TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Handreiking besluitvorming implementatie BIR

voor bestuurders en beveiligingsfunctionarissen van Zelfstandig Bestuursorganen (ZBO's)

Versie 1.1 – 22 - 01 - 2015

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Samenvatting

Doel van de handreiking

Overheidsorganisaties hebben de behoefte uitgesproken om naar één gemeenschappelijk kader voor informatieveiligheid toe te groeien. De Baseline Informatiebeveiliging Rijksdienst (BIR) en de daarvan afgeleide Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG) en Waterschappen (BIWA) vullen deze behoefte in.

De inzet van de Taskforce BID en het Ministerie van BZK, Directoraat Generaal Organisatie en Bedrijfsvoering Rijk (DG OBR), is dat ook de ZBO's het VIR en de BIR in 2014 gaan omarmen.

In deze handreiking wordt een aantal beslisstappen beschreven, waarmee bestuurders van ZBO's richting kunnen geven aan de invoering van de BIR, op een manier die het beste past bij de organisatie.

Hiervoor zijn vier stappen benoemd die antwoord geven op de volgende vragen:

Stap 1: Wat is de huidige positie van de ZBO op het gebied van informatieveiligheid?

Stap 2: Welk ambitieniveau heeft de ZBO op het gebied van informatieveiligheid?

Stap 3: Welk invoeringstraject sluit het beste aan op het ambitieniveau van de ZBO?

Stap 4: Wat is nodig om te beginnen?

Leeswijzer

Deel I van de handreiking richt zich op de sturende rol van de bestuurder.

Deel II van de handreiking richt zich op de uitvoerende rol van de CISO[1] / Informatiebeveiligingsfunctionaris die betrokken is bij de voorbereiding van de besluitvorming en de daadwerkelijke implementatie.

[1] Chief Information Security Officer

Inhoudsopgave

DEEL I: Sturing geven aan de invoering van de BIR

De Taskforce BID is begin 2013 ingesteld door Minister Plasterk van het ministerie van BZK voor een periode van twee jaar. De opdracht is te komen tot versterking van de gerichtheid op en verankering van informatieveiligheid in de reguliere processen en informatieketens binnen de verschillende overheidslagen. De Taskforce zet in op een generieke programmering om dit einddoel op een eenduidige en efficiënte wijze te realiseren. Vanuit deze generieke programmering is een vertaling gemaakt naar de specifieke situatie van elke overheidslaag.

Zelfstandig Bestuursorganen (ZBO's) nemen in dit traject een speciale positie in. ZBO's zijn in beginsel ook geen expliciete overheidslaag, maar zijn wel gelieerd aan de departementen. De nadruk voor de ZBO's ligt daarom specifiek op de adoptie van het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijk (BIR). Met het adopteren van VIR/BIR leggen de ZBO's die nog geen normenkader hebben zich vast op het inrichten van processen die leiden tot grotere beheersing op het vlak van informatieveiligheid. De ZBO's die al wel een normenkader hebben, committeren zich aan een gemeenschappelijke basis door de adoptie van het VIR en de BIR, al dan niet vertaald naar hun eigen situatie.

Waarom invoering van de Baseline Informatiebeveiliging Rijksdienst (BIR) bij ZBO's?

Het IT-landschap binnen de overheid wordt steeds complexer en de onderlinge afhankelijkheid tussen organisaties neemt steeds verder toe. Er is behoefte aan één gemeenschappelijke taal om te kunnen communiceren over de beveiligingseisen die gesteld worden aan de informatievoorziening. Voor een betrouwbare uitwisseling van informatie tussen ketenpartners is groeiende behoefte aan een gemeenschappelijk beveiligingskader. Organisaties willen daarbij ook graag op een eenduidige en transparante wijze sturen op en verantwoording afleggen over informatieveiligheid.

De BIR-2012 biedt één normenkader voor de beveiliging van de informatiehuishouding van het Rijk. Daarmee biedt de BIR één heldere set afspraken, zodat een bedrijfsonderdeel weet dat gegevens die worden verstuurd naar een ander onderdeel van de rijksdienst, of door een ander onderdeel worden beheerd of verwerkt, op het juiste beveiligingsniveau (in termen van vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld. De BIR is gestructureerd volgens de ISO27001 normen, waarbij een aantal Rijksspecifieke normen is toegevoegd.

Bij informatieveiligheid gaat het vooral over het streven naar een excellente bedrijfsvoering en dienstverlening. Ieder Zelfstandig Bestuursorgaan (ZBO) dat verantwoordelijk is voor informatie van burgers, bedrijven en instellingen, voelt de verantwoordelijkheid om deze informatie zorgvuldig te bewerken en te beheren. Informatiebeveiliging maakt daar een cruciaal onderdeel van uit. De invoering van de BIR is daarbij geen doel op zich, maar helpt juist de risico's binnen de ZBO te beheersen en hier op een eenduidige en herkenbare wijze

over te communiceren. Dit draagt bij aan transparantie en creëert vertrouwen tussen (keten)partners en richting burgers en bedrijven.

Waarom een handreiking BIR voor bestuurders van ZBO's?

Het ZBO-landschap is zeer divers, zowel in de aard en het maatschappelijk belang van de dienstverlening, de omvang van de ZBO, als in de veronderstelde risico's op het gebied van informatieveiligheid. Dit gegeven maakt dat iedere ZBO-bestuurder een eigen afweging zal maken over de manier waarop informatieveiligheid het beste kan worden verankerd in de organisatie.

Voor bestuurders is het van belang om richting te geven, de uitvoering te organiseren, kaders mee te geven en tot slot de voortgang te monitoren. De daadwerkelijke uitvoering van de implementatie vindt plaats door de medewerkers.

Deze handreiking geeft richting bij het starten en/of aanscherpen van verbeterinitiatieven op het gebied van informatieveiligheid. Welke bestuurlijke vraagstukken zijn relevant bij informatieveiligheid binnen een ZBO en welke toegevoegde waarde levert de invoering van de BIR voor de doelstellingen van de organisatie? Welke beslissingen moeten genomen worden om tot invoering van de BIR over te kunnen gaan?

Het doel van deze handreiking is niet om een uitputtend overzicht te geven van alle regelgeving waaraan een ZBO moet voldoen of hoe op detailniveau implementatie van beheersmaatregelen moet plaatsvinden.

Deze handreiking geeft in vier overzichtelijke beslisstappen aan op welke wijze positiebepaling en implementatie van de BIR binnen een ZBO zo effectief en efficiënt mogelijk kan worden bestuurd.

Iedere stap wordt kort ingeleid en eindigt met een beslispunt.

De bestuurder kan sturing geven aan het doorlopen van deze stappen en de uitvoering hiervan beleggen in de organisatie, bij de functionaris die belast is met informatieveiligheid. In Deel II worden voor de beveiligingsfunctionaris of CISO concrete handreikingen gegeven voor de uitvoering van de stappen.

