



Dienst ICT Uitvoering
*Ministerie van Economische Zaken,
Landbouw en Innovatie*



Dienst ICT Uitvoering
*Ministerie van Economische Zaken,
Landbouw en Innovatie*



Dienst ICT Uitvoering
*Ministerie van Economische Zaken,
Landbouw en Innovatie*



Agenda

- Inleiding
- Werner Mulders
'ISO 27001 en het veranderingstraject binnen DICTU'
- Paul van Domburg
'Geen ISO 27001 zonder pragmatiek!'
- Vragen



Inleiding

- Sprekers:
 - Werner Mulders
'ISO 27001 en het veranderingstraject binnen DICTU'
 - Paul van Domburg
'Geen ISO 27001 zonder pragmatiek!'
- Wat doet DICTU?
- Aanleiding voor deze presentatie



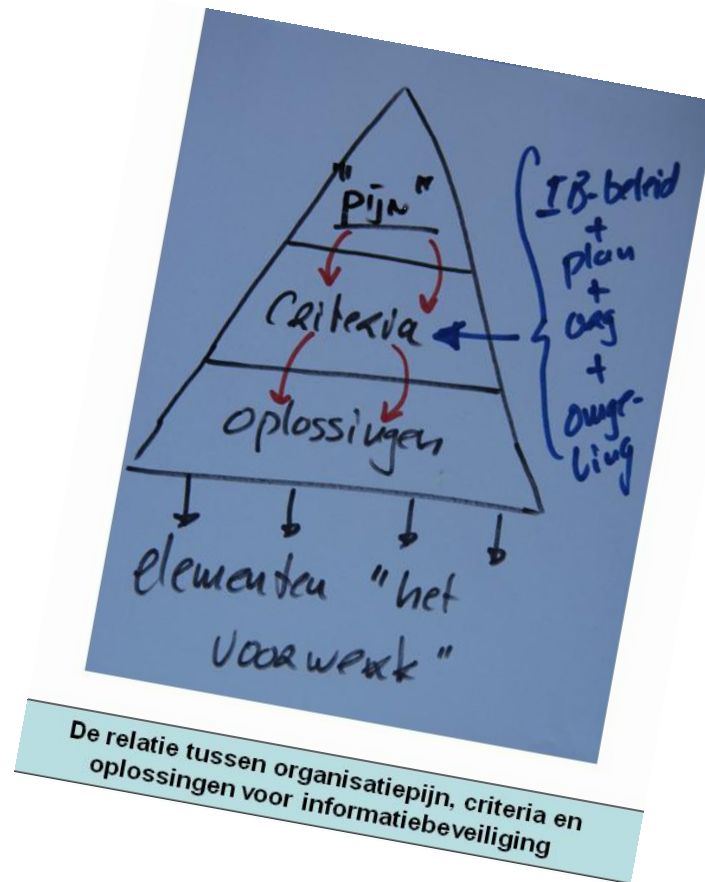
Introductie

- Drs. Ing. Werner Mulders
- Zelfstandig organisatieadviseur en verandermanager
- Gericht op het verbeteren van IT organisaties
- Bedrijfskunde (Drs.) en Informatica (Ing.)
- Ervaring bij veelheid aan zelfstandige en bedrijfsinterne IT organisaties
- Leven naast werk: gezin, bergbeklimmen, gletsjertochten



Hoe begin je meestal met informatiebeveiliging?

- Standaard ingrediënten
- Project voor invoeren beheersmaatregelen
- Opleveren aan de lijnorganisatie





Bij DICTU (even geleden...)

- Veel verplichte regelgeving. Dito compliance-inspanningen
- Informatiebeveiliging te veel gericht op de inhoud, de details
- Daardoor heel veel 'point solutions'
- Lijnorgansatie zijdelings betrokken
- Te weinig aandacht voor basisvoorwaarden

Sprake van managen?



