INFORMATIE
BEVEILIGINGS
DIENST

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en ENSIA

26 maart 2015

Jule Hintzbergen, IBD

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE
BEVEILIGINGS
DIENST

Agenda

- ✓ De Informatiebeveiligingsdienst voor gemeenten (IBD)
- ✓ De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- ✓ Eenduidige Normatiek Single Information Audit (ENSIA)
- ✓ Hoe kunnen gemeenten hier nu al op inspelen?

INFORMATIE BEVEILIGINGS DIENST

Wat is er aan de hand?

Vier gemeenten plat door virusbesmetting - update

Gepubliceerd: Donderdag 9 augu
Auteur: René Schoemaker

De computersystem
door een

elt ook clientcertificate

in beveiliging data van

Datadelen bij gemeenten brengt privacy in gevaar

30 okt. 2013 door René Schoemaker

Nieuws - De privacy van burgers komt in gevaar als de gemeenten allerlei privégegevens van inwoners gaat . Het College Bescherming brandbrief

Gepubliceerd
Auteur

emeenten falen erns
urgers

11 n
Nie
pe

een onderzoek n
geconstateerd d
heeft voldoende
procent voldoet

16 maart 2015

Steeds meer besmettingen met cryptoware in Nederland

Het aantal

eten
t

17 maart 2015

Ransomware hindert voorbereiding verkiezingen Lochem

Door een infectie met 'ransomware', schadelijke software die computers onbruikbaar maakt, zijn veel documenten van de gemeente Lochem geblokkeerd. De infectie dreigde ook een probleem voor de verkiezingen te vormen, maar inmiddels zijn de noodzakelijke systemen veiliggesteld.

r identiteits

et slachtoffers van
liteit te make
laties

g op duize

10 feb. 2014

Nieuws - De gebruiken nc doen dat ove gaat om hond

Duizenden, wel computers bij lo na 8 april nog W

derlandse gemeenten do
5 juli 2013, 15:47 door Redactie, 3 reacties

sche spionnen zijn zeer actief in Nederlar
arbuiten hebben voorzien. Dat zegt het pl
heidsdienst (AIVD) Marc K

rcriminelen kapen 150.000 Nederlandse
Redactie, 11 reacties

heid zaten, hebben zo'n 150.000 Nederlandse
ieerde campagne die van

iten werker
n vooraf w
en.

vereniging Nederlandse Gemeenten (VNG
Security Center (NCSC) is er geen flauw be
omvang van mogelijke problemen met
besturingssyste

INFORMATIE
BEVEILIGINGS
DIENST

Informatieveiligheid

- Het gaat om het vergroten van de weerbaarheid van gemeenten tegen ICT-verstoringen en –dreigingen.

- Dat start bij vergroten van bewustzijn van en de sturing op informatiebeveiliging, ook bij bestuurders.

- Implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG):
    - Strategische en Tactische variant van de BIG gereed op IBD-community en -website (Wat)
    - Producten Operationele variant (Hoe)
    - www.ibdgemeenten.nl

Doelen van de IBD

1 BEWUSTZIJN

2 INCIDENTEN

3 PROJECTEN

De IBD-dienstverlening strekt verder…

De IBD-dienstverlening strekt verder…

- **Helpdesk van de IBD**

  De IBD heeft een helpdesk, waar gemeenten al hun vragen over informatiebeveiliging kunnen stellen.

- **Website en Community**

  Een website en community waar gemeenten kennis en ervaring op informatiebeveiligingsvlak kunnen uitwisselen.

- **Leveranciersonafhankelijk**

  De IBD is leveranciersonafhankelijk en ondersteunt een ‘level playing field’ voor leveranciers actief in het gemeentelijk domein

Beschikbare kennis, producten en diensten van de IBD

- Incidentdetectie en -coördinatie
  - I.s.m het Nationaal Cyber Security Centrum (NCSC)- NRN
  - I.s.m. leveranciers
- Bewustwording
  - Regiobijeenkomsten
  - Presentaties, workshops, congressen
- Projecten
  - Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - ICT-Beveiligingsassessment DigiD
  - Verlagen van de audit-last (Taskforce BID, project ENSIA)
  - Ondersteunen projecten binnen KING
    - Decentralisaties
    - GEMeentelijke Model Architectuur (GEMMA)

INFORMATIE
BEVEILIGINGS
DIENST

Incident detectie en coördinatie

- Steeds meer gemeenten weten de IBD te vinden.
- Waar bellen gemeenten over?
  - Advies BIG
  - Incidenten
  - Aansluiten IBD
  - Advies ICT-vraagstukken
  - DigiD
  - Preventie
  - Privacy
  - Overige vragen

INFORMATIE
BEVEILIGINGS
DIENST

De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

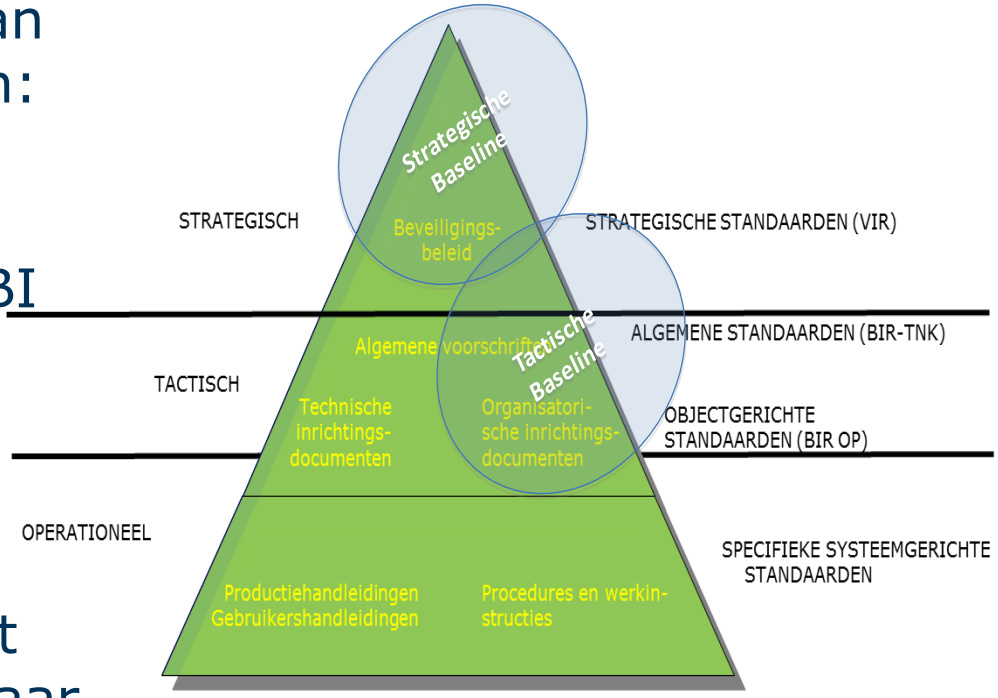
BIG: Doel

1. Gemeenten op een vergelijkbare manier efficiënt laten werken met informatieveiligheid.
2. De BIG is een hulpmiddel voor gemeenten om aan alle eisen op het gebied van informatieveiligheid te kunnen voldoen.
3. **De BIG vermindert de auditlast bij gemeenten.**
4. Gemeenten zijn met de BIG een aantoonbaar betrouwbare partner.

