QuickScan BIR

Versie 1.0

21-01-2014

Inhoud

Inhoud **2**
Inleiding **3**
Doelstelling QuickScan BIR 4
Stappenplan QuickScan BIR 4
Uitvoering QuickScan BIR 4
Stap 1: Bepalen scope **5**
Scope bepalen 5
Detailbeschrijving processen en systemen 6
Dreigingsprofiel 6
Personele inzet 7
Stap 2: BIV Beveiligingsniveau bepalen **8**
1. Valideren Scope QuickScan BIR 8
2. Classificatie van het proces 8
3. Inventarisatie en classificatie van de informatiesystemen 10
4. Betrouwbaarheidseisen die aan het proces met ondersteunende systemen worden gesteld 11
Beschikbaarheid van het proces of ondersteunende systemen: 11
Integriteit van het proces met ondersteunende systemen: 13
Vertrouwelijkheid van het proces met ondersteunende systemen: 15
Stap 3: Dreigingsprofiel bepalen **17**
Dreigingen BIR 18
Stap 4: Rapportage vaststellen resultaten workshop **19**
Conclusie 20
Bijlage 1: Totstandkoming Quickscan BIR **22**
De totstandkoming van de Quickscan BIR 22
Het beveiligingsniveau van de BIR is in dit instrument als volgt aan de Quick Scan gelieerd: 22
De gevoeligheid van de informatie 22
De classificatie van processen & systemen: 22
De betrouwbaarheidseisen BIV: 22
Dreigingsprofiel: 23
Hoe om te gaan met comply & explain en de uitkomsten van een uitgevoerde quickscan 23
Op welke wijze kan het instrument geschikt gemaakt worden voor gebruik bij andere overheden? 23
Bijlage 2: Handleiding QS-BIR **24**
Inleiding 24
Voorbereiding 24
Inventariseren benodigde informatie voor scoping 24
Selectie deelnemers QS-BIR workshop 24
Uitnodigen deelnemers QS-BIR workshop 25
De workshop QS-BIR 26
QS-BIR workshop 27

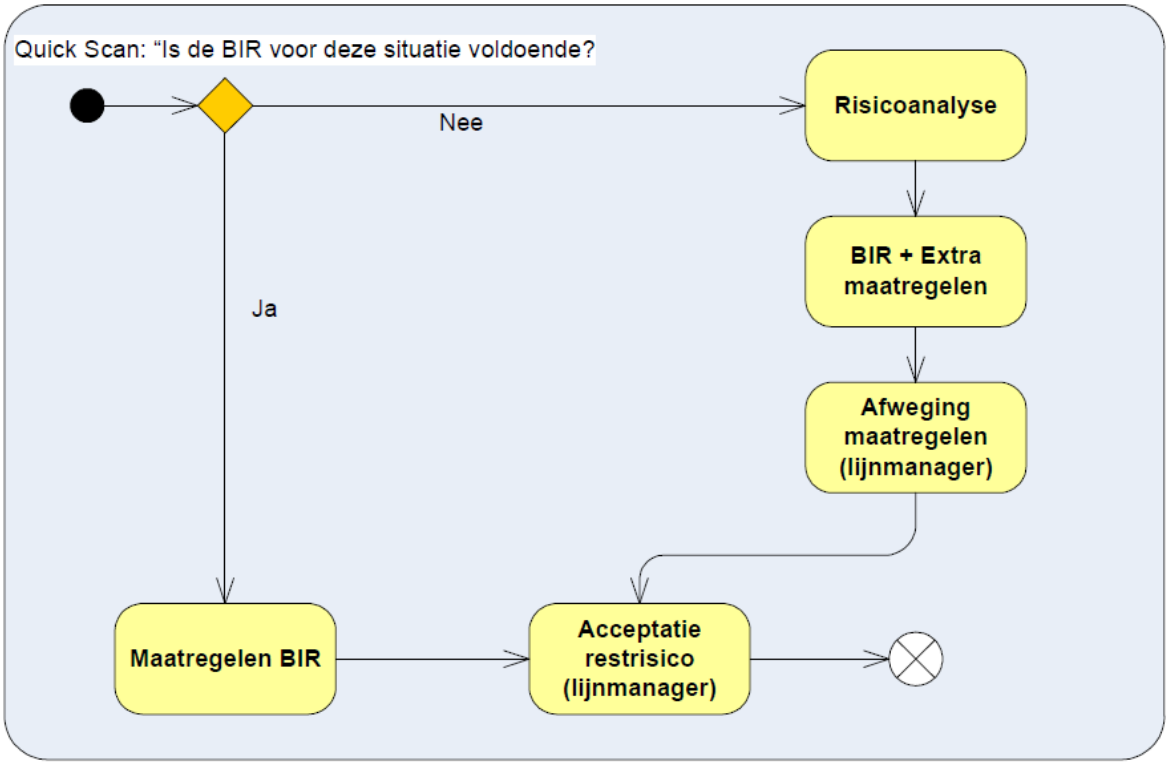
Inleiding

Binnen de overheid geldt het Voorschrift informatiebeveiliging rijksdienst (VIR) als methodische aanpak van informatiebeveiliging. De Baseline Informatiebeveiliging Rijksdienst (BIR) is een uitwerking van een deel van het VIR, wat tevens de basis is voor de uiteindelijke implementatie van het VIR. De BIR beschrijft het minimale beveiligingsniveau waaraan elk systeem binnen de rijksoverheid moet voldoen. Voor elk informatiesysteem moeten dus minimaal de beveiligingsmaatregelen uit de BIR geïmplementeerd worden.

