COURSEWARE

Certified BIO2 Professional – Foundation (CBP-F)

Baseline Informatiebeveiliging Overheid Courseware

Ruben Zeegers

Van Haren PUBLISHING

Certified BIO Professional

Certified BIO2 Professional
–
Foundation (CBP-F)

Colofon

Titel:	Certified BIO2 Professional – Foundation (CBP-F) - Baseline Informatiebeveiliging Overheid Courseware
Auteurs:	Ruben Zeegers
Uitgever:	Van Haren Publishing, ‘s-Hertogenbosch
ISBN Hard copy:	978 94 018 1273 3
Druk:	Eerste editie, eerste oplage, oktober 2020 Tweede editie, eerste oplage, januari 2025
Vormgeving:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2025

Voor verdere informatie over Van Haren Publishing, e-mail naar: info@vanharen.net

Over deze courseware

Deze courseware is opgesteld door experts in het vakgebied van Business informatiemanagement, met veel praktijkervaring op het gebied van het produceren en verzorgen van trainingen. De input voor het materiaal bestaat uit bestaande publicaties en de ervaring en expertise van de auteur(s). Het materiaal sluit aan op de exameneisen van APMG en is tevens door APMG geaccrediteerd.

Het doel van de courseware is om de trainer en cursist maximaal te ondersteunen bij zijn of haar opleiding/cursus of voorbereiding op een examen. Het materiaal is modulair opgebouwd en sluit qua opbouw en volgorde aan op de hoofdstukindeling van het BiSL-frameworkboek en op de exameneisen van het BiSL Foundation-examen van APMG.

Om de trainer en deelnemer van de training optimaal te ondersteunen in de beheersing van de theorie, zijn er oefenexamens, opdrachten en uitwerkingen toegevoegd aan het materiaal. Tevens zijn discussievragen opgenomen waarin veelal een verwijzing is opgenomen naar de eigen ervaringen van de cursisten om zo de vertaling van praktijk naar theorie te maken, waardoor de leerstof mogelijk beter "landt".

Waar van toepassing en noodzakelijk voor het Foundation-examen wordt in de sheets verwezen naar de bijbehorende literatuur, waarin de cursist additionele informatie kan vinden over een bepaald onderwerp. Op alle pagina’s is voldoende ruimte opengelaten voor het maken van persoonlijke aantekeningen. Er zijn dus geen aparte notitiepagina’s opgenomen.

Dit courseware-pakket is compleet, en het biedt voldoende vrijheid aan de trainer om in zijn verhaal af te wijken van de opbouw van de sheets ofwel om niet alle sheets of opdrachten te behandelen. En hopelijk voegt de trainer eigen ervaringen en voorbeelden toe! De cursist heeft altijd zelf de mogelijkheid deze onderwerpen in eigen tijd nogmaals door te nemen. Dit wordt eenvoudig gemaakt doordat deze courseware en het BiSL-frameworkboek dezelfde structuur hebben.

De laatste module bevat enkele tips en trucs voor het examen. Daarmee vormt deze courseware, samen met het frameworkboek, de perfecte combinatie om de theorie eigen te maken en goed te begrijpen.

Andere uitgaven van Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven op gebied van Best Practices, methodes en standaarden in de volgende vier domeinen:

- IT en IT Management
- Architectuur (Enterprise en IT)
- Business Management en
- Project Management

Van Haren Publishing publiceert ook voor organisaties en bedrijven zoals: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Onderwerpen zijn (per domein):

IT and IT Management
ABC of ICT
ASL®
CATS
CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture
ArchiMate®
GEA®
Novius Architectuur
Methode
TOGAF®

Business Management
BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

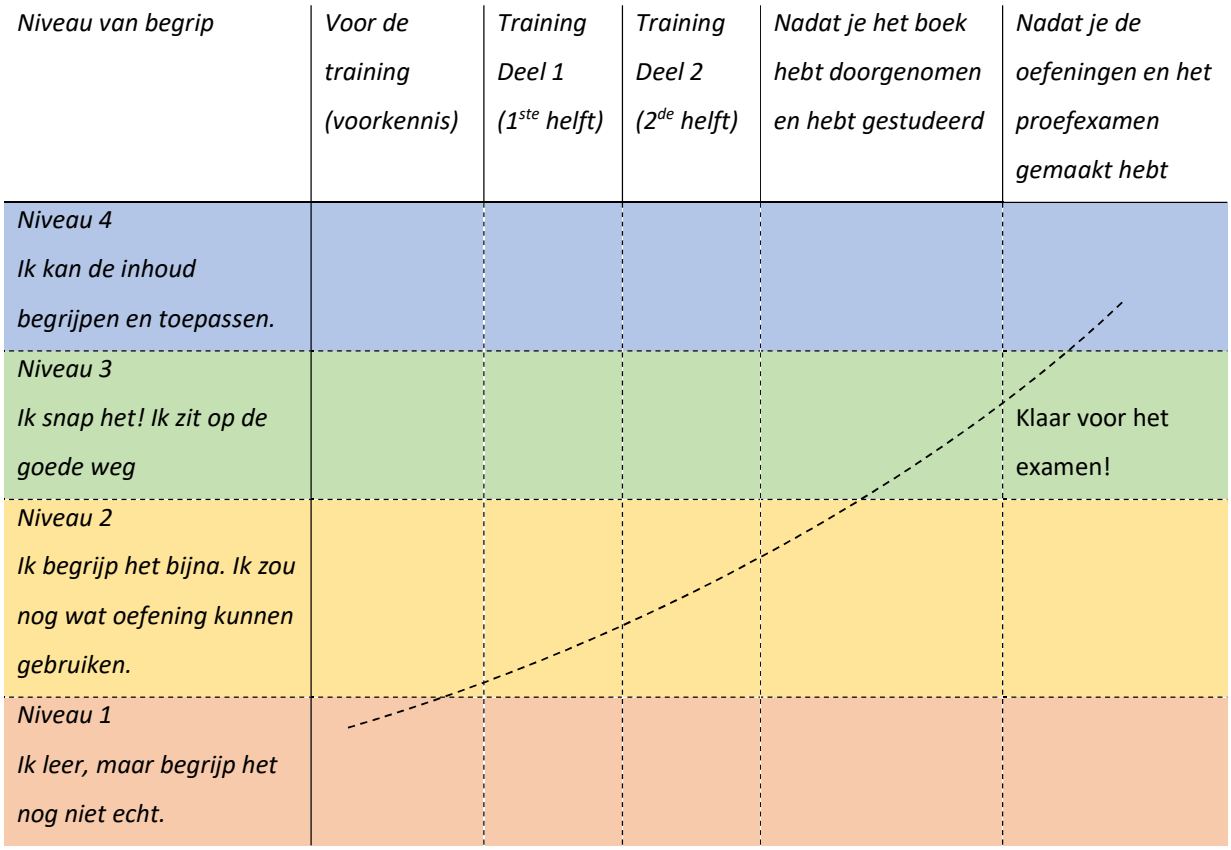
Project Management
A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

