



Belastingdienst

BIO: workshop t.b.v. MDT-GO

Achtergrond en toepassing binnen de
Belastingdienst

28-3-2024



Agenda dag 2

BIV in de domeinarchitectuur

TBB's revisited: classificatiebeleid Belastingdienst

BIO binnen de Belastingdienst, herijking programma BIO

Opzet informatiebeveiligingsbeleid BD, referentiearchitectuur
IB, generiek beleid

Gebruik BIO in de controlelijst: artikelen en vraagstelling



Even terug: BIV in
domeinarchitectuur
OVM

Bedrijfsproces	BIV
BP Afhandelen servicevragen EB	122
BP Behandelen aanvraag vergunning inrichting voor kolen EB	122
BP Behandelen bezwaar/beroep EB	222
BP Behandelen verzoek EB	222
BP Bewaken leververplichting EB	222
BP Uitnodigen tot het doen van aangifte EB	122
BP Uitvoeren toezicht EB	122
BP Vaststellen klantafspraken EB	122
BP Verwerken aangifte EB	122
BIV-waarde ABM en TMB	222

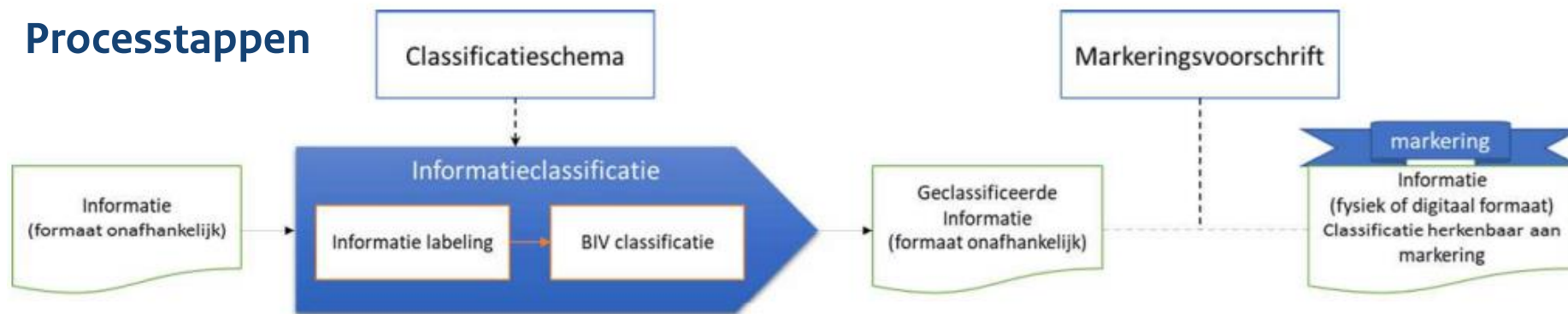
Bron: Addenda bij Domeinarchitectuur 2023-1 OVM - Overzichten

Extra aandacht voor het completeren van de BIV-classificaties en BCM-metrieken, alsmede (op het detailniveau van de architectuur) inzicht in compliantie met privacykaders, BIO en Archiefwet. Kaders op dit gebied gelden al enkele jaren, maar informatie is bij veel domeinen nog incompleet. Belangrijke bijdragen zijn nodig van business-medewerkers zoals datacoördinatoren en business security officers








TBB-GO: dataclassificatie

Processtappen



1. Informatielabeling obv wet-en regelgeving, BD-beleid, specifieke stakeholders
 - a. Belang hierbij onder andere rubricering, cruciaal belang, privacy belang, strafrechtelijk belang en archiefbelang
 - b. Inzicht in bijzondere groepen zoals VIP's, gegevens van bijzondere groepen mdw.
2. Classificatie
 - a. BIV-classificatie adhv bedrijfsprocessen met gestructureerde gegevens
 - b. Overige informatie → vertrouwelijkheidslabel
3. Markering volgens Traffic Light Protocol TLP

Dataclassificatie BD visueel

Vertrouwelijkheidsniveau conform VIR-BI	Classificatieniveau	BIV classificatie	Markering
Openbaar	Openbaar	Niet van toepassing	<div>TLP: CLEAR</div> 
Departementaal vertrouwelijk	Belastingdienst intern	BIV=xx1	<div>TLP: GREEN</div> 
	Belastingdienst vertrouwelijk	BIV=xx2	<div>TLP: AMBER</div> 
	Belastingdienst zeer vertrouwelijk	BIV=xx3	<div>TLP: AMBER+STRICT</div> 
Staatsgeheim confidentieel	Staatsgeheim confidentieel	Niet van toepassing	<div>TLP: RED</div> 
Staatsgeheim geheim	Staatsgeheim geheim	Niet van toepassing	
Staatsgeheim zeer geheim	Staatsgeheim zeer geheim	Niet van toepassing	

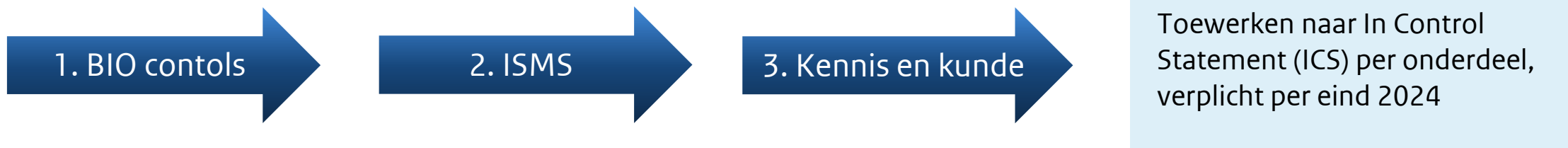


BIO binnen de Belastingdienst

Inrichting en programmering volgens Programma Herijking BIO:

