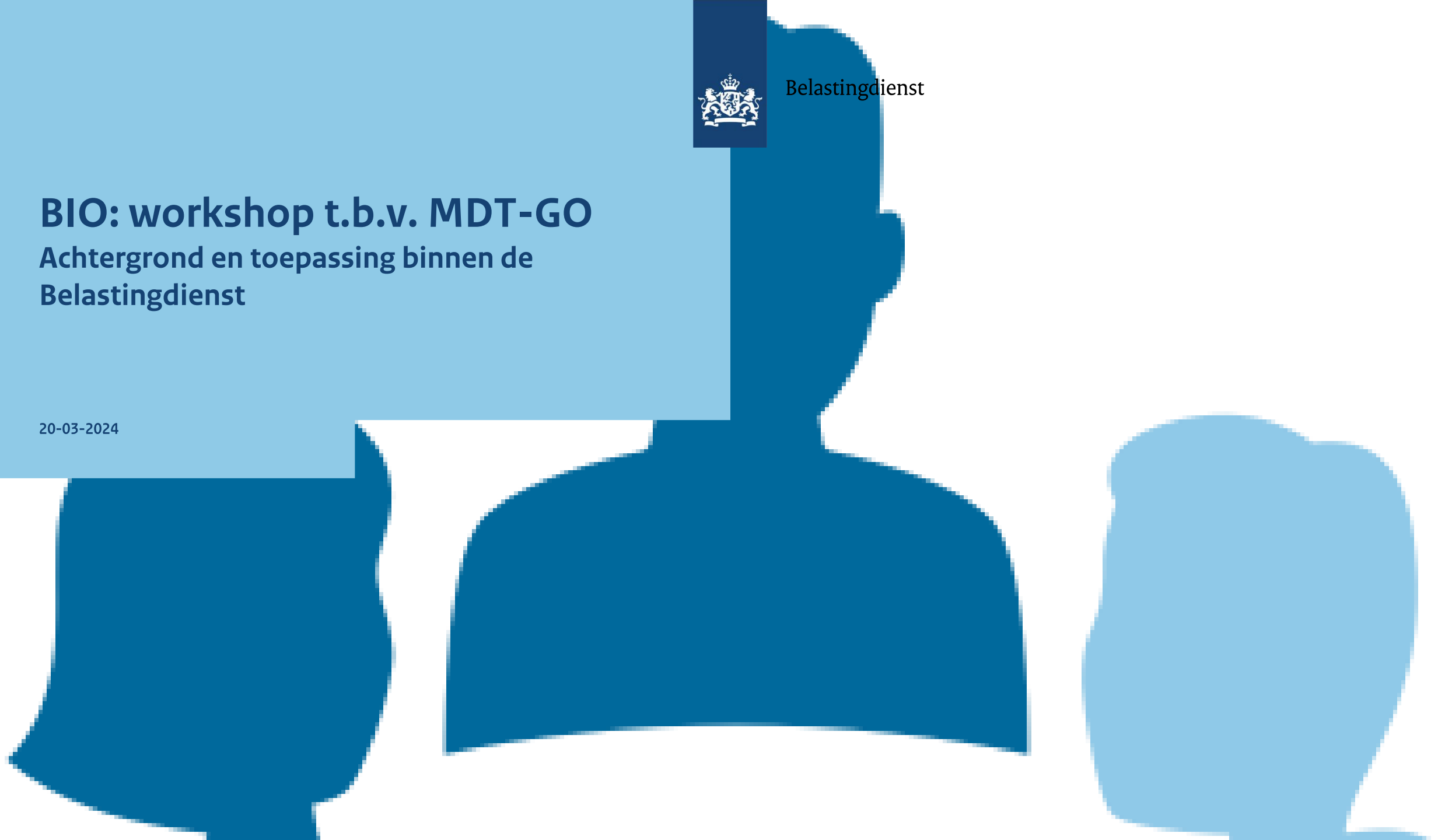
Belastingdienst

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

Achtergrond en toepassing binnen de Belastingdienst

20-03-2024



Vandaag in het BD-nieuws

Collega's zijn alerter op phishing

De resultaten van de phishing-oefening van 6 februari tonen aan dat we MinFin-breed beter zijn geworden in het herkennen van phishing. Bovendien hebben meer collega's deze verdachte e-mail gemeld. De collega's van Domeinen Roerende Zaken (DRZ) hebben het vaakst gemeld, liefst 51%! Daarom krijgen zij de wisselbeker voor 'Secure Dream Team'.

