Hoe implementeer je de NEN7510 ?

Inspiratiesessie NEN 7510 / ISO 27001

Aart Bitter, 12 september 2012

Keep It Simple (1)

- Doe een risicoanalyse en kies beveiligingsmaatregelen
- Implementeer de geselecteerde maatregelen
- Voer het ISMS uit onder verantwoordelijkheid van de Directie
- Bewaak de werking van de maatregelen
- Voer verbeteringen door

Keep It Simple (2)

- En voor het verkrijgen van een certificaat moet dit alles **AANTOONBAAR** zijn

- Toolkits, o.a.:
  - www.nen7510.org
  - www.iso27001security.com

Valkuilen bij de implementatie (1)

- Grote druk om direct na de implementatie van een ISMS over te gaan tot certificering.
- Overzicht kwijtraken van de “echte” eisen van ISO 27001 / NEN 7510.
- De maatregelen zijn niet (meer) terug te herleiden aan de risicoanalyse.
- Beveiligingsbeleid is vaag (“high level”) of te complex en gedetailleerd.

Valkuilen bij de implementatie (2)

- Gebrek aan management commitment.
- Te snel inzetten van en vertrouwen op “tools”.
- “De cirkel is niet rond”- wie doet er nu uiteindelijk wat.
- Te veel gedocumenteerd.
- Bewustwording van medewerkers, externen etc. “vergeten”.

Do & Don'ts

…van een ISMS NEN 7510 implementatie

PLAN: het ISMS vaststellen

One size does not fit all.
Kijk naar uw specifieke risico's.

DO: implementeren en uitvoeren

De keten is zo sterk
als de zwakste schakel.