- Invulling geven aan alle BIO-controls: opzet, bestaan en werking
- Leveren waar mogelijk ondersteuning t.b.v. beschrijven maatregelen
- BSO is afgevaardigde/contact voor het programma
- Opstellen en invullen van controleraamwerk t.b.v. uit te voeren maatregelen
- Toewijzen van controls en verbeteracties, lange en korte termijn

3 sporen worden gevolgd





BIO binnen de Belastingdienst

1. BIO controls

Spoor 1 BIO controls:

- Onderscheid in korte en lange termijn acties
- Voor álle 112 BIO controls zal het BIO-programmateam ondersteunen bij het inzichtelijk krijgen van de (gap met betrekking tot de) opzet en het bestaan van de 112 BIO controls.
- Prioriteitsstelling van toepassing vanwege grootte organisatie: indeling hoofdstukken BIO naar fase
- Inrichting van controleraamwerk
- Scope van de BIO (specifiek: de dienstenonderdelen, domeinen, processen en IV-systemen) gebaseerd op de 15 domeinen
- DA als uitgangspunt

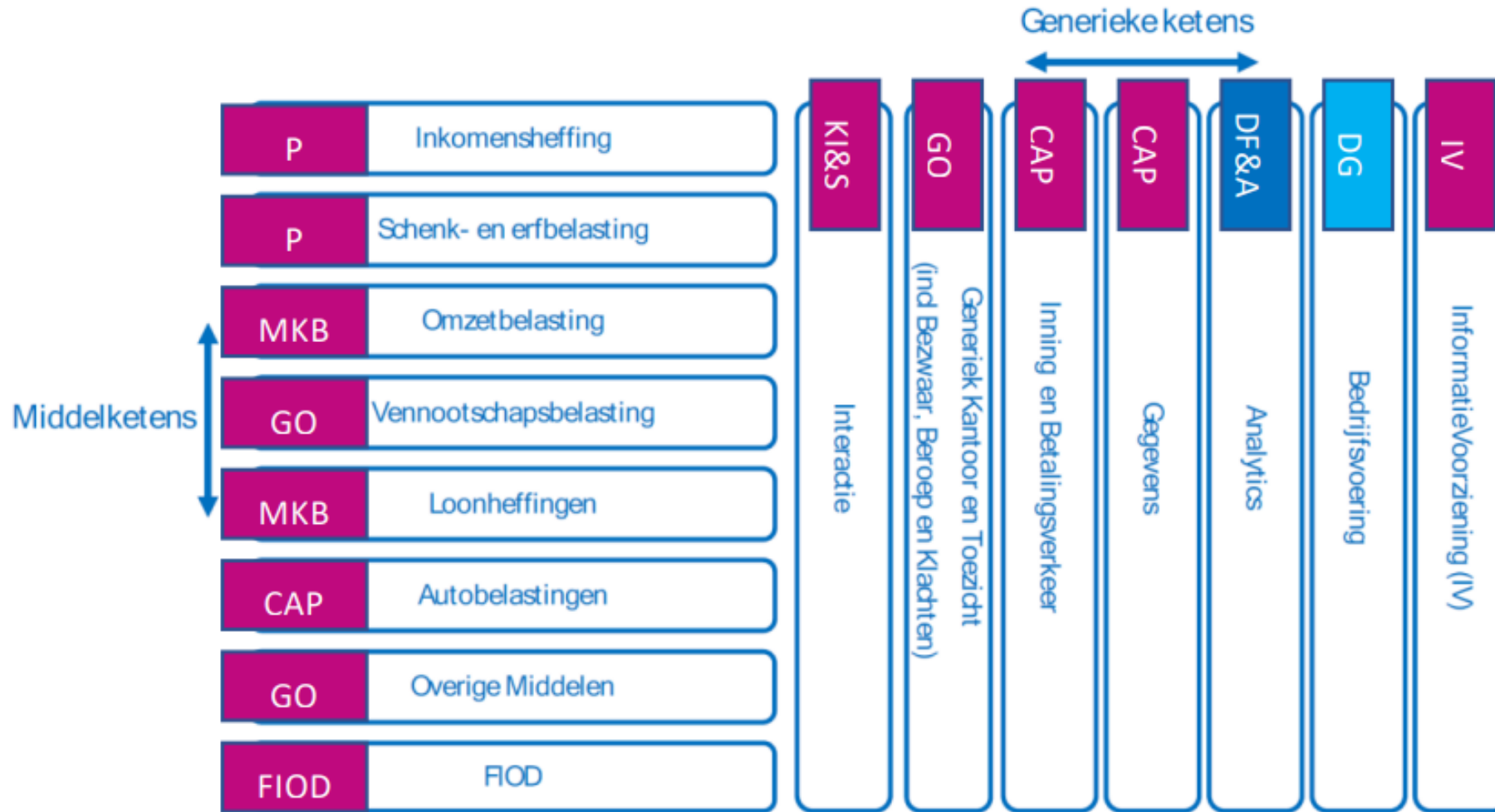
Vraagstelling:

- Welke bedrijfsprocessen en informatie/IV systemen hierin worden gebruikt door welke dienstenonderdelen;
- Of hiervoor onderdelen vanuit het BIO normenkader van toepassing zijn;
- Of daaraan invulling is gegeven qua opzet;
- Welke dienstonderdelen (delen van) deze processen uitvoeren en systemen gebruiken;
- Of de noodzakelijke opzet en bestaan kunnen worden aangetoond.



