BIO | Baseline Informatiebeveiliging Overheid

BIO voor VIAG

Henk Wesseling (BZK)
Kees Hintzbergen (IBD)

Waar komen we vandaan?

- **Gestart ten tijde van Taskforce BID**
- **Januari 2015**
- **Werkgroep normatiek 2016**

Baselines voor informatieveiligheid
- BIR voor Rijksdienst
- IBI voor Provincies
- BIG voor Gemeentes
- BIWA voor Waterschappen

BIO Baseline Informatiebeveiliging Overheid

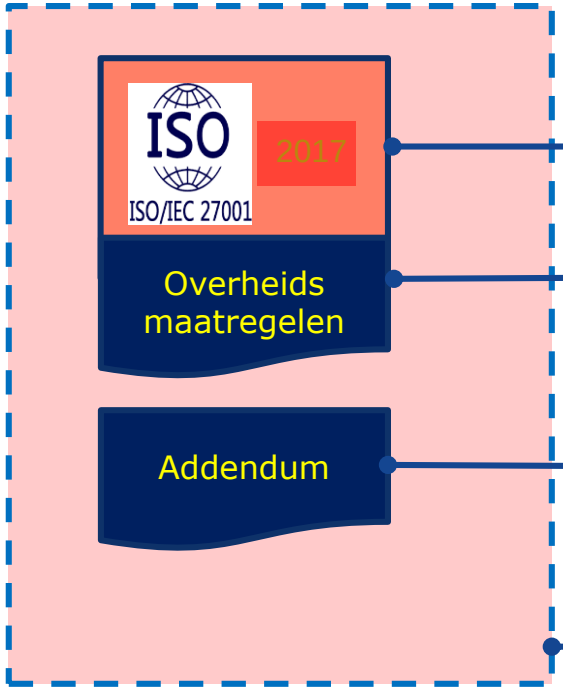
Uitgangspunten

- Hanteerbaar en efficiënt
- Risicomanagement is en blijft uitgangspunt
- De rol bepaalt wijze van verantwoording
- Belang bepaalt diepgang verantwoording
- Veilige samenwerking in ketens en bij gegevensuitwisseling
- Transitie

BIO
Waarom ook alweer?

- Urgentie op politieke niveau
- Reguliere bijstelling (evaluatie)
- Nieuwe ISO 27002:2013
- Operationele verbeteringen
- Gezamenlijke ontwikkeling
  - Gedeelde taal, samenwerken in ketens
  - Allemaal hetzelfde, basisnorm
  - In de pas lopen met de NEN/ISO en de markt!

Wat is de BIO?



ISO 27002:2017 = Pas toe of leg-uit norm

Relevante en passende maatregelen per BBN

Specifieke maatregelen, tekstblokken of verwijzingen per overheidslaag

BIO = ISO Controls + verplichte overheidsmaatregelen + risico-based maatregelen voor niet uitgewerkte controls (zijn de meeste maatregelen)

BIO en toepassing

BasisBeveiligingsNiveaus (BBN)

Niveau	
BBN 1	**Minimale beveiligingsniveau voor alle overheidssystemen**
BBN 2	**Uitgangspunt voor alle informatiesystemen**
	Vertrouwelijke informatie (max DepV, privacygevoelige, commercieel vertrouwelijk, informatie in het kader van beleidsvorming)
	Incidenten leiden tot bestuurlijke commotie
	Onzekerheid of informatie van derden open is
	Veiligheid van andere systemen wordt beïnvloed
BBN 3	**BBN2 + weerstand tegen statelijke actoren of vergelijkbare dreigers nodig (o.b.v. vertrouwelijkheid)**
	Wordt nog nader uitgewerkt; op basis van VIR-BI en andere relevante regelgeving aangevuld met het NAVO-verdrag voor beveiliging van informatie

Basisbeveiligingsniveaus
Beschikbaarheid, Integriteit en Vertrouwelijkheid

- BBN1
  - Wat mag minimaal verwacht worden?

