Syllabus

Certified BIO Professional - Practitioner (CBP-P)

Version 1

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

Inhoudsopgave

Beschrijving

Deze syllabus beschrijft de examinering voor de Certified BIO 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

Aanwezigheid contacturen:	Minimaal 16 uur = 67%
Aantal opdrachten:	4 samen te voegen tot één geheel
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: (welke van de volgende is NIET juist)	Ja, leesvaardigheid wordt ook getest
Zijn er vragen waarbij meerdere antwoorden worden gevraagd:	Ja, dit maakt een detail georiënteerd examen 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 9789401810272 Baseline Informatiebeveiliging Overheid (BIO) gebaseerd op de ISO 27002:2022
Aanvullende documentatie:	
Baseline Informatiebeveiliging Overheid NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 Informatiebeveiligingsdienst	https://bio-overheid.nl https://www.nen.nl https://www.informatiebeveiligingsdienst.nl Handreiking-GAP-analyse-v2.01.docx GAP-analyse-BIO-v2.3-ISO27701.xlsx IBD_dreigingsbeeld_2023-2024_DEF-versie.pdf handreiking-indeling-bio-v104zv-aan-iso-iec-27002-2022-v11-def.xlsx
Centrum Informatiebeveiliging en Privacybescherming	https://www.cip-overheid.nl BIO Self-Assessment: - bio-sa-factsheet-095.pdf - CIP_BIO_SA_individueel_v1_03-def.xlsx de-16-criteria-van-de-bio-sa-v10.pdf handreiking-sturen-op-informatieveiligheid.pdf 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 plaform (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.

Exameneisen en Specificatie

Om de leerdoelen af te dekken is de certificering opgedeeld in verschillende examenvoorwaarden. Deze examenvoorwaarden bestaan weer uit gespecificeerde exameneisen. 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		