Voor de meest recente informatie over VHP uitgaven, bezoek onze website: www.vanharen.net.

Inhoudsopgave

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.



(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	

Agenda

Dag 1

9:00 - 9:30	**Introductie** Kennismaking, over de training en examen
9:30 - 12:00	**Module 1:** Begrippen en inleiding BIO
12:00 - 12:45	Lunch
12:45 - 17:00	**Module 2:** Organisatorische maatregelen **Praktijkopdracht** Risicoanalyse

Dag 2

9:00 - 12:00	**Begrippenbespreking** Gezamenlijke bespreking dag 1 **Module 3:** Mensgerichte en Fysieke maatregelen
12:00 - 12:45	Lunch
12:45 - 17:00	**Module 4:** Technologische maatregelen **Praktijkopdracht** ISMS

Syllabus
Certified BIO2 Professional (CBP) Foundation

Dit materiaal bevat diagrammen en teksten gebaseerd op:
Foundation training Baseline Informatiebeveiliging Overheid

Inhoudsopgave

Beschrijving

Deze syllabus beschrijft de examinering voor Certified BIO2 Professional Foundation (CBP-F). Dit betreft de certificering voor de Baseline Informatiebeveiliging Overheid (BIO). De BIO2 stelt een gezamenlijk basisniveau voor informatiebeveiliging voor alle overheidsorganisaties. Met een CBP-certificering is kennis van informatiebeveiliging binnen de overheid aantoonbaar.

Samenvatting

De CBP-F-certificering bestaat uit training, een praktijkopdracht en een examen. Door de praktijkopdracht wordt praktische toepasbaarheid van de BIO getest. Met het examen wordt kennis van de BIO2 getoetst.

Belangrijke voordelen van certificering

- Aantoonbare kennis van begrippen en principes van de BIO.
- Vertaling van de BIO naar de praktijk.

Doelgroep

De CBP-F-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 wie meer inzicht wil krijgen in de BIO2, maar hierin niet direct een functie heeft, zoals overheidsadviseurs of organisaties die diensten leveren aan de Overheid.

Functies waarvoor de CBP-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 BIO2- en CBP-F-certificering

De BIO2 is de verplichte standaard voor Informatiebeveiliging voor Rijk, Provincies, Waterschappen en Gemeentes. De BIO2 wordt aanbevolen voor andere overheidsorganisaties, publiek-private samenwerkingen en organisaties waarbij de overheid de enige aandeelhouder is.

Achtergrond BIO2

De BIO is een baseline waarbij uitgegaan wordt van een minimaal (verplicht) niveau van beveiliging. Zie meer over de BIO2 op: https://bio-overheid.nl

CBP-F-Certificering

De BIO2 is dus de standaard voor informatiebeveiliging van de Nederlandse Overheid. Professionals die Certified BIO2 Professional zijn hebben kennis over deze BIO-standaard en zijn in staat hier in de praktijk invulling aan te geven.

Certificeringseisen

Certificering bestaat uit drie vereiste onderdelen:

- 16 uur training (inclusief praktijkopdracht)

- behalen van de praktijkopdracht
- behalen van het multiple-choice examen

Training en praktijkopdracht

Training is een verplicht onderdeel voor CBP-certificering. Tijdens de training wordt invulling gegeven aan de praktijkopdracht. CBP-certificering kan alleen door training te volgen bij erkende CBP-trainingsaanbieders. Een erkende CBP-trainingsaanbieder is: https://bio-training.nl

Studie inspanning (ECTS)

De verwachte te leveren studie inspanning bedraagt 24 uur. Het aantal contact-uren voor de BIO Foundation cursus bedraagt 16 uur en daarnaast 8 uur zelfstudie. Er wordt niet verwacht dat de cursist diepgaande kennis heeft betreffende informatiebeveiliging. Echter moet er wel een basisniveau zijn betreffende belangrijkste begrippen en best practices van informatiebeveiliging.

Leerdoel classificatie

De BIO Foundation certificering volgt de Bloom levels 1 en 2.
Volgens de Bloom Taxonomie houdt dat het volgende in:

1. Onthouden: De cursist wordt getest op de volgende vaardigheden: het herkennen en onthouden van feiten, termen, basale concepten of antwoorden op vragen zonder het precies te begrijpen.
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.

Examen

Aantal multiple choice vragen:	60
Duur (minuten) van het examen:	60 min.
Minimaal te behalen score voor slagen:	70%
Open/Gesloten boek:	Gesloten
Taal:	Nederlands
Fysiek exemplaar & 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-literatuur.

BIO2 Professional - Foundation (CBP-F) Courseware	Certified BIO2 Professional – (CBP-F) Baseline Informatiebeveiliging Overheid - Courseware - Nederlands: ISBN 9789401812733

Aanvullende documentatie:

Baseline Informatiebeveiliging Overheid	https://bio-overheid.nl/category/producten
NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002	https://www.nen.nl
Informatiebeveiligingsdienst	https://www.informatiebeveiligingsdienst.nl

Regelgeving en beleid

Certified BIO2 Professional is een term en een begrip die 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 niet 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 de certificering. Een cursist kan eenmaal het examen afnemen per keer dat het examen besteld is. Wanneer de persoon niet slaagt voor het examen, moet er een nieuw examen worden besteld en succesvol worden afgenomen om alsnog gecertificeerd te raken.