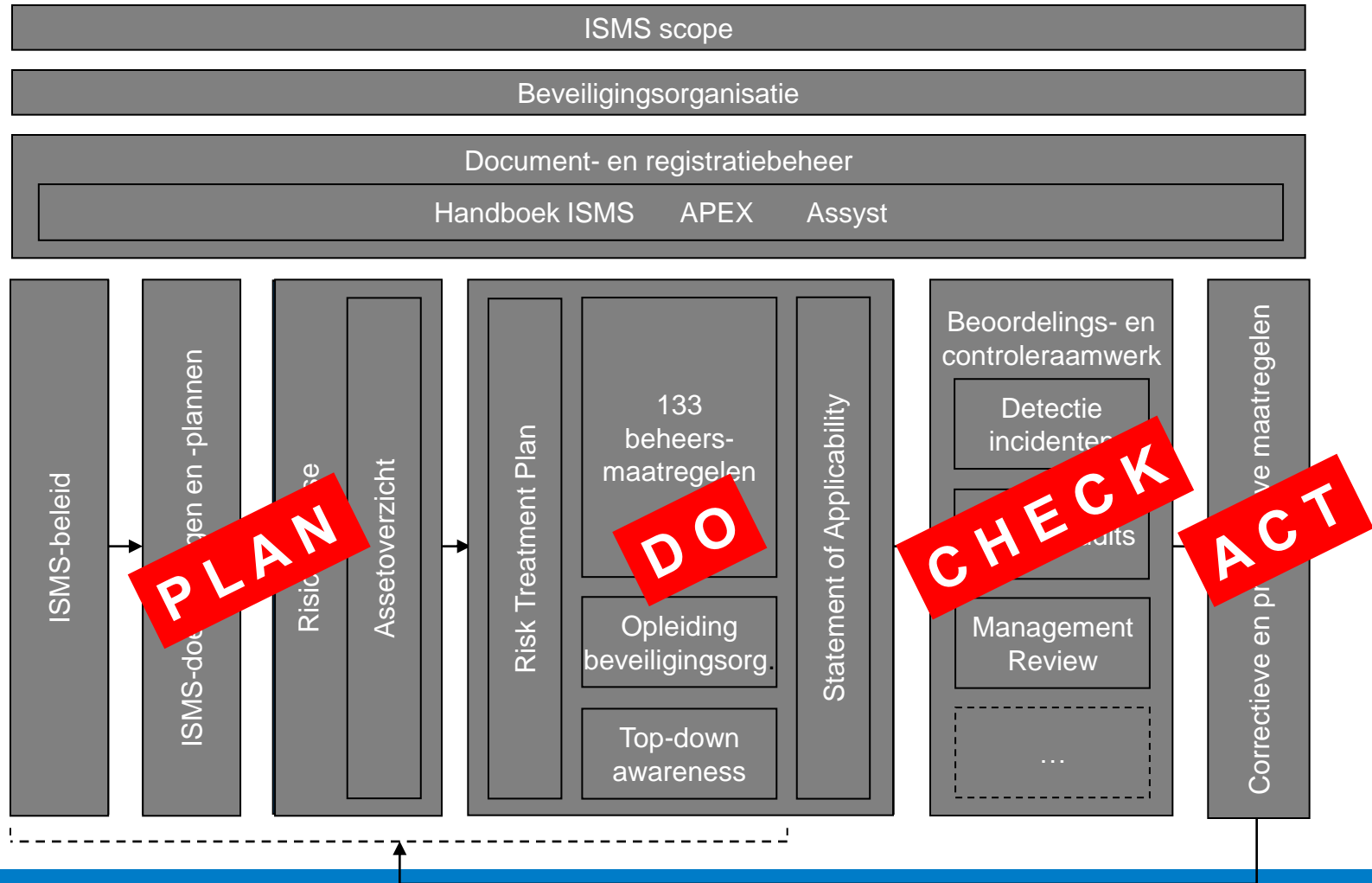
En toen ...

- IB-maatregelen geïmplementeerd, IB-organisatie ingericht ...
- Aantal auditbevindingen nam toe!

Problemen dienden zich aan. Wat misten we?