1 Oriëntatie huidige situatie

1.1 Inleiding

Sommige (vaak kleinere) ZBO's hebben de uitvoering van informatieveiligheid ondergebracht op directieniveau, terwijl andere ZBO's een omvangrijke governance hebben ingericht, met diverse (staf-) functionarissen die dagelijks werken aan dit onderwerp. Bij veel ZBO's is informatieveiligheid een terugkerend thema op de bestuurstafel. Zo zijn veel ZBO's al bezig met invoering van de BIR of oriënteren zich op de invoering hiervan. Een aantal ZBO's is zelfs ISO27001 gecertificeerd. In een aantal gevallen hebben ZBO's te maken hebben met complexe en soms ook aanvullende (inter-) nationale wet- en regelgeving op het gebied van informatieveiligheid. Het aantoonbaar 'in control zijn' wordt hierbij een steeds belangrijker gegeven.

Voor deze handreiking zijn drie typen ZBO's gedefinieerd die ieder hun eigen aanpak kunnen hanteren voor informatieveiligheid. In Deel II is een vragenlijst opgenomen die kan helpen bij het vaststellen welke benadering het meeste aansluit op de eigen situatie. Deze inschatting is bepalend voor de vervolgstappen.

1.2 Beslispunt

Bepaal welk type ZBO het meeste overeenkomt met de eigen situatie. Onderstaand worden drie 'ideaaltypen' beschreven. In de praktijk kan er sprake zijn van een combinatie van typen.

Type A

Eerste oriëntatie op BIR

- er is een beperkte mate van volwassenheid op het gebied van informatieveiligheid
- informatieveiligheid is niet per definitie een terugkerend thema aan de bestuurstafel
- risicoanalyse heeft nog niet plaatsgevonden
- eerste oriëntatie op de BIR of ISO27001
- vaak een kleinere ZBO

Type B

Normenkader grotendeels ingevoerd

- een relatief grote mate van volwassenheid op het gebied van informatieveiligheid is al bereikt
- informatieveiligheid staat nadrukkelijk op de bestuurlijke agenda
- beleid is risk based
- BIR, ISO27001 of een daarvan afgeleid normenkader is geheel of gedeeltelijk ingevoerd
- governance van informatieveiligheid is ingericht
- vaak middelgrote tot grote ZBO

Type C

BIR naast andere wet- en regelgeving

- een relatief grote mate van volwassenheid op het gebied van informatieveiligheid is al bereikt, waarbij men zich vaak extra bewust is vanwege andere specifieke wetgeving

- informatieveiligheid staat nadrukkelijk op de bestuurlijke agenda
- beleid is risk based
- governance van informatieveiligheid ingericht
- complexe, soms (inter-) nationale wet- en regelgeving op gebied van (informatie-) veiligheid
- BIR en/of ISO27001 is hierdoor niet altijd het leidende normenkader. Er is andere, vaak sectorspecifieke wetgeving
- vaak middelgrote tot grote ZBO

2 Ambitie

2.1 Inleiding

De ambitie van ZBO's op het gebied van informatieveiligheid, en de positie ten opzichte van de BIR, wordt primair ingegeven door de verwachte meerwaarde voor de verbetering van de dienstverlening aan burgers, bedrijven en instellingen, naast de risicobeheersing van de eigen bedrijfsvoering. Deze is breder dan alleen informatieveiligheid, maar informatieveiligheid kan een bijdrage leveren aan het beperken van de bedrijfsvoeringsrisico's.

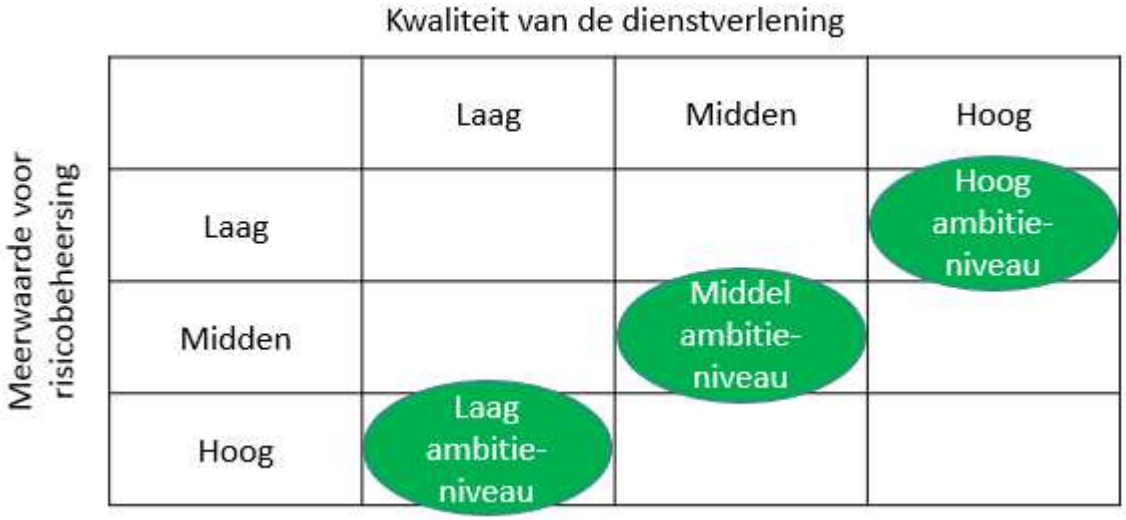
Vragen daarbij zijn: levert de BIR een bijdrage aan het meer in control zijn op het gebied van informatieveiligheid? Draagt dit bij aan het vergroten van het vertrouwen in de dienstverlening van de ZBO en de betrouwbaarheid van de informatievoorziening?

2.2 Beslispunt

Bepaal het ambitieniveau van de organisatie op het gebied van informatieveiligheid:

- Geef een score voor de mate waarin informatieveiligheid bijdraagt aan de kwaliteit van dienstverlening van de ZBO.
- Geef een score voor de mate waarin informatieveiligheid bijdraagt aan het beheersen van de risico's voor het primaire proces en de bedrijfsvoering.

Onderstaande tabel is een hulpmiddel om het eigen ambitieniveau te scoren en daarover te communiceren.



De uiteindelijke score is een belangrijke input voor de bestuurlijke afweging over de invoering van de BIR.

3 Bestuurlijke afweging

3.1 Inleiding

Nu het beeld van de huidige situatie en het ambitieniveau van de ZBO bekend zijn, kan worden bepaald welke invoeringsstrategie het beste past bij de eigen organisatie. Het belangrijkste criterium daarbij is de afweging tussen de verwachte meerwaarde van de invoering van de BIR en de benodigde inspanning en in te vullen randvoorwaarden.