Leerdoelen Certified BIO2 Professional

De leerdoelen geven weer wat deelnemers moeten kennen om Certified BIO Professional te worden. Deelnemers moeten de BIO begrijpen en toe kunnen passen in de praktijk. Het certificaat dat deelnemers na het slagen voor het examen krijgen dient als bewijs dat de deelnemer onderstaande onderdelen uit de BIO begrijpt en weet toe te passen:

- Begrijpen wat de doelen en het toepassingsgebied van de BIO zijn;
- De BBN's begrijpen en deze weten te bepalen voor een proces/organisatie;
- De relatie tussen BBN's en risicomanagement;
- De belangrijkste principes van risicomanagement;
- De belangrijkste rollen ten aanzien van informatiebeveiliging kennen en weten wat deze inhouden;
- Begrijpen wat de vereisten zijn mbt verantwoording over informatiebeveiliging;
- Begrijpen wat een ISMS is conform ISO27001;
- Begrijpen en kunnen duiden welke eisen aan het ISMS uit de ISO27001 voor zijn/ haar organisatie relevant zijn;
- Basisbegrip hebben van verschillende beveiligingsmaatregelen uit de BIO en hoe deze toe te passen.

Exameneisen en -specificatie

Om de leerdoelen af te dekken is de certificering opgedeeld in exameneisen. Deze exameneisen bestaan weer uit gespecifieerde examenspecificaties. Onderstaande tabel beschrijft de verschillende modules (exameneisen) en subonderwerpen (examenspecificaties). Daarnaast geeft het ook de weging aan, die de verhoudingen van de vragen die in het examen worden gesteld laat zien.

Module	Exameneisen	Specificatie	Weging %
1.	Doel en toepassingsgebied van de BIO		10%
1.1		Doel	
1.2		Toepassingsgebied	
1.3		Achtergrond BIO (ISO2700x reeks)	
1.4		Andere relevante normenkaders	
2	Informatiebeveiliging		10%
2.1		Basisconcepten	
2.2		Informatiebeveiligingsbeleid	
3	ISMS		25%
3.1		Management van informatiebeveiliging	
3.2		Algemeen ISMS	
4	Risicomanagement en BBN's		20%
4.1		Risicomanagement begrippen	
4.2		Basis Beveiligingsniveaus (BBN)	
4.3		Risicoanalyse methoden	
5	Governance		20%
5.1		SG, directie, college en raad	
5.2		Management	
5.3		CISO	
5.4		Medewerkers	
6	Verantwoording		5%
6.1		In Control Verklaring	
6.2		Explains	
7	Controls en maatregelen		5%
7.1		ISO maatregelen en overheidsmaatregelen	
7.2		Typen maatregelen (logisch, fysiek en organisatorisch)	
7.3		BBN's en maatregelen	
8	Leveranciers en derde partijen		5%
8.1		Eisen aan leveranciers en derde partijen	
8.2		Overeenkomsten en naleving	

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Aantekeningen:

De **Baseline Informatiebeveiliging Overheid** (BIO) is op 1 januari 2019 van kracht geworden en vormt sindsdien de basisnorm voor informatiebeveiliging binnen alle overheidslagen in Nederland.

De BIO vervangt de voormalige baselines voor informatieveiligheid die specifiek waren voor Rijksoverheid, Gemeenten, Waterschappen en Provincies, en brengt deze samen in één uniforme standaard.

De BIO is gebaseerd op de internationaal erkende **ISO 27001-** en **ISO 27002**-normen voor informatiebeveiliging. Deze normen bieden een gestructureerd kader voor het identificeren en beheren van risico's rondom informatiebeveiliging.

Van Haren Publishing heeft samen met een aantal security professionals uit de praktijk bijgedragen aan de totstandkoming van het Certified BIO Professional (CBP) materiaal, examen en certificering voor CBP-foundation en CBP-Practitioner.

De CBP is dé training voor de BIO en wordt door overheden als standaard en vereiste gesteld.

De initiatiefnemer van de CBP training is **Ruben Zeegers**. Hij is tevens de auteur van deze courseware en hoofdontwikkelaar van het CBP examen. Ruben is een ervaren security professional die sinds 2007 publieke en private organisaties begeleidt met het verder professionaliseren van fysieke beveiliging, informatiebeveiliging en privacy. Ruben is gastdocent, spreker, auteur en tevens eigenaar van adviesbureau Security Risk Watch.

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Aantekeningen:

Welkom bij deze tweedaagse training! We starten graag met een **voorstelronde**, zodat we iets meer over elkaar te weten komen. In deze groep hebben we vaak deelnemers met diverse achtergronden en uiteenlopende niveau's van kennis en ervaring. Dit maakt dat we elkaar niet alleen kunnen inspireren, maar ook veel van elkaar kunnen leren.

Het doel van deze training is om de BIO (Baseline Informatiebeveiliging Overheid) toepasbaar te maken in jouw eigen praktijk. Door persoonlijke voorbeelden en vragen mee te nemen, zorgen we ervoor dat je deze training optimaal kunt benutten voor jouw groei en leerbehoeften.

We werken bewust in kleine groepen. Dit geeft ons de mogelijkheid om dieper in te gaan op specifieke vragen en onderwerpen die voor jullie belangrijk zijn. Daarom willen we jullie aanmoedigen om tijdens de sessies actief vragen te stellen en ervaringen te delen. Het kan zijn dat iemand anders in de groep op een specifiek onderwerp meer kennis heeft; dat biedt een mooie kans om van elkaar te leren en praktische tips uit te wisselen.

Laten we samen zorgen voor een interactieve en waardevolle training. We kijken ernaar uit om samen met jullie aan de slag te gaan!