Voor sommige systemen is het beveiligingsniveau van de BIR niet voldoende omdat het proces met ondersteunende systemen hogere eisen stellen zodat er zwaardere beveiligingsmaatregelen getroffen moeten worden. Om dit te achterhalen wordt een tweetal instrumenten gebruikt:

QuickScan BIR
Om te achterhalen of voor een proces met ondersteunende systemen zwaardere beveiligingsmaatregelen noodzakelijk zijn dan de BIR voorschrijft is het instrument “QuickScan BIR” ontwikkeld. Wanneer uit de QuickScan BIR naar voren komt dat de BIR maatregelen voldoende zijn is hiermee de analyse afgerond en dienen de maatregelen van de BIR ingevoerd te worden.

Risicoanalyse
Indien blijkt dat de beveiligingseisen van het proces met ondersteunende systemen hoger liggen dan de BIR, dan zal een vervolgonderzoek plaatsvinden (een risicoanalyse) om te bepalen in welke mate dit het geval is en welke extra aanbevelingen/maatregelen van toepassing zijn.



Doelstelling QuickScan BIR

De QuickScan BIR is bedoeld als instrument om te bepalen of de risico's voor een proces met ondersteunende systemen voldoende door de BIR worden afgedekt. Als dit niet het geval is dan moet met een aanvullende risicoanalyse vastgesteld worden welke extra beveiligingsmaatregelen nodig zijn. Deze aanvullende risicoanalyse maakt geen onderdeel uit van de QuickScan BIR.

Stappenplan QuickScan BIR

In de QuickScan BIR wordt in vier stappen een globale analyse gemaakt van de betrouwbaarheidseisen die worden gesteld aan een proces met ondersteunende informatiesysteem(en) om vervolgens een keuze te maken tussen de maatregelen uit de Baseline of het uitvoeren van een risicoanalyse.

Bij het bepalen van de betrouwbaarheidseisen wordt per proces met ondersteunende systeem(en) in kaart gebracht aan welke mate van betrouwbaarheid het systeem moet voldoen. Dit gebeurt op grond van de beveiligingskenmerken **B**(eschikbaarheid), **I**(ntegriteit) en **V**(ertrouwelijkheid).
De QuickScan BIR bestaat uit een viertal stappen:

Stap 1: Bepalen scope QuickScan BIR en selecteren te betrekken personen
Stap 2: BIV beveiligingsniveau bepalen
Stap 3: Dreigingsprofiel bepalen
Stap 4: Rapportage

Uitvoering QuickScan BIR

De QuickScan BIR wordt in workshopverband uitgevoerd (gemiddeld 2 uur). Voorafgaand aan de workshop zal de workshopbegeleider de scope (welk proces, systeem(en)) met de opdrachtgever afstemmen zodat deze tijdens de workshop enkel gevalideerd hoeft te worden. De workshop wordt uitgevoerd met de eigenaar(en) van het proces / system(en) en een aantal representatieve gebruikers van het system(en). Tijdens de workshop (stap 2 en stap 3) wordt bepaald in welke mate men afhankelijk is van het proces & ondersteunende systeem of de groep van systemen en welk dreigingsprofiel er is. Op basis van deze analyse wordt het vereiste beveiligingsniveau bepaald.

Het resultaat van de QuickScan BIR wordt verwoord in een rapportage. Deze wordt vooraf afgestemd met de opdrachtgever, die met vaststelling van het rapport ook het beveiligingsniveau bepaalt voor de informatiesystemen die tot de scope van de quickscan behoren. Hiermee voldoet de opdrachtgever aan de vereisten van artikel 4a van het VIR 2007. Indien geen hogere eisen worden gesteld dan in de Baseline opgenomen, heeft de opdrachtgever tevens invulling gegeven aan artikel 4b van het VIR 2007.

Stap 1: Bepalen scope

De uitvoering van de QuickScan BIR vereist resources vanuit de organisatie. Het is derhalve essentieel deze zo efficiënt mogelijk uit te voeren. Dit vereist voorbereiding en afstemming met de opdrachtgever en de te betrekken functionarissen. Stap 1 van de QuickScan BIR beschrijft de wijze waarop de scope bepaald wordt en welke functionarissen deelnemen aan de workshop uit stap 2.

Scope bepalen

Bepaal de scope van de QuickScan: welk deel van het proces en welke systemen betreft het?
De scope kan uitgaan van een proces met één of meerdere ondersteunende systemen of één systeem dat meerdere processen ondersteund. Geef in onderstaande tabel aan welke processen met ondersteunende systemen tot de scope van de analyse behoren.

	Proces A	**Proces B**
	Korte beschrijving van het proces	*Korte beschrijving van het proces*
Systeem 1	*Beschrijving van de ondersteunende functie van het systeem voor het proces*	*Beschrijving van de ondersteunende functie van het systeem voor het proces*
Systeem 2	*Beschrijving van de ondersteunende functie van het systeem voor het proces*	*Beschrijving van de ondersteunende functie van het systeem voor het proces*

Detailbeschrijving processen en systemen

Vul per proces dat tot de scope behoort onderstaande tabel in. Vallen meerdere processen onder de scope dan moet per proces een tabel ingevuld worden.

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 informatiesystemen	*de informatiesystemen die worden gebruikt bij de activiteiten in het proces:* - *<informatiesysteem>*

Vul per systeem dat tot de scope behoort onderstaande tabel in.

