IT-auditor, repressief of juist preventief optreden?

Ronald Paans

Noordbeek B.V.
vrije* Universiteit *amsterdam

18 april 2008

Een persoonlijke visie met een smiley

File: IT-audit preventief RPaans versie 0.3

ronald.paans@noordbeek.com
www.noordbeek.com
Phone +31 71 3416911

DE REPRESSIEVE ROL VANDAAG

- **De IT-auditor vormt een oordeel over de betrouwbaarheid, wat dat ook mag zijn... (manco: actuele definities)**
- **In feite over vertrouwelijkheid, integriteit, beschikbaarheid, controleerbaarheid (CIAA), effectiviteit en efficiëntie**

- **Volgens een aanpak uit het begin der tachtiger jaren, aangezien wij al bijna twee decennia geen goeroes meer hebben (manco: moderne management control en principle based)**
- **De IT-auditor is altijd te laat. ITers werken *"zich uit de naad"* en de *"betweter"* komt *achteraf* vertellen wat zij beter hadden moeten doen**

- **De populariteit van het beroep ligt laag bij management en ITers, die klagen over de golf aan *"rode kaarten"* en auditors die er *"niet veel van begrijpen"***

STELLING

- **80 % van de huidige IT-audit rapporten bevat een oordeel waar de klant niet veel mee kan**

Motivatie (Wat zie ik in de praktijk ?)

- **Niet vanuit de echte risico's voor de ondersteunde bedrijfsprocessen**
- **Onvoldoende begrip voor de cultuur bij management en omgeving, zowel bij de gebruikers als bij de IT**
- **Onvoldoende inzicht in de werkelijke eisen, die moeten worden gelegd op de technische en organisatorische infrastructuur**
- **Te veel generaliseren**
- **Kopiëren matige tot slechte werkprogramma's, zonder op de echte issues in te gaan (niet voldoende normatief, te veel best practice)**
- **Geen adequate methoden en technieken voor zorgvuldige oordeelsvorming**
- **Niet weten wanneer een positief oordeel te geven, wanneer een partieel goed oordeel, en wanneer een afkeurende oordeel (de kantelpunten zijn niet gedefinieerd) Etc. etc.**

Lees dit met een smiley

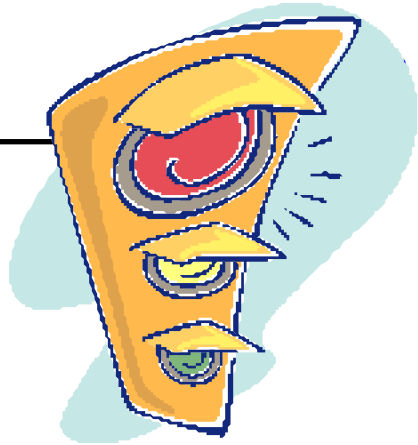
STATUS

- Stagnatie in vaktechnische ontwikkeling
- Bestaande hulpmiddelen (ISO 27001/2, Cobit, NIST, ITIL etc.) leveren geen adequate totaal oplossing
- In negentiger jaren nog forse inzet van IT-auditors volgens de klassieke aanpak (AO/IC, Memo DNB, CoP, BCM etc.)
- Afgelopen jaren forse omzet dankzij SOx
- Nu SOx afneemt, eigenlijk *te* weinig werk, omdat klassieke methode niet meer blijkt aan te slaan op de markt

STELLING

- De IT-audit aanpak krijgt het Jurassic Parc imago (net als de mainframe)

VRAAG: Wat hebben wij de klant voor nieuws te bieden?



WAT WIL DE IT-AUDITOR DE MARKT BIEDEN?

- Vertrouwen (zekerheid: het is niet goed)
- Vertrouwen (zekerheid: het is deels goed)
- Vertrouwen (zekerheid: het is goed)

WAAROM? (Is er behoefte aan ons werk? JAZEKER!)

- Maatschappelijk verkeer: Kan men vertrouwen op de processen die relevant zijn voor de burgers, en op de daaronder liggende IT? (Belastingdienst, UWV, SVB, Rijkswaterstaat, Defensie, Justitie, gemeentes, waterschappen, openbaar vervoer etc.)
- Idem: Kan men vertrouwen op de financiële gegevens van beursgenoteerde fondsen en andere organisaties (aandelen, beleggingen, pensioenen etc.)
- Business-to-consumer, business-to-business : idem

Er is behoefte aan een goed onderbouwde risicoinschatting

LEVEREN WIJ VANDAAG DE ZEKERHEID OM DIT VERTROUWEN OP TE BASEREN?

