PROVINCIE :: UTRECHT

INFORMATIESESSIE INFORMATIEVEILIGHEID EN AVG

25 juni 2018

Paul Frencken

Johan van Middelkoop

GEBRUIKTE AFKORTINGEN

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming (ook wel de privacy wetgeving)
WBP	Wet Bescherming Persoonsgegevens (voorloper van de AVG)
IBI	Interprovinciale Baseline Informatievoorziening (standaard maatregelen voor informatie beveiliging voor de provincies, uitwerking van de ISO27001)
BIR	Baseline Informatiebeveiliging Rijksoverheid
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheden (vervanger van de IBI, BIRG en BIG)
ISO27001	Internationale standaard met maatregelen voor informatiebeveiliging
CCO	Corporate Control
IPO	InterProvinciaal Overleg
IB	Informatie Beveiliging
MIBP	Masterplan Informatie Beveiliging en Privacy
GS	Gedeputeerde Staten
CERT/CSIRT	Computer Emergency Response Team / Computer Security Incident Response Team (team wat samengesteld wordt als er een IB incident is, bijvoorbeeld datalek of een hack poging)
PDCA	Plan Do Check Act (Continu verbeter cyclus)
P&C	Planning & Control (Verantwoordingscyclus)
CISO	Chief Information Security Officer
FG	Functionaris Gegevensbescherming
PO	Privacy Officer
SO	Security Officer
IBP	Informatie Beveiliging en Privacy

UITGANGSSITUATIE AVG

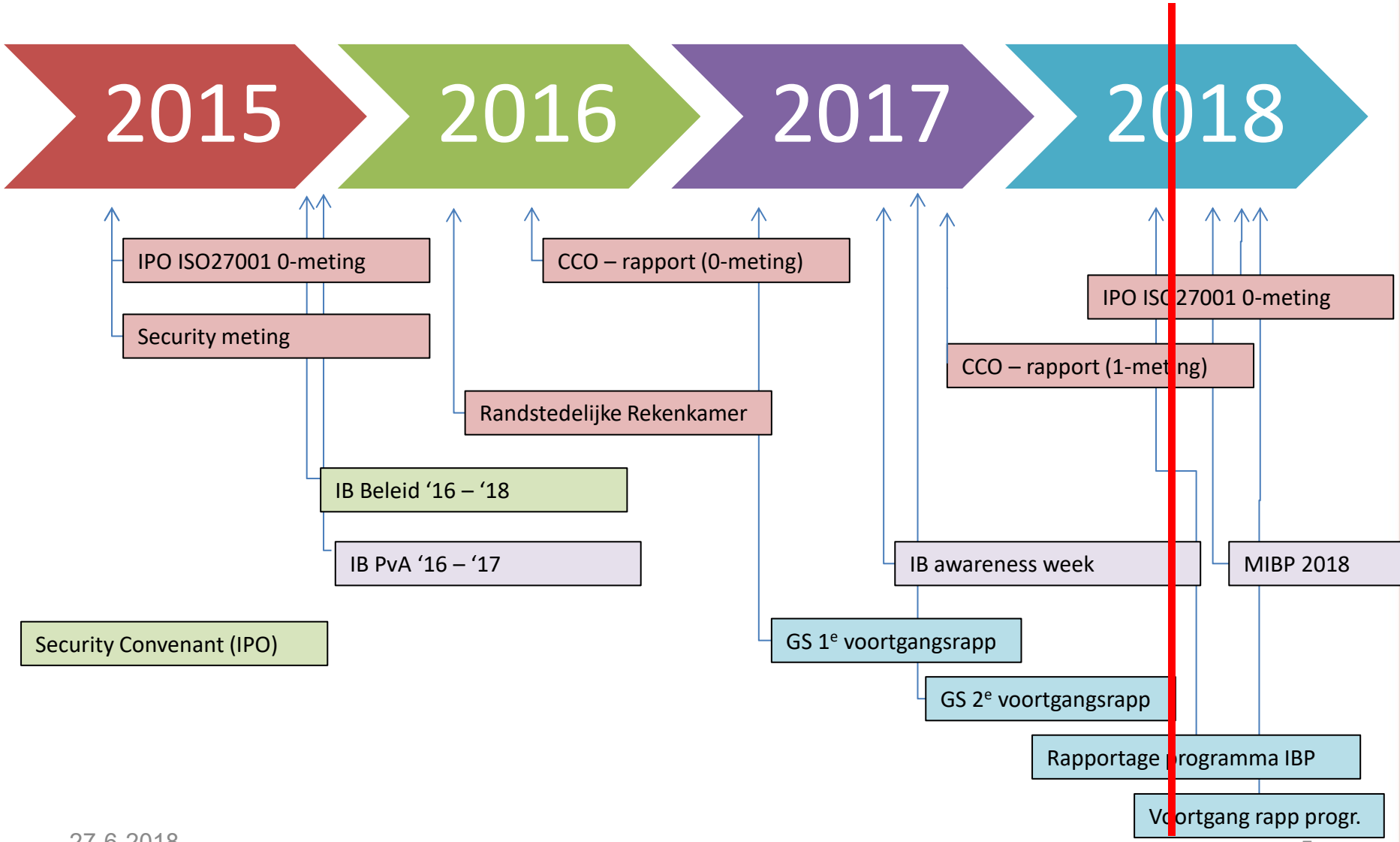
- Wbp niet goed geïmplementeerd (vergt inhaalslag);
- Te laat gestart met implementatie AVG;
- Eerdere poging AVG implementatie gestrand;
- Implementatie duurt ongeveer 1 a 2 jaar, afhankelijk van complexiteit organisatie en vertrekpunt;
- Feitelijke start in februari 2018, dus minder dan 4 maanden voor van toepassing zijn AVG (25 mei).