Op een malafide link klikken in een e-mail of een onbekend bestand downloaden kan vergaande gevolgen hebben voor jezelf en de organisatie. Phishing-berichten worden ook steeds geraffineerder. Het is daarom belangrijk dat je de kenmerken van phishing herkent.

Wees alert en meld het

Krijg je verdachte mailtjes (met of zonder bijlagen), apps of een sms of twijfel je over de aard van een bericht? Maak er melding van door het bericht door te sturen naar: valse-email@belastingdienst.nl . Heb je per ongeluk op de link in een verdacht bericht geklikt meld dit dan bij de ICT servicedesk 888 (088-1588 888) en stuur dan de mail naar valse-email@belastingdienst.nl

Zorg dat je altijd verdachte e-mailberichten meldt, ook als je al per ongeluk op een link hebt geklikt of je gegevens hebt gedeeld. Alleen dan blijft de schade beperkt en kan er snel ingegrepen worden. Wil je meer weten over phishing? Bekijk deze pagina over phishing.

Agenda dag 1

Intro en korte inventarisatie kennis en ervaring

1. Achtergrond BIO
2. Opzet van de BIO, even inzoomen
3. Basisbeveiligingsniveaus
4. Processtappen informatiebeveiliging volgens BIO
5. Beschikbaarheid, integriteit en vertrouwelijkheid
6. Risicomanagement
7. TBB’s
8. Glossary

BIO | Baseline Informatiebeveiliging Overheid

Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht om de veiligheid verder te vergroten. De BIO vervangt de baselines informatieveiligheid voor Rijk, Gemeenten, Waterschappen en Provincies. Van BIR, BIG, BIWA en IBI naar BIO. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de NEN-EN-ISO/IEC 27001:2017 en de NEN-EN-ISO/IEC 27002:2017. Voor een veilige digitale overheid. Helder, actueel en veilig.

Bron: https://www.bio-overheid.nl/over-de-bio

Over BIO

Achtergrond BIO

Hier komen we nog op terug!

*Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van **vertrouwelijkheid**, **beschikbaarheid** en **integriteit** alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen*

Bron: VIRBI

De BIO is:

- een gemeenschappelijk **normenkader**, gebaseerd op de internationale normen ISO 27001 en 27002 voor de beveiliging van de **informatie(systemen)** van de overheid;
- een concretisering van een aantal normen naar **concrete maatregelen** die **verplicht** door alle bestuurslagen moeten worden nageleefd