Naam van het Systeem	
Systeemeigenaar	*<naam van de systeemeigenaar>*
De gebruikers van het systeem	*Degene die werkzaam zijn met het systeem* - *<wie is de interne gebruiker / klant?>* - *<wie is de externe gebruiker / klant?>* - *<aantal gebruikers / klanten>*
De output van het systeem	
Koppelvlakken met andere systemen	*Een architectuurplaatje kan in dit geval verhelderend werken.*
Het system ondersteunt de volgende processen	
Kritische momenten	*Beschrijf de kritische momenten dat het systeem gebruikt wordt. Bijvoorbeeld de piekperiodes.*

Dreigingsprofiel

Om in stap 3 het dreigingsprofiel te bepalen kan het toegevoegde waarde hebben om inzicht te hebben in de opgetreden beveiligingsincidenten. Maak ik dat geval een inventarisatie van de opgetreden beveiligingsincidenten. Dit kan bijvoorbeeld door de (beveiligings)incidenten van de Servicedesk op te vragen.

Personele inzet

Het is van belang bij het selecteren van de functionarissen voor de workshop dat men voldoende kennis heeft van het te onderzoeken proces met ondersteunende systemen. De volgende functionarissen dienen minimaal om input te worden gevraagd:

- systeem-/proceseigenaar
- de eindgebruiker/key-user/ representatieve gebruiker in het proces / van het ondersteunende systeem
- functioneel beheerder
- optioneel:
    - vertegenwoordiger van de service provider
    - de projectleider
    - de informatiebeveiligingsfunctionaris
    - de medewerker gegevensbescherming
    - informatiemanager
    - architect

Workshopleider
Per workshop wordt (bij voorkeur) een tweetal senior adviseurs ingezet. De ervaring leert dat dit leidt tot de beste resultaten. Eén adviseur richt zich op de inhoud en de registratie daarvan, de ander begeleidt het proces. De interviewers moeten de volgende kennis bezitten:

- De business / organisatie
- Systemen en bekend zijn met de SLA's
- Informatiebeveiliging in het algemeen
- Ervaring met het uitvoeren van Quick scans

De scopebeschrijving wordt voorafgaand aan de workshop aan de deelnemers toegestuurd.

Voor een snel en soepel verloop is het verstandig dat de adviseur aan het begin van de workshop een algemene inleiding geeft in het gebied van informatiebeveiliging en de definities die gehanteerd worden verduidelijkt. Hierbij wordt met name gedoeld op:

- Baseline informatiebeveiliging
- BIR
- Beveiligingsniveau
- BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid)
- Classificeren

Stap 2: BIV Beveiligingsniveau bepalen

1. Valideren Scope QuickScan BIR

Van belang is het om goed in beeld te hebben wat de scope van de analyse wordt. In de voorbereidingsfase (stap 1) is de scope beschreven. Neem deze scope als uitgangspunt en valideer dit met de workshop deelnemers. Van belang is het om goed in beeld te hebben of er bijvoorbeeld geen ondersteunende informatiesystemen ontbreken.

2. Classificatie van het proces

Voor het realiseren van de doelstellingen van de organisatie moeten de bedrijfsprocessen goed functioneren. Ieder proces wordt geclassificeerd naar belangrijkheid. In onderstaande tabel worden de classificaties weergegeven.

Classificatie: Kritisch strategisch	**Taak: Kerntaak**
In relatie tot de doelstellingen van het ministerie speelt het bedrijfsproces een primaire rol. Het hoort bij de primaire taken waarop het ministerie direct wordt aangesproken. Het ministerie ontleent haar bestaansrecht aan het uitvoeren van deze taken. - Het betreft een maatschappelijk vitaal proces - De instelling krijgt 80% of meer van de inkomsten uit dit proces, c.q. het budget van de organisatie wordt voor meer dan 80% uitgeput door dit proces. - Als de activiteit stilvalt of niet goed verloopt, heeft dit ernstige gevolgen voor het voortbestaan van de organisatie, c.q. het brengt het ministerie in een hachelijke positie.	

Classificatie: Strategisch	**Taak: Afgeleide kerntaak**
Het proces heeft een directe relatie naar het uitvoeren van de doelstellingen van het ministerie. Het is het primaire proces van de directie, agentschap, raad, etc. - Aan het proces kan een ontwikkelpotentieel worden toegekend. Met andere woorden, het wordt in de toekomst belangrijker in verband met mogelijke veranderingen in de strategische doelstellingen van het ministerie. - Een aanzienlijk deel van de omzet (50% - 80%) wordt gegenereerd met dit proces of een aanzienlijk deel (50% - 80%) van het te besteden budget komt ten goede aan dit proces. - Het proces heeft te maken met de uitvoering van wettelijke taken.	

Classificatie: Bijdragend	Taak: Bijzaak
Er is slechts sprake van een indirecte relatie met de hoofdactiviteiten van het ministerie. Het ontbreken echter van het “bijdragende proces” heeft binnen het primaire proces effectiviteits- en efficiencyverliezen tot gevolg.	

Classificatie: Ondersteunend	Taak: Voorwaardenscheppend
De activiteiten waaraan de typering “handig om te hebben” kan worden toegekend. Deze activiteiten hebben geen directe relatie naar het voortbrengen van de producten/diensten waaraan de instelling haar bestaansrecht ontleent. In de meeste gevallen is hier sprake van een ondersteunende rol naar de lijn. De activiteiten vormen een waardevolle support van het primaire proces.	

Argumentatie van de gekozen classificatie voor het proces
Beschrijf hier de keuze die is gemaakt voor de classificatie. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen classificatie.