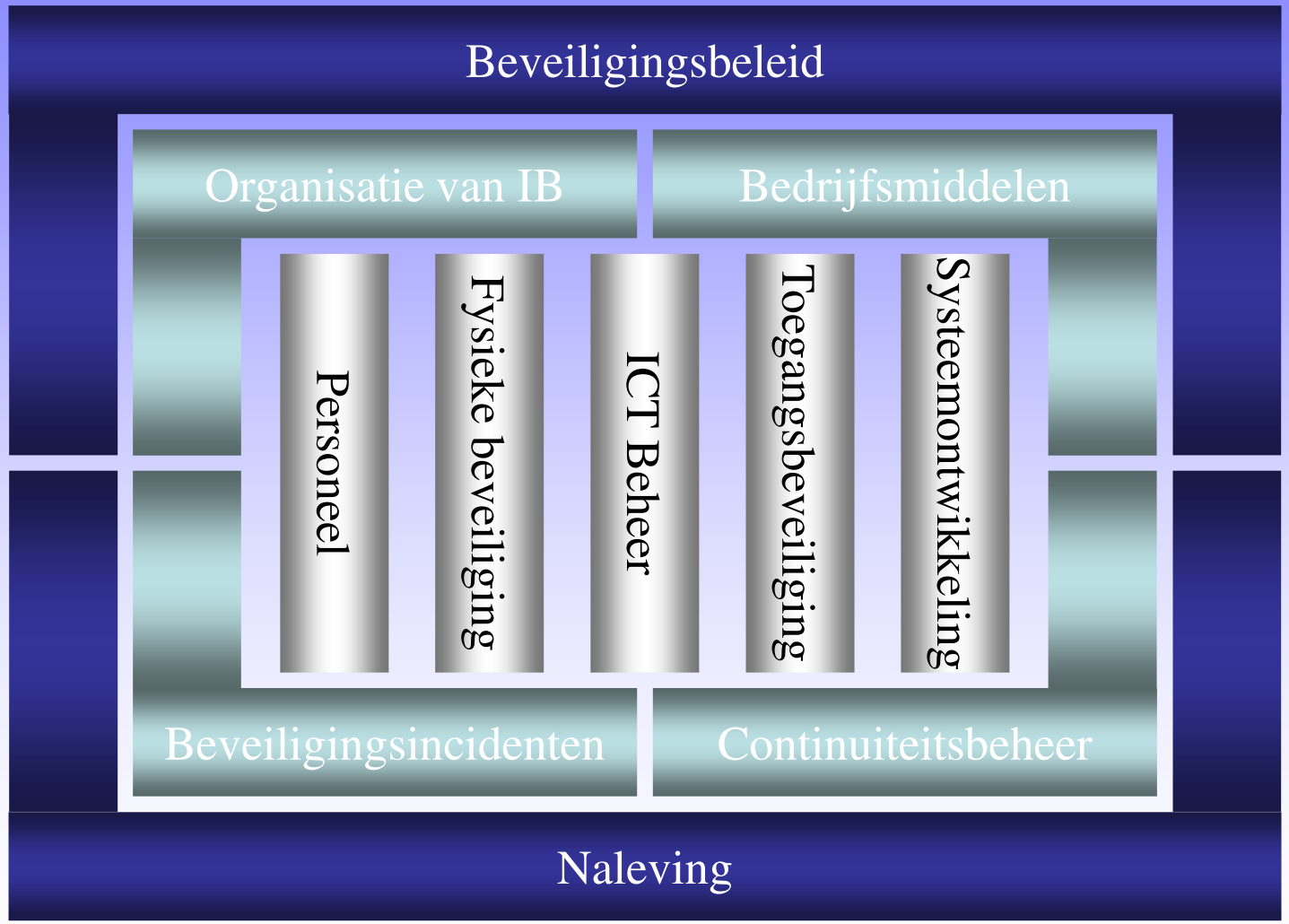
CHECK: bewaken en beoordelen

Operationele controles, interne audits, directiebeoordeling, “incidenten en klachten”