Achtergrond BIO

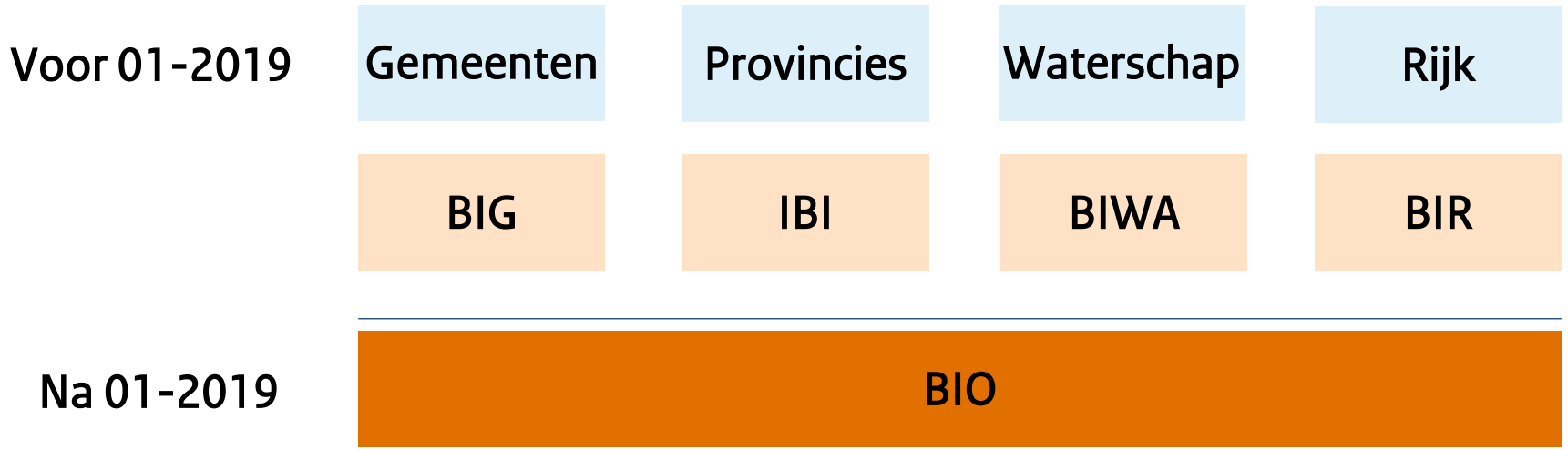
Even kort over ISO27001/27002

- Internationaal erkende norm voor informatiebeveiliging
- Met name voor ICT-bedrijven die aan willen/moeten tonen te voldoen aan gestelde eisen in de norm
- Je kan een certificeringstraject hiervoor gaan inrichten
- Wordt vaak als eis gevraagd bij inkoop/aanbesteding
- 27002 is verdieping en biedt handvatten voor inrichting van normen in ISO27001

Andere relevante normeringen/wetgeving

- Informatiebeveiliging in de zorg: NEN7510 (management), 7512 (gericht op informatieuitwisseling in de zorg), 7513 (logging, vastlegging acties op patiëntendossiers)
- Specifieke norm: ISO27701, gericht op inrichting van een privacy information management system (PIMS, vergelijkbaar met een ISMS). Als add-on op de ISO27001
- NIS2: Network and Information security directive vanuit Europa. Wordt nader uitgewerkt in (opvolger van) wet Beveiliging netwerk-en informatiesystemen (Wbni). Gericht op met name cybersecurity. Van toepassing op meerdere sectoren, decentrale overheden. Zorgplicht en meldplicht beveiligingsincidenten

Achtergrond BIO: ontwikkeling



Dus van toepassing op de rijksoverheid, provincies, waterschappen en gemeenten.

Tevens van belang voor informatieuitwisseling met ketenpartners (publiek-privaat en privaat)

BIO gebaseerd op risicomanagement binnen overheidsorganisaties: mogelijkheid om PDCA-cyclus toe te passen. Hierbij letten op beheersbaar maken van risico's en kansen, inzage in bedreigingen (intern en extern) en vast te stellen maatregelen hierbij. Uiteindelijk verantwoording kunnen afleggen en verbeteringen doorvoeren.

Verbijzondering: VIRBI 2013

VIRBI (zie wetten.overheid.nl)

- Betreft voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2013
- Waarvan kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, bondgenoten of van 1 of meerdere ministeries
- En waarop specifieke rubricering van toepassing is!

Rubricering

- Staatsgeheim Zeer Geheim
- Staatsgeheim Geheim
- Staatsgeheim Confidentieel
- Departementaal Vertrouwelijk

Met daarbij verbijzonderde eisen t.a.v. informatiebeveiliging

Te denken valt aan specifieke autorisaties, detectie van inbraak, ingericht op basis van risicomanagement

Voorbeeld VIRBI Logische toegangsbeveiliging

Logische toegangsbeveiliging		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Toegang tot een account wordt na een aantal direct achtereenvolgende foutieve inlogpogingen geblokkeerd.	5	3	3	3
B	Maatregel Toegang tot systemen kan op groepsniveau worden bepaald.	V	V	V	niet toegestaan
C	Maatregel Toegang tot bijzondere informatie wordt op individueel niveau bepaald.			V	V

Nog een voorbeeld VIRBI Verzending gerubriceerde informatie

6. Verzending van gerubriceerde informatie

Doelstelling

Het waarborgen van een wederzijds verenigbaar beveiligingsniveau voor de vertrouwelijkheid van bijzondere informatie.

Eisen

Er dient te zijn voorzien in een passende set van verenigbare maatregelen indien bijzondere informatie het ministerie verlaat.