3. Inventarisatie en classificatie van de informatiesystemen

Om het proces goed te kunnen laten functioneren wordt gebruik gemaakt van een aantal ondersteunende informatiesystemen. In onderstaande tabel is een overzicht gegeven van mogelijke classificaties van het informatiesysteem. De classificaties geven een waarde die men hecht aan het informatiesysteem ter ondersteuning van het proces.

Typering	**Waardering**
Vitaal (V)	- Het uitvoeren van de bedrijfsprocessen of het tot stand brengen van producten/diensten is (nagenoeg) onmogelijk zonder de inzet van het informatiesysteem. - Inzet van het informatiesysteem is van levensbelang voor een goede uitvoering van het bedrijfsproces.
Nuttig (N)	- Het informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of de voortbrenging van producten/diensten. - Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk. - Inzet van het informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. - Het informatiesysteem wordt door veel (interne / externe) medewerkers / klanten gebruikt.
Ondersteunend (O)	- Het informatiesysteem geeft support bij de activiteiten binnen het bedrijfsproces en is ‘handig om te hebben’.

Geef in onderstaande tabel per informatiesysteem (IS) aan in hoeverre het bedrijfsproces afhankelijk is van het ondersteunende informatiesysteem/ de informatiesystemen.

Informatiesysteem	**Belang (V,N,O)**	**Argumentatie**
Naam IS		*Beschrijf hier de keuze die is gemaakt voor de classificatie van het informatiesysteem.* *Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen classificatie.*

4. Betrouwbaarheidseisen die aan het proces met ondersteunende systemen worden gesteld

Het belang dat de organisatie toekent aan het proces kan verder gedetailleerd worden naar de betrouwbaarheidsaspecten beschikbaarheid, vertrouwelijkheid en integriteit. Per betrouwbaarheidsaspect wordt het belang van het proces met ondersteunende systemen uitgedrukt in een kwalitatieve waarde. De volgende waarden worden gehanteerd:
Zeer Laag (ZL), Laag (L), Midden (M), Hoog (H), Zeer hoog (ZH)

Beschikbaarheid van het proces of ondersteunende systemen:

Beschikbaarheid =

Zeer Hoog	Slechts in uitzonderlijke gevallen mag het proces of ondersteunende systemen niet operationeel zijn. Nul tot vier uur uitval is toegestaan en kan leiden tot - maatschappelijke onrust - kan levensbedreigende situaties tot gevolg hebben - kan grote financiële gevolgen hebben voor de staat
Hoog	Nauwelijks uitval van het proces met ondersteunende systemen gedurende de openingstijd is toegestaan. Vier tot acht uur uitval is toegestaan en kan - leiden tot vragen in de bestuursraad - leiden tot vragen van belangengroeperingen / klanten - negatieve publiciteit opleveren in de media - leidt tot vragen in de Tweede Kamer
Midden	Een enkele keer uitval van het proces met ondersteunende systemen is aanvaardbaar. Eén tot drie dagen uitval is toegestaan en kan - leiden tot klachten bij de directe gebruikers / klanten. - leiden tot vragen/ klachten bij het management.
Laag	Uitval van het proces met ondersteunende systemen voor een week (ook in piekperiodes) heeft nauwelijks of geen gevolgen voor de organisatie of klanten/ gebruikers. - Het is vervelend of - Het leidt hoogstens tot vragen bij gebruikers/ klanten.
Zeer Laag	Uitval van het proces met ondersteunende systemen voor een langere periode heeft geen gevolgen voor de organisatie of klanten / gebruikers.

Argumentatie van de gekozen beschikbaarheid van het proces met ondersteunende systemen
Beschrijf hier de keuze die is gemaakt voor de gekozen beschikbaarheid. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen beschikbaarheid. - *Beschrijf bijvoorbeeld de minimale eisen die gesteld worden aan de beschikbaarheid (ook in de piekperiodes). Komt dit overeen met de afgesloten SLA?* - *Welke eisen worden gesteld aan bijvoorbeeld het weer beschikbaar hebben van de data bij verlies?* - *Zijn er wettelijke termijnen die gehaald moeten worden?* - *Zijn er contractuele verplichtingen qua beschikbaarheid afgesproken naar klanten?* - *Zijn er politieke processen die een bepaalde beschikbaarheid/ response tijd vereisen?*

Integriteit van het proces met ondersteunende systemen:

Integriteit =

Zeer Hoog	Het bedrijfsproces eist foutloze informatie. Het risico is dusdanig hoog dat de hoogste eisen aan de integriteit van de gegevens wordt gesteld. In deze risicoklasse zijn gegevensverwerkingen opgenomen waarbij fouten grote consequenties voor de organisatie hebben. Het betreft onder andere gegevens waarop besluitvorming en verantwoording is gebaseerd, en gegevens gebruikt in een gerechtelijk proces. Wanneer de informatie niet integer is kan het leiden tot: - maatschappelijke onrust - levensbedreigende situaties - grote financiële gevolgen voor de staat
Hoog	De integriteit van de gegevens die in deze risicoklasse vallen is dusdanig van belang dat er negatieve gevolgen ontstaan voor de organisatie bij niet integer zijn. Het niet integere zijn van de gegevens - heeft op den duur financiële consequenties - leidt tot vragen in de bestuursraad. - Leidt tot klachten bij groeperingen of grote groepen van gebruikers - Levert imagoschade op / negatieve publiciteit in de media
Midden	Het gaat hier om informatie waaraan ten aanzien van de correctheid, volledigheid, actualiteit, authenticiteit, controleerbaarheid en consistentie geen bijzondere eisen worden gesteld. De informatie hoeft niet altijd foutloos te zijn. Het gaat dan om gegevens waarbij integriteit wel gewenst is, maar waarbij het niet integer zijn niet leidt tot schade van enige omvang. Het kan - leiden tot vragen bij gebruikers of - leiden tot klachten bij gebruikers. - leiden tot vragen/klachten bij het management.
Laag	Het gaat hier om informatie waaraan ten aanzien van de correctheid, volledigheid, actualiteit, authenticiteit, controleerbaarheid en consistentie lage eisen worden gesteld. Bij het niet integer zijn van de gegevens - is het vervelend maar goed te herkennen en te herstellen.
Zeer Laag	Het gaat hier om data die niet integer is. Bij de verwerking van deze data weet men dat de data niet correct, volledig of actueel zou kunnen zijn. Deze data wordt bijvoorbeeld gebruikt om trends waar te nemen. Bijvoorbeeld Twitter berichten.