BIO binnen de Belastingdienst

1. BIO contols





Opzet, bestaan en werking BIO-controls

3.1 Definities opzet, bestaan en werking

Binnen dit programmaplan wordt gesproken over opzet, bestaan en werking van de BIO controls. Wij hanteren hierbij de definitie zoals vastgesteld binnen de Belastingdienst (letterlijk geciteerd)²:

- Opzet: Aanwezige documentatie van getroffen of nog te treffen beheersmaatregelen op basis van doelstellingen en risico's. Voorbeeld: vastleggingen in de vorm van beleidsstukken, risicoanalyses, organisatieschema's, (procedure)-beschrijvingen, plannen, handboeken en AO/IC beschrijvingen.
- Bestaan: Aantoonbaar functioneren van bovengenoemde getroffen beheersmaatregelen op één bepaald moment. Voorbeeld: nalopen van een proces waarbij de daadwerkelijke geautomatiseerde en/of handmatige procesgang, inclusief de aangebrachte maatregelen worden vastgelegd in de vorm van (uitzonderings-)rapportages, aansluitingen, verwerkingsverslagen, (autorisatie)logging, goedkeuringen, controleverbanden, etc. Indien een proces volledig is geautomatiseerd kan bijvoorbeeld ook gebruik gemaakt worden van process mining.
- Werking: Het bewezen consequent functioneren van bovengenoemde getroffen beheersmaatregelen gedurende een langere periode, meestal een kalenderjaar conform een reguliere managementcyclus.



Het ISMS: geen tool maar een (continu) proces

2. ISMS

- Geeft invulling PDCA verbetercyclus Informatiebeveiliging
- Uitvoering geven aan risicoanalyses om zo maatregelen in kaart te brengen
- Betreft vnl. hoofdstukken 5 en 6 BIO, strategie en organisatie Informatiebeveiliging
- Verplichting om te kunnen voldoen aan ISO27001
- Gebruikte ondersteunende tooling bijv. Confluence

Binnen het ISMS onderscheid in:

- Een beleidsdomein waar strategische richting wordt gegeven
- Een uitvoeringsdomein waar maatregelen worden ingericht en uitgevoerd
- Een toezichtsdomein waar onafhankelijke toetsing (audits vanuit de 3e lijn) plaatsvindt op aandachtsgebieden en waarover onafhankelijk gerapporteerd wordt naar het bestuur.

■ Huidige status ISMS binnen BD

Onduidelijk, daarom

- IST-inventarisatie ISMS
- Toewerken naar SOLL-situatie
- Hierop GAP-analyse van toepassing
- Uitwerking routekaart ISMS BD

Integraal beveiligingsbeleid en RA IB

❑ Integraal beveiligingsbeleid BD

- Stammt uit 2019
- Gebaseerd op risicomanagement
- Met aandacht voor de omgeving (politiek, bestuurlijk en technologisch) en eigen organisatie (bewustwording, integriteit en digitale vaardigheid)
- Een generiek beveiligingsniveau wordt gehanteerd (BBN2)

❑ Verantwoordelijkheidsgebieden IB

- Bedrijfscontinuïteit
- Personele veiligheid en integriteit
- Fysieke beveiliging
- informatiebeveiliging

Privacybescherming vormt
integraal onderdeel hiervan

❑ Principes integrale beveiliging

- Beveiligingskeuzes obv risicomanagement
- Beschermen van geclassificeerde bedrijfsmiddelen (o.a. toegang en autorisatie o.b.v. *need-to-know*, *need-to-do* en *least privilege*)
- Ontwikkeling veilige processen, systemen en fysieke objecten
- Continue verbetering