Nee, wij zijn nog te veel rule-based bezig. Toetsen van regeltjes, waarbij het de vraag is waarom die regeltjes er zijn. Zoals

- **Zijn er niet meer dan 5 beheeraccounts? (waarom 5?)**
- **Is het 's nachts te verlichten gebouw wit geschilderd met antiklimverf ?**
- **Zit er een hash total op ieder bestand ?**
- **Weet u zeker of uw collega de back-up tape goed labelt ?**
- **Rapporteert u het aantal calls per uur aan uw klant ?**
- **Is er functiescheiding bij het technisch beheer van kast 512 ?**
- **Zijn pagina's van beheerdocumentatie doorlopend genummerd ?**

Principle-based auditing breekt nog niet echt door (helaas)

GENOEG GEMOPPERD !

WAT IS NU DE OPLOSSING ?

OFTEWEL, HOE KOMT HET VAKGEBIED VANUIT HET TWEEDE MILENNIUM NU IN DE 21ste EEUW ?

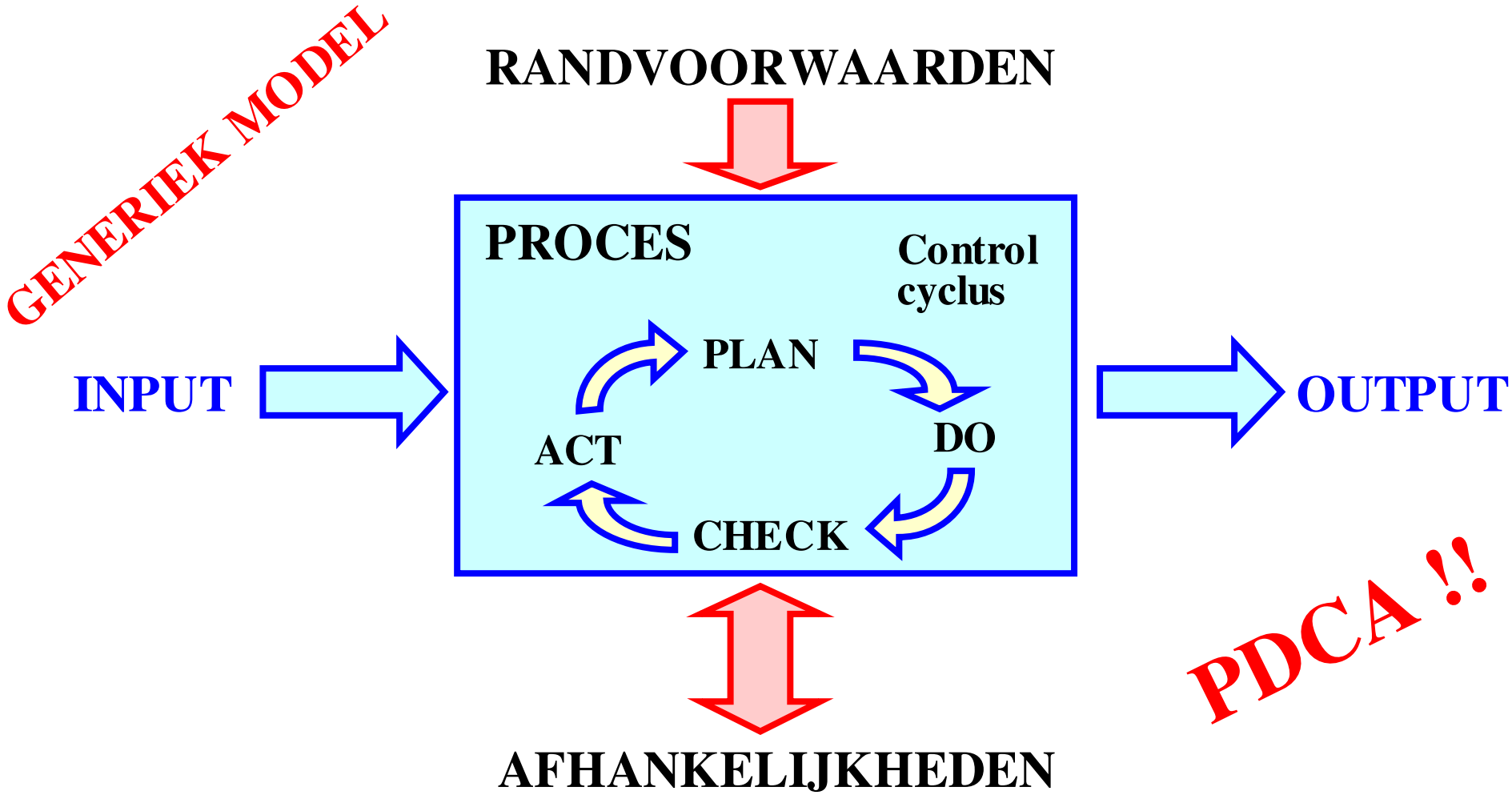
- Eerst luisteren naar bestuurders
- Dan luisteren naar management
- Plus luisteren naar ITers
- En dan een visie ontwikkelen