De vertrouwelijkheid van informatie moet tijdens (elektronisch) transport buiten gecontroleerd gebied gehandhaafd blijven

		Dep.V	Stg.C	Stg.G	Stg.ZG
A	Maatregel Digitale verzending van bijzondere informatie dient met ministerieel goedgekeurde cryptografische middelen te geschieden. De ministeriële goedkeuring vindt plaats op basis van advies van de Werkgroep Bijzondere Informatiebeveiliging (WBI) of diens rechtsopvolger over de beveiligingswaarde van de cryptografische middelen.		V	V	V
B	Maatregel Digitale verzending van informatie die krachtens een internationaal verdrag of een internationale overeenkomst is verkregen, dient met door de verstrekkende instantie goedgekeurde cryptografische middelen te worden verzonden.			V	V
C	Maatregel Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.	V	V	V	V

Opzet BIO: totaal 114 controls

De onderdelen

- ❑ BIO 5 Informatiebeveiligingsbeleid
- ❑ BIO 6 Organiseren informatiebeveiliging
- ❑ BIO 7 Veilig personeel
- ❑ BIO 8 Beheer bedrijfsmiddelen
- ❑ BIO 9 Toegangsbeveiliging
- ❑ BIO 10 Cryptografie
- ❑ BIO 11 Fysieke beveiliging
- ❑ BIO 12 Beveiliging bedrijfsvoering
- ❑ BIO 13 Communicatiebeveiliging
- ❑ BIO 14 Informatiesystemen
- ❑ BIO 15 Leverancier relaties
- ❑ BIO 16 Beheer Informatiebeveiligingsincidenten
- ❑ BIO 17 Informatie beveiligingsaspecten van BCM
- ❑ BIO 18 Naleving

https://www.bio-overheid.nl/bio-practices/

Opzet BIO: vanuit CSO Healthcheck Belastingdienst

Referentie	Onderwerp	BIO Ref	ID	Vraag
BIO 6	Organiseren informatiebeveiliging	6.1.1	1	Zijn binnen het dienstonderdeel de verantwoordelijkheden voor informatiebeveiliging toegewezen, gecommuniceerd en is de rol van Business Security Officer (BSO) ingevuld?
		6.1.5	2	Is informatiebeveiliging geïntegreerd in de projecten van het dienstonderdeel?
		6.2	3	Wordt tijdens werkoverleggen en HR gesprekken aandacht besteed aan gedragsaspecten van veilig werken buiten kantoor?
BIO 7	Veilig personeel	7.2.2	4	Hebben alle medewerkers (inclusief contractanten) een passende bewustzijnsopleiding en -training gehad, inclusief een regelmatige bijscholing over beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie?
		7.3	5	Worden bij beëindiging of wijziging van het dienstverband de verantwoordelijkheden en taken m.b.t. informatiebeveiliging besproken met de medewerkers of contractanten?
BIO 8	Beheer bedrijfsmiddelen	8.1	6	Heeft het dienstonderdeel in (samenspraak met de ketens) een inventarisatie opgesteld van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten?
		8.1	7	Zijn alle medewerkers en contractanten aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen?
BIO 9	Toegangsbeveiliging	9.2.5	8	Wordt het toekennen en intrekken van toegangsrechten minimaal jaarlijks beoordeeld door de eigenaar van de bedrijfsmiddelen?
BIO 11	Fysieke beveiliging	11.1	9	Het dienstonderdeel heeft gebieden met gevoelige of essentiële informatie geïdentificeerd en daar, i.o.m. de facilitair dienstverlener, passende beschermende maatregelen getroffen?
		11.2	10	Wordt ‘clear desk’/'clearscreen' beleid actief gepromoot en toegepast binnen het dienstonderdeel?
BIO 12	Beveiliging bedrijfsvoering	12.1	11	Wijzigingen in werkprocessen binnen het dienstonderdeel worden geverifieerd op informatie beveiligingsaspecten
		12.1.1	12	Binnen het dienstonderdeel zijn bedieningsprocedures (handleiding/werkinstructies) gedocumenteerd en beschikbaar voor alle gebruikers
BIO 15	Leveranciersrelaties (zie ICO-wizard)	15.1	13	Het dienstonderdeel verifieert dat, bij inkoop en aanbestedingstrajecten de informatiebeveiligingsaspecten worden opgenomen in het contract
BIO 16	Beheer informatiebeveiliging incidenten	16	14	Binnen het dienstondereel worden informatiebeveiligingsincidenten gemeld, geanalyseerd en leidt dit tot structurele verbeteringen
BIO 18	Naleving	18.2	15	Beoordeelt de directie binnen haar verantwoordelijkheidsgebied de naleving van de informatieverwerking en bijbehorende procedures aan de hand van de van toepassing zijnde beleidsregels, normen en andere beveiligingseisen?