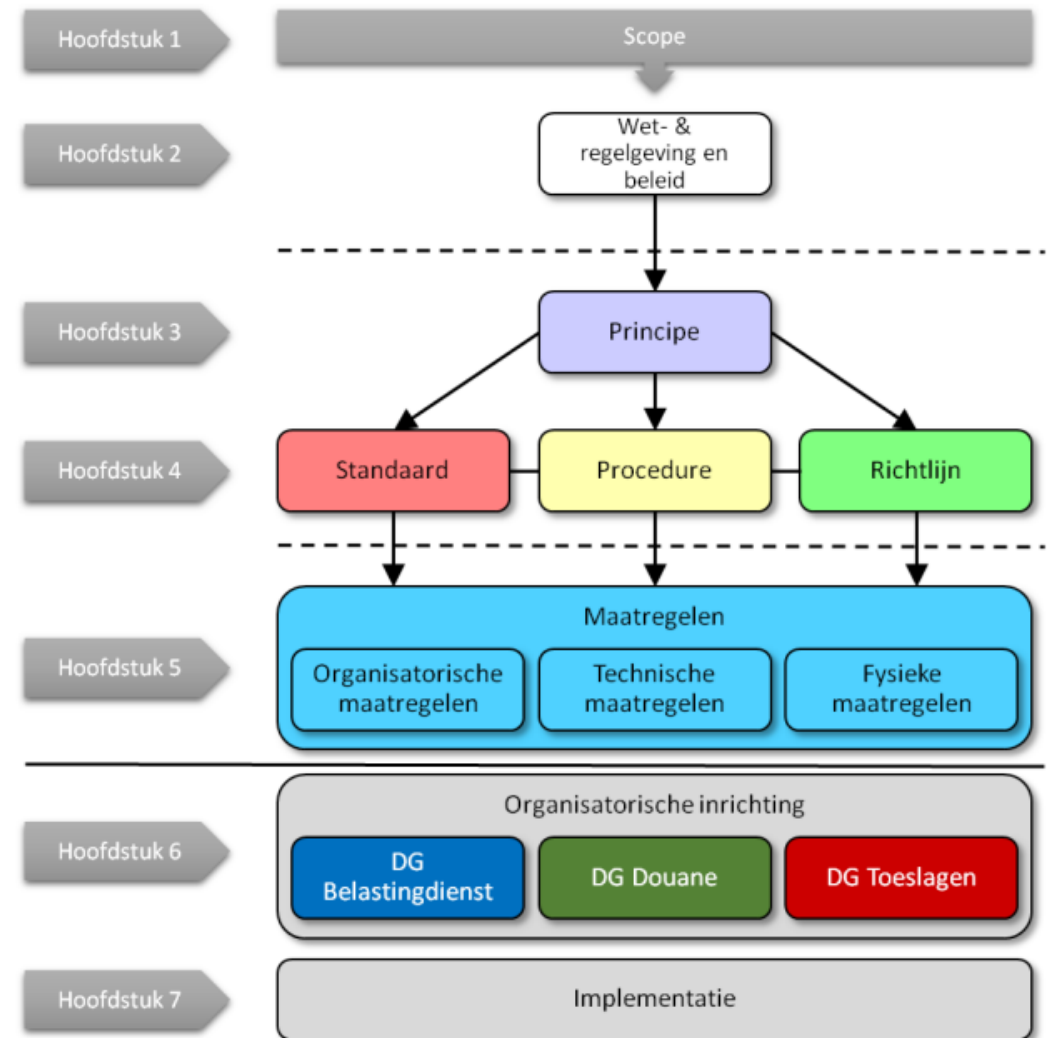


Kort over IB referentiearchitectuur

- Beschrijft kaders IB
- Die vertaling zijn van wet-en regelgeving, aanwezig (departementaal) beleid
- Helpt lijndirecties en domeinen bij het bepalen van te nemen maatregelen
- Daarnaast overzicht in generieke maatregelen BD-breed die al genomen zijn
- Afgeleid van principes volgens NORA, zie [Beveiliging - NORA Online](#)

Verder uitwerking in

- Domeinarchitectuur IB
- (Specifieke) domeinarchitecturen
- Architecturen generieke domeinen



