EIC Inspiration 17 oktober 2018

EIC goes ISO 27000

Programma

- Raad + Daad
- ISO 27001-certificering bij EIC
- Uitgangspunten
- Security (& privacy) issues in de praktijk

Voorstellen: Ad van 't Hoenderdal

- drs. Econometrie
- Functioneel ontwerper, (product)manager alarmcentrale, productmanager remote ICT-beheer
- Zelfstandig sinds 7/7/'07
- Consultant ISO 20000, ISO 22301 en ISO 27001
- tevens Functionaris Gegevensbescherming
- www.raadplusdaad.nl / ad@raadplusdaad.nl

raad + daad

Raad + Daad: klanten

- Branche: meestal ICT, zakelijke dienstverlening
- # mdws: 5-150
- Ook start-ups
- Groeiend, en dus grotere/formelere klanten
- Regulering wordt strakker (datalekken, privacy)



raad + daad

Toch even: wat is ISO 27000?

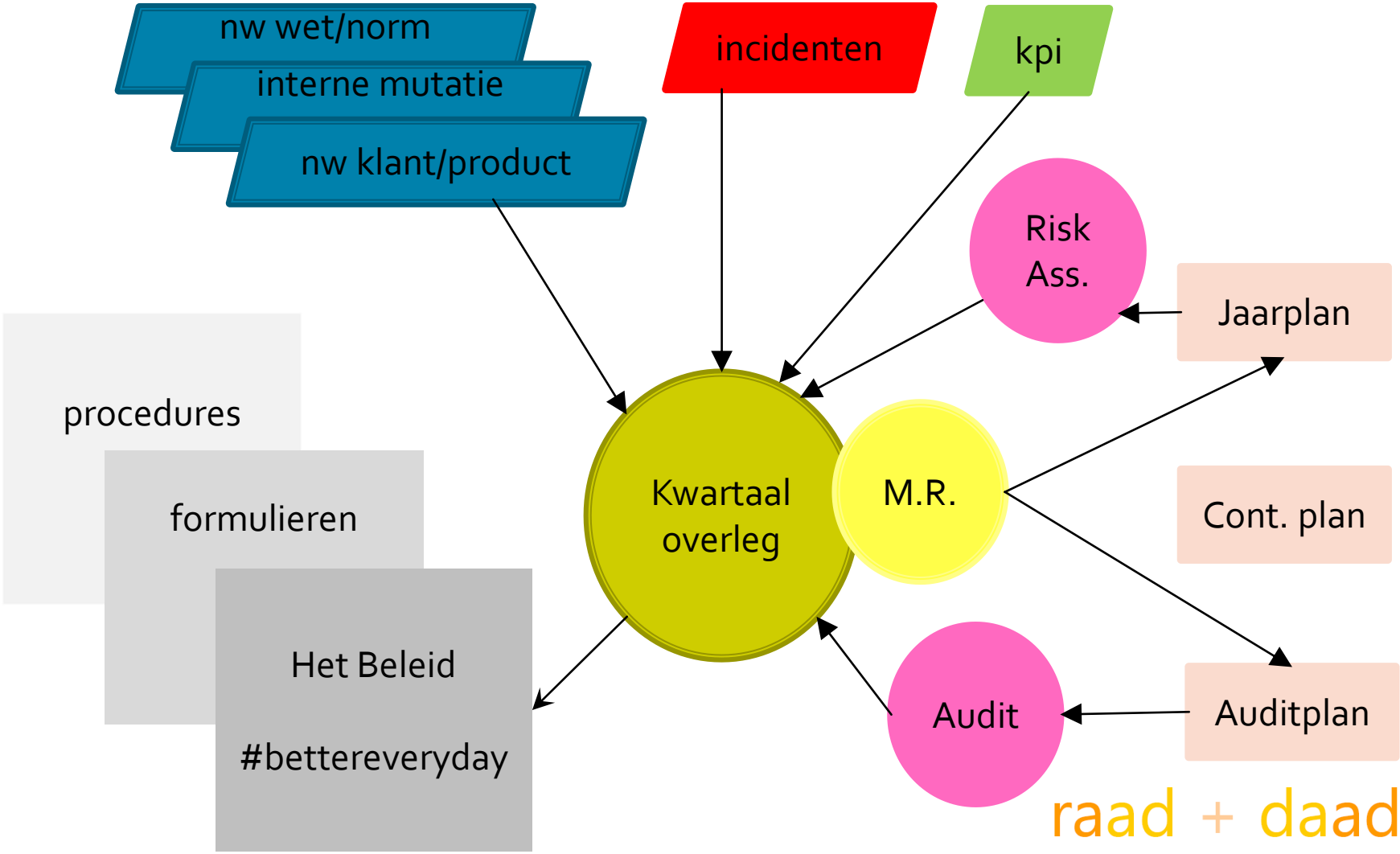
- Internationale norm
- Informatiebeveiliging
- B/I/V
- Veel breder dan IT
- Verschil ISO 27001 / ISO 27002
- Information Security Management System
- Certificeerbaar (RvA)

Implementatie ISO 27001 bij EIC

- ✓ Kick-off, projectplan, projectteam
- ✓ Risk assessment en prioritering van maatregelen
- ✓ Opstellen verbeterplan
- Uitvoeren verbeterplan en vaststellen IB-beleid
- Inrichten ISMS (het management systeem)
- Uitvoeren interne audits (Q4)
- Certificeringsaudit (Q1)

raad + daad

En hoe ziet een I(S)MS er dan uit?



Uitgangspunten

- Het oude ISO 9001 heeft het imago van ISO-normen danig verpest
- Nu context → risico's → maatregelen
- De business stelt eisen aan security, niet andersom
- Bouw geen nieuwe bureaucratie

Uitgangspunten

- Niet "de boeken afstoffen"
- informatiebeveiliging moet intrinsiek worden (geen externe verplichting), en vooral bijdragen aan kwaliteit
- "Het gaat niet om de bestemming, maar om de reis." (vgl.: de Deming-cirkel)

Tot zover eerst

Zijn er vragen?