Ambitieniveau

Type ZBO's	Laag	Midden	Hoog
A	FIT/GAP	FIT/GAP	BIR
B	FIT/GAP	BIR	BIR
C	FIT/GAP + Aanvullende norm	BIR + Aanvullende norm	BIR + Aanvullende norm

BIR:

Op basis van een risicoafweging van de kritieke processen in de organisatie wordt bepaald of de organisatie de BIR volledig wil invoeren. Het is denkbaar dat onderdelen van de BIR niet, of niet in die mate, van toepassing zijn op de organisatie. Hier kan beargumenteerd worden afgeweken van de BIR met een zogeheten 'explain'. Het hebben van een aantal 'explains' wil niet zeggen dat de ZBO niet 'in control' is, maar dat gemotiveerd op basis van een risicoafweging wordt afgeweken van de BIR, de risico's daarvan bekend zijn en ook

worden geaccepteerd, dan wel dat daarvoor een verbetertraject voor wordt ingezet of alternatieve maatregelen voor gehanteerd worden.

FIT/GAP:
Er zijn situaties denkbaar, bijvoorbeeld voor heel kleine organisaties, waar de BIR niet past als normenkader of waar een normenkader op zichzelf al erg veel is. In dit geval is het raadzaam om voor de kritieke processen een zogenaamde 'FIT/GAP'-analyse uit te voeren, zodat de organisatie inzicht heeft in waar het staat ten opzichte van de BIR en welke onderdelen van de BIR wel bruikbaar zijn.

BIR+ Aanvullende normen:
Wanneer ZBO's gehouden zijn aan aanvullende (inter-)nationale wet- en regelgeving zullen zij aanvullende maatregelen doorvoeren, bovenop de BIR of bovenop de onderdelen van de BIR die voor hen bruikbaar zijn.

3.2 Beslispunt

- Bepaal de invoeringsstrategie voor de BIR. Dit kan grofweg leiden tot drie mogelijke invoeringstrajecten:
    1. De BIR volledig integreren in het beleid voor informatieveiligheid.
    2. Uitvoeren van een FIT/GAP-analyse op de kritieke processen en alleen de noodzakelijke maatregelen van de BIR treffen.
    3. BIR of delen van de BIR implementeren naast andere, vaak sectorspecifieke, wetgeving.

4 Realisatie

4.1 Inleiding

De kern van deze stap is het daadwerkelijk sturing geven aan de realisatie. Dit vraagt naast een duidelijk commitment van de leiding, alsook heldere afspraken over de rollen en verantwoordelijkheden, de inzet van mensen en middelen en de wijze van rapportage over de voortgang. Veelal vindt de realisatie projectmatig plaats. Uit praktijkgevallen blijkt dat directe betrokkenheid van bestuur, directie en lijnmanagement voor een succesvolle invoering essentieel is.

Een apart aandachtspunt daarbij is de verantwoording over de invoering van de BIR en over de gemaakte afweging tussen 'comply or explain'. De BIR dient een integraal onderdeel uit te maken van de bedrijfsvoering van de ZBO. Deze verantwoording kan daarom het beste worden opgenomen in het jaarverslag.

4.2 Beslispunt

- Bepaal de wijze van invoeren en de daarbij behorende organisatorische, personele, financiële en managementinformatie aspecten.

- Bepaal de wijze van verantwoording over de invoering van de BIR.

DEEL II Voorbereiden van besluitvorming over de invoering van de BIR

1 Oriëntatie huidige situatie

In deze stap wordt aan de hand van een vragenlijst een typering van de ZBO bepaald. Deze typering is richtinggevend voor de vervolgstappen voor informatieveiligheid.

1.1 Organisatorische aandachtspunten

Organisatie en leiderschap	Is er een bestuurder die informatieveiligheid in portefeuille heeft? Is er een beveiligingsfunctionaris? Is er al een beveiligingsbeleid?
Personeel en cultuur	Ga na bij welke medewerkers nu taken m.b.t. informatieveiligheid zijn belegd (tactisch en operationeel). Is er een beeld van de manier en zorgvuldigheid waarmee medewerkers met informatie omgaan? Tijdens de oriëntatie is het nog niet direct noodzakelijk het personeel te informeren en te sturen op een beveiligingsbewuste cultuur. Wel kan inzet van personeel nodig zijn bij de positiebepaling. Houd ook rekening met inzet van medewerkers in het vervolgtraject.
Financiën	Ga na of er een apart budget voor informatieveiligheid op de begroting staat, of deel uitmaakt van andere begrotingsposten. Tijdens de oriëntatie is nog geen sprake van investeringen. De kosten kunnen het beste binnen de lopende begroting worden opgevangen. Houd rekening met benodigde middelen voor het vervolgtraject.
Management informatie	Ga na wat nu al wordt vastgelegd en gerapporteerd over informatieveiligheid. Leg alle besluitvorming vanaf de oriëntatie vast.

1.2 Hulpmiddel

Bepaal welk type ZBO het meeste overeenkomt met de eigen situatie. Onderstaand worden drie ‘archetypen’ genoemd. In de praktijk kan er sprake zijn van een combinatie van typen.

Type A

Eerste oriëntatie op BIR

- er is een beperkte mate van volwassenheid op het gebied van informatieveiligheid
- informatieveiligheid is niet per definitie een terugkerend thema aan de bestuurstafel
- risicoanalyse heeft nog niet plaatsgevonden
- eerste oriëntatie op de BIR of ISO27001
- vaak kleinere ZBO

Type B

Normenkader grotendeels ingevoerd

- informatieveiligheid staat nadrukkelijk op de bestuurlijke agenda
- beleid is risk based
- BIR, ISO27001 of een daarvan afgeleid normenkader is geheel of gedeeltelijk ingevoerd
- governance van informatieveiligheid is ingericht
- vaak middelgrote tot grote ZBO

Type C

BIR naast andere wet- en regelgeving

- een relatief grote mate van volwassenheid op het gebied van informatieveiligheid is al bereikt, waarbij men zich vaak extra bewust is vanwege andere specifieke wetgeving
- informatieveiligheid staat nadrukkelijk op de bestuurlijke agenda
- beleid is risk based
- governance van informatieveiligheid ingericht
- complexe, soms (inter-) nationale wet- en regelgeving op gebied van (informatie-) veiligheid
- BIR en/of ISO27001 is hierdoor niet altijd het leidende normenkader. Er is andere, vaak sectorspecifieke wetgeving
- vaak middelgrote tot grote ZBO

Ter verificatie van de oriëntatie op de huidige situatie kunnen ook onderstaande beschrijvingen worden gebruikt. In de praktijk kan het zo zijn dat de huidige situatie bij een ZBO een combinatie van de genoemde typen is of dat slechts delen van de typologie van toepassing zijn. Ga dan voor het vervolg uit van de typering die het dichtste licht bij de eigen situatie.

1.2.1 Eerste oriëntatie op BIR

Type A

Deze organisaties zijn in beperkte mate volwassen op het gebied van informatieveiligheid. Voor deze (vaak relatief kleine) ZBO is informatieveiligheid geen specifiek thema op de bestuurderstafel. Er wordt niet periodiek gerapporteerd over openstaande risico's en acties en de taken op het gebied van informatieveiligheid zijn vaak belegd bij functionarissen die dit uitvoeren naast hun eigen (lijn)verantwoordelijkheid.