Figuur 1: Opbouw referentiearchitectuur Integrale Beveiliging



Principes voor business & applicatie architectuur

Burgers en bedrijven kunnen veilig zaken doen met de belastingdienst

Functiescheiding

Gegevensbeveiliging correspondeert met gegevensclassificatie

Gegevensbronnen zijn afgeschermd

Gegevenstransport via expliciet toegestane services

Generieke functies zijn inherent veilig

Herleidbaarheid van handelen

Persoonsgegevens hebben een bewaartermijn

Persoonsgegevens worden met gegevensfuncties beheerd

Transacties zijn herstelbaar

Verwerkingskenmerken worden geregistreerd

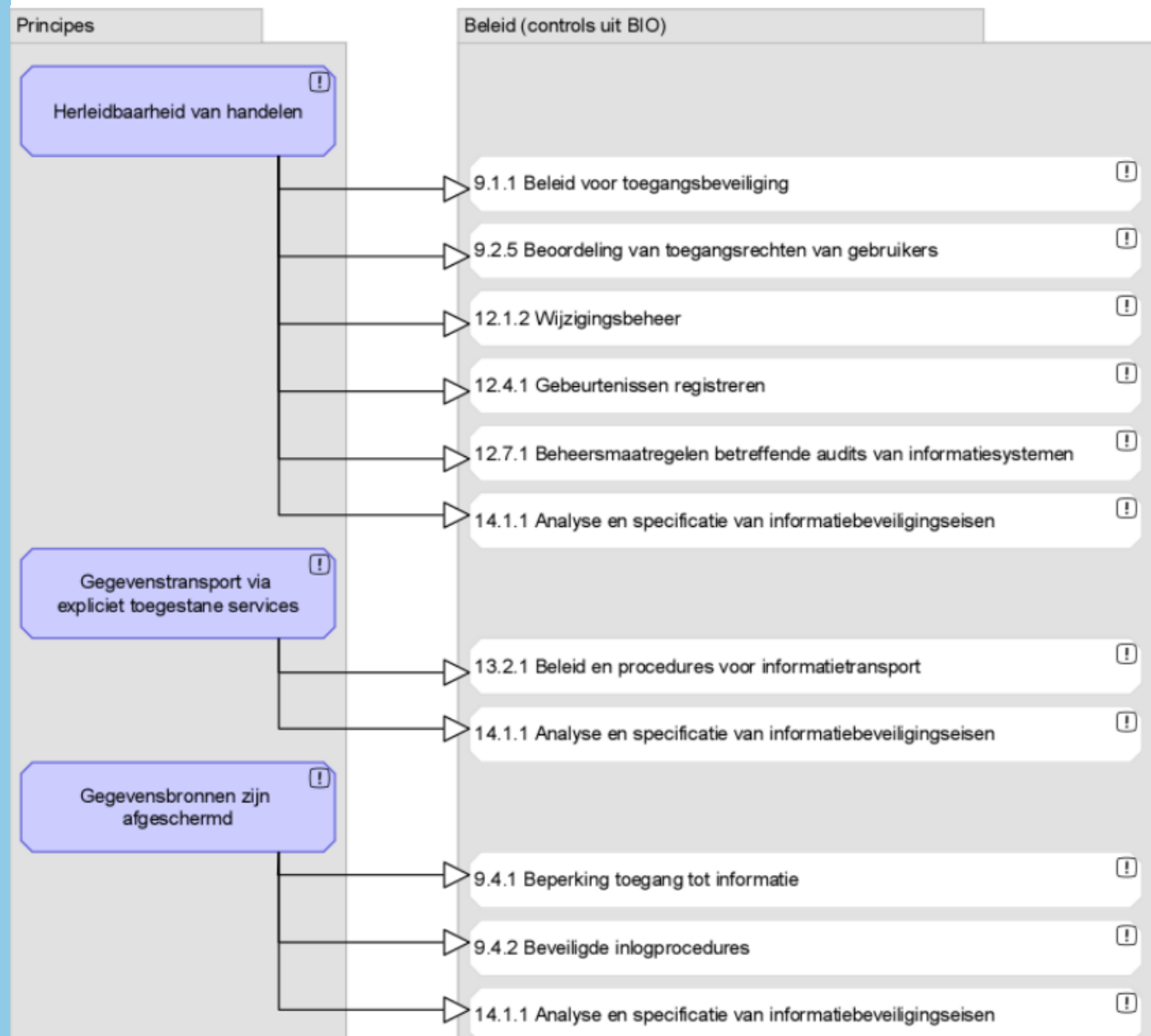
DA Informatiebeveiliging

Figuur 3 Architectuurprincipes



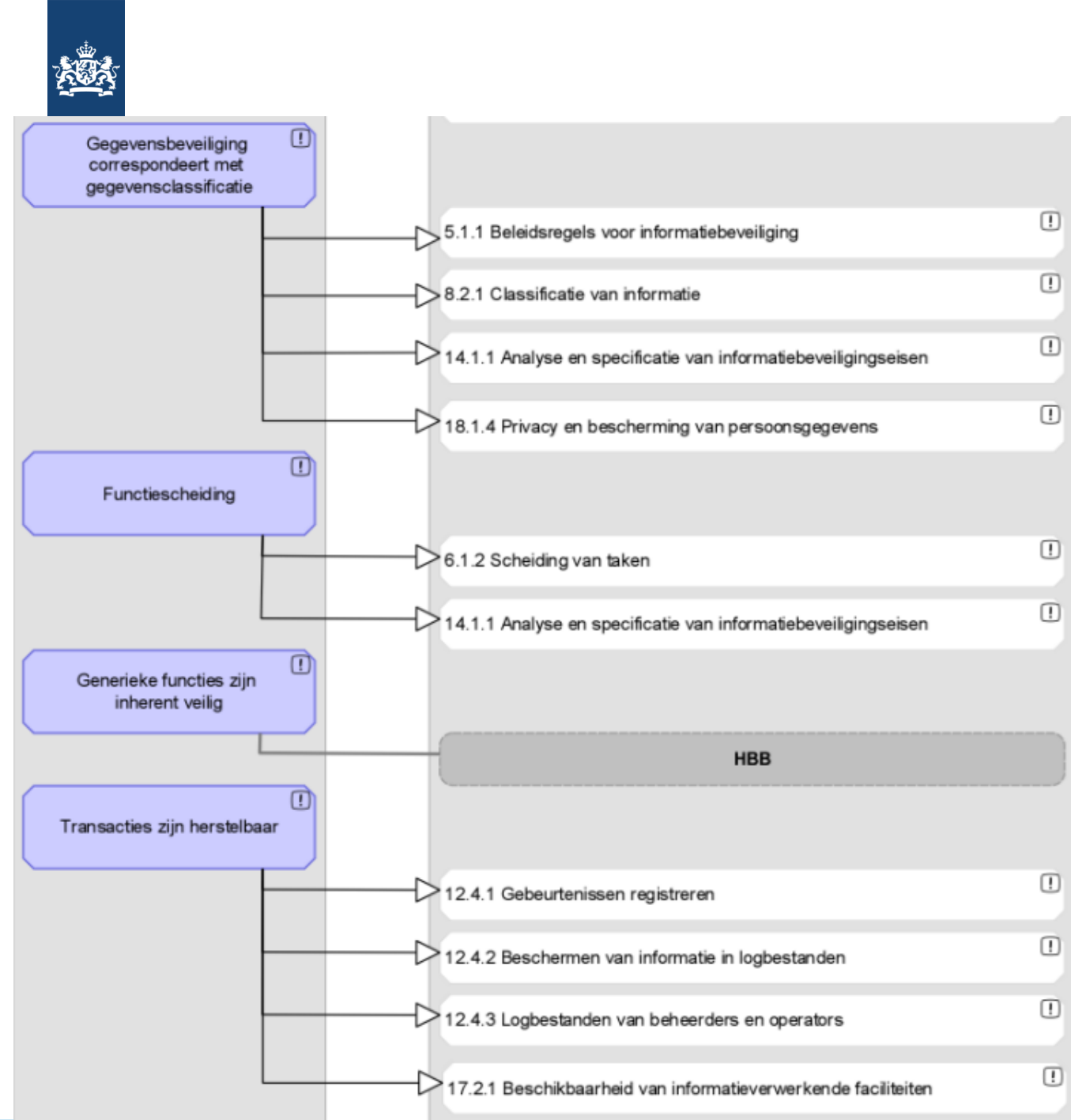
Koppeling BIO-controls aan architectuurprincipes

Uit: RA-IB Compliance Belastingdienst



Koppeling BIO-controls aan architectuurprincipes

Uit: RA-IB Compliance Belastingdienst





DA Informatiebeveiliging

- Volgt uitgangpunten RA Informatiebeveiliging
- Gericht op ongestoorde bedrijfsvoering van de Belastingdienst
- Kader voor solutionarchitecten
- Maakt inzichtelijk wat er op de Belastingdienst afkomt van buiten
 - Wet-en regelgeving
 - Dreigingsbeeld (mondiaal)
 - Maatschappelijk/klantverwachting
 - Technologisch m.n. AI, open source
 - Interne digitalisering
 - Social media gebruik zakelijk
 - Cloudoplossingen



DA Informatiebeveiliging

Wat moet er beter?