Beschikbaarheid, integriteit en vertrouwelijkheid: het BBN als uitgangspunt

Beschikbaarheid	Integriteit	Vertrouwelijkheid	BBN
Laag	Laag	Laag	BBN1
Midden	Midden	Midden	BBN2
Midden	Midden	Hoog	BBN3

Toelichting

- BBN1 Beschikbaarheid is laag
  - Systeem mag 2 weken uitvallen
  - Geen gevolgen voor burgers en bedrijven
  - Max dataverlies bijv. 28 uur
- BBN2 Integriteit is midden
  - Juistheid, tijdigheid en volledigheid waarborgen
  - Verlies van informatie kan leiden tot forse schade (financieel, politiek, publiek respect)
- BBN3 Vertrouwelijkheid is hoog
  - Verlies van informatie heeft grote impact
  - Niet uit te leggen wanneer deze informatie niet gerubriceerd is

Basisbeveiligingsniveaus, wat zijn dat?

1. Opgesteld en ingericht ten behoeve van werking risicogebaseerd informatiebeveiliging
2. Standaard beveiligingsniveaus met bijbehorende beveiligingseisen, een classificatie
3. Per BBN vastgesteld aan welke controls uit de ISO27002 moet worden voldaan.
4. Keuze van niveau bepaald door proceseigenaar op basis van risicomanagement.
5. Hiervoor beschikbaar, de BBN-toets

20190514-Baselinetoets-BBN-BIO-1.02-DEF.xlsx

Beschikbaarheid, integriteit en vertrouwelijkheid

Waar hebben we het eigenlijk over?

- Beschikbaarheid
  - Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen)
- Integriteit
  - Integriteit betreft het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan. De juistheid en volledigheid van de informatie is een directe verantwoordelijkheid van de eigenaar van het informatiesysteem en de hem ondersteunende managers en medewerkers
- Vertrouwelijkheid
  - Vertrouwelijkheid betreft het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder andere om het beveiligen van de toegang tot de gebouwen, de informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, trojan horses). En het gaat ook om maatregelen om te voorkomen dat de eigen medewerkers toegang krijgen tot informatie die niet voor hen is bedoeld (‘need to know’)

Het basisbeveiligingsniveau toegelicht

Vaststellen basis beveiligingsniveau (BBN):

- BBN1
  - Wat minimaal mag worden verwacht van een organisatie om zorgvuldig met informatie en data om te gaan
  - Aan de hand van controls en maatregelen uit wet-en regelgeving wordt een basisniveau IB afgedwongen
- BBN2
  - Is uitgangssituatie voor alle informatiesystemen binnen de overheid
  - Wanneer er vertrouwelijke informatie wordt verwerkt
  - Incidenten leiden tot bestuurlijke commotie
  - Te beschermen belang maximaal Departementaal Vertrouwelijk (DepV)
  - Maatregelen BBN1 verzwaard door bijvoorbeeld afhankelijkheden in ketens en netwerken

Het basisbeveiligingsniveau toegelicht

Vaststellen basis beveiligingsniveau (BBN):

- BBN3
  - Bescherming van minimaal DepV-data en documenten tegen o.a. statelijke actoren
  - Aangesloten op relevante NAVO-regelgeving
  - Van toepassing op geclassificeerde gegevens, systemen en processen niet zijnde BBN2 (DepV of hoger)
  - Verlies van informatie heeft grote impact
  - Informatie met een rubricering wordt door derden aangeleverd (zie vraagstelling in controlelijst)
  - Infrastructuur moet ook uit kunnen gaan van BBN3-classificatie en bijbehorende beschermende maatregelen

Risicoanalyse noodzakelijk

Processtappen informatiebeveiliging volgens BIO

Gebruik van de quickscan informatiebeveiliging

Te doorlopen stappen

- Bepaal scope, context en rubricering

<Naam van het Informatiesysteem>	
Informatiesysteem-eigenaar	<naam van de informatiesysteemeigenaar>
De gebruikers van het informatiesysteem	Degene die werkzaam zijn met het informatiesysteem • <wie is de interne gebruiker / klant?> • <wie is de externe gebruiker / klant?> • <aantal gebruikers / burgers>
De output van het informatiesysteem	
Koppelvlakken met andere informatiesystemen	Een architectuurplaatje kan verhelderend werken
Het informatiesysteem ondersteunt de volgende processen	
Kritische momenten	Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes

<Naam van het proces>	
Proceseigenaar	<naam van de proceseigenaar>
De klant van het proces	De klant is degene die direct aan het eind van het proces het resultaat (de output) afneemt: • <wie is de interne klant?> • <wie is de externe klant?>
De output van het proces	<De output is het resultaat van handelen in het proces>
Koppelvlakken met andere processen	• <aanleverende processen/ organisaties> • <afnemende processen/organisaties>
Gebruikte systemen	De informatiesystemen die worden gebruikt bij de activiteiten in het proces: • <informatiesysteem>

Rubricering van informatie:

Het vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven.

