



HOE KAN HET ISMS U ONTZORGEN?



SEGMENT

Een slimme implementatie én
goede borging van de BIG



VISIE



VERDIEPEN



VERBINDEN



VERANDEREN

1

Introductie

2

Baseline Informatiebeveiliging Gemeenten

3

Standaard aanpak

4

Slimme aanpak in zes stappen

5

Implementatie

6

Waar moet ISMS aan voldoen?



Ingrid van Zeeland MA

Ervaring:

- 20 jaar ervaring gemeenten bij en voor gemeenten, o.a. Hoofd ICT (CIO) Den Bosch. Directeur SEGMENT en Partners.
- SEGMENT, netwerkorganisatie van veranderkundig en vakinhoudelijk professionals voor gemeenten. Met 190 docenten en 50 samenwerkingspartners
- Missie: gemeenten leren leren en ondersteunen op actuele thema's
- Beste gemeentebrede opleider voor de overheid 2014!



Opleidingen

LEES VERDER

Agenda
In company
Diplomatrajecten



e-Learning

LEES VERDER

Cursus aanbod
Verkiezingsinstructies



Verandermanagement

LEES VERDER

Workshops
Subsidie A+O fonds
Advies en begeleiding



Projecten

LEES VERDER

Informatieveiligheid/ISMS
Strategische personeelsplanning



René Ijpelaar

RE CEH CISA

- Auditing en security expert
- Projectleider
Informatiebeveiliging
(Aranea)
- DigiD assessments (BKBO)
- BAG inspecties (Dekra)
- Gecertificeerd ISO 27001
lead auditor (RSM Wehrens)
- Ontwikkelaar ISMS
(SEGMENT)

E-mail:

rene@segmentenpartners.nl



Resy van Gils Gemeente Hilvarenbeek

Verantwoordelijk voor
informatieveiligheid op het
gebied van:

- Kwaliteitszorg
- Gegevensbeheer
- Verordeningen, procedures en documenten
- Zelfevaluaties en audits (o.a. BRP / DigiD)



1

Introductie

2

Baseline Informatiebeveiliging Gemeenten

3

Standaard aanpak

4

Slimme aanpak

5

Implementatie

6

Waar moet ISMS aan voldoen?



Baseline Informatiebeveiliging Gemeenten



Waar begon het ook al weer?

1-1-2013: VNG & KING -> Informatie Beveiligings Dienst IBD

29-11-2013: resolutie Informatieveiligheid VNG ledenvergadering

12-2-2015: convenant informatieveiligheid tussen:

- Vereniging van Gemeentesecretarissen (VGS),
- Vereniging Directeuren Publieksdiensten (VDP),
- Nederlandse Vereniging voor Burgerzaken (NVVB),
- DataLand,
- IMG100.000+,
- Federatie van Algemene Middelenmanagers bij de Overheid (FAMO),
- VIAG
- Vereniging van Griffiers

Baseline Informatiebeveiliging Gemeenten (BIG)

Doel:

1. Gemeenten op een vergelijkbare manier efficiënt en veilig informatieveiligheid.
2. Gemeenten een hulpmiddel bieden om aan alle eisen Informatieveiligheid te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten zijn een aantoonbaar beter.