Het onderwerp wordt belangrijk gevonden, maar risico's worden niet zeer hoog ingeschat en beveiligingsmaatregelen worden zoveel mogelijk getroffen op basis van common sense en niet op basis van een gestructureerde risico-analyse. Een eerste oriëntatie op de BIR of ISO27001 heeft mogelijk al wel plaatsgevonden.

In enkele gevallen wordt wel periodiek een audit uitgevoerd naar de meest basale (vaak technische) beveiligingsmaatregelen. De governance rond informatieveiligheid is beperkt ingericht.

1.2.2 Normenkader grotendeels ingevoerd

Type B

Voor deze (vaak grotere) ZBO staat informatieveiligheid al langere tijd nadrukkelijk op de agenda. Deze organisaties hebben al een behoorlijke mate van volwassenheid op het terrein van informatieveiligheid bereikt. De risico's worden ingeschat op grond van een gestructureerde risicoanalyse en de BIR. ISO27001 of een daarvan afgeleid normenkader is ingevoerd of verkeert in een (ver-)gevorderd stadium van invoering. Mogelijk is ook al sprake van een ISO-certificering. De governance is gedegen ingericht, met functionarissen en gremia voor informatieveiligheid, periodieke rapportages aan directie, etc. Voor de kritieke processen, informatiesystemen en/of diensten zijn eigenaren aangewezen en periodiek worden risicoanalyses uitgevoerd.

1.2.3 BIR naast andere wet- en regelgeving

Type C

ZBO wordt niet alleen geconfronteerd met generieke beveiligingseisen, maar heeft ook te maken met andere wet- en regelgeving waarin specifieke eisen zijn opgenomen. Vaak moet hier ook separaat verantwoording over plaats vinden. De BIR en/of ISO27001 wordt daarom door deze ZBO niet per definitie als het leidende normenkader voor informatieveiligheid gezien. Het is wel aannemelijk dat wel aan de beheersmaatregelen uit deze standaarden wordt voldaan. Deze organisaties zijn in een behoorlijke mate volwassen op het terrein van informatieveiligheid. Dit wordt mede veroorzaakt door andere, vaak sectorspecifieke wet- en regelgeving. Voor deze (vaak middelgrote tot grote) ZBO staat informatieveiligheid nadrukkelijk op de bestuursagenda. De risico's structureel geanalyseerd en is er vaak een governancestructuur ingericht op het gebied van informatieveiligheid.

2 Ambitie

In deze stap wordt een uitwerking gegeven van de activiteiten voor het bepalen van het ambitieniveau dat de ZBO nastreeft met de verbetering van de informatiebeveiliging. Daarbij wordt nagegaan welke meerwaarde de invoering van de BIR heeft ten opzichte van de huidige situatie.

2.1 Organisatorische aandachtspunten

Organisatie en leiderschap	Bij het bepalen van de ambitie is de rol van de bestuurder essentieel. Hier worden namelijk de doelstellingen bepaald voor informatieveiligheid. Deze moeten naadloos aansluiten op de missie en strategie van de ZBO.
Personeel en cultuur	Bepaal de consequenties van het gekozen ambitieniveau voor personeel en organisatiecultuur, alsook hoe zich dat verhoudt tot de bestaande cultuur. Maak, indien nodig, een begin met het vergroten van het bewustzijn.
Financiën	Er dient rekening gehouden te worden met het feit dat het een langdurig traject is waar veel mensuren in gaan zitten, vooral de invoering van de BIR. De implementatie van de BIR zal in de projectbegroting moeten worden opgenomen. Bovendien is de het beheer en onderhoud van de BIR binnen de organisatie geen eenmalige exercitie. Houdt daarom rekening met structurele inzet van mensen en middelen.
Managementinformatie	Alle overwegingen die een rol hebben gespeeld tijdens het bepalen van de ambitie, moeten worden gedocumenteerd. Dit is belangrijk ter verantwoording van alle vervolginitiatieven op het gebied van informatieveiligheid.

2.2 Hulpmiddel

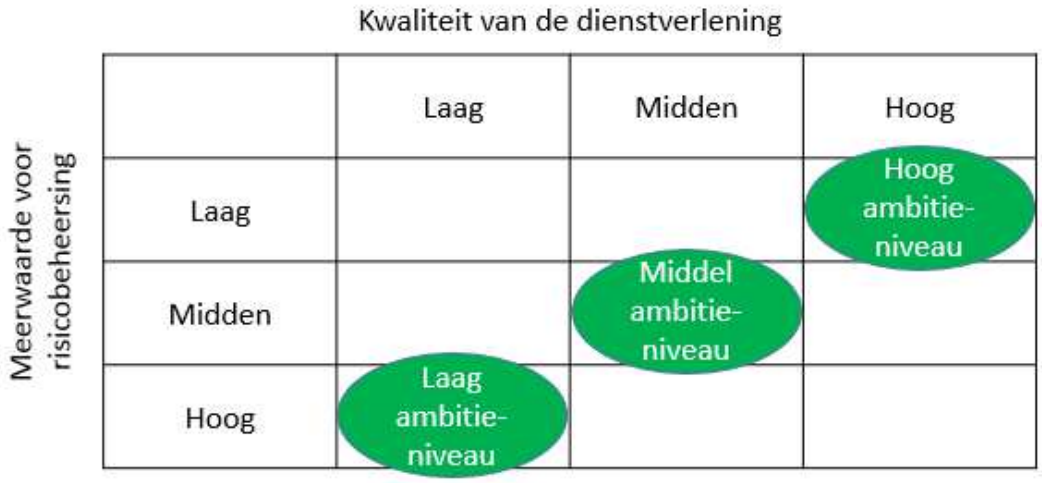
De ambities van de organisatie op het gebied van informatieveiligheid worden ingegeven door de verwachte meerwaarde voor de organisatie ten aanzien van de dienstverlening en

de risicobeheersing (de mate waarin risico's beheerst kunnen worden). Onderstaande checklist is hierbij een hulpmiddel.