Programma

- Algemeen

Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen

Agenda

Dag 1		Dag 2	
9:00 - 9:30	**Introductie** Kennismaking, over de training en examen	9:00 - 12:00	**Begrippenbespreking** Gezamenlijke bespreking dag 1
9:30 - 12:00	**Module 1**: Begrippen en inleiding BIO		**Module 3**: Mensgerichte en Fysieke maatregelen
12:00 - 12:45	Lunch	12:00 - 12:45	Lunch
12:45 - 17:00	**Module 2**: Organisatorische maatregelen	12:45 - 17:00	**Module 4**: Technologische maatregelen
	Praktijkopdracht Risicoanalyse		**Praktijkopdracht** ISMS

Aantekeningen:

Programma

- Algemeen

Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen

Trainingsdoelen

Kennis van informatiebeveiliging voor de overheid

De training geeft u een diepgaand inzicht in de principes en best practices van informatiebeveiliging, specifiek gericht op de overheid.

Kennis van tactisch normenkader

U leert hoe het tactische normenkader van de BIO in de praktijk werkt en hoe dit uw organisatie kan helpen om te voldoen aan de vereisten.

BIO vertaling naar de praktijk

De training gaat verder dan theorie en laat u zien hoe u de BIO kunt toepassen in uw dagelijkse werk.

Aantekeningen:

Programma

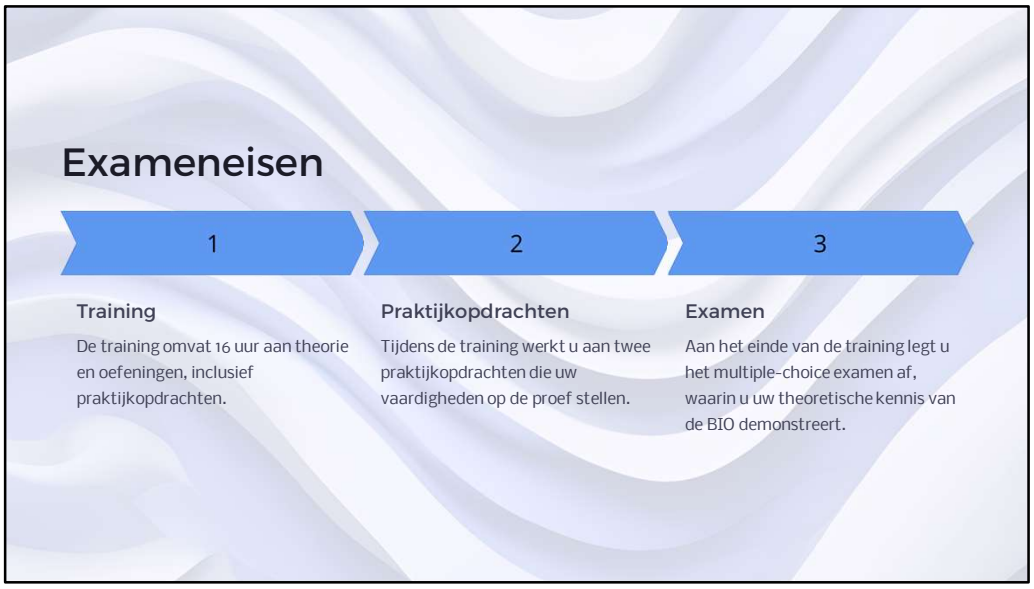
- Algemeen

Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen



Aantekeningen:

Programma

- Algemeen

Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen

Examenspecificaties

60	60
Vragen	Duur
Het examen bestaat uit 60 multiple-choice vragen.	U heeft 60 minuten de tijd om de vragen te beantwoorden.
70%	-
Cesuur	Hulpmiddelen
U moet minimaal 70% van de vragen goed beantwoorden om te slagen.	Er zijn geen hulpmiddelen toegestaan tijdens het examen.

Aantekeningen:

Programma

- Algemeen

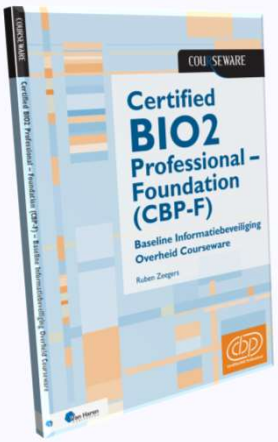
Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen

Examenstof



Extra Literatuur

BIO 2.0
De BIO 2.0, gepubliceerd op de website van de BIO, biedt een uitgebreide handleiding met alle vereisten en richtlijnen voor informatiebeveiliging binnen de overheid.

ISO 27001/2
ISO 27001 en ISO 27002 vormen de basis voor een Information Security Management System (ISMS). De ISO 27001 beschrijft de eisen voor een ISMS en de ISO 27002 biedt best practices voor de implementatie van controls.

NIS2
De NIS2-richtlijn versterkt de cybersecurity van essentiële diensten door hen te verplichten beveiligingsmaatregelen te nemen en incidenten te melden.

BIO-overheid.nl
De BIO-website is een centrale hub voor informatie over de BIO, inclusief documentatie, trainingen en certificeringen.

Aantekeningen:

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor informatiebeveiliging binnen de Nederlandse overheid, waaronder het Rijk, gemeenten, provincies en waterschappen. De BIO is gebaseerd op de standaarden NEN-ISO/IEC 27001 en 27002 en biedt richtlijnen voor het beschermen van overheidsinformatie en -systemen.
BIO 2.0 wordt behandeld voor het CBP-Foundation examen en dient als een referentiebron voor de onderwerpen die aan bod komen.
ISO 27001 en 27002 zijn nauw verwante normen voor informatiebeveiliging:
•**ISO 27001** biedt een raamwerk voor het opzetten, implementeren, beheren en verbeteren van een Information Security Management System (ISMS). Het helpt organisaties om risico's te identificeren en te beheersen en legt nadruk op beleidsvoering, risicobeoordeling, en audits.
•**ISO 27002** biedt gedetailleerde beveiligingsmaatregelen ter ondersteuning van het ISMS, zoals best practices voor toegangsbeheer, fysieke beveiliging en netwerkbeveiliging. Het fungeert als een praktische aanvulling op ISO 27001.
De **NIS-richtlijn** is een Europese maatregel om de cybersecurity van essentiële diensten te versterken. In 2023 werd NIS vervangen door **NIS2**, die strengere eisen stelt en een bredere groep organisaties omvat.
Op **BIO-overheid.nl** vinden overheidsorganisaties hulpmiddelen voor de implementatie van de BIO, zoals handreikingen, inkoopeisen voor cybersecurity, en praktische BIO-uitwerkingen. Voor ondersteuning kunnen organisaties terecht bij het Centrum Informatiebeveiliging en Privacybescherming (CIP), dat samenwerkt met BIO-overheid.nl. Kortom, BIO-overheid.nl is een belangrijke bron voor overheidsorganisaties die streven naar een effectieve informatiebeveiliging.