UITGANGSSITUATIE INFORMATIEVEILIGHEID

Bevindingen externe en interne rapporten – waaronder CCO audit - laten tekort zien op informatieveiligheid:

- Onvoldoende sturing, beheersing, verantwoording;
- Gebrek aan verantwoordelijkheid;
- Geen corporate systematische aanpak;
- Onvoldoende urgentie, belang;
- Nog onvoldoende awareness, kennis;
- Ontbreken afspraken, gebrek aan regie;
- Geen duidelijke samenhang beleid, uitvoeringsbeleid en uitvoering.

Waar komen we vandaan?



BELANGRIJKSTE RISICO'S INFORMATIEVEILIGHEID

Mensen:

- Eigenaarschap wordt onvoldoende genomen
- Medewerkers zijn onvoldoende bewust van de gevolgen van hun handelen m.b.t. informatiebeveiliging (deels onbewust onbekwaam)
- Corporate aanspreekpunt voor IB in business ontbrak

Processen / procedures:

- Informatiebeveiliging onvoldoende ingebed en geborgd ('afgedwongen') in processen en procedures
- Vertragen/mislukken projecten en verbeteractiviteiten (onvoldoende eigenaarschap, nemen verantwoording, onvoldoende actieve samenwerking)
- Onvoldoende voorbereid op cybersecurity incidenten (CERT/CSIRT, communicatie, forensisch onderzoek etc.)
- Ontbreken pdca- cyclus, p&C-cyslus, managementinformatie

Techniek:

- Onvoldoende inzicht in beveiligingsstatus van de infrastructuur (bijv. logging en monitoring, kwetsbaarheden), alleen reactief / ad hoc handelen mogelijk;
- Inrichting van toegangsrechten zijn onvoldoende inzichtelijk;
- Geen goedgekeurd samenwerkingsplatform voor het delen van bestanden;
- Niet alle IT omgevingen zijn bekend.

URGENTE AANPAK !!!