Onderwerp	Overwegingen
Meerwaarde van de BIR voor de kwaliteit van de dienstverlening van de ZBO	→ ***laag*** *–De ZBO verwerkt vrijwel geen vertrouwelijke informatie. Burgers, bedrijven en instellingen stellen geen of nauwelijks eisen op het gebied van informatiebeveiliging. De invoering van de BIR kan bijdragen aan de continuïteit van de dienstverlening, maar levert nauwelijks meerwaarde op voor de efficiency van de organisatie.* → ***midden*** *– Burgers, bedrijven en instellingen stellen eisen aan de betrouwbaarheid van de dienstverlening. De BIR kan meerwaarde opleveren voor het vertrouwen in de dienstverlening van de ZBO.* → ***hoog*** *– De ZBO vervult bijvoorbeeld een belangrijke rol in één van de (vitale) infrastructuren. Burgers, bedrijven en instellingen stellen hoge eisen aan de kwaliteit van de dienstverlening. De BIR, eventueel naast andere wet- en regelgeving, draagt direct bij aan het vergroten van het vertrouwen in dienstverlening van de ZBO.*
Veronderstelde risico's in de eigen bedrijfsvoering op het gebied van informatieveiligheid en de meerwaarde voor de risicobeheersing	→ ***laag*** *– Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van de informatieverwerking zijn niet cruciaal voor de uitvoering van de primaire taak; het (volledig) invoeren van de BIR lijkt een zwaar middel gezien de beperkte risico's.* → ***midden*** *– Bij de primaire processen, maar ook de ondersteunende processen (bijvoorbeeld de afscherming van personeelsgegevens) speelt BIV een belangrijke rol. Toepassen van de BIR kan noodzakelijk zijn om de exacte risico's op het gebied van informatieveiligheid beter te kunnen achterhalen en te beheersen.* → ***hoog*** *– De beveiliging van de informatievoorziening is cruciaal voor het imago en het uitoefenen van de primaire taak van de ZBO en heeft een groot afbreukrisico. Aan BIV worden meer dan gebruikelijke eisen gesteld. Het invoeren van een evenwichtige standaard, zoals de BIR heeft absoluut meerwaarde voor de algehele informatieveiligheid binnen de ZBO en daarmee aan het mitigeren en van risico's.*

De scores op bovenstaande vragen kunnen geplot worden op een matrix. Daarmee kan gevisualiseerd worden welke meerwaarde de ZBO verwacht van invoering van de BIR en in welke mate dat bijdraagt aan het ambitieniveau van de organisatie op het gebied van informatieveiligheid.

Vanzelfsprekend zijn afwijkende scores mogelijk, het is een benadering. In dat geval is het belangrijk vast te stellen welk belang het zwaarste telt voor de ZBO. In de praktijk blijkt vaak het belang van de externe dienstverlening vaak doorslaggevend te zijn voor het bepalen van het ambitieniveau.



De uiteindelijke score op deze tabel is een belangrijke input voor de bestuurlijke afweging over de invoering van de BIR.

3 Bestuurlijke afweging

Nu het beeld van de huidige situatie en het ambitieniveau van de ZBO bekend zijn, kan worden bepaald welke invoeringsstrategie het beste past bij de eigen organisatie. Het belangrijkste criterium daarbij is de afweging tussen de verwachte meerwaarde van de invoering van de BIR en de benodigde inspanning en in te vullen randvoorwaarden. Onderstaande tabel is een leidraad bij de afweging, maar andere keuzes zijn natuurlijk denkbaar.

Ambitieniveau

Type ZBO's	Laag	Midden	Hoog
A	FIT/GAP	FIT/GAP	BIR
B	FIT/GAP	BIR	BIR
C	FIT/GAP + Aanvullende norm	BIR + Aanvullende norm	BIR + Aanvullende norm

BIR:
Op basis van een risicoafweging van de kritieke processen in de organisatie wordt bepaald of de organisatie de BIR volledig wil invoeren. Het is denkbaar dat onderdelen van de BIR niet, of niet in die mate, van toepassing zijn op de organisatie. Hier kan beargumenteerd worden afgeweken van de BIR met een zogeheten 'explain.' Het hebben van een aantal 'explains' wil niet zeggen dat de ZBO niet 'in control' is, maar dat gemotiveerd op basis van een risicoafweging wordt afgeweken van de BIR, de risico's daarvan bekend zijn en worden geaccepteerd, dan wel dat daarvoor een verbetertraject wordt ingezet.

FIT/GAP:
Er zijn echter situaties denkbaar, bijvoorbeeld voor heel kleine organisaties waar de BIR niet past als normenkader of waar een normenkader op zichzelf al te veel is. In dit geval is het raadzaam om voor de kritieke processen een zogenaamde 'fit-gap'-analyse uit te voeren, zodat de organisatie inzicht heeft in waar het staat ten opzichte van de BIR en welke onderdelen van de BIR wel bruikbaar zijn.

+ Aanvullende norm:
Wanneer ZBO's gehouden zijn aan aanvullende (inter-)nationale wet- en regelgeving zullen zij aanvullende maatregelen doorvoeren bovenop de BIR of bovenop de onderdelen van de BIR die voor hen bruikbaar zijn.

In deze stap wordt bepaald welk invoeringstraject het beste kan worden gevolgd, gegeven de analyse van de huidige situatie en het ambitieniveau van de organisatie. Daarbij gelden in grote lijnen dezelfde organisatorische aandachtspunten als bij het bepalen van de ambitie.

3.1 Organisatorische aandachtspunten

Organisatie en leiderschap	Bij afweging van het invoeringstraject is de rol van de bestuurder essentieel. Hier worden namelijk bepaald wat haalbaar is voor de organisatie en wat niet. Deze keuze is bepalend voor de uit te voeren activiteiten.
Personeel en cultuur	In deze fase zal ook gekeken moeten worden in hoeverre er

	ingezet moet worden op organisatieleren. Indien er nog niets op dit vlak gedaan wordt, kan het raadzaam zijn een apart traject over bewustzijn op te zetten. Ook kan bekeken worden of bepaalde medewerkers specifieke training op het gebied van informatiebeveiliging en BIR moeten volgen.
Financiën	Tijdens de afweging van het invoeringstraject wordt een inschatting gemaakt van de benodigde projectkosten en de benodigde investeringen. Hierbij dient er rekening mee gehouden te worden de invoering van de BIR een langdurig traject kan zijn waar veel mensuren in gaan zitten. Bovendien is de invoering van de BIR geen eenmalige exercitie, het beheersysteem dat er voor moet zorgen dat in continuïteit aan de BIR wordt voldaan, vraagt inspanning van de hele organisatie. De hoogte voor het invoeringstraject en het structurele budget moet bestuurlijk worden afgestemd.
Management informatie	Alle overwegingen die een rol hebben gespeeld tijdens de afweging van het invoeringstraject moeten worden gedocumenteerd. Hierbij wordt de afweging gemaakt of alle onderdelen van de BIR volledig ingevoerd worden (waarbij beargumenteerd van bepaalde onderdelen van de BIR, die niet, of niet in die mate van toepassing zijn op de ZBO, kan worden afgeweken middels een 'explain') of dat een zogenaamde FIT/GAP-analyse wordt uitgevoerd. Dit is belangrijk ter verantwoording van alle vervolg initiatieven op het gebied van informatieveiligheid.

3.2 Hulpmiddel

De onderwerpen in onderstaande checklist kunnen dienen als leidraad in de bestuurlijke afweging over hoe het invoeringstraject er uit zou moeten zien. De focus ligt daarbij op een inschatting van de benodigde inspanningen om het beoogde ambitieniveau te bereiken. De lijst is zeker niet uitputtend en bepalend. De genoemde onderwerpen moeten meer gezien worden als 'punten ter overweging'.