→ BBN2
  - Valt de maatregel onder goed huisvaderschap?

- BBN3
  - Gerubriceerde informatie (DepV) & weerstand geavanceerde dreigingen

B=L – I=L – V=L

B=M – I=M – V=M

B=M – I=M – V=H

Schaal: Laag, Midden, Hoog

BasisBeveiligingsNiveaus (BBN)

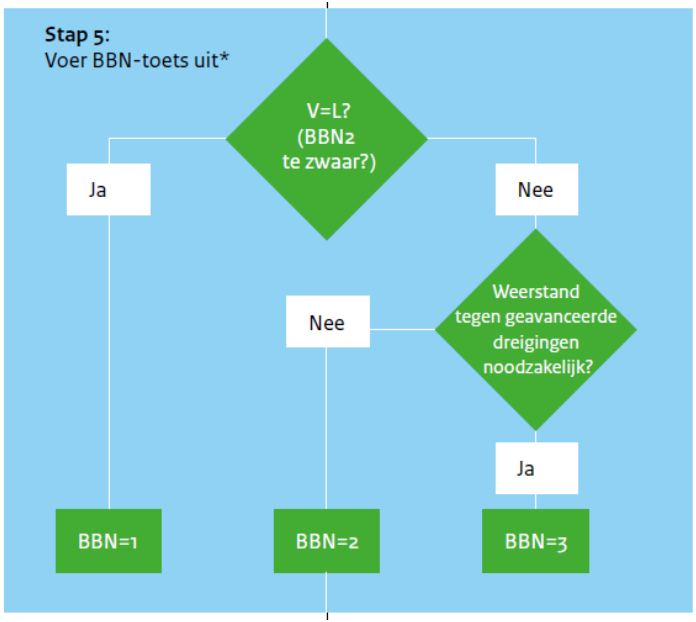
BBN3	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot

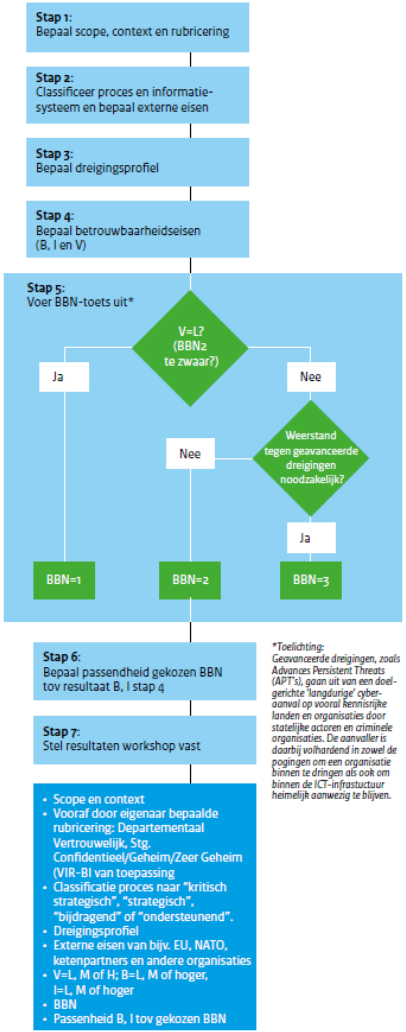
BBN2	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot

BBN1	
Beschikbaarheid = Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van het ministerie of uitvoeringsorganisatie; leidt nog niet uit het niet

Vertrouwelijkheid = Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de Rijksdienst, waar o.a. vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens, kan leiden tot: - politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of - diplomatieke schade te herstellen door ambtelijke opschaling; of - financiële gevolgen: niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of - verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of - bindende aanwijzing van de AP in verband met schending van de privacy; of - directe imagoschade, bijvoorbeeld door negatieve publiciteit.

