6.4 Disciplinaire procedure
- A.6.5 Verantwoordelijkheden na beëindiging of wijziging van het dienstverband
- A.6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten
- A.6.7 Werken op afstand
- A.6.8 Melden van informatiebeveiligingsgebeurtenissen



## A.7 Fysieke beheersmaatregelen (1v2)

- A.7.1 Fysieke beveiligingszones
- A.7.2 Fysieke toegangsbeveiliging
- A.7.3 Beveiligen van kantoren, ruimten en faciliteiten
- A.7.4 *Monitoren van fysieke beveiliging: Het gebouw en terrein behoort voortdurend te worden gemonitord op onbevoegde fysieke toegang.*
- A.7.5 Beschermen tegen fysieke- en omgevingsdreigingen
- A.7.6 Werken in beveiligde zones
- A.7.7 'Clear desk' en 'clear screen'
- A.7.8 Plaatsen en beschermen van apparatuur
- A.7.9 Beveiligen van bedrijfsmiddelen buiten het terrein



## A.7 Fysieke beheersmaatregelen (2v2)

- A.7.10 Opslagmedia
- A.7.11 Nutsvoorzieningen
- A.7.12 Beveiligen van bekabeling
- A.7.13 Onderhoud van apparatuur
- A.7.14 Veilig verwijderen of hergebruiken van apparatuur



## A.8 Technologische beheersmaatregelen (1v4)

- A.8.1 'User endpoint devices'
- A.8.2 Speciale toegangsrechten
- A.8.3 Beperking toegang tot informatie
- A.8.4 Toegangsbeveiliging op broncode
- A.8.5 Beveiligde authenticatie
- A.8.6 Capaciteitsbeheer
- A.8.7 Bescherming tegen malware
- A.8.8 Beheer van technische kwetsbaarheden
- A.8.9 Configuratiebeheer



## A.8 Technologische beheersmaatregelen (2v4)

- A.8.10 *Wissen van informatie: In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie behoort te worden gewist als deze niet langer nodig is.*
- A.8.11 *Maskeren van gegevens: Gegevens behoren te worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.*
- A.8.12 *Voorkomen van gegevenslekken (Data leakage prevention): Maatregelen om gegevenslekken te voorkomen behoren te worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.*
- A.8.13 Back-up van informatie
- A.8.14 Redundantie van informatieverwerkende faciliteiten



## A.8 Technologische beheersmaatregelen (3v4)

- A.8.15 Logging
- A.8.16 Monitoren van activiteiten
- A.8.17 Kloksynchronisatie
- A.8.18 Gebruik van speciale systeemhulpmiddelen
- A.8.19 Installeren van software op operationele systemen
- A.8.20 Beveiliging netwerkcomponenten
- A.8.21 Beveiliging van netwerkdiensten
- A.8.22 Netwerksegmentatie
- A.8.23 *Toepassen van webfilters: De toegang tot externe websites behoort te worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.*



## A.8 Technologische beheersmaatregelen (4v4)

- A.8.24 Gebruik van cryptografie
- A.8.25 Beveiligen tijdens de ontwikkelcyclus
- A.8.26 Toepassingsbeveiligingseisen
- A.8.27 Veilige systeemarchitecturen technische uitgangspunten
- A.8.28 Veilig coderen
- A.8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie
- A.8.30 Uitbestede systeemontwikkeling
- A.8.31 Scheiding van ontwikkel-, test- en productieomgevingen
- A.8.32 Wijzigingsbeheer
- A.8.33 Testgegevens
- A.8.34 Bescherming van informatiesystemen tijdens audits



## Verwijderde maatregelen (1v5)

- A.6.2.1 Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
- A.9.1.2 Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- A.9.2.1 Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
- A.9.2.6 De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.



## Verwijderde maatregelen (2v5)

- A.9.4.2 Indien het beleid voor toegangsbeveiliging dit vereist, beheerst door een beveiligde inlogprocedure.
- A.9.4.3 Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
- A.11.1.6 Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
- A.11.2.5 Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
- A.11.2.8 Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.



## Verwijderde maatregelen (3v5)

- A.13.2.3 Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
- A.14.1.2 Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
- A.14.1.3 Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.
- A.14.2.3 Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.



## Verwijderde maatregelen (4v5)

- A.14.2.4 Wijzigingen aan softwarepakketten worden ontmoedigd, beperkt tot noodzakelijke wijzigingen en alle wijzigingen worden strikt gecontroleerd.
- A.14.2.6 Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.
- A.14.2.9 Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
- A.16.1.3 Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.



## Verwijderde maatregelen (5v5)

- A.17.1.3 De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.
- A.18.1.5 Crypto grafische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, en wet- en regelgeving.
- A.18.2.3 Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.