Onderwerp	Overwegingen
Beschikbaar personeel voor informatieveiligheid	→ ***BIR*** *– invoering van de BIR vraagt enerzijds om een projectteam dat belast is met de invoering van de BIR, anderzijds moeten er structureel rollen en verantwoordelijkheden worden belegd over het beheer en onderhoud van de BIR.*

	→ ***FIT/GAP*** *– de analyse kan in eerste instantie worden uitgevoerd onder leiding van de beveiligingsfunctionaris/CISO. Afhankelijk van de uitkomsten van de FIT/GAP-analyse kan er besloten de BIR alsnog volledig in te voeren of slechts delen van de BIR als dat beter bij de organisatie past. Die uitkomsten zijn bepalend voor de inzet van personeel voor het vervolg. Is er alsnog een projectorganisatie nodig voor de invoering van (onderdelen van) de BIR en zijn de rollen en verantwoordelijkheden goed belegd?* → ***+ Aanvullende norm*** *– in een aantal gevallen zijn ZBO's gehouden aan aanvullende regels op grond van taakspecifieke (inter-) nationale wet- en regelgeving. Daar kunnen aanvullende maatregelen uit voort komen (vaak zwaarder dan de BIR). In het overgrote deel van de gevallen voldoet de organisatie al aan de deze regels en zijn de maatregelen al ingevoerd. Dit zou ook betekenen dat de rollen en verantwoordelijkheden hieromtrent zijn belegd. Zo niet, dan zal dit alsnog moeten gebeuren.*
Beschikbare financiën / budgetten	→ ***BIR*** *– invoering van de BIR brengt minimaal de projectkosten met zich mee. Daarnaast bepaalt een risicoanalyse welke investeringen minimaal nodig zijn.* → ***FIT/GAP*** *- een impact-/dreigingenanalyse kan helpen om te bepalen welke investeringen gerechtvaardigd zijn in relatie tot de totale bedrijfskosten.* → ***+ Aanvullende norm*** *- in deze situatie bestaat vermoedelijk al een belangrijk fundament om invoering en onderhoud van de BIR mogelijk te maken.*
Belang van informatieveiligheid voor (keten)partners	→ ***BIR*** *– Invoering van de BIR kan onduidelijkheden wegnemen over de vraag van (keten)partners hoe informatieveiligheid binnen de ZBO is ingericht. Het maken van afspraken met ketenpartners zou bovendien onderdeel van de invoering moeten zijn.* → ***FIT/GAP*** *– Het is van groot belang om expliciet aandacht aan afspraken met ketenpartners over informatieveiligheid te besteden* → ***+ Aanvullende norm*** *– Indien de aanvullende norm geen specifieke aandacht besteedt aan afspraken met ketenpartners over informatieveiligheid is de BIR bij uitstek een*

	instrument om dit op te pakken. Invoering van de BIR kan onduidelijkheden wegnemen over de vraag van (keten-) partners hoe informatieveiligheid binnen de ZBO is ingericht.
Afspraken met het departement over invoering van de BIR	→ ***BIR*** *- invoering van de BIR kan worden gepland naast of na de andere initiatieven. Afspraken met het departement kunnen onderdeel zijn van de sturingsafspraken en kunnen helderheid verschaffen over de eisen waaraan de ZBO moet voldoen. Dit is echter geen bindende voorwaarde.* → ***FIT/GAP*** *– Afspraken met het departement kunnen onderdeel zijn van de sturingsafspraken en verschaffen helderheid over de eisen waaraan de ZBO moet voldoen. Dit is echter geen bindende voorwaarde. Afhankelijk van de resultaten van de FIT/GAP kunnen deze afspraken alsnog gemaakt worden.* → ***+ Aanvullende norm*** *– Afspraken met het departement kunnen onderdeel zijn van de sturingsafspraken en verschaffen helderheid over de eisen waaraan de ZBO moet voldoen. Dit is echter geen bindende voorwaarde.*
Huidig volwassenheidsniveau van informatieveiligheid	→ ***BIR*** *– invoering van de BIR kan helpen op een evenwichtige wijze de volwassenheid van de van belang zijnde onderdelen en bedrijfsmiddelen te verhogen.* → ***FIT/GAP*** *– De FIT/GAP-analyse geeft inzicht in de mate van volwassenheid op gebied van informatieveiligheid. Afhankelijk van de resultaten kan bepaald worden welke onderdelen van de BIR ingevoerd zouden moeten worden om het volwassenheidsniveau te verhogen. Dit zou bijvoorbeeld tot de beslissing om kunnen leiden om de huidige maatregelen uit te breiden met de specifieke rijksoverheid (R) normen uit de BIR.* → ***+ Aanvullende norm*** *– Afhankelijk van de specifieke eisen die de aanvullende normen stellen zou bepaald kunnen worden welke onderdelen van de BIR ingevoerd zouden moeten worden om het volwassenheidsniveau te verhogen. Dit zou bijvoorbeeld tot de beslissing kunnen leiden om de huidige maatregelen uit te breiden met de specifieke rijksoverheid (R) normen uit de BIR.*

Verschil in volwassenheid op informatieveiligheid voor wat betreft primaire processen versus ondersteunende processen, zoals personeelszaken, inkoop, huisvesting, etc.	→***BIR*** *- de verantwoordelijkheid voor informatieveiligheid reikt verder dan alleen de primaire processen die de dienstverlening van de ZBO ondersteunen. Zeker ten aanzien van het personeel is het van belang te voldoen aan de Wbp vereisten. De BIR kan hierbij helpen dit aantoonbaar te organiseren.* → ***FIT/GAP*** *– De FIT/GAP biedt inzicht in de mate waarin de primaire en ondersteunende processen zijn meegenomen. Afhankelijk van de resultaten kan besloten worden onderdelen van de BIR in toe voeren.* → ***+ Aanvullende norm*** *– aanvullende normen hebben vaak juist betrekking op de primaire processen. Echter, de verantwoordelijkheid voor informatieveiligheid reikt verder dan primaire processen. Zeker ten aanzien van het personeel is het van belang te voldoen aan de Wbp vereisten. Aanvullende BIR-maatregelen zouden kunnen helpen dit aantoonbaar te organiseren.*
Wet- en regelgeving (gerelateerd aan informatieveiligheid)	→ ***BIR*** *– de BIR kan helpen bij het leggen van een relatie met de artikelen uit de relevante wet- en regelgeving (bijvoorbeeld Wet bescherming persoonsgegevens).* → ***FIT/GAP*** *– Afhankelijk van de resultaten.* → ***+ Aanvullende norm*** *– Indien er gekozen wordt om de geldende aanvullende norm met (onderdelen van) de BIR. BIR compliance aantonen is in dit geval slechts een (beperkt) onderdeel van het verantwoordingsproces.*

4 Realisatie

In deze stap wordt inzicht gegeven in de logischerwijs te ondernemen activiteiten, om invulling te geven aan de invoeringstrajecten voor de BIR. Deze activiteiten hebben betrekking op:

1. De BIR volledig invoeren.

Of

2. Het uitvoeren FIT/GAP-analyse en de al zelf getroffen ad hoc maatregelen op het gebied van informatieveiligheid aanvullen met de relevante onderdelen van de BIR.