Producten & diensten

- Bescherming van bedrijfsmiddelen
- buiten de Belastingdienst (public cloud, gedeelde omgevingen, overheidsdiensten)
 - Boven BBN2 niveau (incl. staatsgeheim)

Belastingdienst specifiek dreigingsbeeld

Gegevens & administraties

- Ontbrekende of onvoldoende ingerichte administraties voor generieke beveiligingsprocessen (risico-register, security event administratie, verwerkingen register, GEB administratie, asset-administratie, beveiligingsmanagement systemen)
- Overige processen:
 - veel administraties buiten generieke LTB diensten om benaderbaar (CP, data warehouses, Queries LOA, Q-schijf)
 - onduidelijk in hoeverre generieke diensten veilig zijn
 - Relatie ontwerp – fysieke opslag veelal onduidelijk
- Ontbrekende gegevensclassificatie (alle processen)
- Gegevens in productie bij incidenten rechtstreeks aangepast.
- Gegevens worden zowel in databases als in documenten opgeslagen (dubbel), maar anders geclassificeerd en beveiligd. Daarnaast tegenwoordig ook veel mail/app verkeer

Processen & organisatie

	Aanwezig	Kwaliteit
Bedrijfsmiddel (asset) management	60%	30%
Governance, Risk en Compliance (GRC), incl. kaderstelling voor overige bedrijfsprocessen en bij specifieke	20%	15%
Crisis management (BCM)	70%	50%
Security event management	20%	
Logische Toegangsbeveiliging	80%	40%
Leveren transparantie m.b.t. bedrijfsmiddelen van derden	60%	30%

Applicaties & technologie

- Ontbrekende tooling voor generieke beveiligingsprocessen (GRC)
- Onduidelijkheid over het inzetgebied/mate van veiligheid van generieke IT services, interfaces en bouwblokken (geschiktheid, “hardening”, herleidbaarheid van handelen), bijvoorbeeld de Enterprise Service Bus.
- Ontbrekende voorzieningen voor het veilig delen van informatie buiten de Belastingdienst (hiervoor wordt nu bij gebrek aan beter Cloud en KA ingezet)
- Onzekerheid over de veiligheid/integriteit van software componenten/code
- IMS (LTB) is end-of-life



BIO Vraagstelling in de controlelijst

7. Vertrouwelijkheid, betrouwbaarheid, beschikbaarheid en toegang	7.1	Need to know, need to do en least privilege Onderdeel van 7.3: BIV-classificatie: bepaal en geef aan welke rol toegang moet hebben tot welke gegevens en informatie op basis van need to know en least privilege rekening houdend met de functiescheiding (zie 7.2).	Invulling van need to know, need to do en least privilege zijn opgenomen in beleid van de Belastingdienst. De invulling op operationeel niveau kan op verschillende manieren plaatsvinden. Vanuit een ruime of enge interpretatie. Als je uitgaat van vertrouwen van de medewerker en dat deze alleen daar naar kijkt wat nodig is voor de werkzaamheden heeft dat waarschijnlijk een ruime toegang tot gevolg. Als het uitgangspunt dat een medewerker alleen dat kan zien waar de medewerker mee bezig is, heeft dit een zeer strikte toegang tot gevolg.	Art. 5, lid 1, onderdeel f, lid 2 AVG Art. 24, lid 1 AVG Art. 32 AVG Art. 35, lid 7, onderdeel d AVG Nr. 2, 7, 9 DUTO-eisen Nr. 6.1.4 BIO Nr. 9.2.2.2 BIO Nr. 9.4.1 BIO Nr. 9.4.1.1 BIO Nr. 9.4.1.2 BIO Nr. 9.4.2 BIO Nr. 14.1.1 BIO Nr. 14.1.1.1 BIO Nr. 18.1.4 BIO
---	-----	--	---	---

BIO-nr	BIO Titel	BIO Tekst	Uitvraag MDT
9.2.2.2	Gebruikers toegang verlenen	Vastgesteld is welke functiescheiding is toegepast en welke rechten verleend	Welke functies worden onderkend in het bedrijfsproces en hoe komt dit tot uitdrukking in het toekennen van rechten aan gebruikers van systeem X?
9.4.1 BIO	Beperking toegang tot informatie	Beperken van toegang tot informatie en systeemfuncties beperkt in overeenstemming met beleid toegangsbeveiliging (LTB)	Op welke manier wordt logisch toegangsbeheer toegepast bij het verlenen van toegang tot systeem X/informatie op de Q-schijf
9.4.1.1 BIO	Beperking toegang tot informatie	Maatregelen van toepassing t.a.v. isoleren van informatie met specifiek belang (TBB's, VIP's)	Welke maatregelen zijn getroffen om specifieke toegang mogelijk te maken tot geclassificeerde informatie?
9.4.1.2 BIO	Beperking toegang tot informatie	Alleen informatie met specifiek belang in te zien en verwerken voor uitoefen van taak (least privilege)	Hoe wordt het mogelijk gemaakt dat gebruikers alleen die informatie kunnen verwerken die ze nodig hebben voor hun werkzaamheden?
9.4.2 BIO	Beperking toegang tot informatie	Vanuit toegangsbeveiligingsbeleid, toegang moet worden beheerst door een beveiligde inlogprocedure	Is er sprake van een beveiligde inlogprocedure voor systeem X en waarom is dat?