Argumentatie van de gekozen integriteit van het proces met ondersteunende systemen
Beschrijf hier de keuze die is gemaakt voor de gekozen integriteit. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen integriteit. - *Beschrijf waarom welke integriteitseisen aan de informatie worden gesteld.* - *Zijn er workarounds, is er bijvoorbeeld een papieren schaduwdossier, worden fouten snel herkend, etc.* - *Zijn er fouttoleranties afgesproken met klanten / afnemers?*

Vertrouwelijkheid van het proces met ondersteunende systemen:

Vertrouwelijkheid =

Zeer Hoog	Het risico is dusdanig hoog dat het is gerechtvaardigd de hoogste eisen te stellen aan de maatregelen die genomen moeten worden om de gegevens te beveiligen. In deze risicoklasse zijn gegevensverwerkingen opgenomen waarbij kennisname door ongeautoriseerden (buitenstaanders, ingehuurd personeel, alle eigen medewerkers) grote politieke, maatschappelijke of financiële gevolgen voor het ministerie ontstaan bijv. Wbp risicoklasse III / staatgeheimen. Bij ongeautoriseerde openbaar wording - leidt tot vragen in de Tweede Kamer - maatschappelijke onrust - kan levensbedreigende situaties tot gevolg hebben - kan grote financiële gevolgen hebben voor BV Nederland
Hoog	De gegevens zijn alleen toegankelijk voor direct betrokkenen. Bedrijfsbelangen of personen worden niet direct ernstig geschaad als ongeautoriseerden (buitenstaanders, ingehuurd personeel, alle eigen medewerkers) toegang krijgen, maar het heeft we een negatieve impact op de organisatie (bijv. imago). Wbp risicoklasse II (verhoogd risico) of DepV. Informatie. - leidt tot vragen/klachten bij het management of - leidt tot vragen in de bestuursraad - negatieve publiciteit
Midden	Gegevens zijn alleen ter inzage voor een bepaalde groep. Bedrijfsbelangen of personen worden niet ernstig geschaad als ongeautoriseerden (buitenstaanders, ingehuurd personeel) toegang krijgen. Het gaat om gegevens waarbij het kennisnemen door ongeautoriseerden niet gewenst is, maar niet leidt tot schade van enige omvang. In deze risicoklasse past onder andere informatie waarover bijvoorbeeld wel in de media wordt gepubliceerd, maar niet leiden tot politieke, maatschappelijke of financiële consequenties. Wbp risicoklasse I (basis niveau). Bij openbaar worden van de gegevens - leidt het hoogstens tot vragen bij gebruikers / klanten of - leidt het tot klachten bij gebruikers
Laag	Het gaat hier om semi-openbare gegevens. De in deze klasse opgenomen gegevens vormen bij normaal gebruik geen risico. De risico's van betrokkene bij verlies op onbevoegd of onzorgvuldig gebruik van de gegevens zijn zodanig dat standaard (informatie) beveiligingsmaatregelen toereikend zijn. Het gaat dan om gegevens waarbij het kennisnemen door ongeautoriseerden (buitenstaanders) niet gewenst is, maar niet leidt tot schade van enige omvang. Bij openbaar worden van de gegevens heeft het:

	- geen gevolgen of - is het vervelend
Zeer Laag	Het gaat hierbij om openbare gegevens. De gegevens hoeven niet afgeschermd te worden. Geen enkele beveiliging op de gegevens is noodzakelijk. Het is juist zaak dat deze gegevens openbaar worden gemaakt voor publicatie.

Argumentatie van de gekozen vertrouwelijkheid van het proces met ondersteunende systemen
Beschrijf hier de keuze die is gemaakt voor de gekozen vertrouwelijkheid. Van belang is het dat goed wordt gedocumenteerd wat de onderliggende keuzes zijn voor de gekozen vertrouwelijkheid. - *Beschrijf wat voor soort informatie in het proces en systeem wordt verwerkt. Is dit privacy gevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie en welke belangen worden geschaad bij het openbaar worden van deze informatie.* - *Worden er wettelijke eisen aan de vertrouwelijkheid gesteld (bijv. Wbp)?* - *Zijn er contractuele verplichtingen qua vertrouwelijkheid afgesproken naar klanten?*

Stap 3: Dreigingsprofiel bepalen

De BIR maatregelen beschermen tegen een aantal dreigingen en dreigers. Van belang is het om vast te stellen of het te analyseren proces met ondersteunende informatiesystemen doelwit kunnen/ kan zijn van andere dreigingen of dreigers die in de BIR worden beschreven.
Ga voor het proces met ondersteunende systemen na of er dreigingen / dreigers zijn die niet in de BIR voorkomen. De BIR sluit sowieso de volgende dreigingen uit:

- Terreurgroep
- Inlichtingendienst
- Georganiseerde criminaliteit

Mochten deze dreigingen voorkomen, dan is de BIR qua beveiligingsniveau niet toereikend en zult u een aanvullende risicoanalyse moeten uitvoeren.

