COURSEWARE

Certified BIO (CBP) Practitioner Courseware

Voor implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

Martin Goudzwaard & Arie Linsen

Van Haren PUBLISHING

CBP® PRACTITIONER
Certified by Van Haren CERTIFY

Certified BIO (CBP)
Practitioner Courseware

Colofon

Title:	Certified BIO (CBP) Practitioner Courseware Voor implementatie van de Baseline Informatiebeveiliging Overheid (BIO)
Authors:	Martin Goudzwaard & Arie Linsen
Publisher:	Van Haren Publishing, Zaltbommel
ISBN Hard Copy:	978 9401 8102 72
Edition:	Eerste editie, eerste druk, September 2023
Design:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2023
	Voor verdere informatie over Van Haren Publishing, e-mail naar: info@vanharen.net of bezoek onze website: www.vanharen.net

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

Over deze courseware

Deze courseware is opgesteld door experts in het vakgebied, 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 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 en op de exameneisen.

Om de trainer en deelnemer van de training optimaal te ondersteunen in de beheersing van de theorie, zijn er cases, huiswerkopdrachten en de uitwerkingen toegevoegd aan het materiaal. Ook zijn discussiemomenten 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 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.

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 deze 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 de diagram Zelfreflectie op begrip, kun je de voortgang van je eigen training evalueren.

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

(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 gemaakt hebt	

Agenda

Dag 1	
0	Kennismaking
1	Inleiding
	Pauze
1.1	Doel, achtergrond, context, ect. opfrissen
1.2	Relatie met ISO 27001/2, vooruitblik naar 2022 versie
	Lunch
2	Governance deel 1
2.1	Stakeholder analyse
	Pauze
2.2	Bewustwording stakeholders
Dag 2	
3	Waar staan we?
3.1	Huidige volwassenheidsniveau informatieveiligheid van organisatie
	Pauze
3.2	Huidige beveiligingsniveau organisatie breed in kaart brengen
	Lunch
3.3	Huidige beveiligingsniveau per proces/systeem in kaart brengen en BBN niveau bepalen
	Pauze
3.4	Risicoanalyse uitvoeren

Dag 3	
4	Wat gaan we doen
4.1	Welke maatregelen moeten er genomen worden?
	Pauze
4.2	De gekozen maatregelen implementeren
	Lunch
5	Governance deel 2
5.1	Het monitoren van het beveiligingsniveau en indien noodzakelijk aanpassen van beheersdoelstellingen en gekozen maatregelen
	Pauze
5.2	Het borgen van het continue proces van verbeteren van de informatieveiligheid

CBP-P dag 1

Certified Baseline Informatiebeveiliging Overheid Professional - Practitioner

MODULE 0

KENNISMAKEN VERWACHTINGEN VOORKENNIS

Doelstelling

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

COURSEWARE

Kennismaken

Wie ben ik (docent)?

- Wat zijn mijn verwachtingen.

Kennismaken

- Kenningsmakingsopdracht 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?

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.

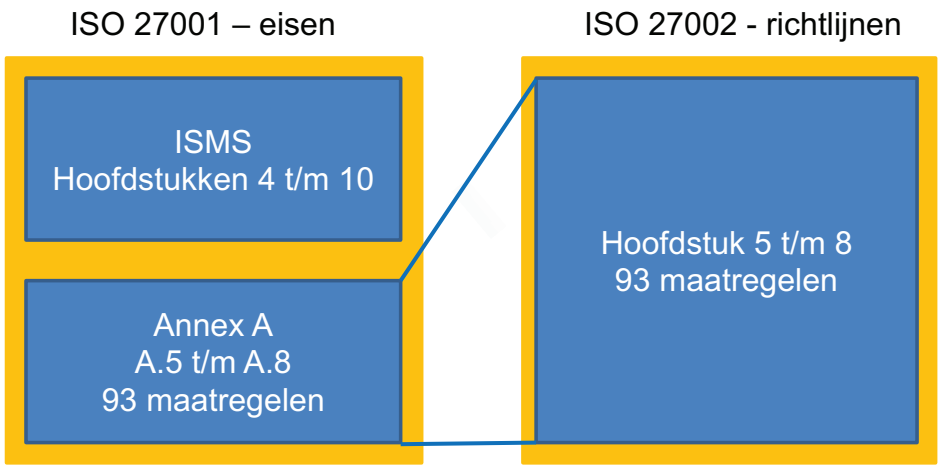
COURSEWARE

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 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 attribuut 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, attribuut 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

 32

Domeinen

Veiligheidsdomeinen is een attribuut om controles vanuit vier informatiebeveiligingsdomeinen te bekijken

- Governance en ecosysteem
- Bescherming
- Verdediging
- Veerkracht

 33

Voorbeeld

Tabel A.1 — Matrix van beheersmaatregelen en attribuutwaarden

Identificatie-code beheers-maatregel ISO/IEC 27002: 2022	Naam beheers-maatregel	Type beheers-maatregel	Informatie-beveiligings-eigenschappen	Cybersecurity-concepten	Operationele capaciteiten	Beveiligings-domeinen
5.1	Beleidsregels voor informatie-beveiliging	#Preventief	#Vertrouwelijk-heid #Integriteit #Beschikbaar-heid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Veerkracht
5.2	Rollen en verantwoorde-lijkheden bij informatiebe-veiliging	#Preventief	#Vertrouwelijk-heid #Integriteit #Beschikbaar-heid	#Identificeren	#Governance	#Governance_en_Ecosysteem #Bescherming #Veerkracht

A5 Organisatorische beheersmaatregelen (1v4)

Rood = nieuw !

A.5.1 Beleidsregels voor informatiebeveiliging

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

 36

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

 37

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

 38

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

 39

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 routering, 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.

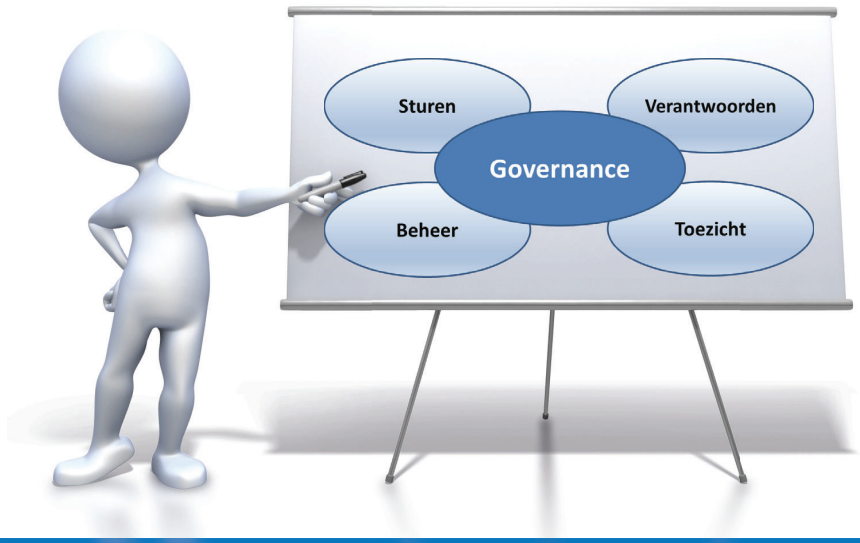
COURSEWARE

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



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