→dan de VIRBI van toepassing, inclusief te nemen maatregelen per rubriek

Processtappen informatiebeveiliging volgens BIO

- Gebruik van de quickscan informatiebeveiliging

Te doorlopen stappen via een workshop

1. Bepaal scope, context en rubricering
2. Classificeer proces en informatiesysteem
3. Bepaal het dreigingsprofiel
4. Bepaal betrouwbaarheidseisen (BIV-waarden)
5. Voor de BBN-toets uit adhv Dataclassificatietoets BIO/hanteer Quickscan BIO
6. Bepaal passendheid BBN

   In deze stap wordt per onderzocht proces en/of informatiesysteem de passenheid van het gekozen BBN bepaald door na te gaan welke extra schade kan ontstaan of welke schade waarschijnlijk niet aan de orde zal zijn voor de bij dit BBN behorende niveaus van “Beschikbaarheid” en “Integriteit”.
7. Stel resultaten vast

Procesclassificatie:

- Ondersteunend
- Bijdragend
- Strategisch
- Strategisch kritisch

Systeemclassificatie

- Nuttig (N)
- Belangrijk (B)
- Vitaal (V)

Informatiebeveiliging is risicomanagement

Hoezo?

- Risico's in het kader van informatiebeveiliging zien toe op de betrouwbaarheidseisen integriteit, beschikbaarheid en vertrouwelijkheid.
- Risicomanagement identificeert, beoordeelt en behandelt risico's, die mogelijk een negatieve impact hebben op de doelen van de organisatie, door het waarborgen van de betrouwbaarheid van de informatie(voorziening) en de continuïteit van de dienstverlening.
- Bij informatiebeveiliging staat risicobeheersing centraal

Samenvatting strategisch toprisico 3 Informatiebeveiliging (1/2)

Risico-omschrijving	*Doordat de informatiebeveiliging (binnen de infrastructuur) onvoldoende aantoonbaar op orde is, kan de beschikbaarheid, integriteit en vertrouwelijkheid van de BD-data van burgers en bedrijven niet gegarandeerd worden*.
Conclusie over mate van beheersing strategisch top risico en het restrisico (huidig en verwacht)	*Huidige situatie* Op dit moment wordt het informatiebeveiligingsrisico nog niet voldoende beheerst. Veel beveiligingsmaatregelen zijn geïmplementeerd, maar het ontbreekt veelal aan de aantoonbaarheid (van de juiste werking), zoals ook aangegeven bij maatregel 2c op de volgende dia. *Verwachting na uitvoering van de door u opgenomen beheersmaatregelen* De verwachting is dat de mitigerende maatregelen (zie volgende dia) in 2024, grotendeels geïmplementeerd kunnen worden. Uiteraard is er een afhankelijkheid van o.a. de (opdrachten-)portfolio en de beschikbaarheid van voldoende financiële middelen en personeel. Zo gauw er een exception optreedt, zal dit in de 4-maandelijkse rapportage vermeld worden. Na implementatie van de maatregelen en de realisatie van het OBIO-programma (IV&D), verwachten wij dat er sprake zal zijn van een acceptabel restrisico. *Ter informatie:* Voor de IV-organisatie ligt de nadruk op preventieve maatregelen om beschikbaarheid, integriteit en vertrouwelijkheid van de data, zoveel als mogelijk, te garanderen. Veel beheersmaatregelen zijn geïmplementeerd, maar ontbreekt het veelal aan inzicht, overzicht en aantoonbaarheid. Het is dan ook noodzakelijk om de aantoonbaarheid op orde te brengen (risico wordt dus nog onvoldoende beheerst); waarmee eventueel ook wordt vastgesteld of er nog aanvullende beveiligingsmaatregelen geïmplementeerd moeten worden. **Inhoudsdeskundige: xx** | **1e lijns RM: xx**