ACT: onderhouden en verbeteren

Verbeteringen,
Correctieve en preventieve maatregelen

Beveiligingsbeheersmaatregelen



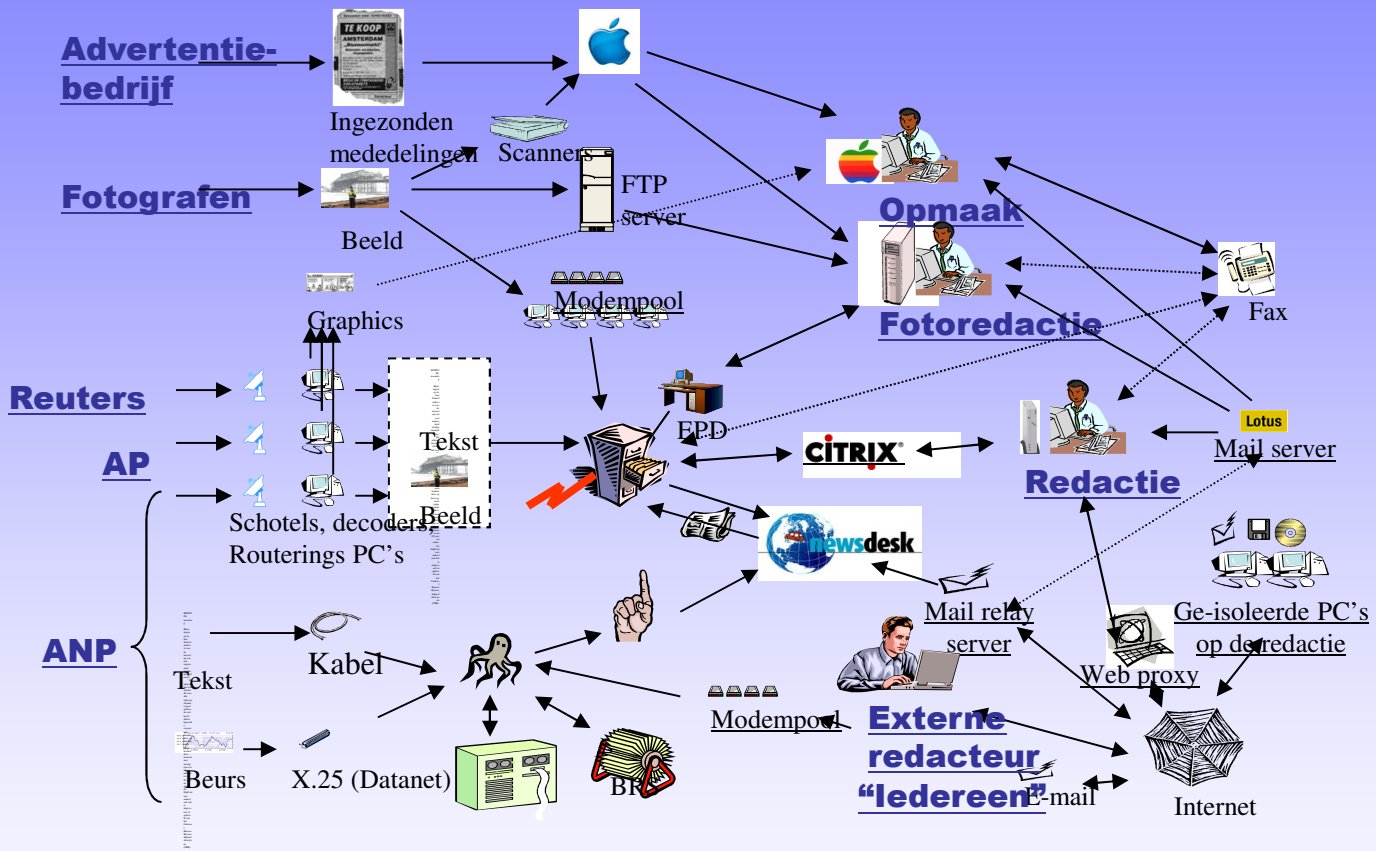
5 Beveiligingsbeleid

Schrijf alleen op waar uw organisatie iets aan heeft, maar wel volgens NEN7510, 4.7.

6 Organisatie van informatiebeveiliging

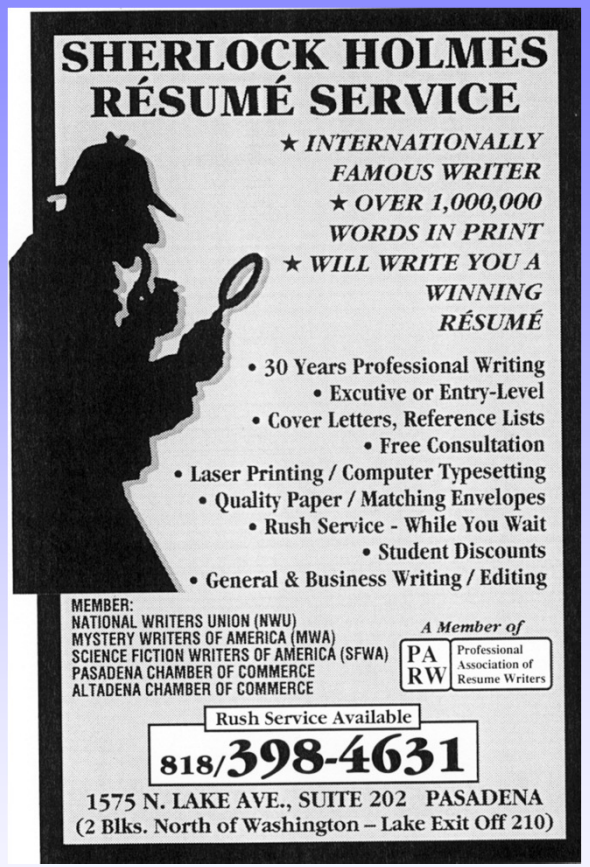
Training en awareness
En uw hele organisatie moet meedoen…