Programma

- Algemeen

Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen

Leeswijzer Courseware Boek

Module-indicator

Elk onderdeel van de training is duidelijk gelabeld met een module-indicator, zodat u altijd weet waar u zich in de training bevindt.

BIO Verwijzing

Het courseware bevat verwijzingen naar relevante hoofdstukken uit de BIO-documentatie, waardoor u de theorie direct kunt raadplegen tijdens de training.

Ruimte voor Eigen Aantekeningen

Het courseware bevat ruimte voor uw eigen notities, zodat u de belangrijke punten tijdens de training kunt vastleggen.

Aanvullende of Verdiepende Informatie

Naast de basisinformatie biedt het courseware aanvullende bronnen, zoals voorbeelden en best practices, om uw kennis te verdiepen.

Aantekeningen:

Programma

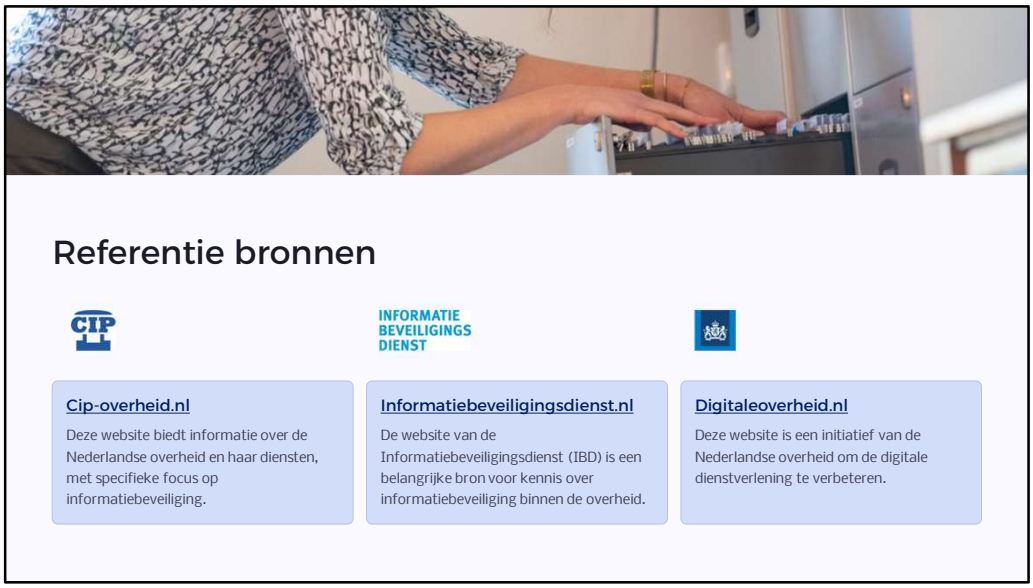
- Algemeen

Module 1: Begrippen en inleiding BIO

Module 2: Organisatorische maatregelen

Module 3: Fysieke en mensgerichte maatregelen

Module 4: Technologische maatregelen



Referentie bronnen

Cip-overheid.nl	**Informatiebeveiligingsdienst.nl**	**Digitaleoverheid.nl**
Deze website biedt informatie over de Nederlandse overheid en haar diensten, met specifieke focus op informatiebeveiliging.	De website van de Informatiebeveiligingsdienst (IBD) is een belangrijke bron voor kennis over informatiebeveiliging binnen de overheid.	Deze website is een initiatief van de Nederlandse overheid om de digitale dienstverlening te verbeteren.

Aantekeningen:

Programma

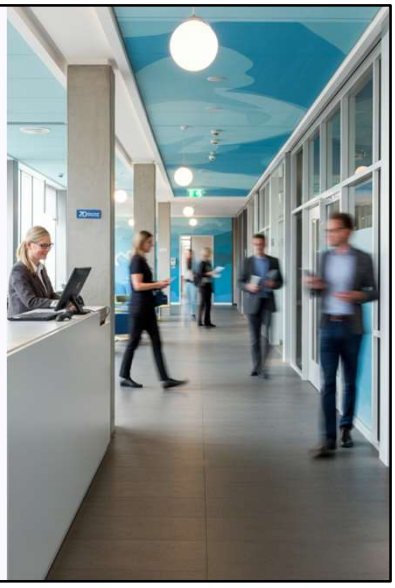
- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Module 1:

Begrippen Informatiebeveiliging

De basisprincipes van informatiebeveiliging.

Leer de definities van belangrijke begrippen, zoals vertrouwelijkheid, integriteit en beschikbaarheid.



Aantekeningen:

Basisbegrippen van Informatiebeveiliging
Het kennen en begrijpen van deze begrippen is essentieel, zowel voor de implementatie van maatregelen als voor het creëren van bewustzijn binnen een organisatie. Dit document bespreekt de belangrijkste begrippen, hun betekenis, en waarom ze belangrijk zijn in de praktijk.