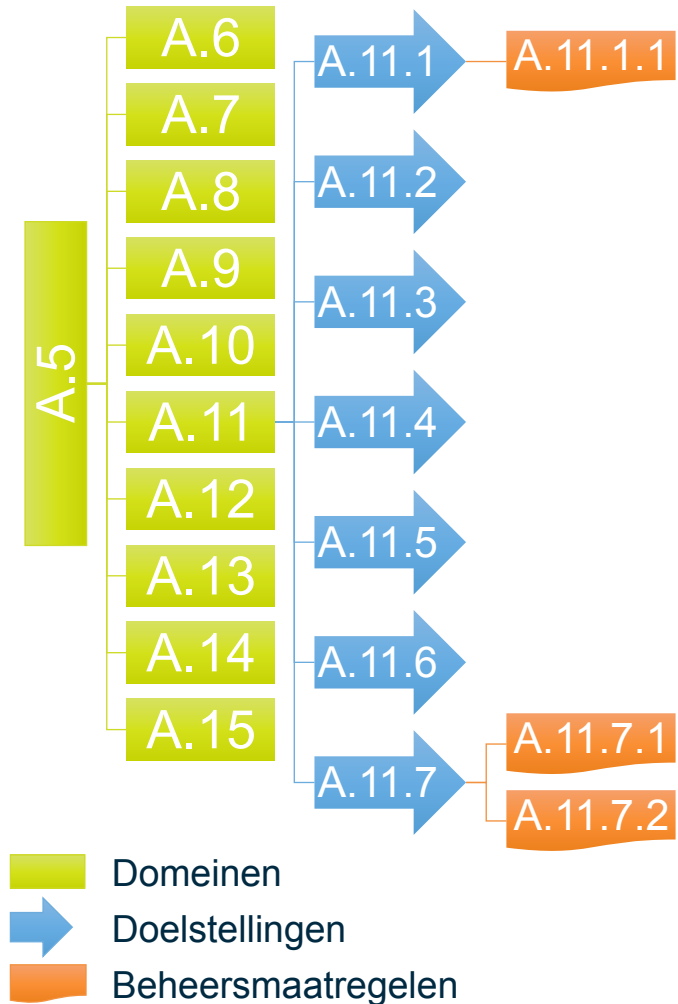
“BIG”
betekent
39 doelstellingen
in 11 domeinen,
133 mogelijke
beheersmaatregelen en 303
mogelijke beveiligings-
maatregelen.”



Baseline Informatiebeveiliging Gemeenten

11 domeinen:

- A.5 Beveiligingsbeleid
- A.6 Organisatie van de informatiebeveiliging
- A.7 Beheer van bedrijfsmiddelen
- A.8 Personele beveiliging
- A.9 Fysieke beveiliging en beveiliging van de omgeving
- A.10 Beheer van communicatie- en bedieningsprocessen
- A.11 Logische toegangsbeveiliging
- A.12 Verwerving, ontwikkeling en onderhoud van informatiesystemen
- A.13 Beheer van informatiebeveiligingsincidenten
- A.14 Beheer van bedrijfscontinuïteit
- A.15 Naleving



De best practice ISO27002 van ISO27001

1. Pas toe of leg uit:

- Top is verantwoordelijk.
- Bedrijfsprocessen zijn “in control”
- Zeg wat je doet; doe wat je zegt en laat zien dat je gedaan hebt wat je hebt gezegd.

2. Een werkende verbetercyclus:

- Informatieveiligheid is geen eenmalige actie, maar permanente verbetercyclus.
- Selecteer maatregelen uit best practices van ISO 27002 volgens het principe ‘Pas toe of leg uit’.



1

Introductie

2

Baseline Informatiebeveiliging Gemeenten

3

Standaard aanpak

4

Slimme aanpak

5

Implementatie

6

Waar moet ISMS aan voldoen?



Standaard aanpak

Bestaat uit:



1. Management commitment
2. Benoem verantwoordelijken
3. Voer een GAP analyse uit (303)
4. Benoem de “quick wins”
5. Voer de impactanalyse uit
6. Verkrijg goedkeuring van het management
7. Maak het informatiebeveiligingsplan en lever de deliverables

Inventarisatie



Heeft u al de GAP analyse uitgevoerd?



Inventarisatie

Heeft u al de impactanalyse
uitgevoerd?



Mijn ervaring

- Gap analyse 303 vragen
- Veel werk en complex, stoot mensen af
- Veel mensen nodig om feiten boven water te krijgen
- Impactanalyse krijgt weinig aandacht
- Validatie nodig
- Als je doorzet is het een goed instrument!



1

Introductie

2

Baseline Informatiebeveiliging Gemeenten

3

Standaard aanpak

4

Slimme aanpak

5

Implementatie

6

Waar moet ISMS aan voldoen?