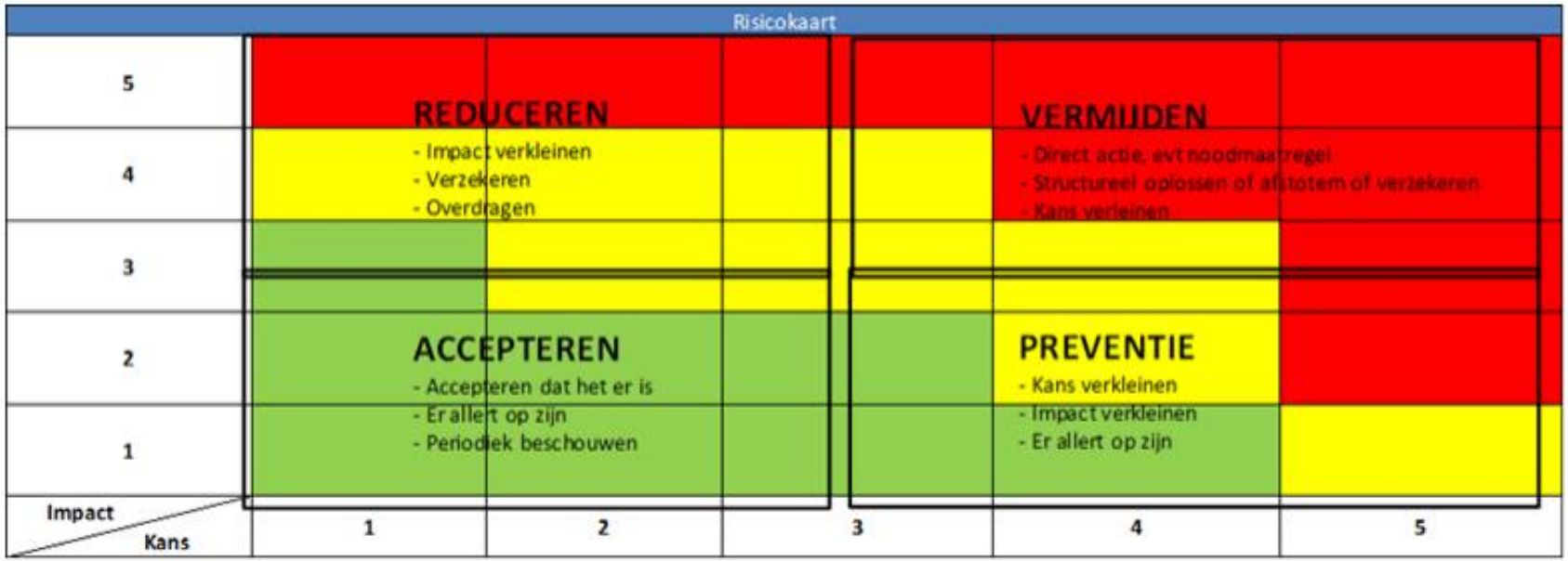
Risicomanagement: 6 stappen volgens COSO

Het proces van risicomanagement bestaat in veel modellen uit zes stappen:

1. Bepaal doelstelling: wat wil de organisatie bereiken.
2. Identificeer risico's: een dreiging is een onzekere gebeurtenis met mogelijke gevolgen voor de doelstelling.
3. Identificeer mogelijke impact: een risico is een dreiging waaraan een kans en gevolg toegevoegd zijn.
4. Beoordeel de risico's: een organisatie moet van tevoren bepalen hoeveel risico gelopen mag worden, door het maken van een risicoprofiel en de risicobereidheid uit te werken en de belangrijkste risico's te prioriteren.
5. Beheren van risico's, 4 manieren
6. Monitoring: gedurende het hele proces volgen van risico's (meten, controleren en rapporteren) en de werking van maatregelen door deze maatregelen ook te koppelen aan het incidentmanagement proces.

https://www.coso.org/Documents/COSO-2015-3LOD.pdf

Resultaat risicoanalyse: de heatmap



Figuur 4: risicostrategie heatmap

- Vermijden: alle mogelijke beheersmaatregelen treffen om het risico's te vermijden
- Preventie: beheersmaatregelen selecteren die de kans en/of impact verkleint, maar waarbij een restrisico overblijft
- Reduceren: overdragen/verzekeren: het risico wordt overdragen aan een andere partij (denk aan een brandverzekering)
- Accepteren: het (rest)risico wordt geaccepteerd en er worden hiervoor geen beheersmaatregelen getroffen

Een laatste uitstapje, TBB

TBB

"TBB: Personen, informatie, informatiesystemen, materieel, goederen, imago en objecten, waarbij in geval van compromittering, of de mogelijkheid van compromittering, nadelige gevolgen, of een risico daarop, kan ontstaan voor de vertrouwelijkheid, beschikbaarheid en integriteit van de primaire processen van de rijksoverheid, delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries."