BIO Vraagstelling in de controlelijst

7.2	Autorisaties waaronder functiescheiding Onderdeel van 7. BIV: bepaal en geef aan of de toegang tot de gegevens in dit proces onderdeel is van een overkoepelende toekenning van autorisaties Functiescheiding Bepaal en geef aan of de volgende bevoegdheden strikt gescheiden liggen of dat meerdere bevoegde bij één persoon worden belegd; bewarende, registrerende, uitvoerende, controlerende en beschikkende taken. Onderbouw indien meerdere bevoegdheden bij één persoon mogen liggen, waarom dit voldoet en waarom dit nodig is.	De toegang tot de gegevens in het proces moeten geregeld zijn via IMS en moet voldaan worden aan de vereisten vanuit LTB. Indien dit niet mogelijk is, beschrijf de afwijking en de te treffen maatregelen. Dit voorschrift is bedoeld om de integriteit van de gegevens te borgen. Het moet voorkomen worden dat er teveel bevoegdheden bij één persoon komen te liggen. Dit heeft dan tot gevolg dat er meerdere personen naar hetzelfde gegeven moeten gaan kijken. Terwijl vanuit AVG-perspectief wellicht toegang beperkt zou moeten worden.	Art. 5, lid 1, onderdeel f, lid 2 AVG Art. 24, lid 1 AVG Nr. 6.1.4 BIO Nr. 9.2.2.2 BIO Nr. 9.4.1 BIO Nr. 9.4.1.1 BIO Nr. 9.4.1.2 BIO Nr. 9.4.2 BIO Nr. 14.1.1 BIO Nr. 14.1.1.1 BIO Nr. 18.1.4 BIO Nr.'s 2, 7, 9 DUTO-eisen
-----	---	--	---

BIO-nr	BIO Titel	BIO Tekst	Uitvraag MDT
<i>Doelstelling vanuit de BIO9.4: onbevoegde toegang tot systemen en toepassingen voorkomen, beperken van het risico op verlies en misbruik gevoelige gegevens en beïnvloeding beschikbaarheid van informatiesystemen</i>			
9.4.1 BIO	Beperking toegang tot informatie	Beperken van toegang tot informatie en systeemfuncties beperkt in overeenstemming met beleid toegangsbeveiliging (LTB)	Op welke manier wordt logisch toegangsbeheer toegepast bij het verlenen van toegang tot systeem X/informatie op de Q-schijf
9.4.1.1 BIO	Beperking toegang tot informatie	Maatregelen van toepassing t.a.v. isoleren van informatie met specifiek belang (TBB's, VIP's)	Welke maatregelen zijn getroffen om specifieke toegang mogelijk te maken tot geclassificeerde informatie?
9.4.1.2 BIO	Beperking toegang tot informatie	Alleen informatie met specifiek belang in te zien en verwerken voor uitoefen van taak (least privilege)	Hoe wordt het mogelijk gemaakt dat gebruikers alleen die informatie kunnen verwerken die ze nodig hebben voor hun werkzaamheden?
9.4.2 BIO	Beperking toegang tot informatie	Vanuit toegangsbeveiligingsbeleid, toegang moet worden beheerst door een beveiligde inlogprocedure	Is er sprake van een beveiligde inlogprocedure voor systeem X en waarom is dat?



BIO Vraagstelling in de controlelijst

7.3	BIV-classificatie gegevens en proces Bepaal en geef aan de classificatie van de assets, te weten gegevens en het proces.	<p>De beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens moet geborgd zijn. De Belastingdienst kent hierbij een standaard niveau van beveiliging (BBN 2). Uit de clATwee van de vier assets dienen hier geclassificeerd te worden. Zie hiervoor de bijlage bij de RA IB, BIV-classificatie. Onderdeel is daarvan is het uitvoeren van een risicoanalyse. De BIV-classificatie is onderdeel van de domeinarchitectuur en moet vanuit daar worden uitgevoerd. Beschikbaarheid van gegevens heeft een relatie met Business continuity management. Een van de uitwerking van integriteit volgt uit 6.11, integriteit van informatieobjecten.</p> <p>Let op. Bij gebruik van generieke functies dient het beveiligingsniveau van die generieke functies in overeenstemming te zijn met het beveiligingsniveau benodigd voor de betreffende gegevens.</p>	<p>Art. 5, lid 1, onderdeel f, lid 2 AVG Art. 24, lid 1 AVG Art. 32 AVG Art. 35, lid 7, onderdeel d AVG Nr. 6.1.4 BIO Nr. 8.2.1 BIO Nr. 8.2.1.1 BIO Nr. 14.1.1 BIO Nr. 14.1.1.1 BIO Nr. 18.1.4 BIO Nr.'s 2, 9 DUTO-eisen</p>
-----	--	--	--

BIO-nr	BIO Titel	BIO Tekst	Uitvraag MDT
8.2.1	Classificatie van informatie	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging	Welke BIV-waarden zijn van toepassing op de onderscheiden informatieobjecten en is dit geborgd in de domeinarchitectuur
8.2.1.1	Classificatie van informatie	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is	Hoe is de BIV voor dit bedrijfsproces tot stand gekomen en welke bescherming is noodzakelijk geacht?
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen	Worden eisen t.a.v. informatiebeveiliging meegenomen in nieuwe ontwerpen voor systeem X? En bij procesherontwerp?
14.1.1.1	Analyse en specificatie van informatiebeveiligingseisen	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO	
18.1.4	Privacy en bescherming persoonsgegevens	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving	