## Samengevat

|                           | 2013 |
|---------------------------|------|
| Aantal maatregelen 2013   | 114  |
| Samengevoegde maatregelen | 16   |
| Verwijderde maatregelen   | 19   |
| Nieuwe maatregelen        | 14   |
| Aantal maatregelen 2022   | 93   |



## MODULE 2 GOVERNANCE DEEL 1

### Doelstellingen:

1. De stakeholders kunnen identificeren die binnen jullie organisatie betrokken zijn bij de implementatie van de BIO en deze stakeholders kunnen betrekken bij de implementatie.
2. In staat zijn om het gewenste niveau van informatieveiligheid binnen jullie organisatie te achterhalen.

COU SEWARE

©2023 - All training materials are sole property of Van Haren Publishing BV  
and are not to be reproduced in any form or shape without written permission.

## Wat is governance?

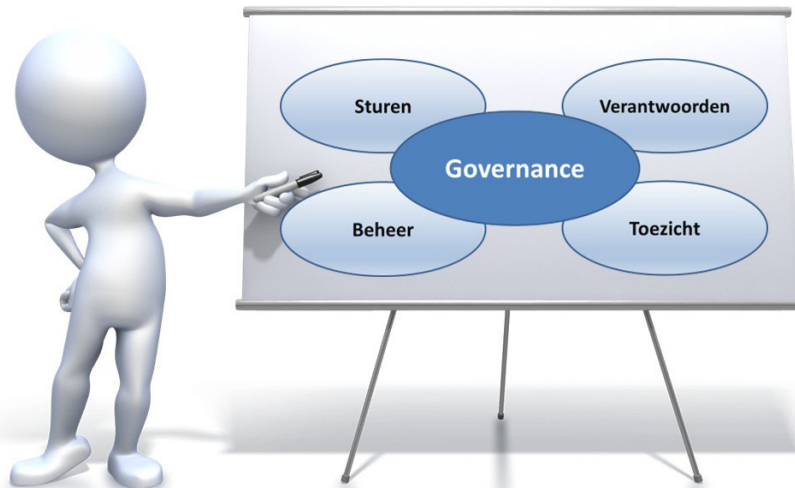


Governance is het waarborgen van de onderlinge samenhang van de wijze van sturen, beheersen en toezicht houden van een organisatie gericht op een efficiënte en effectieve realisatie van beleidsdoelstellingen, alsmede het daarover communiceren en verantwoording afleggen



Doel governance: borging van de effectiviteit van de organisatie

## Activiteiten governance



© Van Haren Publishing

52

## Activiteiten governance



### Sturen

Richting geven aan de realisatie van organisatiedoelen:

- Inrichten van de organisatie
- Vormgeven van processen

### Verantwoorden

Over alle opgedragen taken en gedelegeerde bevoegdheden moet informatie worden verschaft plus het recht op decharge

### Beheer

- Invoering maatregelen en procedures
- Handhaving maatregelen en procedures

### Toezicht

Vaststellen dat de doelstellingen worden gerealiseerd



© Van Haren Publishing

53

## 10 Bestuurlijke principes

1. Bestuurders bevorderen een veilige cultuur
2. Informatiebeveiliging en privacy is van iedereen
3. Informatiebeveiliging en privacy is risicomanagement
4. Risicomanagement is onderdeel van de besluitvorming
5. Informatiebeveiliging en privacy behoeft ook aandacht in (keten)samenwerking
6. Informatiebeveiliging en privacy is een proces
7. Informatiebeveiliging en privacy kost geld
8. Onzekerheid dient te worden ingecalculeerd
9. Verbetering komt voort uit leren en ervaring
10. Het bestuur controleert en evalueert



Bron: Oplegnotitie VNG op de BIO

© Van Haren Publishing

54

## Wat staat er in de BIO? 1v2



Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(-systemen)



Informatiebeveiliging is een cyclisch proces, volgens de Plan-Do-Check-Act cyclus (PDCA)



Deze Plan-Do-Check-Act cyclus maakt het lijnmanagement verantwoordelijk voor het treffen van maatregelen op basis van risicomanagement



De Secretaris/algemeen directeur van een organisatie is eindverantwoordelijk voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie



© Van Haren Publishing

55

## Wat staat er in de BIO? 2v2



Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast



Het lijnmanagement is verantwoordelijk voor de implementatie van de maatregelen op basis van deze betrouwbaarheidseisen



In sommige organisaties heet de eindverantwoordelijke *bestuursvoorzitter* of *directeur* en moet de term secretaris/algemeen directeur als 'directeur' of 'bestuursvoorzitter' worden gelezen



## BIO en NIS2

- Wat is NIS2?
  - Network and Information Security Directive 2
  - Bedoeld om Europa beter te beschermen tegen cyberaanvallen
  - Is breder dan alleen de overheid (raakt alle kritieke sectoren/organisaties)
  - EU-lidstaten dienen NIS2 te verankeren in nationale wetgeving
- BIO versie 2 is in lijn gebracht met NIS2
  - Hoewel de BIO verplicht is voor overheidsorganisaties, is het geen wetgeving
  - Wetgeving om NIS2 te verankeren is in de maak \*)

\*) situatie voorjaar 2026