7 Beheer van bedrijfsmiddelen



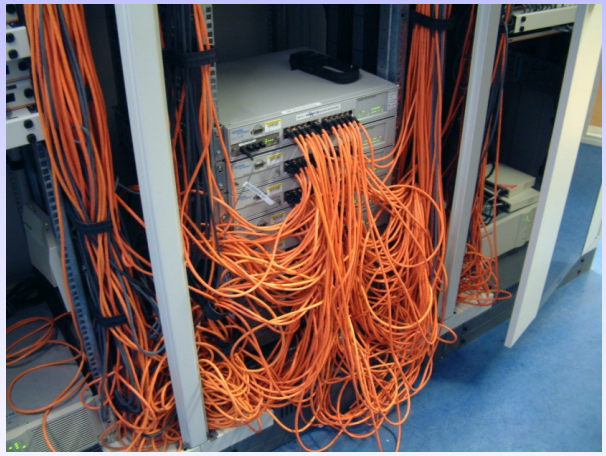
Weet wat u heeft: uw bedrijfsmiddelen informatie, software, apparatuur, diensten, …

8 Personeel



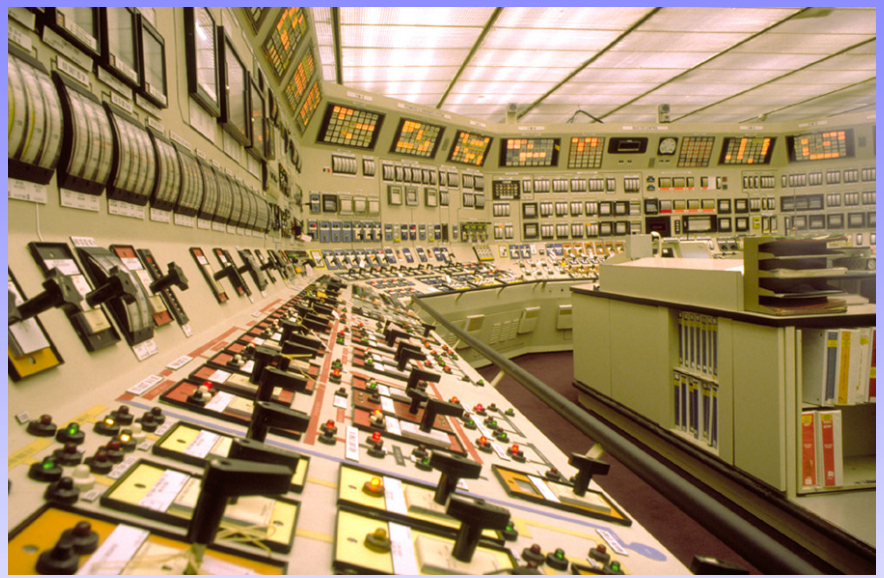
Medewerkers, ingehuurd personeel en externen (ja, zelfs de auditors)

9 Fysieke beveiliging en beveiliging van de omgeving



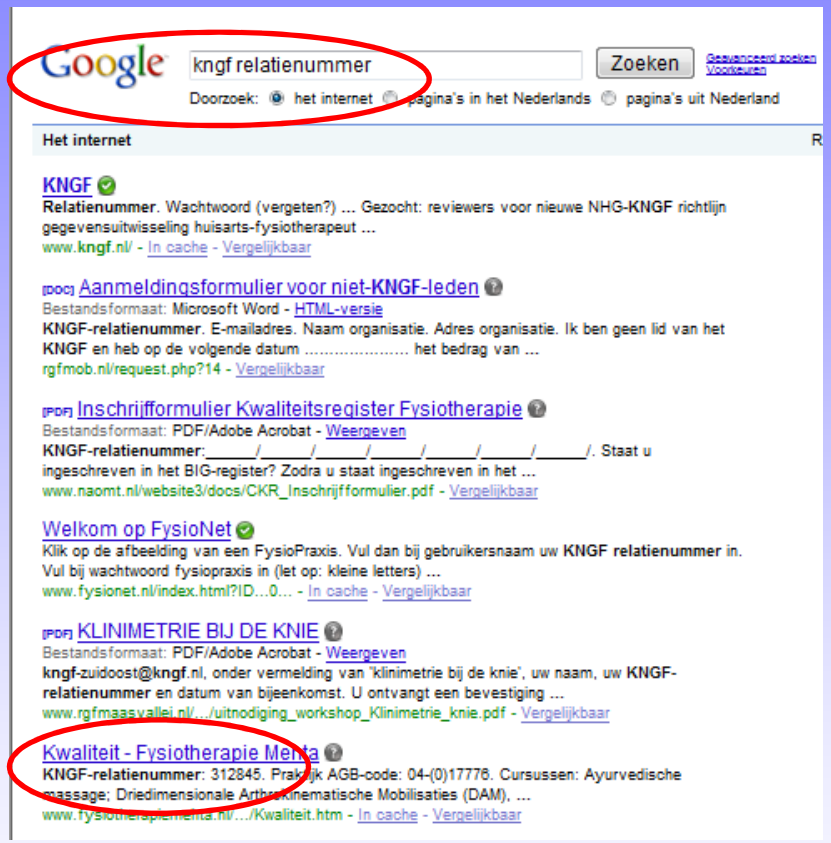
Het een is niet het ander… en veel “maatregelen” zijn toch “vanzelfsprekend”?