INFORMATIE BEVEILIGINGS DIENST

BIG: Uitgangspunten

- Gekozen voor een optimale aansluiting bij de wereld van geaccepteerde standaarden:
  - Bijvoorbeeld: ISO 27001:2005, ISO 27002:2007, VIR, VIR-BI en BIR.
- Basis beveiligingsniveau gebaseerd op normen en wetgeving:
  - Inclusief mapping vanuit normen en wetgeving naar de maatregelen.



Strategische variant BIG

- Scope:
  - Bedrijfsvoeringsprocessen en onderliggende informatiesystemen en informatie van de gemeente
- Uitgangspunten:
  - B&W integraal verantwoordelijk
  - Basisniveau Departementaal Vertrouwelijk
  - Schengen-principe gehanteerd
  - Gerichte risicoafweging voor afwijkende situaties of wanneer een hoger beveiligingsniveau nodig is
- Randvoorwaarden:
  - Rol management
  - Risicomanagement
  - Bewustwording
  - Integrale aanpak

Tactische variant BIG

- Indeling als internationale beveiligingsnorm ISO/IEC 27002:2007
- Basisset aan maatregelen die voor alle gemeenten geldt
- Bevat maatregelen uit aansluitnormen van de basisregistraties:
  - GBA / BRP
  - PUN
  - BAG
  - SUWI wet
  - WBP en laatste richtsnoeren
- Randvoorwaarden, stappenplan

Operationele variant BIG

- Opgebouwd uit aanvullend beleid, procedures, handreikingen, aanwijzingen en patronen
- Geven vooral antwoord op het ‘hoe’
  - detaillering, invulling maatregelen
- Producten:
  - Prioriteit: bepaald middels uitvraag
  - Aantal: 50+ producten
  - Kwaliteitsborging: review door gemeenten

Voordelen van de BIG

- **Gemeenten hebben nu allemaal hetzelfde kader.**
- Bewustwording neemt toe bij gemeenten en daarmee ook de vragen.
- Gemeenten zijn meer in control:
  - gemeenten worden volwassen opdrachtgevers qua beveiliging, en dat dwingt leveranciers tot volwassen opdrachtnemerschap.
- Duidelijkheid voor leveranciers:
  - geen verschillende beveiligingseisen van verschillende gemeenten.
  - Onderscheidende factor voor leveranciers.
- Security by design

Hoofdstappen implementatie BIG

- Aanstellen IBF / CISO
- Prioriteren (volledige BIG of delen van de BIG)
- GAP-analyse (eventueel alleen essentiële systemen)
- Impactanalyse
- Selecteren maatregelen
- Informatiebeveiligingsplan
- Voortgangsrapportage
- Controle / audit
- Verantwoording

ENSIA

- Eenduidige
- Normatiek
- Single
- Information
- Audit

Organisaties binnen de diverse overheidslagen zijn net als andere organisaties verplicht om jaarlijks audits uit te laten voeren. Doel van deze audits is het meten en/of controleren van de informatiebeveiliging. Een auditopgave vraagt veel van een gemeente; van extra inspanning tot aan logistieke en budgettaire problemen. Het doel van ENSIA is om te komen tot een vermindering van de verantwoordings- en auditinspanning bij de overheden, waaronder gemeenten.

ENSIA

- Waar komen we vandaan?
- Waar willen we naartoe?
- Coördinatie is een randvoorwaarde
- ENSIA is een eerste stap
- ENSIA 2015

INFORMATIE
BEVEILIGINGS
DIENST

Waar komen we vandaan?

