TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Implementatie BIR

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

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

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Implementatie BIG’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt een handreiking voor de implementatie van de Baseline Informatiebeveiliging Rijksdienst door organisaties binnen de Rijksoverheid.

Doelgroep

Dit document is van belang voor de bestuurlijke eindverantwoordelijke voor wat betreft de eindverantwoordelijkheid voor de implementatie van de BIR en de verantwoordelijke voor de implementatie van de BIR.

Reikwijdte

Dit document heeft betrekking op alle maatregelen van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- GAP-analyse
- Toelichting op GAP-analyse
- Informatiebeveiligingsbeleid
- Quick Scan BIR

Inhoudsopgave

1 Introductie

1.1 Inleiding

Met het ontwikkelen van de Baseline Informatiebeveiliging Rijksdienst (BIR) is een belangrijke stap voor meer informatieveiligheid gezet. Dit document biedt een handreiking voor de implementatie van de BIR binnen Rijksoverheidsorganisaties.

De BIR staat niet op zichzelf, maar is een samenhangende set van maatregelen die in overeenstemming gebracht is met andere initiatieven, zoals het Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007). Daarnaast zijn er baselines bij onder andere gemeenten, waterschappen en provincies, die in lijn met de BIR lopen. Alle deze baselines zijn gebaseerd op de ISO 27001 en 27002. Deze normen gelden als verplichte open standaard voor de overheid en maken deel uit van de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie.

Het implementeren van de BIR kan het beste in een aantal stappen gebeuren. Iedere stap is afhankelijk van de voorgaande stap en is belangrijk voor de volgende stap. Iedere stap heeft een bepaald doel en het resultaat is een gecontroleerde invoering van de BIR met een verankering binnen de organisatie. Een volledige implementatie van de BIR is in veel gevallen niet in één jaar afgerond. Het is belangrijk om bij de implementatie van de baseline ‘in control’ te komen door stapsgewijs en planmatig te werk te gaan. Zoals in deze handreiking wordt beschreven, zijn de uitkomsten van een GAP-analyse een goed startpunt voor het vaststellen van de prioritering in de implementatie. De uitvoering van maatregelen kan in een jaarlijks vast te stellen informatiebeveiligingsplan worden beschreven.

1.2 Uitgangspunten

De BIR geldt als dé minimale set van informatiebeveiligingsmaatregelen, die organisaties binnen de Rijksoverheid moeten invoeren. Ongeacht het proces of het systeem: de BIR geldt voor alle bedrijfsvoeringsprocessen van de Rijksoverheidsorganisatie. Deze uniformiteit aan maatregelen vergroot de veiligheid en de beheersbaarheid. Een aantal maatregelen werken van zichzelf organisatiebreed: deze maatregelen gelden voor iedereen en werken efficiënter en effectiever als ze centraal worden opgepakt.

Een implementatie van de BIR heeft een aantal specifieke voordelen ten opzichte van andere methodieken of standaarden voor informatieveiligheid. Deze voordelen zijn als volgt:

- Er hoeft niet voor ieder proces of systeem een risicoanalyse uitgevoerd te worden;
- Alle organisaties hanteren en gebruiken dezelfde norm;
- Alle organisaties kunnen onderling informatie uitwisselen, die betrekking heeft op de BIR, zoals beleid, proces en procedure beschrijvingen over onderwerpen op gebied van informatiebeveiliging;
- De BIR ondersteunt organisaties en maakt het gemakkelijker om bewust veilig te zijn. Incidenten zijn niet te voorkomen - 100% veilig bestaat niet - maar door juist gebruik van de BIR kan voorkomen worden dat een incident meer impact krijgt dan nodig is.

- De BIR biedt de mogelijkheid om aanvullende maatregelen te nemen als dat nodig is. Dit wordt beschreven in het document “dataclassificatie”.

2 Achtergrondinformatie

In hoofdstuk 3 van de Baseline Informatiebeveiliging Rijksdienst (BIR) zijn de stappen beschreven voor de implementatie van de BIR. In dit hoofdstuk wordt een korte achtergrond geschetst over de implementatie van de BIR.

2.1 De rol van de directie

De directie speelt een cruciale rol bij het uitvoeren van het informatiebeveiligingsbeleid. Zo maakt de directie een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de organisatie hebben, de risico's die de organisatie hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet de directie het beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

De directie zou informatiebeveiliging moeten beschouwen als een integraal onderdeel van de bedrijfsvoering, specifiek gericht op het beheersen van de risico's ten aanzien van de processen, de informatiesystemen en de onderliggende ICT-infrastructuur. Evenals andere onderdelen binnen bedrijfsvoering heeft informatiebeveiliging structurele aandacht van de directie nodig. De directie, en daarnaast ook de informatiemanager, zal voldoende kennis en inzicht op het gebied van informatiebeveiliging moeten hebben om de juiste keuzes te kunnen maken.