Belang van deze Begrippen
Eigen kennis
Het kennen van deze begrippen stelt professionals in staat om geïnformeerde beslissingen te nemen en adequaat te reageren op beveiligingsuitdagingen. Zonder deze kennis is het moeilijk om risico's te begrijpen of passende maatregelen te nemen.
Kennisdeling binnen de organisatie
Het uitleggen van deze begrippen aan collega's en stakeholders bevordert een gezamenlijk begrip van informatiebeveiliging. Dit leidt tot een cultuur van beveiligingsbewustzijn, wat essentieel is voor het succes van beveiligingsinitiatieven.
Compliance en regelgeving
Veel van deze begrippen, zoals persoonsgegevens en risicomanagement, zijn verweven met wettelijke vereisten. Het begrijpen van deze concepten helpt organisaties te voldoen aan regelgeving en voorkomt boetes of andere sancties.
Effectieve implementatie van maatregelen
Het implementeren van beveiligingsmaatregelen zonder de onderliggende begrippen te begrijpen, kan leiden tot ineffectieve of zelfs contraproductieve resultaten. Kennis van deze begrippen zorgt ervoor dat maatregelen goed worden afgestemd op risico's en bedrijfsdoelen.
De Belangrijkste Begrippen
Betrouwbaarheidsaspecten, Persoonsgegevens, Veiligheidsdomeinen, Risico's, Maatregelen, Bedrijfsmiddel, Waarde van bedrijfsmiddelen, Kwetsbaarheid, Dreiging, Risico, Incident, Schade, Risicomanagement, Risicoanalyse, Controls en overheidsmaatregelen, Classificatie, PDCA, ISMS

Aantekeningen:

Definitie van informatiebeveiliging

Informatiebeveiliging kent wereldwijd geen uniforme definitie, maar de kernprincipes **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** staan centraal.

Het beheersen van informatierisico's vereist een samenhangend pakket maatregelen dat aansluit op een risico-gestuurde aanpak.
Deze aanpak is essentieel, zeker binnen grote en complexe organisaties, om systematisch en professioneel risicobeheersing te realiseren.

Maatregelen zijn niet vrijblijvend: ze brengen kosten met zich mee en kunnen zelf nieuwe risico's introduceren, zoals operationele beperkingen of afhankelijkheid van technologieën. Het balanceren tussen risico's en maatregelen is daarom een voortdurende uitdaging.

Zonder dit evenwicht kunnen organisaties over- of onderbeveiliging creëren, wat leidt tot inefficiëntie of ongewenste kwetsbaarheden.

Een duidelijk gedefinieerde aanpak voor informatiebeveiliging helpt organisaties niet alleen risico's te identificeren en beheersen, maar biedt ook een kader om kosten en baten van maatregelen beter af te wegen.

Zo ontstaat een professioneel en duurzaam beveiligingsbeleid dat de organisatie beschermt tegen ongewenste incidenten.

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Betrouwbaarheidsaspecten

Vertrouwelijkheid

Beveiliging van informatie tegen ongeoorloofde toegang. Alleen geautoriseerde personen kunnen de informatie inzien.

Integriteit

Zorgdragen dat de informatie correct, volledig en ongewijzigd is. Beschermen tegen manipulatie en vervalsing.

Beschikbaarheid

Zorgen voor toegankelijkheid van de informatie wanneer en waar dat nodig is. Beveiliging tegen storingen en onderbrekingen.

Aantekeningen:

De BIV, ook wel betrouwbaarheidsaspecten genoemd (Beschikbaarheid, Integriteit, Vertrouwelijkheid), bestaat uit kernconcepten binnen informatiebeveiliging en wordt ook toegepast binnen de Baseline Informatiebeveiliging Overheid (BIO).

Het helpt organisaties om de impact van risico's op informatie te beoordelen en passende beveiligingsmaatregelen te treffen. Vanuit de BIO wordt BIV als volgt benaderd:

Beschikbaarheid: De mate waarin informatie en systemen toegankelijk zijn wanneer nodig. Binnen de BIO wordt dit cruciaal geacht voor de continuïteit van overheidsdiensten.

Integriteit: De betrouwbaarheid en correctheid van informatie. De BIO legt nadruk op het waarborgen dat gegevens niet onopgemerkt gewijzigd of vernietigd kunnen worden.

Vertrouwelijkheid: Het beschermen van informatie tegen ongeautoriseerde toegang. De BIO stelt eisen om te voorkomen dat gevoelige gegevens in verkeerde handen vallen. Door de BIV-classificatie toe te passen, kan een overheidsorganisatie bepalen welke beveiligingsmaatregelen prioriteit hebben, in lijn met de BIO-richtlijnen.

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Aantekeningen:

Classificatie kan op verschillende manieren worden ingedeeld, afhankelijk van het doel en de context. Enkele veelgebruikte indelingen zijn:
BIV-classificatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Deze methodiek wordt veel toegepast binnen informatiebeveiliging om te bepalen welke mate van beveiliging een specifiek systeem of dataset nodig heeft. Bijvoorbeeld, een systeem dat de nationale veiligheid ondersteunt, vereist een hogere vertrouwelijkheid dan een openbaar toegankelijk informatiesysteem.
Privacy versus niet-privacy: Classificatie op basis van het al dan niet verwerken van persoonsgegevens. Hierbij wordt gekeken of informatie herleidbaar is tot een individu en of deze informatie bijzondere bescherming vereist volgens de AVG (Algemene Verordening Gegevensbescherming).
Kans x impact: Een veelgebruikte methodiek in risicomanagement waarbij risico's worden geclassificeerd door de kans van optreden te vermenigvuldigen met de impact. Dit helpt bij prioritering van maatregelen, waarbij risico's met een hoge score als eerste worden aangepakt.
VIR-BI (Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie) kent de volgende classificaties voor de beveiliging van informatie: Departementaal Vertrouwelijk, Confidentieel, Geheim, Zeer Geheim.

Deze classificaties worden door de overheid gebruikt en gedetailleerd beschreven in de VIR-BI. Dit document biedt een raamwerk voor het waarborgen van de vertrouwelijheid en integriteit van gevoelige informatie, met name binnen de publieke sector. Het biedt richtlijnen voor beveiligingsmaatregelen die passen bij de mate van gevoeligheid, zodat risico's beperkt blijven en vertrouwelijke gegevens niet in verkeerde handen terechtkomen.