Argumentatie van de van toepassing zijnde dreigingen en dreigers
Bepaal welke dreigingen / bedreigers van toepassing zijn op het proces met ondersteunende systemen. Dit kunt u doen door te bekijken hoeveel exposure het proces heeft. Is het bijvoorbeeld een proces / dienstverlening dat veel in de media is geweest of worden er in het proces / ondersteunende systeem gegevens verwerkt die interessant kunnen zijn voor specifieke doelgroepen (bijvoorbeeld financiële gegevens, persoonsgegevens). Hiernaast kunt u nagaan welke incidenten er hebben plaatsgevonden.

Dreigingen BIR

BIV-aspect	Dreigingsprofiel	Bedreigingen
Dreigingen specifiek voor Departementaal Vertrouwelijk	- De onbetrouwbare medewerker - Wraakzuchtige medewerker - De verontruste burger - Actiegroep - Crimineel opportunist - Contractor - Georganiseerde internet crimineel	- Infiltratie light - Publiek benaderbare sociale netwerken - Verhoor (fysiek geweld tegen personen) - Hacking op afstand - Malware (met en zonder remote control) - Crypto kraken - Draadloze netwerken interceptie - Draadloze netwerken actief benaderen - Beproeving van fysieke, technische en elektronische weerstand
Algemene dreigingen		- Onopzettelijk menselijk handelen - Opzettelijk menselijk handelen - Onbeïnvloedbare externe factoren - Technisch falen

Stap 4: Rapportage vaststellen resultaten workshop

Samenvatting resultaten QuickScan BIR				
Proces beschrijving				
		Proces	**Systeem**	**Boven BIR niveau**
Classificatie proces & Systeem		Kritisch strategisch Strategisch Bijdragend Ondersteunend	Vitaal Nuttig Ondersteunend	Kritisch strategisch + Vitaal Of Strategisch + Vitaal
Betrouwbaarheidseisen - **Beschikbaarheid**		Zeer Laag Laag Midden Hoog Zeer Hoog		Zeer Hoog
Betrouwbaarheidseisen - **Integriteit**		Zeer Laag Laag Midden Hoog Zeer Hoog		Zeer Hoog
Betrouwbaarheidseisen - **Vertrouwelijkheid**		Zeer Laag Laag Midden Hoog Zeer Hoog		Zeer Hoog
Dreigingsprofiel		BIR Anders dan BIR		Anders dan BIR

Conclusie & aanbevelingen

Conclusie

Wanneer het proces en het ondersteunende systeem is geclassificeerd als:

- **Kritisch strategisch proces in combinatie met Vitaal systeem** of
- **Strategisch proces in combinatie met Vitaal systeem**

Dan volstaat de BIR baseline niet en dient een risicoanalyse uitgevoerd te worden.

Wanneer een proces of systeem eisen op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid stelt die op het niveau:

- **Zeer Hoog** dan volstaat de BIR baseline niet en dient een risicoanalyse uitgevoerd te worden.

De uit te voeren risicoanalyse kan zich specifiek richten op dat aspect (BVI) wat boven de BIR-baseline uitkomt.

Aanbevelingen:

Beschrijf hier de conclusie en welke aanbevelingen u doet voor een eventueel vervolg. Welke aspecten uit deze QuickScan kunnen gebruikt worden in bijvoorbeeld de risicoanalyse, het BCP, etc. Waar moet de aandacht op worden gevestigd?

Teken Formulier

Op [datum] heeft een workshop QuickScan BIR plaatsgevonden voor [proces x] met ondersteunende systemen [xxxx].

Bij deze workshop waren aanwezig:

Naam	Functie	Afdeling
	Eigenaar proces / systeem	
	Key-user systeem	
	Functioneel beheerder	

Ik heb kennis genomen van de inhoud van het rapport en stem in met de resultaten van deze QuickScan.

Datum:

Naam:

Functie:

Handtekening:

Laten aftekenen door de proceseigenaar / systeemeigenaar.

Bijlage 1: Totstandkoming Quickscan BIR

De totstandkoming van de Quickscan BIR

Bij de ontwikkeling van de QS-BIR is gebruik gemaakt van informatie die is ontvangen van: Economische Zaken, DICTU, Buitenlandse Zaken, Veiligheid & Justitie, Binnenlandse Zaken en Agentschap NL. De ontwikkeling van de QS-BIR is begeleid vanuit een werkgroep met professionals die praktijkervaring hebben met een soortgelijk instrument binnen hun eigen departement. De deelnemers aan de Werkgroep waren: Economische Zaken, DICTU, Buitenlandse Zaken, Veiligheid & Justitie, Binnenlandse Zaken en de Taskforce BID. De ontwikkeling van het instrument werd begeleid vanuit iComply.

Het beveiligingsniveau van de BIR is in dit instrument als volgt aan de Quick Scan gelieerd:

Met de QS-BIR wordt voor een proces met ondersteunende informatiesystemen op drie manieren getoetst of het beveiligingsniveau van de BIR toereikend is. Er wordt gekeken naar:

- de classificatie van proces & informatiesystemen.
- de hoogte van de eisen die gesteld worden aan de beschikbaarheid, integriteit, vertrouwelijkheid (BIV) van de informatie.
- de dreigingen voor het proces die niet zijn onderkend in de BIR.