De belangrijkste beveiligingsfunctie ligt bij de directie binnen de organisatie. De directie is verantwoordelijk voor de centrale coördinatie en aansturing van de informatiebeveiliging. Belangrijk is dus dat de directie kennis neemt van in elk geval het Voorschrift Informatiebeveiliging Rijksdienst. Binnen de directieteam is één persoon de portefeuillehouder voor informatiebeveiliging. De directie kan de uitvoering van informatiebeveiliging delegeren of uitbesteden, maar de eindverantwoordelijkheid voor informatiebeveiliging en het maken van beleidskeuzes ligt bij de directie. De directie is ook verantwoordelijk voor het aanwijzen van de medewerkers, die een rol krijgen bij de informatiebeveiliging en het toewijzen van de daarbij behorende taken, verantwoordelijkheden en bevoegdheden. Met het toewijzen van taken, bevoegdheden en voldoende tijd en middelen, wordt een begin gemaakt met de invulling van informatiebeveiliging.

De overige beveiligingstaken behoren bij verschillende beveiligingsfuncties. De belangrijkste hiervan zijn:

- De informatiebeveiligingsfunctionaris/CISO;
- De stuurgroep informatiebeveiliging;
- De informatiebeveiligingsauditor;
- Het projectteam informatiebeveiliging.

Bij het toewijzen van taken, verantwoordelijkheden en bevoegdheden spelen twee aspecten een rol:

1. het eigenaarschap van processen en informatiesystemen, en;
2. de beveiligingstaken.

Het eigenaarschap van processen en informatiesystemen ligt in het algemeen bij lijnmanagers. Een lijnmanager is eigenaar van de processen en systemen binnen zijn organisatieonderdeel. De lijnmanager moet er onder meer voor zorgen dat zijn processen en informatiesystemen voldoende beveiligd zijn. De taken die hiervoor uitgevoerd moeten worden kan een manager delegeren of uitbesteden. Het is ook mogelijk om de informatiebeveiliging in een korte periode te versterken door het uitvoeren van een apart project. Hierbij dient aandacht te zijn voor inbedding in de organisatie.

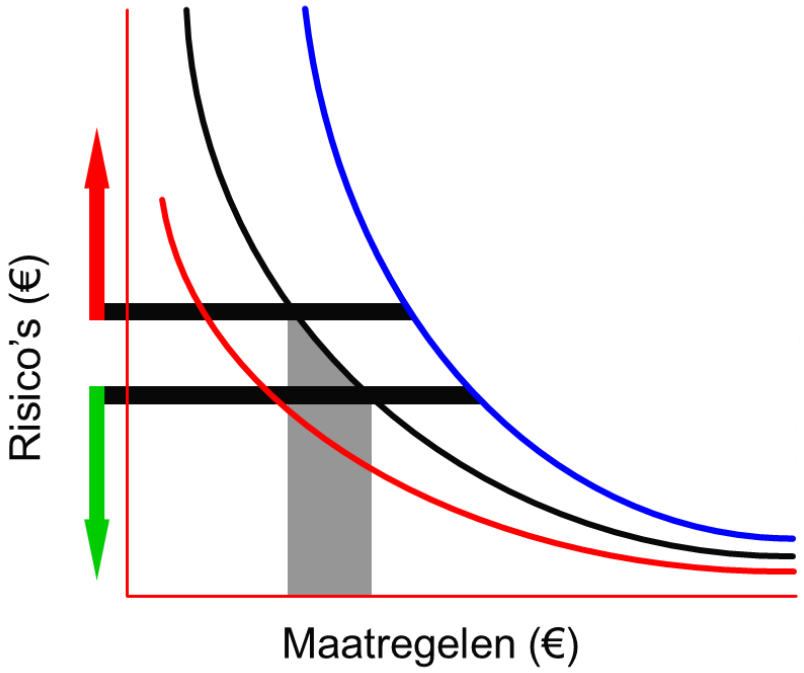
Daarnaast moeten de beveiligingsmedewerkers kunnen rekenen op voldoende steun van de directie en moet er aandacht worden besteed aan de rapportages over behaalde resultaten en beveiligingsincidenten.[1] Vanzelfsprekend dienen incidenten dan ook te worden gemeten en moet duidelijk zijn hoe moet worden gehandeld als er zich incidenten voordoen. Snel en in beslotenheid handelen, is meestal cruciaal, anders zijn sporen veelal niet meer te achterhalen.