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Aantekeningen:

Persoonsgegevens zijn gegevens die herleidbaar zijn naar een natuurlijke persoon die geïdentificeerd is of kan worden. De term "natuurlijke persoon" sluit rechtspersonen en overledenen uit. Persoonsgegevens vallen binnen de privésfeer (een grondwettelijke term).
Informatiebeveiliging betreft de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, in de breedste zin van het woord. Persoonsgegevens zijn een onderdeel van die informatie. Naast persoonsgegevens beschikken organisaties ook over niet-persoonsgebonden gegevens, oftewel bedrijfsgegevens. Deze informatie is niet herleidbaar naar een natuurlijke persoon en valt daarmee niet onder de Algemene Verordening Gegevensbescherming (AVG). Informatiebeveiliging beschermt alle soorten informatie: zowel persoonsgegevens als bedrijfsgegevens. Er geldt echter een wettelijke plicht voor de bescherming van persoonsgegevens, terwijl er geen wettelijke verplichting geldt voor de bescherming van bedrijfsgegevens.

Enkele voorbeelden:
Persoonsgegevens: salarisadministratie, personeelsadministratie, burgergegevens.
Bedrijfsgegevens: bedrijfsadres, begroting, netwerkarchitectuur.
Informatie kan in sommige gevallen persoonsgegevens bevatten, terwijl dat in andere gevallen niet zo is. Dit hangt af van de aard van de gegevens of van wie de gegevens beheert. Zo kan een adres bijvoorbeeld herleidbaar zijn naar een rechtspersoon (bedrijfsadres) en dus geen persoonsgegeven zijn. Een kenteken van een voertuig, dat vaak geen persoonsgegeven is omdat het niet zonder meer herleidbaar is, kan een persoonsgegeven worden wanneer het verzameld wordt door de Rijksdienst voor het Wegverkeer (RDW), die de kennis en expertise heeft om het kenteken herleidbaar te maken.
Technische ontwikkelingen en organisatorische veranderingen kunnen ertoe leiden dat niet-persoonsgegevens persoonsgegevens worden en andersom.

Gerelateerde Veiligheidsdomeinen

Veiligheid

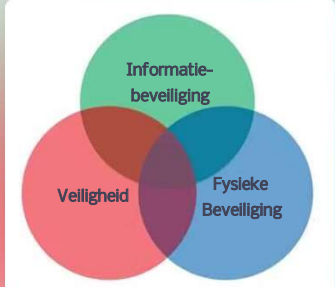
• Beschermen van het welzijn van mensen (♥)

Beveiliging (fysieke beveiliging)

• Beschermen van de continuïteit van de organisatie (€)

Informatiebeveiliging

• Beschermen van informatie (mens & organisatie €)



Aantekeningen:

De termen **veiligheid, fysieke beveiliging en informatiebeveiliging** worden vaak met elkaar verward, maar ze betekenen niet hetzelfde. Hoewel er duidelijke onderlinge verbanden zijn, vormen ze elk een eigen discipline binnen de bredere context van de veiligheidsdomeinen.

Organisaties hebben doorgaans specifieke afdelingen of functies voor elk domein, zoals een veiligheidsfunctionaris, een beveiligingsafdeling en een informatiebeveiligingsteam. Deze opdeling kan leiden tot uiteenlopende, soms tegenstrijdige belangen. Zo ontstaat spanning tussen veiligheid en fysieke beveiliging: fysieke beveiliging focust op het afsluiten tegen risico's zoals diefstal, terwijl veiligheid vraagt om openheid voor snelle evacuatie bij calamiteiten. De veiligheid van mensen heeft daarbij altijd prioriteit boven de bescherming van eigendommen of data. Samenwerking en maatregelafstemming zijn essentieel om een balans te vinden.

Voorbeelden van incidenten illustreren de verschillen:
Veiligheid: Vallen, bedrijfsongevallen.
Fysieke beveiliging: Diefstal, inbraak.
Informatiebeveiliging: Datalekken, hacking.
Denk bijvoorbeeld aan een grote aangestoken brand, of een cyberaanval waarbij kritische systemen van een ziekenhuis worden uitgeschakeld. Maatregelen tegen deze gezamenlijke risico's vereisen een integrale aanpak.

Fysieke toegang (onderdeel van fysieke beveiliging) speelt een verbindende rol binnen alle domeinen: het faciliteert veilige evacuaties (vluchtwegen), voorkomt ongeautoriseerde toegang (binnendringen) en beschermt fysieke informatie en informatie systemen.

Effectief beheer van veiligheidsdomeinen vraagt om een gezamenlijke strategie en integrale aanpak, waarbij samenwerking centraal staat.

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Risico's en Maatregelen

Een risico is de kans dat een dreiging zich realiseert en schade veroorzaakt. Maatregelen zijn acties die worden ondernomen om de kans op schade te verkleinen.

Aantekeningen:

Risico's en maatregelen: wat is de mate van risicobereidheid?

In elk bedrijf zijn risico's onvermijdelijk, vooral als het gaat om de bescherming van bedrijfsmiddelen. Deze middelen – zoals gegevens, systemen en fysieke eigendommen – vertegenwoordigen vaak een aanzienlijke waarde. Het verlies of de beschadiging ervan kan leiden tot ernstige gevolgen, zoals financiële schade, reputatieverlies of zelfs operationele stilstand.

Een risico ontstaat wanneer een kwetsbaarheid in een bedrijfsmiddel wordt blootgesteld aan een dreiging, zoals een cyberaanval, diefstal of een natuurramp. Het samenspel van dreiging en kwetsbaarheid bepaalt de kans op een incident, dat kan resulteren in schade. Hoe waardevoller een bedrijfsmiddel, des te groter de impact van een incident.

Om risico's beheersbaar te maken, zijn gerichte maatregelen nodig. Deze kunnen preventief zijn, zoals het versterken van beveiligingssystemen, detecterend door middel van monitoring, of reactief, zoals een goed gecoördineerd incident response plan. Door risicoanalyses uit te voeren, wordt duidelijk welke kwetsbaarheden en dreigingen prioriteit verdienen. Dit stelt een organisatie in staat om de waarde van bedrijfsmiddelen te beschermen en de impact van mogelijke incidenten te minimaliseren.