Deze drie manieren van toetsen zijn tot stand gekomen uit een combinatie van 'best practices' die reeds bij de diverse ministeries worden gebruikt, op basis van expertise van de werkgroepleden, de IRAM methodiek en beschreven staan in de BIR.

De gevoeligheid van de informatie

De Quick Scan wordt toegepast indien de behandelde informatie het vertrouwelijkheidsniveau Departementaal Vertrouwelijk of WBP risicoklasse 2 (Wet Bescherming Persoonsgegevens) niet te boven gaat. Voor staatsgeheime informatie of informatie van WBP risicoklasse 3 moet altijd een aanvullende risicoanalyse worden gedaan (uiteraard vervalt niet de plicht om ook aan de BIR te voldoen).

De classificatie van processen & systemen:

Wanneer het proces en het ondersteunende systeem is geclassificeerd als:

- Kritisch strategisch proces in combinatie met Vitaal systeem of
- Strategisch proces in combinatie met Vitaal systeem

dan volstaat de BIR baseline niet en dient een risicoanalyse uitgevoerd te worden.

De betrouwbaarheidseisen BIV:

Wanneer een proces of informatiesysteem eisen op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid stelt op het niveau **Zeer Hoog** dan volstaat de BIR baseline niet en dient een risicoanalyse uitgevoerd te worden.

Dreigingsprofiel:

Wanneer een proces met ondersteunende informatiesystemen doelwit kunnen zijn van andere dreigingen of dreigers die in de BIR worden beschreven dient een risicoanalyse uitgevoerd te worden.

Hoe om te gaan met comply & explain en de uitkomsten van een uitgevoerde quickscan

De QS-BIR heeft een adviserend en richtinggevend karakter. De uitkomst van de QS-BIR zijn aanbevelingen voor eventuele vervolgstappen (risicoanalyse, implementatie BIR, etc.). Het is aan de proces/ systeemverantwoordelijke om te bepalen wat er met de resultaten uit de QS-BIR wordt gedaan.

Op welke wijze kan het instrument geschikt gemaakt worden voor gebruik bij andere overheden?

De QS-BIR is zo ontworpen dat deze ook eenvoudig geschikt gemaakt kan worden voor gebruik bij andere overheden: de te volgen processtappen in de QS-BIR zijn generiek toepasbaar. Bij toepassing van de QS-BIR bij andere overheden dan de Rijksoverheid moet onderzocht worden of de van toepassing zijnde baseline overeenkomt met het in de QS-BIR gekozen betrouwbaarheidsniveau “Zeer Hoog” en de dreigingen waartegen de baseline beschermt.

Bijlage 2: Handleiding QS-BIR

Inleiding

In deze bijlage is een handleiding beschreven die dient als ondersteuning voor de workshopleider bij de voorbereiding en uitvoering van de QS-BIR. De QS-BIR bestaat uit een 4-tal stappen. In deze vier stappen wordt een globale analyse gemaakt van de betrouwbaarheidseisen die worden gesteld aan een proces met ondersteunende informatiesysteem(en) om vervolgens een keuze te maken tussen de maatregelen uit de Baseline of het uitvoeren van een risicoanalyse. Voordat deze 4 stappen uitgevoerd kunnen worden dient de volgende voorbereiding te worden getroffen:

- Voorbereiding
    - Inventariseren benodigde informatie voor scoping
    - Selectie en benaderen deelnemers workshop
- De workshop QS-BIR
- Afronden met handtekening onder het verslag.

Voorbereiding

Inventariseren benodigde informatie voor scoping

De BIR is van toepassing op een proces, informatiesysteem of een combinatie hiervan. Om de QS-BIR toe te passen moet de scope gedefinieerd worden. M.a.w. welk proces, informatiesysteem of combinatie van processen met systemen wordt onderzocht? Van belang is dat de scope niet te groot wordt gekozen. Veelal wordt uitgegaan van één proces met ondersteunende systemen of één systeem dat meerdere processen ondersteund.

Om een goed inzicht te verkrijgen in de processen en systemen kan de volgende documentatie behulpzaam zijn:

- Procesbeschrijvingen
- Systeembeschrijvingen / systeemdocumentatie
- Reeds eerder uitgevoerde risicoanalyses of audits

Voorafgaand aan de workshop stemt de procesbegeleider de scope (welk proces, systeem(en)) met de opdrachtgever af zodat deze tijdens de workshop slechts gevalideerd hoeft te worden.

Selectie deelnemers QS-BIR workshop

De QS-BIR wordt middels een workshop van twee uur uitgevoerd met diverse functionarissen. In de QS-BIR worden de eisen die gesteld worden aan processen en systemen onderzocht. Een vertegenwoordiging vanuit de business is daarom vereist. Immers de proces/ systeemeigenaar kan bepalen welke eisen er gesteld worden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van het proces/ systeem. Hiernaast is van belang bij het selecteren van de functionarissen voor de workshop dat men voldoende kennis heeft van het te onderzoeken proces met ondersteunende systemen.

De volgende functionarissen dienen minimaal om input te worden gevraagd:

- systeem-/proceseigenaar
- de eindgebruiker/key-user/ representatieve gebruiker in het proces / van het ondersteunende systeem
- functioneel beheerder
- optioneel:
    - vertegenwoordiger van de service provider
    - de projectleider
    - de informatiebeveiligingsfunctionaris
    - de medewerker gegevensbescherming
    - informatiemanager
    - architect

Niet altijd zal het mogelijk zijn om een workshop te plannen waar alle vereiste functionarissen aanwezig zijn. In plaats van een workshop kunnen dan individuele interviews gehouden worden. Hierbij is het van groot belang dat de argumentatie van de gemaakte keuzes goed wordt gedocumenteerd en gedeeld met de andere functionarissen. Bij individuele interviews ontbreken de groepsdiscussies. Deze dienen dus 'offline' middels reviewsessies plaats te vinden.