BIO Vraagstelling in de controlelijst

7.4	Eisen bij levering gegevens externe partij Indien er gegevens geleverd worden aan en door een externe partij (buiten de Belastingdienst), bepaal en geef aan of deze externe partij eisen aan de beveiliging van de gegevens stelt. Zo ja, neem deze eisen mee in het ontwerp en de maatregelen.	Hiervan kan bijvoorbeeld sprake zijn indien er geleverd wordt aan of door een ander land, zoals de Verenigde Staten die eisen stelt.	Art. 5, lid 1, onderdeel f, lid 2 AVG Art. 24, lid 1 AVG Art. 32 AVG Art. 35, lid 7, onderdeel d AVG Art. 44 AVG Nr. 6.1.4 BIO Nr. 18.1.4 BIO Nr. 9 DUTO-eisen
-----	--	--	---

BIO-nr	BIO Titel	BIO Tekst	Uitvraag MDT
18.1.4	Privacy en bescherming persoonsgegevens	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving	Welke maatregelen zijn getroffen om te voldoen aan de gestelde eisen t.a.v. beveiliging en bescherming van persoonsgegevens
Ik zou echter eerder 18.1.4.2 noemen en toelichten als te hanteren BIO-norm			
18.1.4.2	Privacy en bescherming persoonsgegevens	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging	Welke maatregelen zijn getroffen om te voldoen aan gestelde eisen bij gegevenslevering van o.a. persoonsgegevens (bijv. bij het leveren van persoonsgegevens aan een externe partij)?



BIO en archiefwet

■ Vanuit Nationaal archief

- De BIO heeft onder andere tot doel om het onbevoegd openbaar maken, wijzigen, verwijderen of vernietigen van informatie die op media is opgeslagen te voorkomen.
- Het tijdig en juist vernietigen van informatie die daarvoor in aanmerking komt, verkleint de risico's ten aanzien van informatiebeveiliging, omdat het dan niet meer in de verkeerde handen kan vallen. Security incidenten, zoals datalekken, kunnen optreden doordat digitaal vernietigen van vertrouwelijke informatie niet (goed) is uitgevoerd

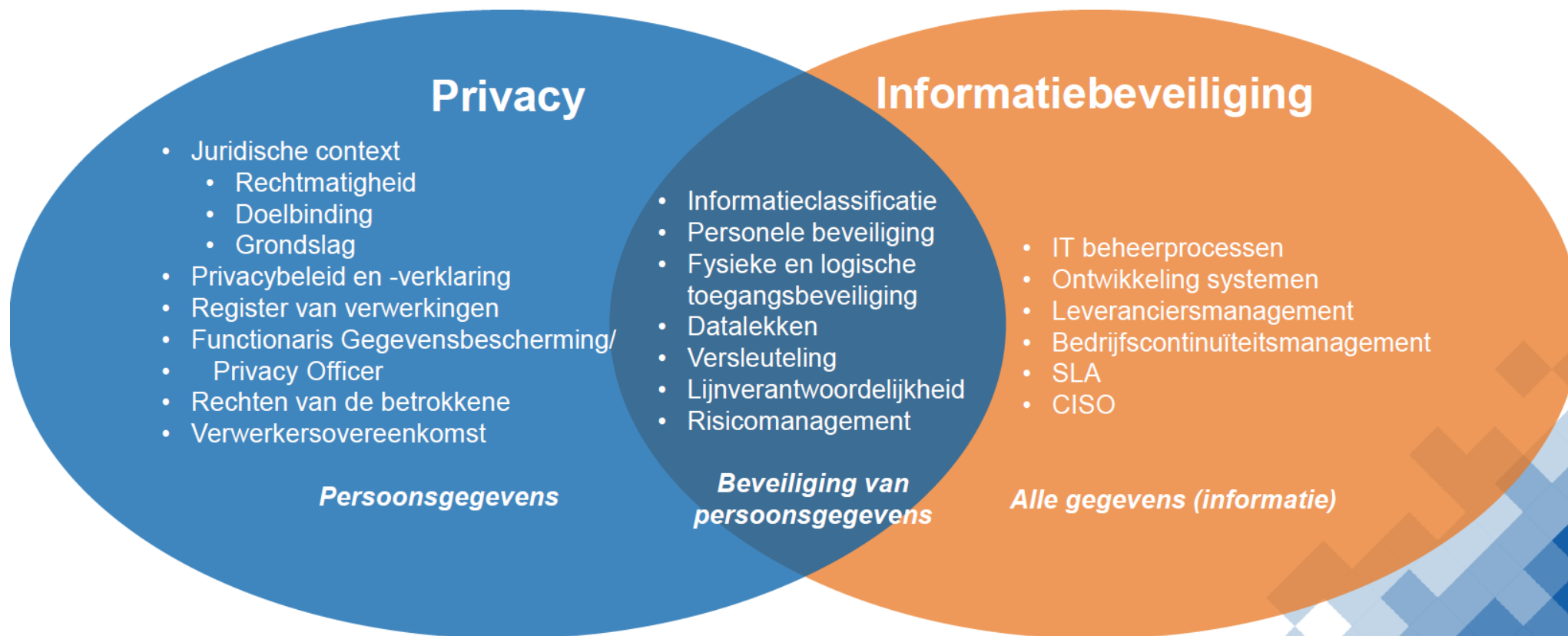


BIO en AVG

Overeenkomsten BIO en AVG

Uitgangspunt:

Gegevensbescherming
beschermt mensen,
informatiebeveiliging
beschermt de organisatie





Einde deel 2 Workshop BIO