2.2 Verschil in perceptie

Afhankelijk van verschillende rollen en posities van mensen in een organisatie wordt er op een andere manier naar informatiebeveiliging gekeken. Bij het opstarten van de implementatie van de BIR is het goed dit in ogenschouw te houden.

De BIR is gebaseerd op de ISO en opgesteld vanuit verschillende *best practices*. Bij beveiligen van informatie is er altijd een spanningsveld tussen: ‘hoeveel functionaliteit wil ik overhouden?’, ‘hoeveel wil ik beveiligen?’, ‘welk restrisico ben ik bereid te lopen?’ en ‘hoeveel mag het kosten?’. Dit spanningsveld tussen verschillende overwegingen (kosten, functionaliteit, veiligheid en restrisico) bij informatiebeveiliging zijn als volgt schematisch weer te geven:[2]

[1] Beveiligingsincidenten worden uitgelegd in het document ‘incident management en response beleid’
[2] Door Marcel Spruit, uit http://www.marcelspruit.nl/papers/bewust_veilig.pdf.



Daarnaast is het goed te beseffen dat er op het gebied van informatiebeveiliging een driehoek te herkennen is: (lijn)managers, beveiligers en gebruikers. De meeste aandacht wordt besteed aan de gebruikers, maar uit onderzoek is gebleken dat zij vaak niet de veroorzaker zijn van de grootste bedreigingen. Juist het spanningsveld tussen (lijn)managers en beveiligers levert een veel groter risico op. Managers zien bijvoorbeeld grote mogelijkheden om de bedrijfsvoering efficiënter te maken door nieuwe toepassingen, zoals BYOD, en de ICT-kosten te beheersen door het inzetten van Cloud-oplossingen. Maar het realiseren van deze doelstellingen introduceert nieuwe beveiligingsrisico's die eveneens adequaat moeten worden geadresseerd.

3 Implementatie

Het stappenplan om de BIR te implementeren wordt beschreven in hoofdstuk 3 van de baseline. De daar benoemde stappen worden in deze beschrijving van de aanpak aangevuld met een aantal extra stappen die belangrijk zijn voor een goede implementatie van de BIR. De volgende stappen zijn onderkend:

1. Management commitment;
2. Benoemen verantwoordelijken;
3. Uitvoering GAP-analyse;
4. Benoemen Quick Wins;
5. Uitvoering impactanalyse;
6. Management goedkeuring;
7. Opstellen informatiebeveiligingsplan.

3.1 Stap 1: Management commitment

Het implementeren van de BIR vraagt om commitment en besluitvorming van de directie van de organisatie. Zij moeten bewust besluiten om de BIR als norm voor het basisbeveiligingsniveau van de organisatie te omarmen op basis van een eigen risicoafweging. Het invoeren van de BIR kan het beste projectmatig worden aangepakt, waarbij een goede inschatting wordt gemaakt van benodigde capaciteit en middelen.

Als informatiebeveiliging nog niet is belegd in de organisatie of wanneer de verantwoordelijkheden onduidelijk zijn, dient dit als eerste te worden gerealiseerd door de directie. Daarnaast zal de directie het besluit moeten nemen de baseline te implementeren.

3.2 Stap 2: Benoemen verantwoordelijken

De BIR bestaat uit maatregelen waarbij de verantwoordelijkheden ten aanzien van de maatregel aan verschillende rollen in de organisatie kan worden toegewezen. Zo zijn er maatregelen voor de afdeling P&O, voor systeembeheer of bijvoorbeeld voor de facilitaire dienst. Daarnaast zijn maatregelen op te splitsen in procedurele maatregelen, beleidsmaatregelen, technische (ICT) maatregelen en fysieke, bouwkundige maatregelen. Veel maatregelen hangen met elkaar samen en zijn voor een juiste toepassing afhankelijk van elkaar. Zo worden technische maatregelen soms genomen om organisatorische maatregelen uitvoerbaar te maken of af te dwingen. Zie voor een nadere uitleg hoofdstuk 3.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR).