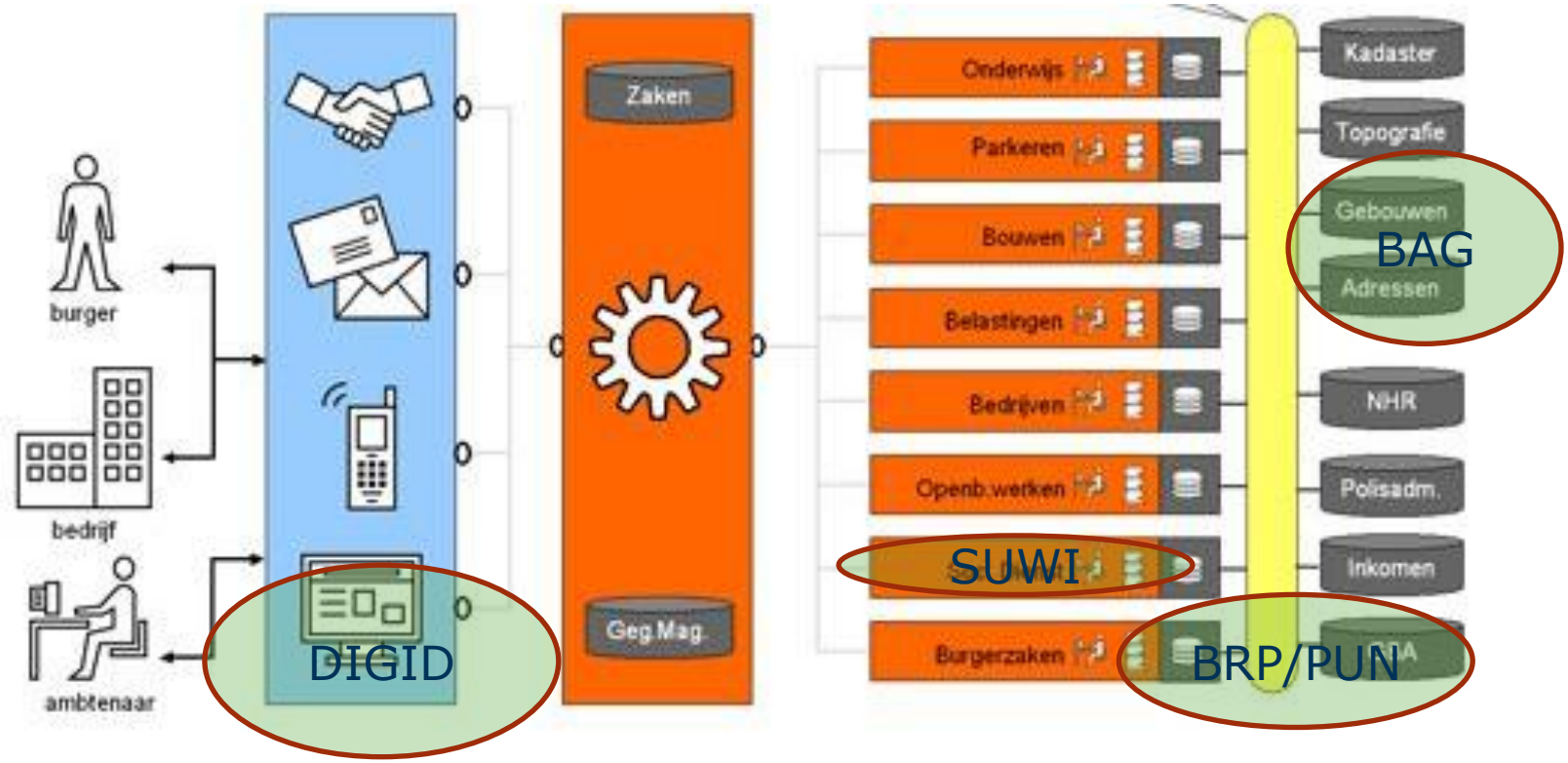
- De huidige verschillende verantwoordingsverplichtingen zijn verzuild. Dit komt voort uit de tijd waarin de verantwoordingsverplichtingen zijn ingericht.
- Gemeenten werkten met verschillende systemen die los van elkaar functioneerden. Gemeenten zijn echter anders (slimmer) gaan werken.
- Informatie stroomt steeds meer door de hele organisatie (via bijvoorbeeld zaaksystemen).
- Met het omarmen van de BIG door het aannemen van de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente', streven gemeenten naar een integrale aanpak van informatiebeveiliging.
- De verschillende verantwoordingsverplichtingen passen daarom niet meer bij de huidige manier van werken.

De huidige werkwijze heeft nadelen

- Effectiviteit:
  - Door de verzuilde verantwoording, wordt een integrale aanpak van informatieveiligheid tegengewerkt. Gemeenten worden immers gestimuleerd dit thema ‘verzuild’ op te pakken, terwijl een integrale aanpak nodig is om dit goed te doen. Dit komt informatieveiligheid bij gemeenten niet ten goede.
- Doelmatigheid:
  - De verschillende verantwoordingsverplichtingen overlappen (deels), dit is inefficiënt. Gemeenten ervaren dit als een onnodig hoge last.

INFORMATIE
BEVEILIGINGS
DIENST

Verantwoordingen in GEMMA architectuur

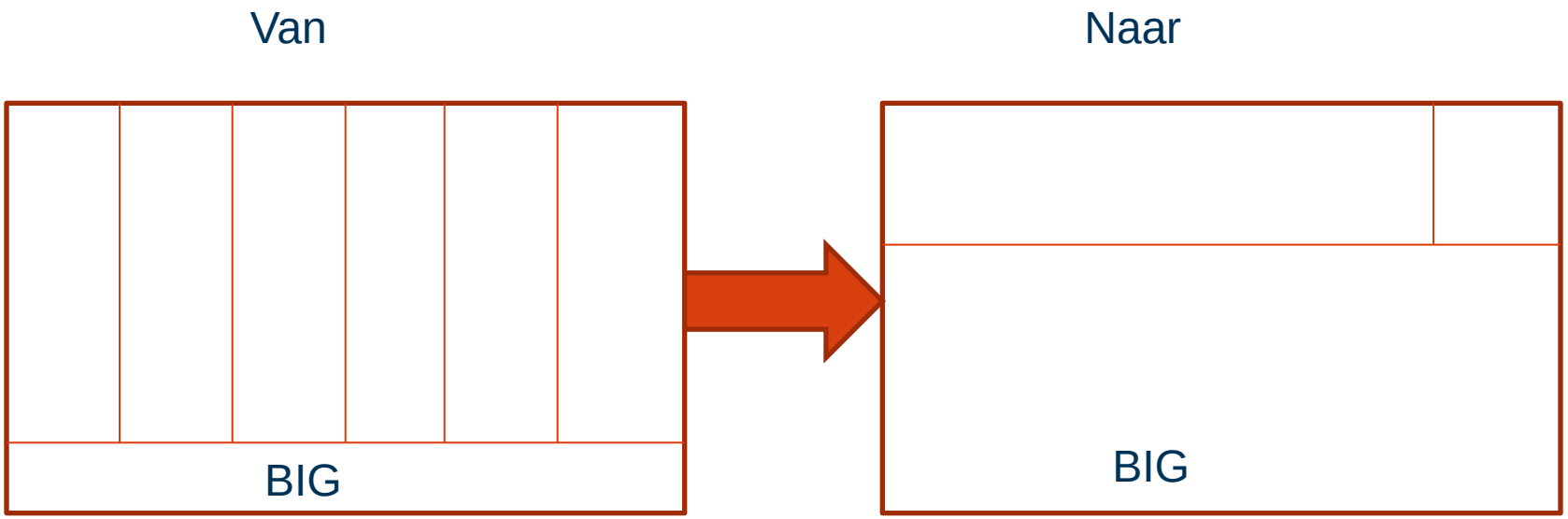


Waar willen we naartoe?

- Het streven is om één integrale verantwoording over de informatievoorziening van gemeenten te doen.
- Het ideaalplaatje voor de toekomst zou een systeem moeten zijn dat rapporteert over het compliant zijn aan bedrijfsregels waartoe ook beveiligingsmaatregelen behoren.
- De eerste stap naar dit ideaalbeeld, is ENSIA: het integreren van alle verantwoordings-verplichtingen over informatiebeveiliging in één verantwoording vanuit de BIG.