- Programma informatieveiligheid en privacy
- O.l.v. algemeen-directeur
- Taskforce aanpak (stuurgroep en programmateam)

Het programma bevat 4 (samenhangende) programmalijnen:

1. Implementatie AVG;
2. (Voorstel) inrichten governance voor informatiebeveiliging en privacy;
3. Masterplan informatiebeveiliging en privacy (MIBP);
4. Gestructureerd in het hier en nu in control komen over informatiebeveiliging en dataprotectie.

Werken in 2 fasen, te weten:

– Fase 1: Tot 25 mei, noodzakelijke basis gerealiseerd:
  - Verwerkingenregister
  - Functionaris gegevensbescherming
  - Model verwerkersovereenkomsten
  - Centraal meldpunt datalekken
  - Privacystatement en algemeen beleid
  - Starten voorlichten en awareness (intranet, presentaties, beantwoording vragen, adviezen)

- Fase 2: Na 25 mei, voor 31 oktober: Borging AVG
  - Controle op verwerkingen en indien nodig aanpassingen initiëren
  - Opstellen uitvoeringsbeleid, richtlijnen, werkwijzen
  - Continu traject awareness, voorlichting en kennisdeling
  - Versterken privacy by design en privacy by default
  - Uitwerken governance gericht op staande organisatie

Werken aan Informatie Beveiliging en Privacy governance:

- Kwartiermakers CISO, FG, PO en SO zijn aangesteld
- Versterken en uitbouwen (bestaande) structuren (kaderstelling & advisering, architectuurboard, portfoliomanagement, primaire processen)
- Rapporteren aan stuurgroep IBP
- Voorstel voor governance
- En voorbereiden borging governance

Meerjarenplan:

- Integrale, risico-gebaseerde informatieveiligheid binnen de provincie Utrecht organisatie (beleid, architectuur, inrichting, maatregelen).
  - Opstellen en invoeren IB architectuur
  - Data classificatie vaststellen en invoeren
- Eigenaarschap en bewustwording;
  - E-learning AVG en Informatiebeveiliging
  - Presentaties bij mt's, domenen, afdelingen, team,
  - Communicatie via Atrium, Yammer, nieuwsbrieven, en andere media
- Eenduidige systematiek risicomanagement en PDCA- en P&C-cycli;
  - Inrichten periodieke IBP controles op maatregelen (o.a. toegang, kwetsbaarheden)
  - Uitvoeren risico-inventarisatie in processen en systemen
- Certificering van ISO27001;
  - Opstellen IB beleid en maatregelen
  - IBP hoofdstukken in portfolio/project proces en templates