Slimme aanpak

Bestaat uit:



1. Verkrijg commitment
2. Beperk de scope
3. Voer de gap analyse en impactanalyse tegelijk uit op beheermaatregel niveau (133)
4. Let dit vast in een Verklaring van Toepasselijkheid
5. Maak het informatiebeveiligingsplan en gebruik een ISMS

Kern: Verklaring Van Toepasselijkheid

- Dashboard
- Overzicht stand van zaken
- Vaststellen verbeterplanning
- Management commitment

Opbouw VVT:

- Pas toe:
 - Eigen documenten of ISMS-documenten
 - Geheel of gedeeltelijk gereed, gepland
- Leg uit:
 - Acceptatie van restrisico's

VVT



Voordelen

- Van globaal naar detailniveau
- Details komen bij implementatie
- Minder weerstand bij de start
- Sneller inzicht met minder inzet
- Meer focus op impactanalyse
- Management is aan zet: VVT



1

Introductie

2

Baseline Informatiebeveiliging Gemeenten

3

Standaard aanpak

4

Slimme aanpak

5

Implementatie

6

Waar moet ISMS aan voldoen?



Implementatie is een project van jaren!



- Fasering en planning
- Vuistregel praktijk:
per maatregel 16 uur per betrokken team.

303 maatregelen. Stel:
200 nog te nemen met
gemiddeld 2 teams
betrokken:

$200 * 2 * 16 = 6400$ uur
Op basis van concrete
voorbeelden

Advies:

Focus aanbrengen door:

1. Slimme aanpak én
2. Gebruik van standaard ISMS.

Dat scheelt tijd!

Projectmatige aanpak Prince 2 ?



Voor:

- Helder mandaat
- Commitment leiding
- Concrete fase overgangen maken tussentijds bijsturen makkelijk
- Standaarden voor documentatie en rapportage beschikbaar

Project raakt vele teams met schuivende prioriteiten!

Tegen:

- PINO
- Risico van overkill projectdocumentatie
- Niet volhouden “management by exception”

Wat is er af als het af is?



Dus eigenlijk:
de complete
Administratieve
Organisatie van
Informatie
Beveiliging

- Een door het college vastgesteld beveiligings BELEID
- Vastgesteld flankerend beleid
- Wat heb je nodig?
 - Implementatieplan
 - Procedures & protocollen
 - Rapportage templates
 - Classificaties
 - Inventarisatie templates
 - Checklists
- Beveiliging geïntegreerd in het werkproces
- Beveiligingsbewuste collega's
- Werkende Deming cirkel



1

Introductie

2

Baseline Informatiebeveiliging Gemeenten

3

Standaard aanpak

4

Slimme aanpak

5

Implementatie

6

Waar moet ISMS aan voldoen?