INFORMATIE
BEVEILIGINGS
DIENST

Toetsen en verantwoorden



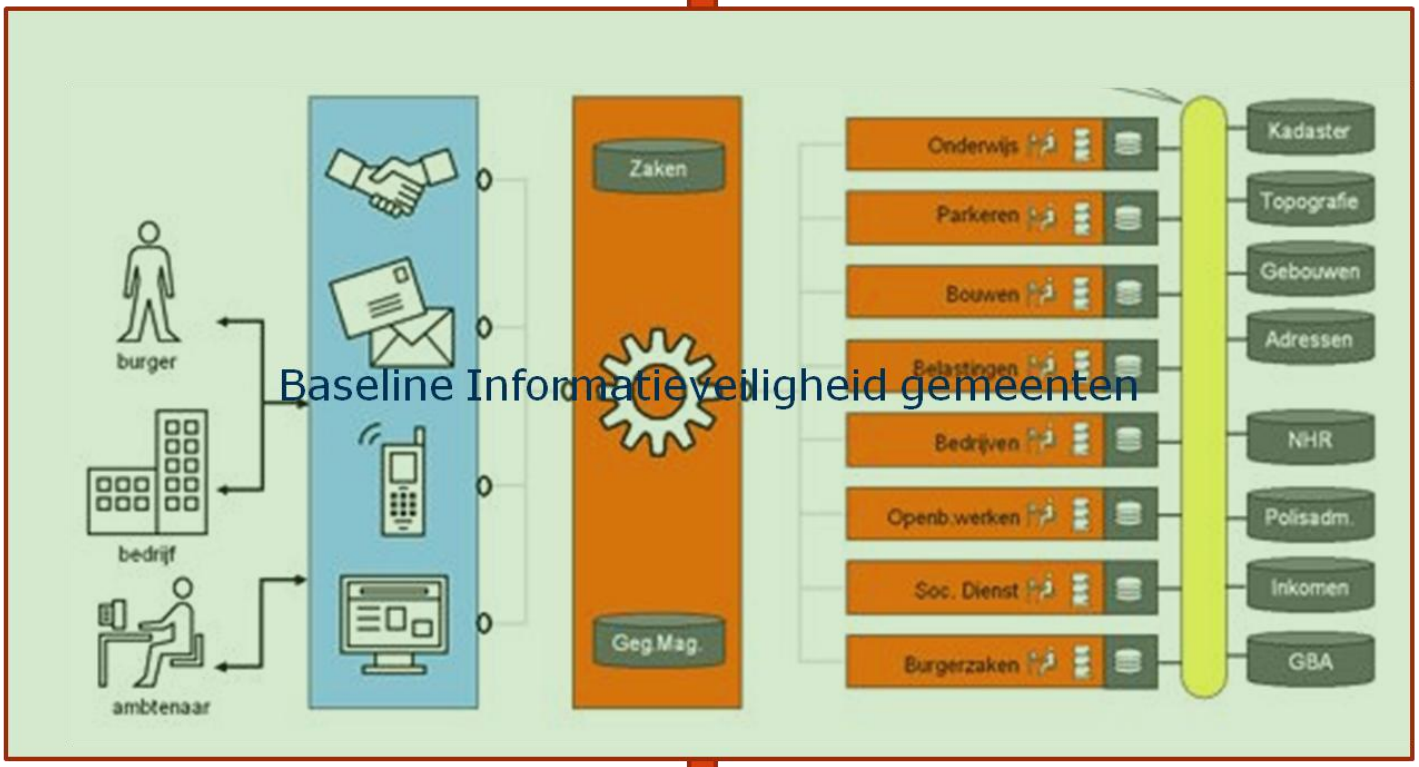
Heterogene verantwoording

Homogene verantwoording

INFORMATIE BEVEILIGINGS DIENST

DIGID SUWI EAID BRP/PUN

Verantwoording tbv beheerstoezicht



Baseline Informatieveiligheid gemeenten

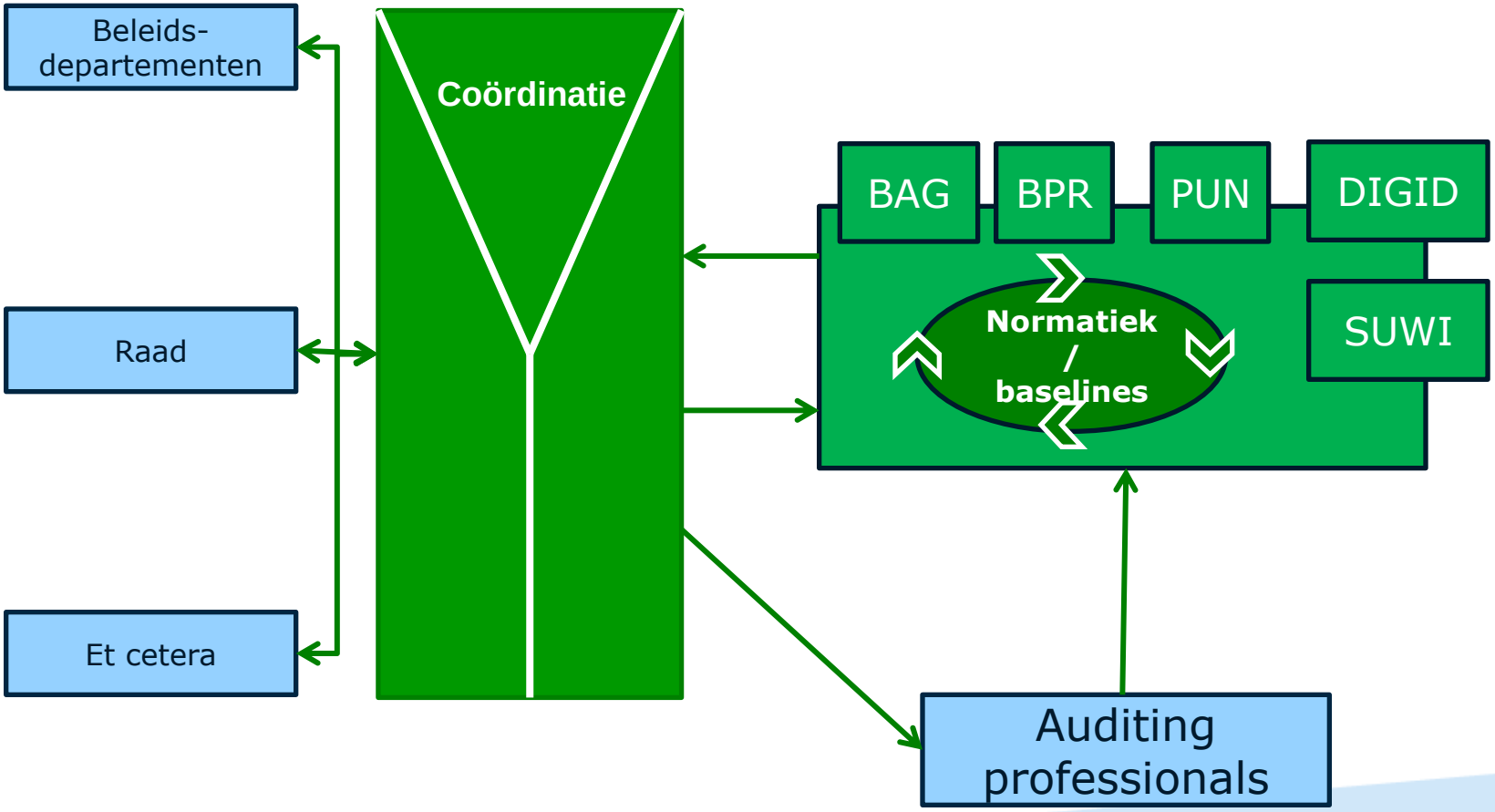
Verantwoording aan lokaal bestuur

Dit vraagt om

- Bereidheid van gemeenten om verantwoording over informatieveiligheid in te richten:
  - daadwerkelijke implementatie BIG;
  - Ingericht proces van systematisch verantwoorden.
- Bereidheid van departementen om bestaande verantwoordingen kritisch te beschouwen:
  - Is de bestaande methodiek relevant in het licht van de BIG?
  - Is de gevraagde informatie relevant vanuit beleidsperspectief?