10 Beheer van communicatie- en bedieningsprocessen



Uw werkzaamheden hebben structuur nodig, het lijken wel protocollen

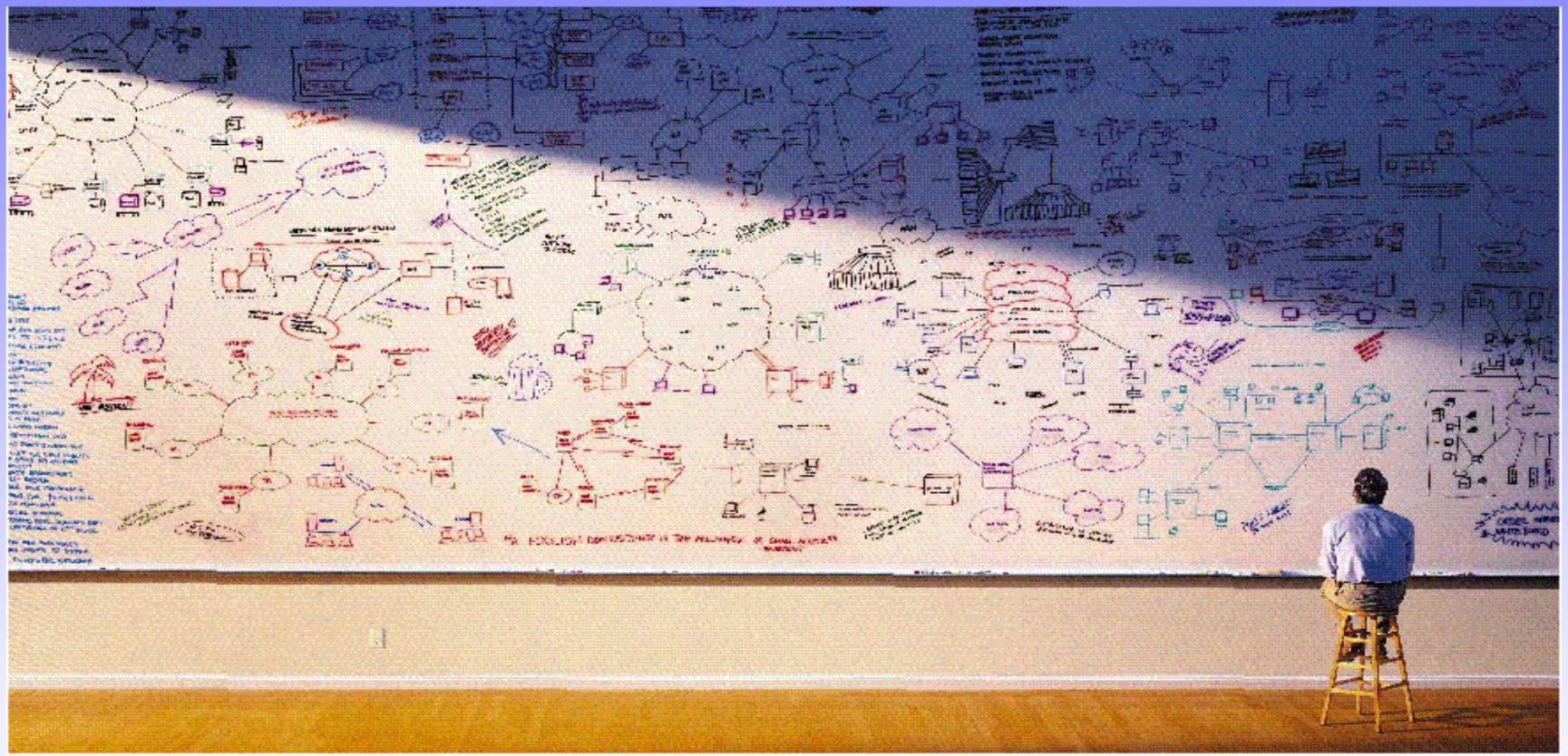
11 Toegangsbeveiliging



want zo wilt u het niet.

En u heeft tegenwoordig heel veel gebruikers

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen



Worden uw patiëntgegevens correct verwerkt en staan ze niet ergens op een testsysteem?

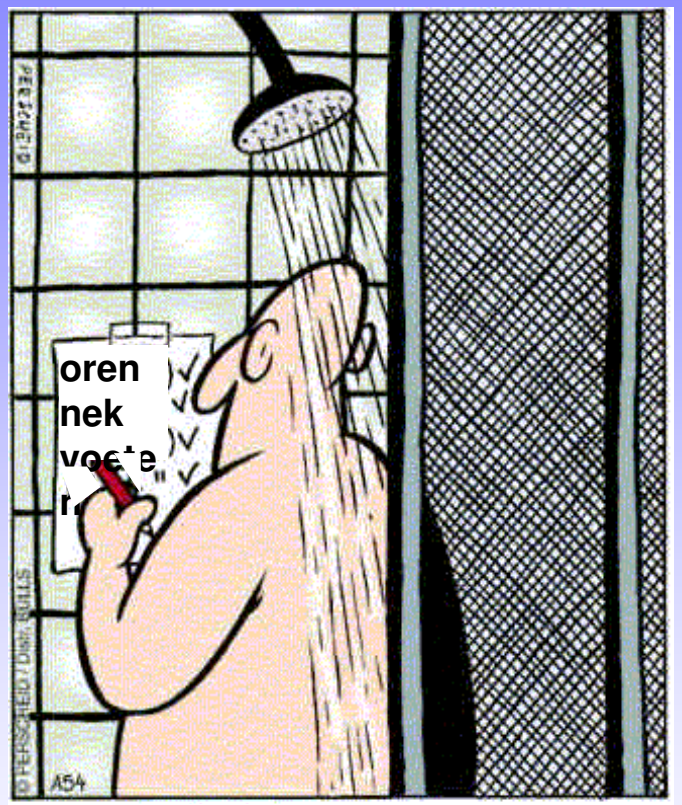
13 Beheer van informatie-beveiligingsincidenten

Wat is een informatiebeveiligingsincident?
Kunt u ze oplossen en voorkomen?

14 Bedrijfscontinuïteitsbeheer

Ten tijde van calamiteiten wilt u niet improviseren. Wat heeft u dan nodig?

15 Naleving



Ken uw wet over privacy en patiëntgegevens en check of uw systemen goed ingericht zijn

Thank you

Information-Security-Governance.com

IT Audits - Security Consulting - Training

Aart Bitter RE

IT Auditor

T: +31 (599) 648 052
M: +31 (6) 573 11 593
E: Aart.Bitter@planet.nl
W: www.information-security-governance.com

ISO-27001 Lead Auditor