Of

3. De al geldende normen op basis van taakspecifieke wet- en regelgeving voor het primaire proces aanvullen met de relevante onderdelen van de BIR (op basis van een FIT/GAP analyse).

4.1 BIR volledig invoeren

Indien het besluit is genomen om de BIR in zijn geheel in te voeren, is het van belang dat de juiste randvoorwaarden worden gecreëerd. Deze randvoorwaarden vormen het fundament onder het implementatietraject. Als daar te weinig aandacht aan wordt besteed, is de kans aannemelijk dat alle inspanningen op langere termijn niet effectief blijken te zijn.

4.1.1 Organisatorische aandachtspunten

Organisatie en leiderschap	• Leg de verantwoordelijkheden van bestuur, directie, CISO (of vergelijkbaar) en lijnmanagers vast. • Het lijnmanagement is resultaatverantwoordelijk voor de invoering van de BIR (1e lijns verantwoordelijkheid). • Wordt er gestuurd op afspraken vanuit de Kaderwet ZBO's en in het bijzonder op informatiebeveiliging (art. 41), indien de kaderwet van toepassing is? Zijn er andere (wettelijke) verplichtingen waar de organisatie zich aan moet houden? • Breng een prioritering aan. Hebt u in beeld wat de kritieke processen zijn? • Voer een stakeholderanalyse uit, betrek stakeholders vanaf het begin en zorg voor hun commitment. • Voer een GAP-analyse uit om het verschil tussen de huidige situatie en de ambitie in kaart te brengen. • Betrokkenheid van de top is zeer belangrijk. De bestuurder benadrukt het belang van informatieveiligheid voor de kwaliteit van de dienstverlening (vertrouwen van burgers en bedrijven) en heeft een voorbeeldfunctie in het vertonen van het juiste gedrag. • Zorg voor borging in de P&C-cyclus
Personeel en cultuur	• Zorg voor voldoende deskundigheid op het gebied van informatieveiligheid en de BIR, om het invoeringstraject te begeleiden en het lijnmanagement te ondersteunen. • Besteed aandacht aan bewustwording en gedrag bij medewerkers
Financiën	• Informatieveiligheid is onderdeel van interne beheersing. De structurele kosten (uren) die samenhangen met het treffen van maatregelen kunnen daarom ten laste worden gelegd van de lijnorganisatie of het reguliere ICT-budget. Het gaat er niet zozeer om waar deze kosten worden belegd, als er maar een rekening

	gehouden wordt met een structurele post. • De implementatie van de BIR kan worden opgenomen in de projectenbegroting.
Management informatie	• Leg de verantwoordelijkheden van bestuur, directie, CISO en lijnmanagers formeel vast. • Stel het informatiebeveiligingsbeleid formeel vast. • Stel het informatiebeveiligingsplan formeel vast.

4.1.2 Hulpmiddel

Tip	*Op informatieveiligheid.pleio.nl en op cip.pleio.nl is een uitgebreid aantal instrumenten beschikbaar, die implementatie van de BIR ondersteunen.*

4.2 Uitvoeren FIT/GAP-analyse en de al getroffen maatregelen, op het gebied van informatieveiligheid, aanvullen met de relevante onderdelen van de BIR

Een besluit om een FIT/GAP-analyse op de BIR uit te voeren, laat onverlet dat er wel zicht moet zijn op de risico's in de bedrijfsvoering van de ZBO, waarbij minimaal de grootste risico's zijn afgedekt.

4.2.1 Organisatorische aandachtspunten

Organisatie en leiderschap	• Het lijnmanagement is resultaatverantwoordelijk voor de invoering van de BIR (1e lijnsverantwoordelijkheid). • Wordt er gestuurd op afspraken vanuit de Kaderwet ZBO's en in het bijzonder op informatiebeveiliging (art. 41), indien de kaderwet van toepassing is. Zijn er andere (wettelijke) verplichtingen waar de organisatie zich aan moet houden? • Breng een prioritering aan. Hebt u in beeld wat de kritieke processen zijn? • Voer een stakeholderanalyse uit, betrek stakeholders vanaf het begin en zorg voor hun commitment. • Betrokkenheid van de top is zeer belangrijk. De bestuurder benadrukt het belang van informatieveiligheid voor de kwaliteit van de dienstverlening (vertrouwen van burgers en bedrijven) en heeft een voorbeeldfunctie in het vertonen van het juiste gedrag. • Zorg voor borging in de P&C-cyclus
Personeel en cultuur	• Zorg voor voldoende deskundigheid op het gebied van informatieveiligheid en de BIR om de FIT/GAP analyse te begeleiden en het lijnmanagement te ondersteunen. • Besteed aandacht aan bewustwording en gedrag bij medewerkers
Financiën	• Het treffen of aanscherpen van de noodzakelijke maatregelen kan investeringen met zich meebrengen.

	• Per maatregel kan een kosten/baten-afweging worden gemaakt.
Management informatie	• Zorg voor een periodieke rapportage over de status van informatieveiligheid binnen de ZBO en bespreek deze rapportage tijdens de bestuursvergaderingen. • Leg de resultaten en besluiten vast.

4.2.2 Hulpmiddel

Indien de BIR niet volledig wordt doorgevoerd, is het minimaal van belang om onderstaande activiteiten uit te voeren:

1. Bepaal de kritieke processen en voer een risicoanalyse uit op het gebied van informatieveiligheid. Deze analyse kan helpen accenten te leggen bij het verbeteren van de informatieveiligheid binnen de ZBO en richting te geven aan het realiseren van de ambitie.
2. Nadat de risicoanalyse is uitgevoerd, is het van belang om tenminste de basis op orde te brengen. Bij het prioriteren van de maatregelen kan vanuit pragmatiek gekozen worden voor quickwins of voor maatregelen die aansluiten bij actuele speerpunten, om zo snel de eerste resultaten te behalen.

Tip	*De risico analyse kan worden uitgebreid met (of onderdeel zijn van) een strategisch risk assessment, waarmee ook andere risico's worden onderzocht.*
	Gebruik de 'Quick scan BIR'. Deze is onder andere te vinden op informatieveiligheid.pleio.nl.

Tip	*Bij 'de basis op orde' kan worden gedacht aan beveiligingsmaatregelen op het gebied van:* *1. Beveiligingsincidenten (misbruik, diefstal, fraude, etc.)* *2. Toegang tot systemen, informatie, gebouwen, etc.* *3. Back-up van systemen en gegevens* *4. Wijzigingsbeheer van belangrijke bedrijfsmiddelen* *5. Netwerkbeveiliging (anti virus, hackers, etc.)* *6. Uitbestede dienstverlening (derde partijen)* *7. Screening en training van personeel (security awareness)*

4.3 De al geldende normen op basis van taakspecifieke wet- en regelgeving aanvullen met de BIR of een FIT/GAP uitvoeren en de geldende kaders aanvullen met de relevante onderdelen van de BIR.