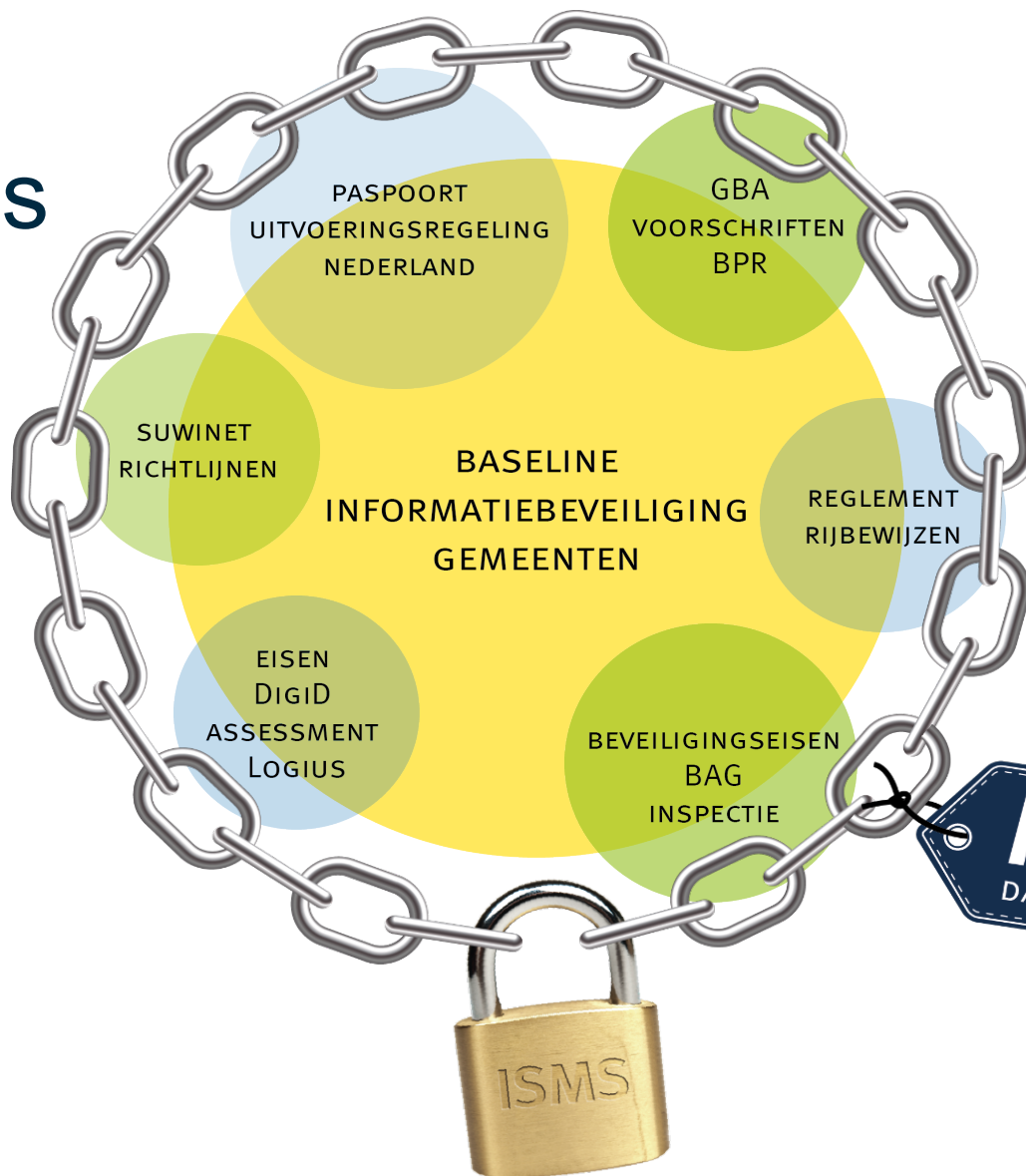


Slimme aanpak en borging BIG





ISMS is



....meer dan
U verwacht





Eisen aan ISMS



- ✓ Het ISMS is de basis voor een adequaat beveiligingsbeheer. Integraal en ondersteunend aan Deming cirkel.
- ✓ Een ISMS voldoet als het op papier levert wat er gebeurt (opzet) en u op basis daarvan kunt controleren.
- ✓ Het is bedoeld voor de CISO zodat hij weet wat de beveiligingsorganisatie moet doen (en wanneer)
- ✓ Praktisch en handzaam op basis van 'Pas toe of leg uit.'
- ✓ Laat een ISMS "meegroeien" met uw implementatie van de BIG.
- ✓ Zo efficiënt mogelijk opgesteld (kosten).
- ✓ Het ISMS moet gemeentebreed zijn en minimaal de bedrijfs-informatiesystemen volgens Gemma bevatten.

"Zorg voor een AO die voldoet en **blijft voldoen** aan de Baseline Informatiebeveiliging Gemeenten!"





Bijhouden van een ISMS

- ✓ Jaarlijks op hoofdlijnen bepalen wat van de BIG van toepassing is en vastleggen in VVT
- ✓ Actueel blijvende vertaling van alle 39 doelstellingen in 11 domeinen met 133 beheersmaatregelen en 303 beveiligingsmaatregelen naar uw situatie met bijbehorende beleidsregels, procedures, voorschriften, checklists, voorbeelden en rapportages
- ✓ Blijvend onderhouden bij wijziging van landelijke regelgeving.