  - Waar noodzakelijk en zinnig aanpassen wet- en regelgeving?
- Een groeipad:
  - Met als eerste stap ENSIA informatieveiligheid.

INFORMATIE
BEVEILIGINGS
DIENST

Coördinatie is een randvoorwaarde



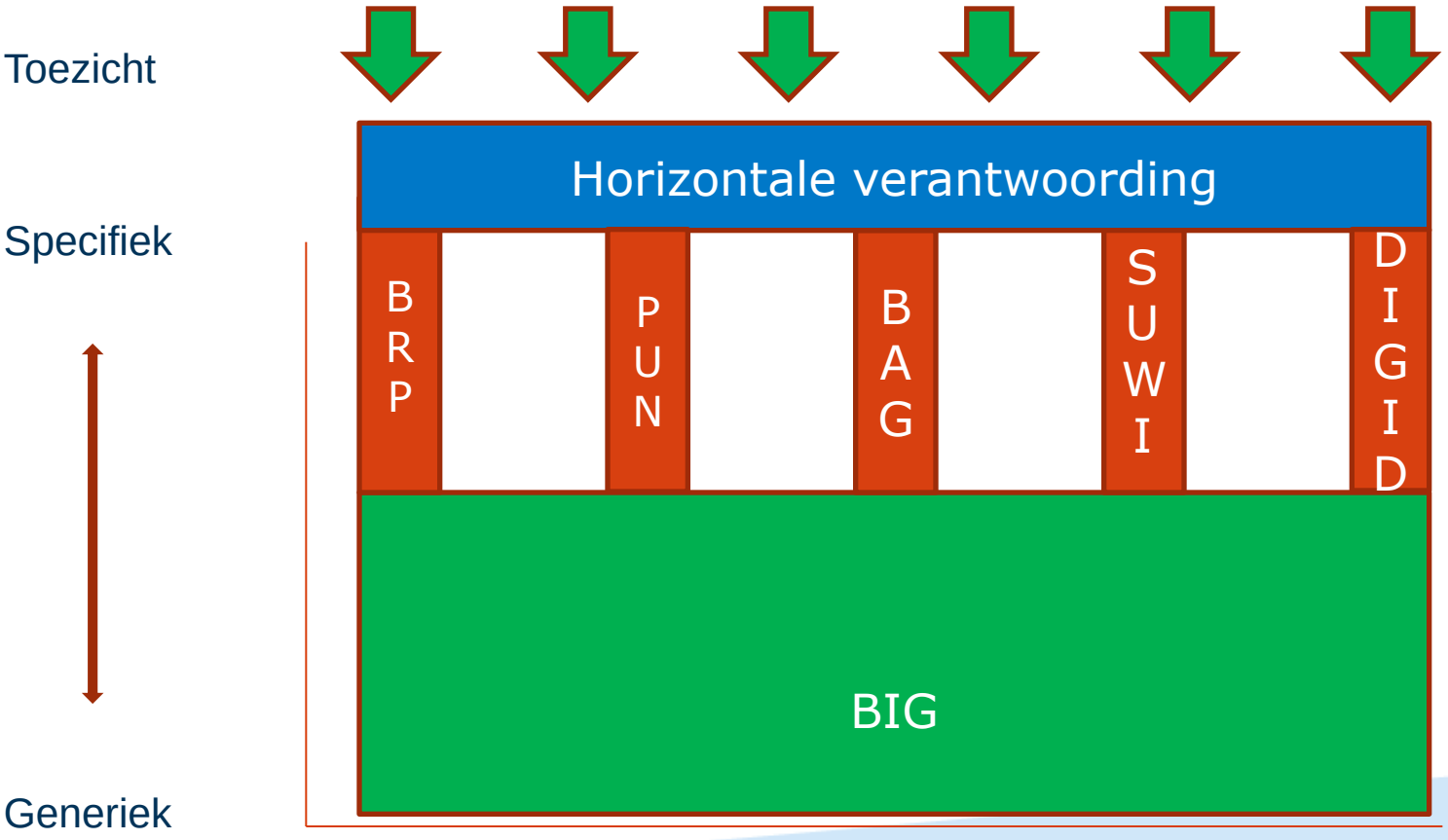
INFORMATIE
BEVEILIGINGS
DIENST

Coördinatie van:

- Gemeentelijk verantwoordingsproces:
  - van informatieveiligheid,
  - naar informatievoorziening.
- Inrichting van audits:
  - Van ‘extern toezicht/audit,
  - Naar ‘self-assessment’ met gedoseerd extern toezicht/audit.
- Gewenste ‘horizontale’ verantwoording:
  - Van bestaande gedetailleerde verantwoording (deels wettelijk),
  - Naar beleidstoezicht op basis van verantwoording over gemeentelijke informatievoorziening.

INFORMATIE
BEVEILIGINGS
DIENST

Uiteindelijk ENSIA?