3.3 Stap 3: Uitvoering GAP-analyse

De volgende stap is het uitvoeren van een GAP-analyse waardoor duidelijk wordt welke maatregelen uit de baseline wel zijn geïmplementeerd en welke nog niet. De uitkomst van de GAP-analyse is een lijst met maatregelen die ontbreken en die geïmplementeerd moeten gaan worden. De GAP-analyse wordt beschreven in een operationeel product voor de BIR met een spreadsheet (GAP-analyse.xlsx), waarin de status van alle maatregelen uit de

baseline wordt uitgevraagd. Er kan worden aangegeven of een maatregel wel, niet of gedeeltelijk is genomen. Er kan voorts een vindplaats, waar de maatregel is aangetroffen als het om een document of beleid gaat, of een opmerking geplaatst worden. Iedere maatregel moet een eigenaar hebben en ook dit kan worden ingevuld. In het status veld kan worden ingevuld of een maatregel een geaccepteerd risico is.

Opsteller :	
Datum :	
Organisatie:	

BIR Nummer	Hoofdgroep	Groep	Maatregel	Vraag
5.1.1.1	5. Beveiligingsbeleid	Beleidsdocumenten voor informatiebeveiliging	Er is beleid voor informatiebeveiliging door het lijnmanagement vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten	Is er een door de organisatie vastgesteld en gepubliceerd informatiebeveiligingsbeleid op basis van de BIR en zijn daarin verantwoordelijkheden op basis van de baseline benoemd?

Vervolg:

DEEL 1 (GAP-Analyse)			DEEL 2 (IMPACT-Analyse)			
Aanwezig	Vindplaats / opmerking	Eigenaar	Status	Actiehouder	Wanneer gereed?	Geaccepteerd risico?
onbekend			Nog niet onderzocht			

De uitkomst van de GAP-analyse is een lijst met maatregelen, die genomen zijn of nog genomen moeten worden. In de Excel-spreadsheet kan in één oogopslag worden gezien hoe het staat met het totaal van de maatregelen per hoofdstuk van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het diagram in dit tabblad kan gebruikt worden om de voortgang zichtbaar te maken voor de directie.

Een maatregel hoeft in deze fase nog geen eigenaar te hebben. Als een maatregel reeds genomen is of gedeeltelijk aanwezig is, dan zou er een eigenaar moeten zijn. Het is belangrijk dat er niet gezocht wordt naar een eigenaar in de zin van GBA of BAG of DigiD. Dergelijke eigenaren houden zich alleen bezig met een maatregel specifiek voor hun organisatieonderdeel of proces (bv. de DigiD-koppeling). Een eigenaar in de zin van de BIR geldt organisatiebreed.

3.4 Stap 4: Benoemen Quick Wins

Quick Wins zijn nog niet geïmplementeerde maatregelen die met relatief weinig inspanning geïmplementeerd kunnen worden en veel effect hebben. Quick Wins bestaan meestal uit procedurele maatregelen. De uitvoering van Quick Wins worden bepaald na een risicoafweging door de directie op basis van specifieke organisatieomstandigheden. De lijst van Quick Wins behoort tot ongeveer 10 maatregelen te bevatten en wordt vooral bepaald door de manier van werken binnen een organisatie. Het specifieke gebruik van informatiesystemen, maar ook de reeds aanwezige mate van informatiebeveiliging, speelt daarbij een rol. Het moet maatregelen betreffen waarmee op korte termijn kan worden gestart of het zijn maatregelen die het grootste risico afdekken.

Enige voorbeelden van Quick Wins zijn: antivirusbeleid, clear desk en clear screen beleid, sleutelprocedures, toewijzen van verantwoordelijkheden en opleidingen over informatiebeveiliging.

Mogelijke Quick Wins

Belangrijke maatregelen die, wanneer deze nog niet zijn geïmplementeerd, tot Quick wins zouden moeten behoren zijn:

- *IB-Beleid (BIR, hfdst 5)*
  Betreft het borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit en incident voortgezet kunnen worden.

- *Beheer informatiebeveiligingsincidenten (BIR, hfdst 13.2)*
  Dit betreft het bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

- *Bewustwording (BIR, hfdst 8.2.2)*
  Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatig bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

- *Business Continuïty Management en Disaster Recovery Planning (BCM / DRP) (BIR hfdst 14)*
  Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

3.5 Stap 5: Uitvoering impactanalyse

De impactanalyse volgt op het uitvoeren van de GAP-analyse en de Quick Wins. De GAP-analyse brengt in kaart welke maatregelen wel of niet genomen zijn. De impactanalyse geeft antwoord op de vraag in welke volgorde maatregelen geïmplementeerd moeten gaan worden. Dit is belangrijk omdat veelal de capaciteit en budget ontbreekt om alle ontbrekende maatregelen in één keer te nemen. Afwegingen hierbij zijn:

- Geaccepteerd risico;
- Beschikbaar budget;
- Noodzakelijke volgordelijkheid tussen onderlinge maatregelen;
- Ontwikkelingen op het gebied van uitbesteding of samenwerking;
- Landelijke ontwikkelingen.

