TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Toelichting op GAP-analyse

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 ‘Toelichting op GAP-analyse’ 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

De GAP-analyse heeft tot doel om te kunnen controleren of en in welke mate organisaties binnen de Rijksoverheid de maatregelen uit de Baseline Informatiebeveiliging Rijksdienst hebben geïmplementeerd. Dit document betreft een toelichting op de GAP-analyse.

Doelgroep

Dit document is van belang voor de verantwoordelijke voor het uitvoeren van een GAP-analyse.

Reikwijdte

Dit document heeft voornamelijk 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)
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI:2012)
- GAP-analyse
- Informatiebeveiligingsbeleid

Inhoudsopgave

1 Toelichting op GAP-analyse

De GAP-analyse heeft tot doel om te kunnen controleren of en in welke mate organisaties binnen de Rijksoverheid de maatregelen uit de Baseline Informatiebeveiliging Rijksdienst (BIR) hebben geïmplementeerd. Een GAP-analyse is een methode om een vergelijking te maken tussen een bestaande of huidige situatie en een gewenste situatie (implementatie van de BIR-maatregelen). Dit document betreft een toelichting op de GAP-analyse ten aanzien van de BIR waarin praktische handreikingen worden geboden om de analyse uit te voeren. De GAP-analyse kan worden uitgevoerd door binnen de organisatie de vragenlijst in de spreadsheet te beantwoorden.

De GAP-analyse bevat alle maatregelen uit de Baseline Informatiebeveiliging Rijksdienst met daarbij controlevragen. De GAP-analyse tegen de baseline aanhouden is een brede onderzoeksvraag en gaat binnen de organisatie over alle processen en applicaties heen. Als bijvoorbeeld gekeken wordt naar maatregel 5.1.1.1. dan kan er binnen de organisatie een informatiebeveiligingsplan bestaan binnen de GBA informatiebeveiliging documentatieset of in de set die gemaakt is voor DigiD. Er is daarmee dan deels voldaan aan de vraag of er een informatiebeveiligingsplan is. Pas als de scope van het plan alle bedrijfsprocessen betreft, kan er van een informatiebeveiligingsplan gesproken worden in de zin van de BIR.

2 Opbouw van de GAP-analyse

De GAP-analyse kan worden uitgevoerd met het Microsoft Excel-bestand ‘GAP-analyse’. De spreadsheet bestaat uit vier tabbladen:

1. Colofon
2. BIR vragenlijst — Alle maatregelen uit de BIR, vraag ter specificatie van de maatregelen en kolommen om de vragen te beantwoorden.
3. Resultaat — Grafieken waarin het resultaat van de analyse automatisch wordt gepresenteerd.
4. Blad1 — Ruimte voor aantekeningen

2.1 Vragenlijst GAP-analyse

Vragenlijst

De kolomopbouw van de vragenlijst voor de GAP-analyse is als volgt:

- BIR-nummer — Het nummer van het BIR-hoofdstuk/paragraaf;
- Hoofdgroep — Hoofdstuk aanduiding (kan gebruikt worden voor selecteren);
- Groep — Aanduiding van groep binnen een BIR-hoofdstuk (kan gebruikt worden voor sorteren);
- Maatregel — Weergave van de maatregel uit de BIR;

- Vraag — Maatregelvraag om de beantwoording scherper te kunnen maken.

Beantwoording deel 1 GAP-analyse

- Aanwezig — Is de maatregel geïmplementeerd binnen de organisatie? Deze kolom bevat keuzes: *Gedeeltelijk*, *Ja*, *Nee*, *Niet van toepassing* en *Onbekend*;
- Vindplaats/opmerking
  1. Vindplaats — Waar is de (beschrijving van de) maatregel gevonden?
  2. Opmerking — Ruimte voor eigen tekst;
- Eigenaar — Naam van de maatregeleigenaar.

Beantwoording deel 2 Impactanalyse

- Status — Wat is de status van de maatregel?;
- Actiehouder — Wie is aanspreekbaar voor de maatregel en/of verantwoordelijk voor implementatie?;
- Wanneer gereed — Wanneer is de implementatie volgens planning gereed?;
- Geaccepteerd risico — Dit beschrijft het besluit van het management.

3 Invullen spreadsheet deel 1 GAP-analyse

Na de vragenlijst is het in het Excel-bestand mogelijk de antwoorden voor de GAP-analyse in te vullen.

De keuzes die gemaakt kunnen worden in de kolom ‘Aanwezig’ zijn als volgt:

- Ja — De maatregel is aanwezig. Vul ook de vindplaats in, wie de maatregel uitvoert, waar de maatregel is vastgelegd en overige bijzonderheden.
- Nee — Er is geen maatregel aanwezig.
- Gedeeltelijk — De maatregel is gedeeltelijk geïmplementeerd.
- Niet van toepassing — De maatregel is niet van toepassing. Vul daarbij ook in waarom de maatregel niet van toepassing is.
- Onbekend: — Het is onduidelijk of de aanwezige maatregel voldoet, er moet te lang naar gezocht worden of er liggen nog een aantal onopgeloste vraagstukken.