Het is van belang dat de BIR-maatregelen aansluiten op de eisen die vanuit andere wet- en regelgeving worden gesteld. De nadruk ligt hier op het aanvullen van de al gehanteerde normen en maatregelen met die elementen uit de BIR die daadwerkelijk toegevoegde waarde hebben. Veelal zullen dit de normen zijn die betrekking hebben op de aanvullende eisen uit VIR of VIRBI en aanvullende bepalingen voor de Rijksdienst (de (R) normen).

4.3.1 Organisatorische aandachtspunten

Organisatie en leiderschap	• Het lijnmanagement is resultaatverantwoordelijk voor de invoering van de BIR (1e lijnsverantwoordelijkheid). • Er is inzicht nodig welk beleid er nu is ten aanzien van informatieveiligheid. • Wordt er gestuurd op afspraken vanuit de Kaderwet ZBO's en in het bijzonder op informatiebeveiliging (art. 41), indien de kaderwet van toepassing is. Zijn er andere (wettelijke) verplichtingen waar de organisatie zich aan moet houden en hoe verhouden deze zich tot de BIR? • Waar hebben de BIR normen meerwaarde ten opzichte van sectorspecifieke regelgeving? • Breng een prioritering aan. Hebt u in beeld wat de kritieke processen zijn? • Voer een stakeholderanalyse uit, betrek stakeholders vanaf het begin en zorg voor hun commitment. • Betrokkenheid van de top is zeer belangrijk. De bestuurder benadrukt het belang van informatieveiligheid voor de kwaliteit van de dienstverlening (vertrouwen van burgers en bedrijven) en heeft een voorbeeldfunctie in het vertonen van het juiste gedrag. • Zorg voor borging in de P&C-cyclus
Personeel en cultuur	• Zorg voor voldoende deskundigheid op het gebied van informatieveiligheid en de BIR om de FIT/GAP analyse te begeleiden en het lijnmanagement te ondersteunen. • Besteed aandacht aan bewustwording en gedrag bij medewerkers
Financiën	• Het treffen of aanscherpen van de noodzakelijke maatregelen kan investeringen met zich meebrengen. • Per maatregel kan een kosten / baten afweging worden gemaakt.
Management informatie	• Zorg voor een periodieke rapportage over de status van informatieveiligheid binnen de ZBO en bespreek deze rapportage tijdens de bestuursvergaderingen. • Zorg dat de relatie tussen de sectorspecifieke normen en regels en de BIR helder gedocumenteerd is en dat onderbouwd is waarom bepaalde keuzes zijn gemaakt. • Leg de resultaten en besluiten vast.

4.3.2 Hulpmiddel

Tip	Het is belangrijk dat de regels voor informatieveiligheid en de BIR niet los staan van de andere wettelijke en niet-wettelijke regels die gelden voor de ZBO. Door de regels voor informatieveiligheid en de BIR te koppelen aan de overige regels, kunnen zij elkaar versterken. Zorg dat de relatie helder is.

4.4 Transparantie en verantwoording

Transparantie en verantwoording zijn een belangrijke thema's bij het vergroten van de informatieveiligheid. Transparantie over de stappen die gezet worden en over de mate waarin een ZBO 'in control' is, kunnen het vertrouwen bij ketenpartners, burgers, bedrijven en instellingen vergroten. Verantwoording richting het departement kan van belang zijn, omdat hiermee invulling wordt gegeven aan de Kaderwet of aanvullende sturings- en verantwoordingsafspraken.

Het jaarverslag is de centrale plaats voor het zichtbaar maken van het standpunt van het bestuur over informatieveiligheid en het naleven van de BIR richting de belanghebbenden. In het jaarverslag kan het bestuur zijn 'in control' statement afgeven. De kern van een 'in control' statement is de uitspraak van het bestuur over op welke wijze de informatieveiligheid wordt beheerst en welke standaarden de ZBO daarbij volgt, dan wel daarvan gemotiveerd afwijkt ('comply or explain'). Deze kan worden aangevuld met bevindingen van een accountant over de implementatie van specifieke maatregelen of de resultaten van een audit.

Tip	Onderstaande in control verklaring kan worden gebruikt: Het management van ……. bevestigt dat: - De organisatie een informatiebeveiligingsbeleid voert dat gericht is op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens, de bescherming van organisatie-informatie en de beheersbaarheid en controleerbaarheid van de processen van informatieverwerking, conform de overheidsnormen voor informatiebeveiliging, zoals samengevat in de [geldende baseline]. Het bestuur heeft het beleid vastgesteld. - De organisatie inzicht heeft in de wijze waarop de verantwoordelijkheden voor informatieveiligheid zijn belegd op bestuursniveau, lijnverantwoordelijkheden, ondersteunende en adviserende verantwoordelijkheden en een onafhankelijke controle. - Elk organisatieonderdeel haar processen definieert in samenhang met processen van andere organisatieonderdelen in de keten, conform het bestuurlijk procesmodel. Voor elk organisatieproces is vastgesteld welke (informatie)middelen kritiek zijn voor het functioneren van dit proces. - De eigenaren van informatie, processen, informatiesystemen/applicaties en infrastructuur zijn vastgesteld. - Er zijn op kritieke informatiestromen en/of middelen formele en gedocumenteerde risicoanalyses uitgevoerd om de beveiligingsmaatregelen te bepalen, waar meer nodig is dan de [geldende baseline] voorschrijft. - Informatiesystemen worden beschermd overeenkomstig de informatie die zij opslaan en verwerken. De beveiligingsmaatregelen zijn zodanig geselecteerd dat een adequaat niveau van informatieveiligheid wordt verkregen. Het bestuur heeft gefundeerd vastgesteld welke risico's acceptabel en niet acceptabel zijn. - Er is een informatieveiligheidsplan vastgesteld met de resultaten van de stappen van de risicoanalyse en de fasering en aanpak om tot implementatie te komen, ten behoeve van een cyclische verankering van het informatieveiligheidsproces. Daar waar wordt afgeweken van het vastgestelde beleid cq. de baseline wordt dit gemotiveerd vastgelegd (comply or explain). - Maatregelen voor beveiligen van informatie, conform de baseline, zijn op een dusdanige wijze zijn ingevoerd dat de goede werking van deze maatregelen effectief en efficiënt kan worden gecontroleerd door het management en onafhankelijke partij(en). - Er is een adequaat proces ingericht voor het identificeren en bestrijden van incidenten en crises, om de weerbaarheid van de organisatie op het gewenste niveau te kunnen houden. - Het functioneren van het proces van informatieveiligheid wordt beoordeeld en gerapporteerd aan het management aan de hand van KPI's.

	- Informatiebeveiliging beschouwd wordt als een continu verbeterproces. Dit geldt niet alleen voor het management systeem van informatiebeveiliging, maar voor de gehele organisatie. Alle medewerkers van de organisatie worden getraind in het gebruik van beveiligingsprocedures.