De impactanalyse concentreert zich op de capaciteitsinzet en kosten die nodig zijn om een maatregel te implementeren. De uitkomsten van de GAP-analyse en de impactanalyse is het verschil tussen de geïmplementeerde maatregelen en een overzicht van de *volgorde* van de nog te implementeren maatregelen. Met het uitvoeren van een GAP-analyse en een impactanalyse ontstaat overzicht waardoor eigenaren kunnen worden benoemd voor iedere maatregel. Een maatregel wordt in organisatie veelal alleen genomen als er een eigenaar is benoemd en aansturing plaatsvindt.

De impactanalyse kan worden ondersteund met een spreadsheet (GAP-analyse.xlsx) dat onderdeel is van de operationele producten van de BIR.

3.6 Stap 6: Management goedkeuring

Het resultaat van bovenstaande stappen moet worden afgestemd met en worden geaccordeerd door de directie van de organisatie. Het doel van deze stap is dat de directie:

- instemt met de uitkomsten van de impactanalyse en met de voorgestelde planning van implementatie;
- instemt met de te verwachten investeringen (tijd en geld);
- beslist welke maatregelen als een geaccepteerd risico niet genomen gaan worden. Voor iedere maatregel, die niet genomen gaat worden moet een gedocumenteerd management besluit worden opgesteld ter ondertekening van de directie, en;
- besluit wie eigenaar wordt van een maatregel als deze geïmplementeerd wordt. Het is aan te bevelen om een eigenaar te zoeken in de organisatie die ‘dicht bij’ de maatregel zit.

Als het uitkomst van de GAP-analyse een aanzienlijke implementatie inspanning betekent, dan is het beter om bij bovenstaande punten te focussen op hoofddoelen in plaats van specifieke maatregelen. Het is aan te bevelen om de directie hierbij als gesprekspartner te kiezen. Voor draagvlak binnen de organisatie is het bovendien belangrijk te laten zien wat al wel geïmplementeerd is.

De uitkomst van deze stap moet zijn:

- de instemming van de directie van de gekozen opzet;
- de instemming van de directie met het implementatiepad, inclusief de prioritering van de ontbrekende maatregelen en de aanwijzing van maatregeleigenaren;
- de wijze van rapporteren aan de directie betreffende de implementatie en de frequentie waarop dat moet gebeuren.

3.7 Stap 7: Maak een Informatiebeveiligingsplan

Als de directie instemming heeft verleend aan het gevoerde beleid en planvorming voor de toekomst, dan is het belangrijk dit in te bedden in de planning en control (P&C)-cyclus van de organisatie volgens de Plan, do, check, act (PDCA)-methodiek. Het inbedden in de P&C-cyclus zorgt ervoor dat informatiebeveiliging wordt verankerd in de bestaande organisatie en dat er voldoende aandacht en middelen worden aangewend om de informatiebeveiliging voortdurend bij te houden.

De basis voor een planmatige aanpak en het implementeren en borgen van informatiebeveiliging is het informatiebeveiligingsplan. Het informatiebeveiligingsplan beschrijft de uitkomst van de hiervoor uitgevoerde stappen. In het informatiebeveiligingsplan is vastgelegd welke maatregelen genomen zijn, welke maatregelen nog genomen moeten worden en welke besluiten daarover genomen zijn. Het informatiebeveiligingsplan beschrijft verder welke activiteiten (zoals een GAP-analyse of impactanalyse) elk jaar worden ingepland en vervolgens worden uitgevoerd. Het informatiebeveiligingplan wordt bij voorkeur opgesteld door de CISO of door een gelijkwaardige rol binnen de organisatie en moet op zijn minst jaarlijks worden bijgesteld (zie maatregel 15.2.1.2 van de BIR).

De rapportages over de voortgang van de uitvoering van het informatiebeveiligingsplan zorgen ervoor dat het op de agenda blijft staan en continue aandacht krijgt op verschillende niveaus in de organisatie. Bij bepaalde hoofdstukken kan worden verwezen naar externe documenten of bijlagen. Een voorbeeld hiervan is het overzicht van bedrijfsmiddelen of de functiebeschrijvingen van het beveiligingspersoneel.