Schermvoorbeeld met keuzes:

Resultaat deel 1 GAP-analyse

Als de vragenlijst is beantwoord, wordt duidelijk hoe de organisatie ervoor staat ten opzichte van de BIR-implementatie. Het resultaat wordt na invullen zichtbaar op het tabblad 'Resultaat' in de bovenste figuur 'Status GAP-analyse'.

Binnen dit tabblad kan cel *B3* tot en met *B14* worden geselecteerd en door middel van de toetsaanslag *ALT-F5* een verversing van de resultaten worden bewerkstelligd. Het figuur geeft een procentuele score aan ten opzichte van het optimale resultaat.

Na het invullen van deel 1 is de GAP-analyse uitgevoerd.

4 Invullen spreadsheet deel 2 (Impactanalyse)

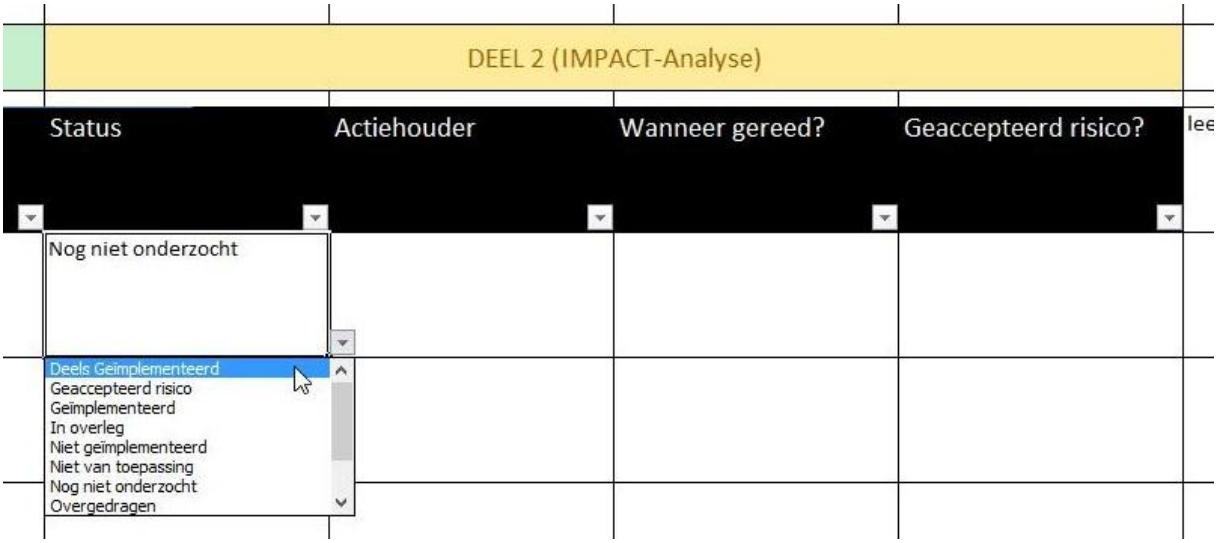
In het tweede deel van het tabblad 'Vragenlijst' van het Excel-bestand kan een impactanalyse worden uitgevoerd. De impactanalyse is een stap in de toewijzing van maatregelen waarbij het van belang is dat een reële planning wordt gemaakt. Hier worden de nog niet gevonden maatregelen of de onbekende maatregelen verder verdeeld in de volgende statussen:

- Deels geïmplementeerd — Een maatregel is deels aanwezig.
- Geaccepteerd risico — Een maatregel wordt niet genomen. Het risico dat wordt gelopen door het niet nemen van de maatregel, wordt geaccepteerd.
- Geïmplementeerd — Een maatregel is volledig geïmplementeerd.
- In overleg — Een maatregel is nog in overleg.
- Niet geïmplementeerd — De maatregel moet nog geïmplementeerd worden.
- Niet van toepassing — De maatregel is niet van toepassing.
- Nog niet onderzocht — De maatregel is nog niet onderzocht.

- Overgedragen — De maatregel is overgedragen (bijvoorbeeld aan een technische beheer organisatie).
- Te implementeren — De maatregel gaat geïmplementeerd worden binnen afzienbare tijd.

De kolommen Actiehouder'' en 'Wanneer Gereed' kunnen worden voorzien van concrete informatie over wanneer en door wie een maatregel wordt geïmplementeerd.

Schermvoorbeeld met keuzes:



Resultaat deel 2 Impactanalyse

Als deel 2 is ingevuld, kan in het tabblad 'Resultaat' bij het onderste figuur 'Status na update en management besluiten' zien welke keuzes gemaakt zijn. Binnen dit tabblad kunnen cel *B30* tot en met *B41* worden geselecteerd en door middel van de toetsaanslag *ALT-F5* een verversing van de resultaten worden bewerkstelligd. Het figuur geeft een procentuele score aan ten opzichte van het optimale resultaat.

Na het invullen van deel 2 is de Impactanalyse uitgevoerd.

5 Voortgang en rapportage

Door de beantwoording van de vragenlijst van de GAP-analyse en de Impactanalyse regelmatig te updaten, kan de voortgang van de BIR-implementatie zichtbaar worden gemaakt. Als er wijzigingen zijn in statussen kunnen deze in de loop van de implementatie van de maatregelen verwerkt worden. De verschillende rekenbladen kunnen samen gebruikt worden voor rapportages aan het management.