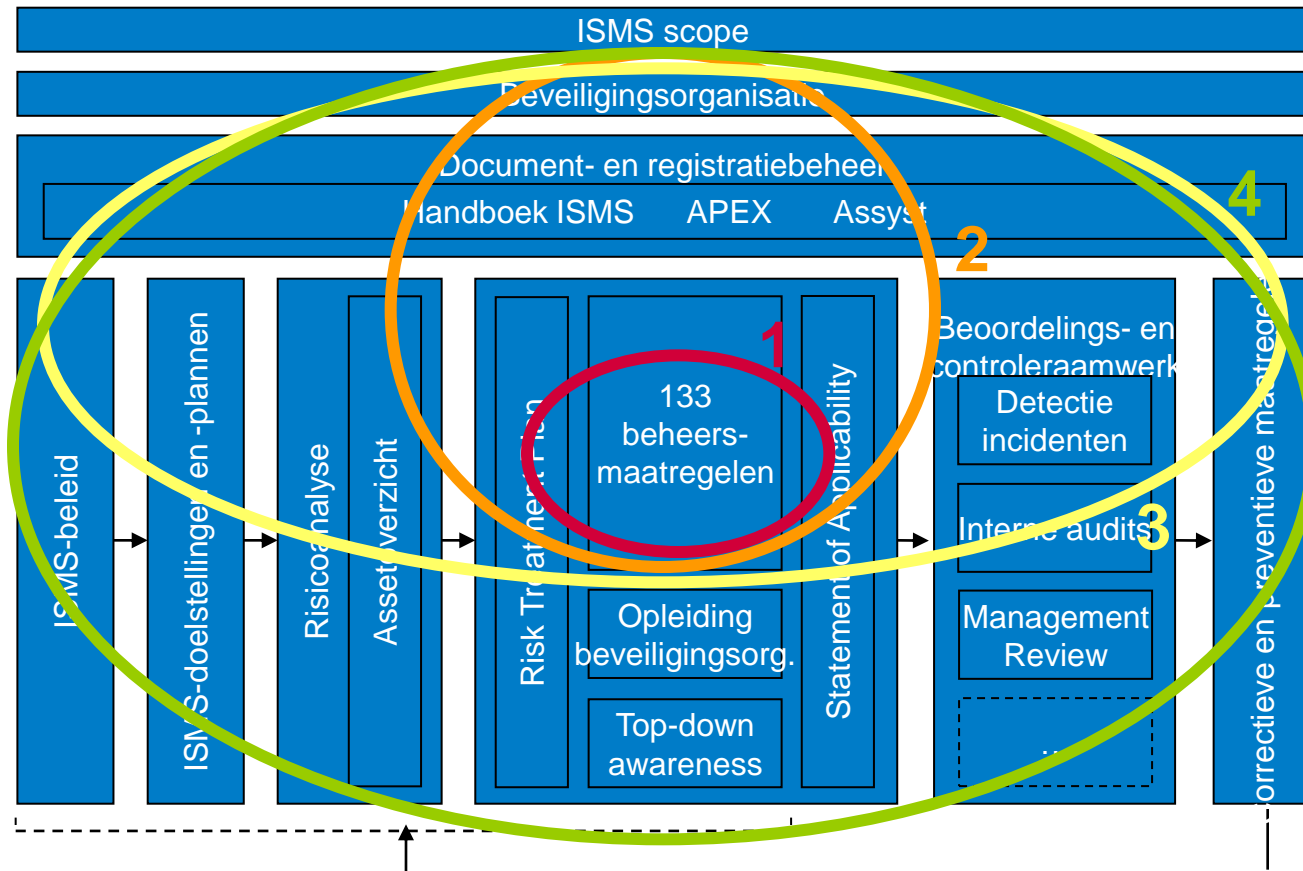


Framework





Het (op)groeimodel



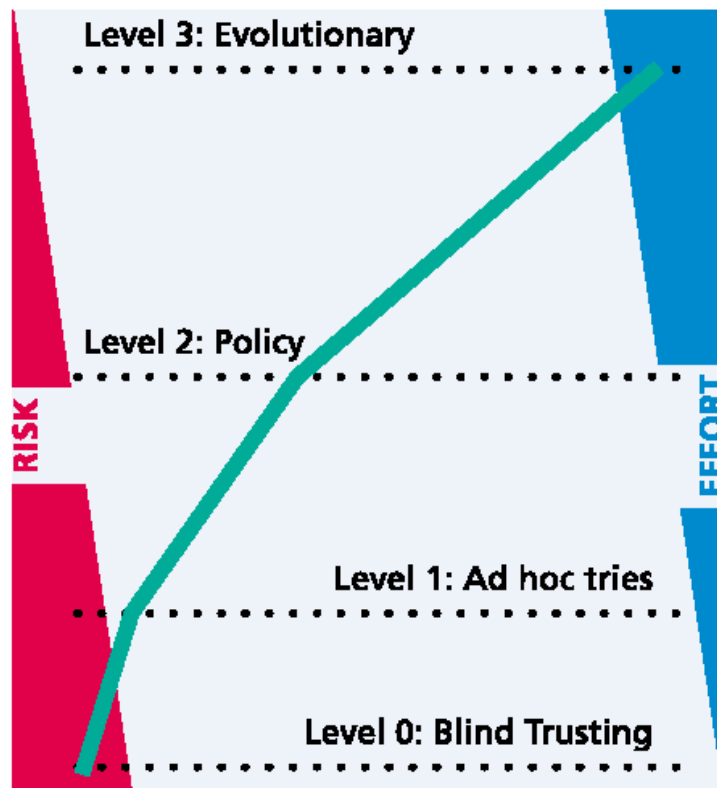


Groeien vanuit te weinig trust en te veel compliance

- Niveau 1: De beheersmaatregelen volgens ISO 27001 appendix A
- Niveau 2: Optuigen van de IB-organisatie en documentbeheer
- Niveau 3: Invullen framework en uitvoeren PDCA
- Niveau 4: Optimaliseren PDCA en beheersen van risico's en assets



Ontwikkelmodel (SMM)



Bron: Fraunhofer Instituut