GESTRUCTUREERDE AANPAK IN HET HIER EN NU

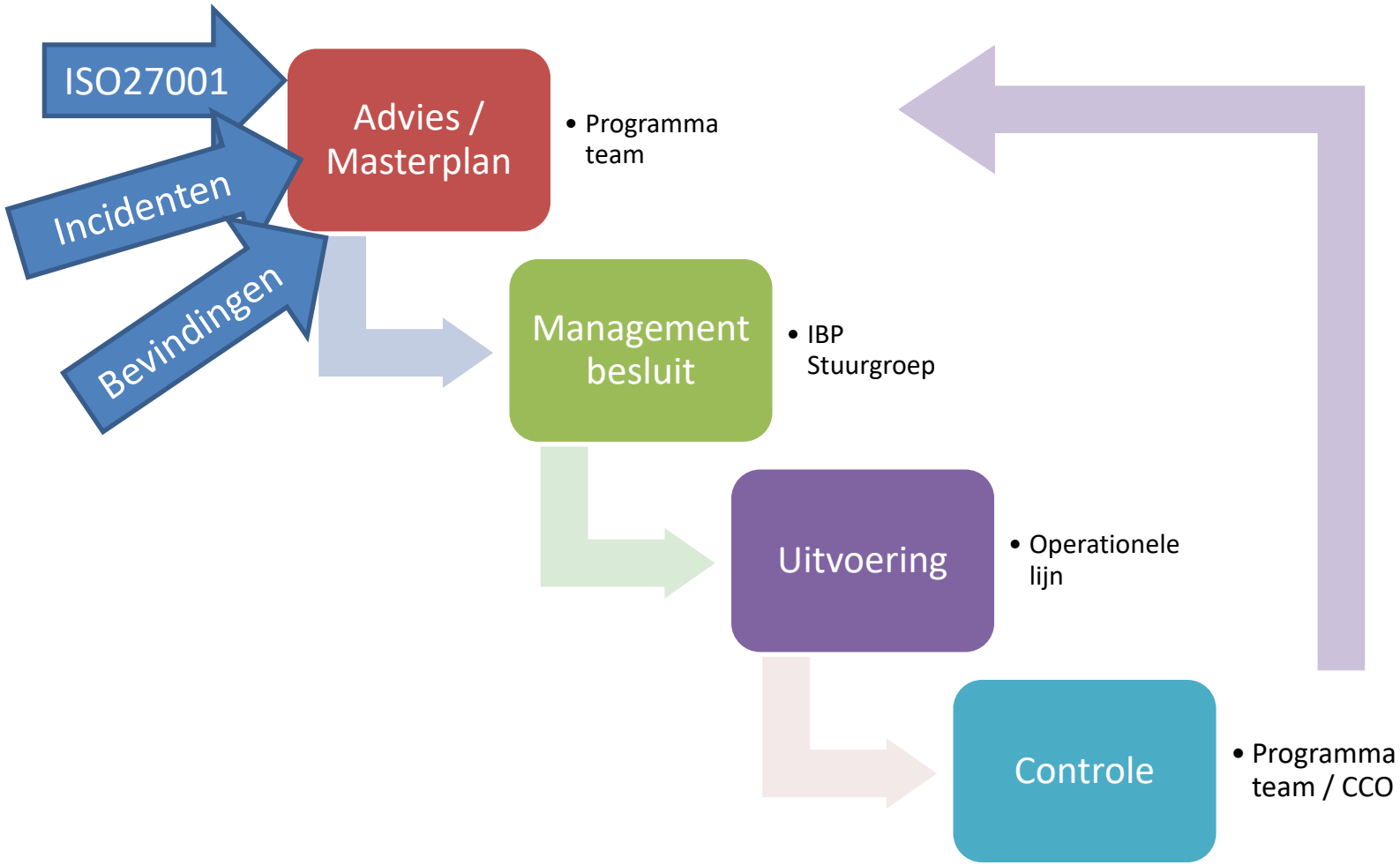
Op dit moment:

- Verbetering beveiliging websites
- Invoeren responsible disclosure
- Coördinatie op oppakken en afhandeling datalekken en security-incidenten
- Aanpassen werkwijzen, aanvullende maatregelen

Op korte termijn:

- Nader te treffen maatregelen
- Logging en monitoring
- Verdere analyse ist-situatie door externe partij (focus op technische weerbaarheid)
- Inrichting werkplek
- Investeringen/inkoop (privacy en security checks)

WERKPROCES IBP



RESUMEREND: IB AANBEVELINGEN I.R.T. AANPAK

- Onvoldoende sturing, beheersing, verantwoording =>

Masterplan IBP, borging verantwoordelijkheid/bewustzijn, controle/rapportage

- Gebrek aan verantwoordelijkheid =>

Kwartiermakend governance inrichten voor staande organisatie

- Geen corporate systematische aanpak; =>

Werkproces IBP , PDCA en P&C cycli

- Onvoldoende urgentie, belang; =>

Taskforce aanpak: middellange termijn en hier en nu (!), o.l.v. algemeen-directeur

- Nog onvoldoende awareness, kennis; =>

Structureel informeren/kennisoverdracht, bijv. E-learning AVG en IB, presentaties, IBP-dossier Atrium, nieuwsbrief, etc.

- Ontbreken afspraken, gebrek aan regie; =>

Stuurgroep IBP (IBP board), IB en P (uitvoerings)beleid

- Geen duidelijke samenhang beleid, uitvoeringsbeleid en uitvoering. =>

IB en P (uitvoerings)beleid

TOT ZOVER….

Heeft u vragen?