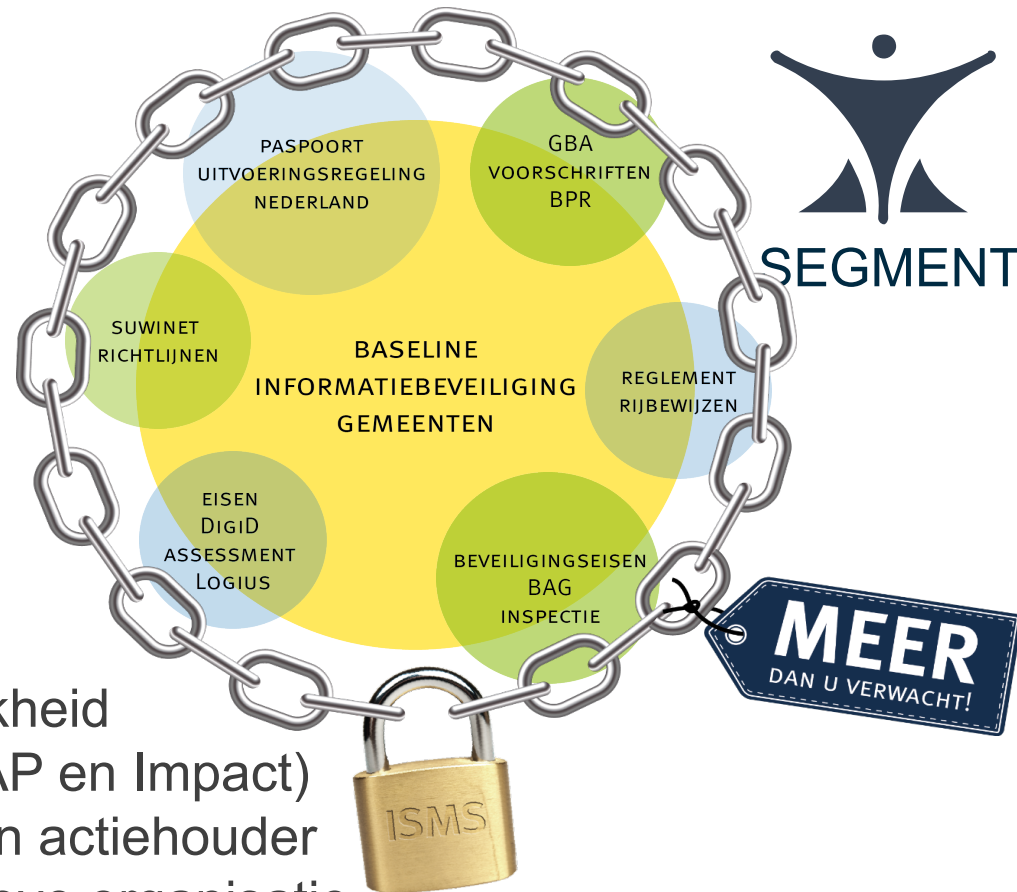




ISMS is:

Een op maat gemaakt informatie-beveiligingsplan:

- met informatiebeleid
- met Verklaring Van Toepasselijkheid (op 133 beheermaatregelen GAP en Impact)
- met maatregelen én planning én actiehouder
- inclusief de gehele administratieve organisatie
- inclusief de Deming cirkel (jaarlijkse controle)
- inclusief onderhoud zodat het actueel is én blijft aan de BIG



Op basis van een standaard ISMS scheelt het u heel veel tijd!



Hilvarenbeek

Ervaring aanpak Hilvarenbeek:
GAP+Impact op 133 beheermaatregelen met
gebruik standaard ISMS op maat gemaakt.

- In hoeveel tijd?
- Weerstand 133 vs 303?
- Samenwerking Equalit en aanpak BIG (ISMS – mogelijkheden efficiency)
- Samenwerking Equalit en aanpak BIG (CISO)
- Wat is het resultaat?



Resy van Gils
Gemeente Hilvarenbeek



Vragen ?



René Ijpelaar
RE CEH CISA



Resy van Gils
Gemeente Hilvarenbeek





SEGMENT

Dank voor uw
Aandacht!



VISIE



VERDIEPEN



VERBINDEN



VERANDEREN