De eerste stap ENSIA-systematiek

- Inrichting zowel horizontale als verticale verantwoording
  - Horizontaal:
    - Self-assessment, centraal beheerde vragenlijst
    - In control statement
    - P&C-cyclus
    - Controle op verantwoording (nader te bepalen)
  - Verticaal
    - Steunt op horizontaal
    - Informatiedeling van resultaten self-assessments voor zover van belang voor beleidstaken, peer review, etc.
    - Beheer nader te bepalen
  - Verdere verantwoording en specifieke uitvragen rond informatieveiligheid in overleg met BZK, stroomlijnen verantwoordingslast staat voorop

ENSIA-pilot 2014

- Die pilot heeft zich gericht op het ondersteunen van het ICS (in control statement van het gemeentebestuur in het jaarverslag.
- De onderbouwing van dat ICS wordt gevormd door het assessment ENSIA.
- De pilot is uitgevoerd met de medewerking van negen gemeenten en de direct betrokken beleidsdepartementen.
- De pilot werd door de betrokken gemeenten positief beoordeeld.

ENSIA vervolg

- Project gaat door onder de vlag van BZK.
- De IBD blijft betrokken.
- Twee plannen
  - Het eerste plan geeft richting aan de uitrol van ENSIA gericht op informatieveiligheid in het gemeentelijk domein daarbij voortbouwen op de pilot. Nog voor de zomer vindt besluitvorming hierover plaats.
  - Het tweede plan richt zich op de mogelijke verbreding van de ENSIA-aanpak buiten de gemeentelijke informatieveiligheid.
    - Verbreding van ENSIA-aanpak provincies en waterschappen.
    - Andere thema's dan informatieveiligheid binnen de informatiehuishouding.

Hoe kunnen gemeenten hier nu al op inspelen?

- Inrichten verantwoording binnen de gemeente
  - Horizontaal
  - Verticaal
- Grote gemeenten
  - Werken naar in control statement per afdeling, samenvatting gemeentebreed
- Kleine gemeenten
  - In control statement gemeentebreed

INFORMATIE BEVEILIGINGS DIENST

Aandachtspunten: Hergebruik van maatregelen?

- Wat goed is, nu niet stukmaken
- Zijn de audits / zelfassessments doorstaan dan is het goed.
- Kopieer op termijn datgene wat er voor de GBA, PUN en SUWI al is binnen de gemeente, dus maak geschikte procedures en beleid ‘algemeen’.
- Haal de dubbelingen bij de processen weg zodat specifieke wettelijke eisen wel blijven bestaan en verantwoord worden.

INFORMATIE BEVEILIGINGS DIENST

Voorbeeld prioriteiten om aan te pakken

- BIG Toppers:
  - ISMS
  - Beleid
  - Incidentmanagement
  - Hardening
  - Patchmanagement
  - Changemanagement
  - Continuïteit
  - Back-up
  - Logging en logging controle
  - IAM
    - accountmanagement en
    - usermanagement centraal

- Processen / systemen:
  - Decentralisaties
  - Financiën

  - 3D-systemen
  - Financieel systeem
  - Dienstverlening zaaksysteem

INFORMATIE
BEVEILIGINGS
DIENST

Vragen?

info@IBDgemeenten.nl

Bezoek ook www.ibdgemeenten.nl

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

Aanvullingen als er tijd over is

INFORMATIE
BEVEILIGINGS
DIENST

BIG-instrumenten, een nadere uitleg

Versie 1.5

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

Instrumenten

- 0-meting
- Impactanalyse
- Baselinetoets
- Diepgaande Risicoanalyse
- Privacy Impact Assessment (PIA)

Instrumenten: GAP-analyse en impactanalyse

- De GAP-analyse is bedoeld om te toetsen in hoeverre de gemeente of een proces/informatiesysteem voldoet aan de BIG.
- De Impactanalyse is bedoeld om de ontbrekende maatregelen ten opzichte van de BIG toe te delen en te plannen,
- dus ook richting leveranciers van informatiesystemen.
- Voorbeeld verantwoordelijken toegevoegd
- Biedt mogelijkheid om te plannen, bijvoorbeeld groepen maatregelen per jaar
- Output voor informatiebeveiligingsplan en verklaring van toepasselijkheid (in control statement)

Instrumenten: baselinetoets

B = Beschikbaarheid
I = Intergriteit
V = Vertrouwelijkheid
P = Privacy

- Zo eenvoudig mogelijk opgezet
- Toetsen door middel van BIV en P vragen
- Tweeledig doel:
  - Een bestaand systeem te toetsen of de baseline voldoende beschermd
  - Toetsen van een nieuw proces/informatiesysteem of de baseline voldoende is of dat er meer nodig is.
- Resultaat:
  - BIG is voldoende
  - BIG is niet voldoende, voer diepgaande risicoanalyse uit en voer eventueel een PIA uit
  - Geeft inzicht in BIV+P ten opzichte van de BIG