Kortom, een effectieve aanpak van risico's vraagt om een strategische balans tussen dreigingen, kwetsbaarheden en de waarde van bedrijfsmiddelen, ondersteund door doordachte maatregelen.

Programma

- Algemeen
- Module 1: Begrippen en inleiding BIO
- Module 2: Organisatorische maatregelen
- Module 3: Fysieke en mensgerichte maatregelen
- Module 4: Technologische maatregelen

Aantekeningen:

Een **bedrijfsmiddel** is een breed begrip dat verder gaat dan alleen informatiebeveiliging. In de financiële boekhouding omvat het alle middelen, zowel materieel als immaterieel, die eigendom zijn van een bedrijf of economische entiteit en waarde genereren. Bedrijfsmiddelen kunnen worden ingezet om economische voordelen te creëren, en sommige, zoals contant geld, kunnen direct in liquide middelen worden omgezet.

Binnen het domein van informatiebeveiliging ligt de focus echter uitsluitend op die bedrijfsmiddelen die gerelateerd zijn aan informatie. Dit omvat bijvoorbeeld gegevens, systemen, software en de infrastructuur die nodig is voor het beheren en beschermen van informatie. Het doel is om de vertrouwelijkheid, integriteit en beschikbaarheid van deze informatie-gerelateerde middelen te waarborgen. Bedrijfsmiddelen zoals contant geld of fysieke eigendommen vallen buiten de scope van informatiebeveiliging, tenzij ze een directe rol spelen in de bescherming of het beheer van informatie.

Organisaties beschikken doorgaans over een grote diversiteit aan bedrijfsmiddelen. Niet alle hiervan zijn even relevant voor informatiebeveiliging. Een Business Impact Analyse (BIA) kan helpen om de bedrijfsmiddelen die essentieel zijn voor cruciale bedrijfsprocessen te identificeren en prioriteren. Hierdoor kunnen beveiligingsmaatregelen gericht worden ingezet op wat echt van belang is.

Aantekeningen:

Het concept „**waarde**" is veelzijdig en kan op uiteenlopende manieren worden geïnterpreteerd. Binnen organisaties wordt de waarde van bedrijfsmiddelen beoordeeld op basis van hun bijdrage aan het succes van de organisatie. Waardeclassificatie biedt inzicht in de rol van een bedrijfsmiddel en helpt bij strategische beslissingen omtrent beheer en bescherming.

Voorbeelden van waardeclassificatie: Waardeclassificatie kan op verschillende manieren worden toegepast:

Economische waarde: De economische waarde van een bedrijfsmiddel kan worden vastgesteld aan de hand van de aanschafkosten of potentiële verkoopopbrengsten. Dit type waarde is relevant voor investeringen, afschrijvingen en vervangingsstrategieën.
Omzet- of winstwaarde: Een bedrijfsmiddel kan worden beoordeeld op basis van de directe of indirecte bijdrage aan omzet of winst. Bijvoorbeeld, een productie-installatie die essentieel is voor de fabricage van producten of software die de efficiëntie verhoogt.
Imago en reputatie: Sommige bedrijfsmiddelen hebben een waarde die niet in cijfers is uit te drukken, zoals data die verband houden met de vertrouwenspositie van de organisatie of iconische gebouwen die het imago versterken.
Kosten van bescherming en herstel: Waarde kan ook worden gekoppeld aan de kosten van bescherming of herstel na incidenten, zoals investeringen in beveiliging of herstel na verstoringen.

Conclusie
Waarde is een veelzijdig begrip dat varieert van economische en omzetwaarde tot reputatie en beschermingskosten. Het systematisch beoordelen van deze aspecten stelt organisaties in staat weloverwogen keuzes te maken en bedrijfsmiddelen optimaal te benutten.

Eigenaarschap van bedrijfsmiddelen

Verantwoordelijkheid

De eigenaar van een bedrijfsmiddel is verantwoordelijk voor het gebruik en de beveiliging ervan.

Gebruik

De eigenaar gebruikt het bedrijfsmiddel om zijn taken uit te voeren.

Centrale Eigenaar

Als meerdere afdelingen een bedrijfsmiddel gebruiken, wordt er vaak een centrale eigenaar aangesteld.

Aantekeningen:

Het **eigenaarschap van bedrijfsmiddelen** is een cruciaal aspect voor een effectieve informatiebeveiliging. Bedrijfsmiddelen omvatten zowel fysieke als digitale middelen, zoals hardware, software, data en de bijbehorende documentatie, die essentieel zijn voor het functioneren van organisaties. Het belang van eigenaarschap ligt in de verantwoordelijkheid die hierbij komt kijken voor het beschermen en beheren van deze middelen.

Eigenaarschap betekent dat er een duidelijke verantwoordelijke is aangewezen die zorgdraagt voor het onderhoud, de beveiliging en de naleving van relevante richtlijnen. Zonder een helder gedefinieerd eigenaarschap kunnen bedrijfsmiddelen kwetsbaar worden voor beveiligingsrisico's, zoals ongeautoriseerde toegang, verlies van gegevens of verstoringen in de dienstverlening. Eigenaarschap biedt structuur en transparantie, waardoor risico's tijdig kunnen worden geïdentificeerd en gemitigeerd.

Daarnaast stelt eigenaarschap organisaties in staat om effectief te reageren op incidenten. Wanneer incidenten plaatsvinden, zoals een datalek of systeemuitval, is het essentieel dat de verantwoordelijke eigenaar snel kan handelen om de schade te beperken. Dit vergroot niet alleen de weerbaarheid van de organisatie, maar draagt ook bij aan het behouden van het vertrouwen van burgers en stakeholders.

Tot slot zorgt eigenaarschap voor een betere afstemming tussen verschillende afdelingen en belanghebbenden binnen de organisatie. Het maakt duidelijk wie verantwoordelijk is voor welke middelen, wat leidt tot efficiënter beheer en naleving van wettelijke en beleidsmatige eisen. Kortom, eigenaarschap van bedrijfsmiddelen vormt een onmisbare schakel in het waarborgen van een robuuste informatiebeveiliging. Het biedt de basis voor verantwoordelijkheid, transparantie en effectieve risicobeheersing.