Voorschrift Informatiebeveilging Rijksdienst (VIR) 2007

Basispresentatie t.b.v. VUrORE

Carl Adamse & Frank Heijligers (BZK)

12 november 2007

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Inhoud

- Aanleiding en Historie
- VIR 2007
- Invoeringsaspecten
- …

Aanleiding en historie

- VIR'94
- Rechtmatigheidsonderzoek ARK 2003
- Evaluatie BZK 2005
  - Advies, gedragen door pSG beraad
  - Bijstelling VIR
  - Samenhang andere regelingen
  - (Sterkere) inbedding in management cyclus
  - Versterking interdepartementale samenwerking
- VIR2007 ← Besluit MR 13 april 2007

VIR 2007 Minder of Weg

- Verplichting A&K analyses
- Verantwoordelijkheidsgebieden
- IB Plan
- Calamiteitenparagraaf

- Minder papier
  - VIR van 59 naar 18 pagina's
- Meer tijd en aandacht voor beveiliging

VIR 2007 Beter/nieuw

- Informatiesystemen in brede zin
- Ketens van informatiesystemen
- Code voor Informatiebeveiliging (ISO norm)
- Samenhang andere regelingen
- Risico-afweging door manager
- P&C cyclus
- Deming circle

Artikel 1 - Begripsbepalingen

In dit besluit wordt verstaan onder:

a. Informatiebeveiliging: het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen;

b. Informatiesysteem: een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Artikel 2 - Plaatsbepaling en reikwijdte

1. Dit voorschrift geldt voor de Rijksdienst waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.
2. Dit voorschrift geldt voor het gehele proces van informatievoorziening en de gehele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.
3. Informatiebeveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.

Artikel 3 - Informatiebeveiligingsbeleid

De secretaris-generaal van een ministerie stelt het informatiebeveiligingsbeleid vast, draagt dit uit en legt verantwoording hierover af. Het beleid omvat ten minste:

a. De strategische uitgangspunten en randvoorwaarden die het ministerie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;

b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;

c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;

d. De gemeenschappelijke betrouwbaarheidseisen en normen die op het ministerie van toepassing zijn;

e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;

f. De bevordering van het beveiligingsbewustzijn;

Artikel 4 – Verantwoordelijkheden lijnmanagement

Het lijnmanagement is verantwoordelijk voor de beveiliging van zijn informatiesystemen. Het lijnmanagement:

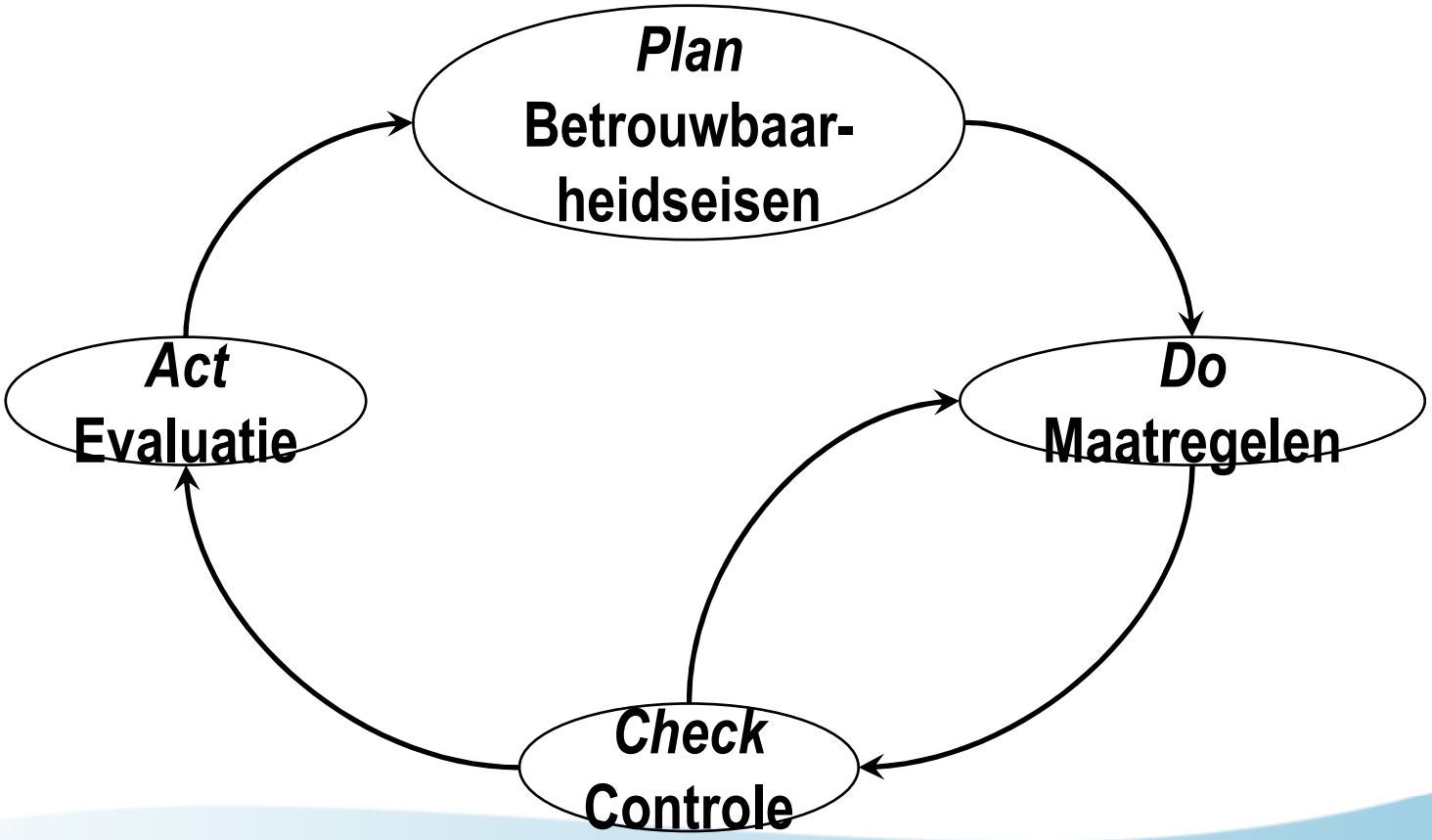
a. Stelt op basis van een expliciete risico afweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;

b. Is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;

c. Stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd;

d. Evalueert periodiek het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen en stelt deze waar nodig bij.

VIR 2007 Deming circle



VIR 2007 Invoeringsaspecten

- VIR is en blijft ingevoerd.
- VIR is strategisch niveau;
- Informatiebeveiliging onderdeel van de mededeling bedrijfsvoering (P&C)
- Deming circle ook bij IB
- Ketens: toewijzing verantwoordelijke manager