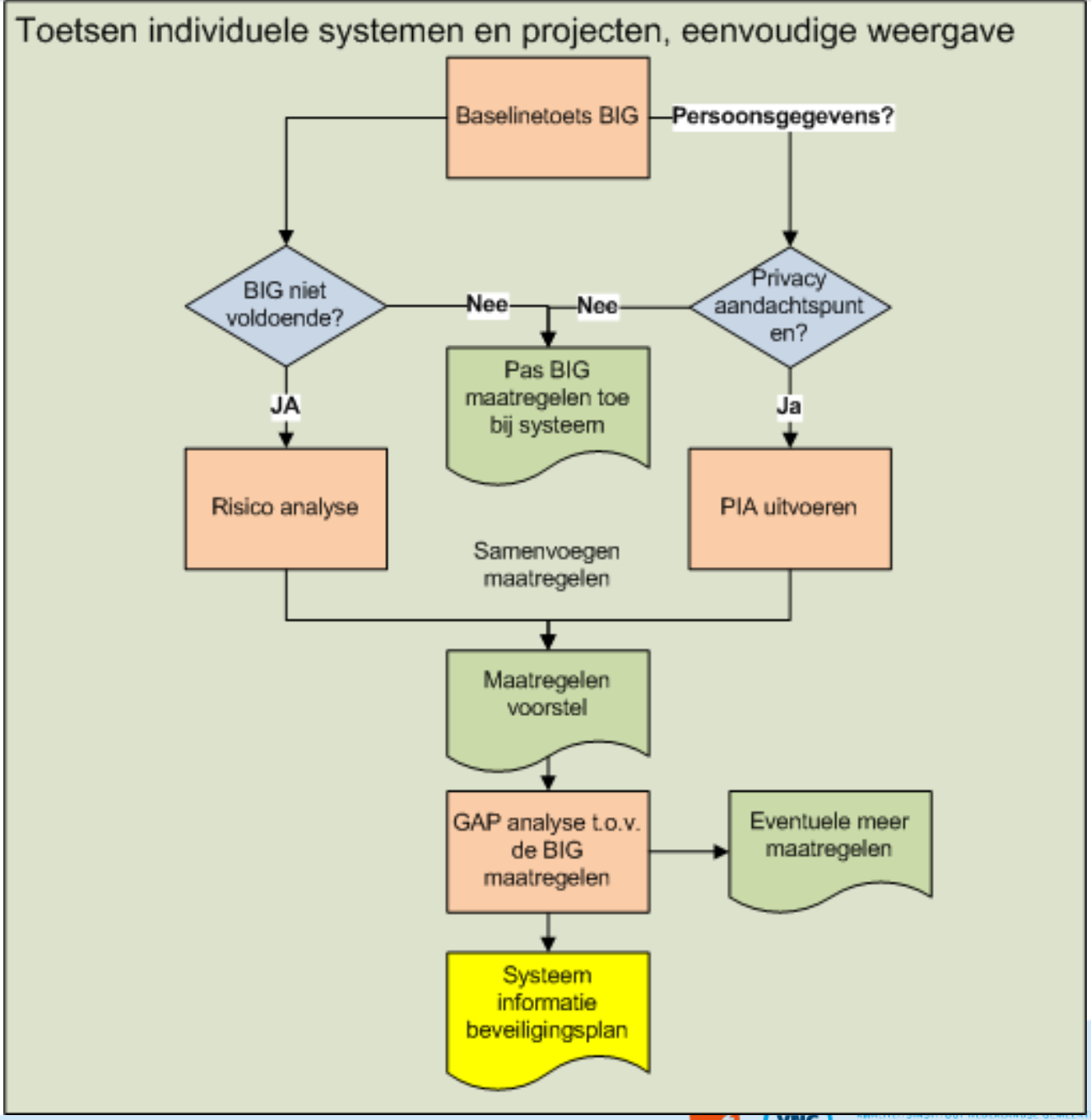
Instrumenten: diepgaande risicoanalyse

- Vervolg op de baselinetoets
- Kan leiden tot aanvullende controls en maatregelen bovenop de BIG-controls en maatregelen
- Minimaal tijd benodigd van proceseigenaar, systeembeheerders et cetera
- In korte tijd te doen
- Mogelijk focus op BIV+P uit baselinetoets

Instrumenten: PIA

- Genoemd in de Privacy Richtsnoeren van Cbp
- Indien de P-vragen uit de baselinetoets aanleiding geven tot een PIA.
- Vragenlijst gericht op privacyvraagstukken.
- Eenvoudige rapportage.
- Leidt tot eventueel aanvullende beveiligings-/privacy-maatregelen
- Toekomst mogelijk verplicht (NL en EU-wetgeving)
- Aantonen dat over privacy is nagedacht!