[Bron: Besluit BVA-stelsel Rijksdienst 2021]

"Bijzondere informatie: informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries."

[Bron: VIR-BI 2013]

"BBN3 is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk ..."

"Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV), (zoals gedefinieerd in het VIR-BI) ..."

[Bron: BIO v1.04]

TBB - Gegevens

Relatie TBB, rubricering en BIV classificatie gegevens

Leidraad TBB	VIR – BI	BIO	Belastingdienst
TBB 1	Staatsgeheim Zeer Geheim	-	BIV xx3
TBB 2	Staatsgeheim Geheim	-	BIV xx3
TBB 3	Staatsgeheim Confidentieel	-	BIV xx3
TBB 4	Departementaal Vertrouwelijk	BBN 3 (BIV 223)	
TBB 4	Departementaal Vertrouwelijk	BBN 2 (BIV 222)	
TBB 4	Departementaal Vertrouwelijk	BBN 1 (BIV 111)	
TBB 4	Ongerubriceerd	BBN 2 (BIV 222)	
TBB 4	Ongerubriceerd	BBN 1 (BIV 111)	

- Over het algemeen verwerkt de BD gegevens met een BIV classificatie 222 en een rubricering Dep.V. Het Generieke Beveiligingsniveau Belastingdienst (GBB) is hierop ingericht.
- Belastingdienst moet compliant zijn aan VIR-BI en BIO en hanteert derhalve een fijnmazigere labeling en BIV classificatie dan TBB classificatie.
- TBB classificatie is te grof voor proportionele bescherming kijkend naar de eisen vanuit de BIO.
- Er zijn geen overheids-/rijkskaders voor BIV classificatie van gegevens met rubricering StgC en hoger. De Belastingdienst hanteert hier vooralsnog Vertrouwelijkheid 3.
- **TBB classificatie van gegevens is af te leiden uit rubricering en BIV classificatie.**

TBB's binnen GO: opnieuw onder de aandacht

TBB naam	Categorie
Klantgegevens: -Adressen en contactgegevens van Vips (w.o. beursgenoteerde organisaties) -Inkomstengegevens van Vips (w.o. beursgenoteerde organisaties) -Belastingafspraken met bedrijven (Rulings)	3
Klantbehandeling: -selectiecriteria voor de aangiftebehandeling	3
Klantgegevens: -Adressen en contactgegevens van personen, bedrijven en organisaties -Inkomstengegevens van personen, bedrijven en organisaties	4
Koersgevoelige informatie van bedrijven -brutowinstmarges; -informatie over voorgenomen fusies of overnames van of door multinationals; en -(andere) beursgevoelige informatie	4
Klantbehandeling -documenten met strategische en/of tactische informatie.	4
Personele gegevens -Persoonsgevoelige informatie (o.a. financiële situatie, gezinssituatie) van overheidspersoneel, en/of van personen met een interessante werkgever (bijvoorbeeld organisaties van openbaar belang), (risico: chantage, corruptie, e.d.). -Personeelsdossiers of persoonsgevoelige informatie (financiële situatie, gezinssituatie) over eigen medewerkers (risico: chantage, corruptie, e.d.).	4
Eigen organisatie -documenten met strategische en/of tactische informatie; - business cases; inkoopgegevens en informatie over (toekomstige) aan- en uitbestedingen (concurrentiegevoelig).	4

Glossary

Meer info over BIO-producten en aanpassing BIO

1. https://www.bio-overheid.nl/ voor hulp bij implementeren en hanteren van de BIO
2. https://www.bio-overheid.nl/bio-practices/ voor heel snel zoeken in de BIO
3. Dossier BIO op digitale overheid.nl
4. Centrum informatiebeveiliging en privacybescherming (CIP): thema-uitwerking BIO
5. Besluit voorschrift informatiebeveiliging rijksdienst 2007
6. Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2013
7. Informatiebeveiligingsdienst VNG
8. Over NIS2 en de BIO: veelgestelde vragen

Einde deel 1 Workshop BIO