QIS & BBN-toets





Controls & overheidsmaatregelen

8.3 Behandelen van media

Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

8.3.1	**1**	**Beheer van verwijderbare media** Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Proceseigenaar Dienstenleverancier
		Handreiking: Mobiele-gegevensdragers	
8.3.1.1	1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a).	
8.3.1.2	2	De wijze waarop vertrouwelijk of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het NBV.	
8.3.2	**2**	**Verwijderen van media** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Dienstenleverancier
		Handreiking: Afvoer-ICT-middelen	
8.3.2.1	2	Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Verwijdering vindt plaats op een veilige manier, bijv. door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO27002 – implementatierichtlijn 8.3.2.a)	
8.3.2.2	2	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	
8.3.3	**2**	**Media fysiek overdragen** Media die informatie bevatten, behoren te worden beschermd tegen	Secretaris/ algemeen directeur

Controls, overheidsmaatregelen en handreikingen

Fysieke beveiliging en beveiliging van de omgeving

Algemene handreiking: Toegangsbeleid

11.1 Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

11.1.1	**1**	**Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	Secretaris/algemeen directeur
11.1.1.1	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	
11.1.2	**1**	**Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Secretaris/algemeen directeur
11.1.2.1	2	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	
		Handreiking: Protocol uitwisseling van persoons gerelateerde beveiligingsinformatie	
11.1.3	**1**	**Kantoren, ruimten en faciliteiten beveiligen**	Proceseigenaar

BIO Baseline Informatiebeveiliging Overheid

BBN3

Kader voor weerbaarheid DepV tegen statelijke actoren

Basis NATO Restricted, D48

Personeel

9.1.1.1	Medewerkers krijgen uitsluitend toegang tot BBN3 informatie indien voor zover de noodzaak tot kennisname van deze informatie bestaat.	SG Proceseigenaar
7.1.2.2	Medewerkers worden geïnformeerd over hun verantwoordelijkheden met betrekking tot BBN3 informatie	SG Proceseigenaar
7.2.2.4	Medewerkers worden geïnstrueerd over de wijze van omgang met BBN3 informatie.	SG Proceseigenaar
7.1.2.3	Medewerkers tekenen een verklaring dat zij hun verantwoordelijkheden begrijpen, geïnstrueerd zijn over de wijze van omgang met BBN3 informatie en bekend zijn met de mogelijke consequenties van (opzettelijk) nalatig handelen. Deze verklaring wordt opgenomen in het personeelsdossier van de medewerker.	SG Proceseigenaar
7.2.2.5	Medewerkers worden initieel en periodiek bewust gemaakt van de noodzaak om te voldoen aan beveiligingsvoorschriften en om te handelen in het belang van de veiligheid.	SG Proceseigenaar
7.2.2.6	Medewerkers worden initieel en periodiek bewust gemaakt van de onderkende dreigingen waaronder statelijke actoren. Medewerkers maken onmiddellijk melding bij de beveiligingsambtenaar of beveiligingscoördinator bij elke benadering of omstandigheid die zij als verdacht of ongewoon beschouwen.	SG Proceseigenaar
7.2.1.2	Medewerkers krijgen uitsluitend toegang tot BBN3 informatie indien voorwaarden van 7.2.2 is voldaan.	SG Proceseigenaar
7.2.2.7	Medewerkers worden er periodiek aan herinnerd dat zij BBN3 informatie uitsluitend delen met hen die een noodzaak hebben tot kennisname van deze informatie.	SG Proceseigenaar
7.1.1.2	Medewerkers waarbij gerede twijfel over loyaliteit en/of betrouwbaarheid bestaat, krijgen geen toegang tot BBN3 informatie.	SG Proceseigenaar
7.3.1.1	Bij vertrek uit een functie waarin kennis is genomen van BBN3 informatie worden medewerkers aantoonbaar op de hoogte gesteld van hun verantwoordelijkheden ten aanzien van de geheimhouding van deze informatie. Dit wordt opgenomen in het personeelsdossier van de medewerker.	SG Proceseigenaar

Fysieke beveiliging


maintenance
planned

BIO Baseline Informatiebeveiliging Overheid