Stappenplan gemeenten



INFORMATIE
BEVEILIGINGS
DIENST

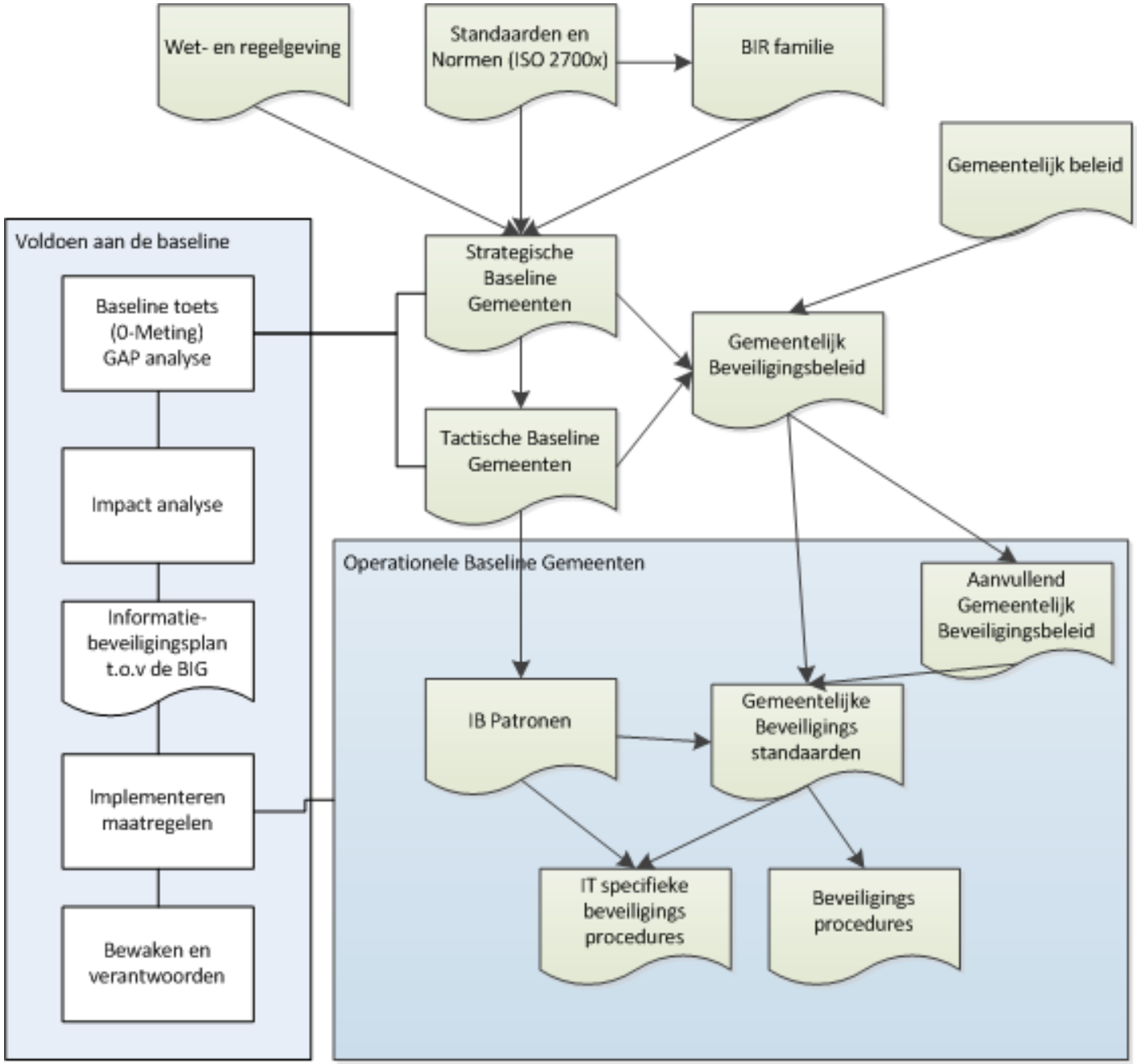
Enkele praatplaten

Versie 1.5

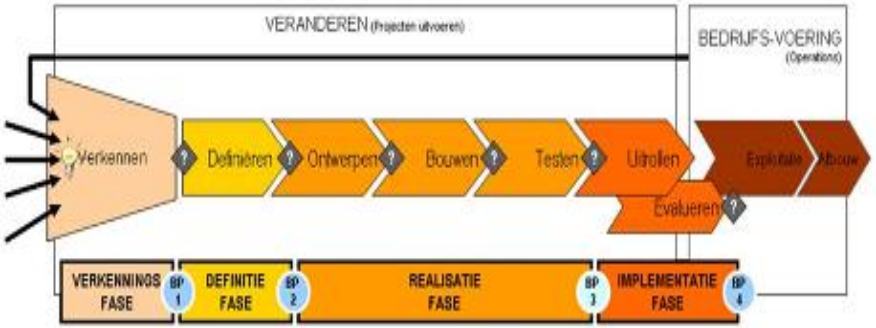
KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN
VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE BEVEILIGINGS DIENST

Samenhang producten



Informatiebeveiliging en Privacy in IV-projecten



Verkenning

Definitie

Realisatiefase

Baselintetoets Informatiebeveiliging en Privacy

B ≤ 8
I ≤ 14
V ≤ 14

B > 8
I > 14
V > 14
P > 3

Diepgaande Risico Analyse en/of Privacy Impact Analyse

Maatregelen Baseline

Maatregelen Baseline +

Ontwerpen
Functioneel Ontwerp
Technisch Ontwerp
Beheer en Governance Ontwerp

Inkoop
Programma van Eisen

Contracten
Leveranciers
Convenant gebruikers
SLA
DAP

Privacy
Functionaris gegevensbescherming
Transparantiedocument
Bewerkersovereenkomst

Projectaudits

Testen
Testplan
Pentest
Functioneel
Technisch

Werkinstructies
Gebruikers
Functioneel beheer
Technisch/applicatie beheer

INFORMATIE
BEVEILIGINGS
DIENST

Overview Baselinetoets en Risicoanalyse Informatiebeveiliging

Versie 1.5

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

INFORMATIE BEVEILIGINGS DIENST

Overzicht Baselinetoets

STAP	1. Intakegesprek voeren	2. Analyseren proces	3. Vaststellen betrouwbaar-heidseisen BIV-P
SETTING	Gesprek met opdrachtgever, meestal projectleider	Afstemming met proceseigenaar	Terugkoppeling aan opdrachtgever
WERKWIJZE	In kaart brengen scope, diepgang, planning, brondocumenten, respondenten etc.	In kaart brengen procesomgeving, Samenhang, inhoud en eisen	Consolideren van de eisen, bepalen vervolgstappen
TOOLS	Baselinetoets	Generiek Procesmodel Waarderings-tabellen	Schema vervolgstappen
RESULTAAT	Plan van Aanpak / planning voorbereiding analyse	Procesmodel en eerste beeld van de eisen	Geconsolideerd beeld van de eisen Inzicht in de Vervolgstappen
UREN INDICATIEF	1 uur opdrachtgever 10 uur voorbereiding en uitwerken	4 uur opdrachtgever 8 uur uitwerken (per proces)	1 uur opdrachtgever

Baselinetoets, tijd benodigd van de opdrachtgever

- Uitgangspunt: scope is één systeem
- Baselinetoets lijkt op A-analyse / BIA-aanpak
  - Sessie/interview met proceseigenaar: 3 à 4 uur
  - Terugkoppeling 1 uur
- Totaal dus zo'n 5 uur tijd benodigd van opdrachtgever
- Overige tijd is voorbereiding en uitwerking door analist

INFORMATIE BEVEILIGINGS DIENST

Overview diepgaande risicoanalyse

Door eigenaar, niet in scope

STAP	4. Analyseren Informatie-systeem	5. Analyseren bedreigingen	6. Vaststellen maatregeldoel-stellingen	7. Opstellen Plan
SETTING	Gesprek met systeemeigenaar, meestal functioneel beheerder	Gesprek met systeemeigenaar, meestal functioneel beheerder	Uitwerking door Analist en terugkoppeling aan opdrachtgever	Terugkoppeling aan opdrachtgever
WERKWIJZE	In kaart brengen informatiesysteem alsmede eisen	Bepalen relevante bedreigingen i.r.t. gevolgen	Formuleren maatregeldoel-stellingen o.b.v. de eisen en relevante bedreigingen	Opstellen implementatieplan per verantwoordelijke
TOOLS	MAPGOOD Invulformulier Waarderings-tabellen	Invulmatrix gevolgen & bedreigingen	BIG Maatregel-Doelstellingen en eigen maatregel-doelstellingen	Opzet implementatieplan
RESULTAAT	MAPGOOD formulier ingevuld en eerste beeld van de eisen	Overzicht van de relevante bedreigingen	Samenhangend pakket maatregel-doelstellingen	Implementatieplan informatiebeveiliging
UREN INDICATIEF	4 uur systeembeheer/ functioneelbeheer 8 uur voorbereiden en uitwerken	4 uur Gesprek(ken) met systeemeigenaar 20 uur voorbereiden en uitwerken	20 uur	20 uur samen met CISO en opdrachtgever

Diepgaande risicoanalyse, tijd benodigd van de opdrachtgever

- Uitgangspunt: één systeem
  - Map goed als dat nog niet is gedaan: tot 4 uur met systeemeigenaar
  - dreigingenanalyse 2 tot maximaal 3 dagdelen met systeemeigenaren
  - maatregelen (op maatregel/doelstelling niveau) vaststellen, alleen de afstemming met proces/ systeemeigenaar 4 uur
- Overige tijd is voorbereiding en uitwerking door analist
- Leidt tot maatregeldoelstellingen die in stap 8 worden aangescherpt. De eigenaar voert dit plan zelf uit.