Uitnodigen deelnemers QS-BIR workshop

De deelnemers aan de QS-BIR workshop kunnen volstaan met een minimale voorbereiding. Met de uitnodiging voor de bijeenkomst ontvangen informatie die hen een goed beeld geeft van het doel, de onderdelen van de bijeenkomst en wat het beoogde resultaat is. Een uitnodiging kan de volgende punten bevatten:

- Inleiding over waarom de QS-BIR workshop wordt gehouden en het doel.
    - Het doel is: In kaart brengen welke eisen gesteld worden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid voor het te onderzoeken proces /informatiesysteem.
    - Het beoogde resultaat van de QS-BIR is een verantwoorde afweging of de Baseline Informatiebeveiliging Rijksdienst (BIR) afdoende beveiliging biedt voor het onderzochte proces /informatiesysteem.

- Korte beschrijving van wat er in de workshop gaat gebeuren:
    - Uitvraag van eisen die aan de processen en systemen worden gesteld op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid.
    - Neem in de uitnodiging een aantal voorbeelden van vragen op die gesteld worden zoals:
        - Hoe lang mag het proces/ systeem eruit liggen voordat er grote schade optreedt?
        - Welke impact heeft het wanneer de informatie in het proces/ systeem niet volledig of correct is?
        - Wordt er met (persoons) vertrouwelijke informatie gewerkt en hoe erg is het als dit op straat komt te liggen?

- De tijdsbesteding: maximaal 2 uur voor de workshop.

- Wat er van de deelnemers verwacht wordt:
    - Vooraf doornemen van de meegestuurde scopebeschrijving
    - Input leveren tijdens de workshop
    - Review van het eindresultaat.

- Bijlage: de QS-BIR, beschrijving van de scope

De workshop QS-BIR

Gestart wordt met achtergrondinformatie over informatiebeveiliging, het concept baseline, beveiligingsniveaus en de BIR.

Introductie informatiebeveiliging, baseline, BIR
Informatiebeveiliging heeft tot doel om op een afgewogen manier (risicomanagement) keuzes te maken over welke beveiligingseisen gesteld moeten worden aan processen en systemen en welke beveiligingsmaatregelen geïmplementeerd moeten worden. Er wordt binnen informatiebeveiliging altijd gekeken naar een drietal aspecten:

- De vereiste beschikbaarheid van informatie
- De vereiste integriteit van informatie (correctheid en volledigheid)
- De vertrouwelijkheid van de informatie (persoonsvertrouwelijk, commercieel vertrouwelijk, etc).

Voor deze drie aspecten worden beveiligingseisen gesteld en maatregelen gedefinieerd. Afhankelijk van de hoogte van de eisen (het beveiligingsniveau) worden meer dan wel minder beveiligingsmaatregelen voorgeschreven. Dit beveiligingsniveau wordt achterhaald door het uitvoeren van risicoanalyses.

Al in 1994 zag de Rijksoverheid in dat de bescherming van informatie goed geregeld moest worden. Hiertoe ontwierp zij het Voorschrift Informatiebeveiliging Rijksdienst (VIR'94). Het VIR beschrijft in grote lijnen dat een manager verantwoordelijk is voor de beveiliging van zijn processen / systemen en dat de afweging tot het nemen van beveiligingsmaatregelen middels een risicoanalyse tot stand moet komen. Om nu niet voor ieder proces / systeem een uitgebreide risicoanalyse verplicht te stellen heeft de overheid een baseline informatiebeveiliging ontworpen: de Baseline Informatiebeveiliging Rijksdienst (BIR). Deze baseline is een set van 'best practices' beveiligingsmaatregelen die als minimum niveau voor ieder proces / systeem geïmplementeerd moet worden.

Omdat de BIR een minimum niveau is kan het voorkomen dat voor kritieke processen en systemen zwaardere beveiligingseisen en beveiligingsmaatregelen noodzakelijk zijn. M.a.w. de BIR kan een onvoldoende beveiligingsniveau voor kritieke processen en systemen hebben. De QS-BIR is ontworpen om op een snelle en eenvoudige manier te achterhalen of de BIR volstaat of dat er met een uitgebreide risicoanalyse bepaald moet worden welke extra beveiligingsmaatregelen noodzakelijk zijn.

Deze workshop heeft tot doel om te bepalen of de BIR volstaat of dat er een uitgebreide risicoanalyse noodzakelijk is.

QS-BIR workshop

Nadat de introductie is gedaan, en de deelnemers zich hebben voorgesteld, kan begonnen worden met de workshop. Van belang is het dat de scope goed wordt gevalideerd. Gebruik hiervoor de invulformulieren zoals beschreven in Stap 1 in de QS-BIR.

Wanneer alle processtappen zijn doorlopen en de voorlopige conclusie is getrokken, is het aan de procesbegeleider om de ingevulde QS-BIR na afloop ter review aan de workshopdeelnemers te sturen. Bij de review is het van belang dat er goed gekeken wordt naar de argumentatie die is gegeven waarom bepaalde keuzes zijn gemaakt.
Na verwerking van de reviewcommentaren wordt de QS-BIR ter ondertekening aangeboden aan de proces/ systeemeigenaar.