WAT VRAAGT EEN BESTUURDER?

- **ROL: De bestuurder realiseert de doelstelling en missie van de organisatie met een afweging van de risico's**
- **Risicomanagement staat centraal (vanuit de marktpositie, bedrijfsprocessen etc.). Zij maken zich zorgen over risico's, maar veel breder dan alleen die van IT**
- **IT-audit in de huidige vorm boeit hen niet of nauwelijks, zij zien IT als een der bedrijfsmiddelen ter realisatie van hun doel**
- **IT-projecten en systeemontwikkeling hebben bij hen een matig imago: *"het gaat toch bijna nooit zoals zou moeten"***
- **Voor hen is dat een fact-of-life en wordt ingecalculeerd**

HOE KOMT MEN BESTUURDERS TEGEMOET?

- Om hen te helpen, is inzicht nodig in hun omgeving: markt, processen, zakenrelaties, stakeholders, concurrenten, toezichthouders, compliance, kwetsbaarheden etc.
- Begrijp waar zij staan, wat hun echte zorgen zijn, en welke echte risico's zij lopen
- Is dit werk voor de IT-auditor? In feite, JA. Zonder dit "hangt" de oordeelsvorming van de IT-auditor
- Is hier een methode voor? NEEN (nog niet...)
- Dus hier ligt de eerste uitdaging: Hoe profileert de IT-auditor zich tot een boardroom gesprekspartner ?
- Antwoord: Opbouwen inzicht en ervaring (klinkt als een cliché)



Het lijkt zo simpel, maar dat is het absoluut niet

BEDRIJFSPROCESSEN

Dit is de eerste stap voor de Nieuwe IT-auditor

- **Begrijp werkelijk de business van de klant**
- **Breng die in kaart, met het gehele krachtenspel**
- **Doe nu eens een echte risicoanalyse, vanuit de rol van de bestuurder en vanuit de echte risico's die de bestuurder loopt**
- **Neem afstand van “regeltjes”, die toch niemand interesseren op het niveau van bestuurders**
- **(Eigenlijk bestond dit deels al in de negentiger jaren, zoals Business Process Analysis, maar dit is deels weggezakt en deels nooit geactualiseerd of toepasbaar gemaakt voor IT-auditing nu)**
- **En kijk naar de Do-Plan-Check-Act cyclus en zie dat CHECK faalt, CHECK en ACT niet zijn gekoppeld, en ACT faalt (het leven is zo simpel :-))**

Step 1. System Characterization

Step 2. Threat Identification

Step 3. Vulnerability Identification

Step 4. Control Analysis

Step 5. Likelihood Determination

Step 6. Impact Analysis (Loss of CIAA)

Step 7. Risk Determination

Step 8. Control Recommendations

Step 9. Results Documentation

Risicoanalyse

- Er zijn goede methoden, zoals NIST 800-30
- Alleen gebrek aan goede input op het punt van bedreigingen
- Nu: aardbeving, overstroming, brand, uitval server etc.
- Nodig: ook marktpositie, omzet, winst, tevredenheid klanten en personeel en stakeholders etc.

ONDERZOEK BIJ PGO IT AUDIT

- Ontwikkelen methode voor risicoanalyse vanuit NIST 800-30, gericht op business en IT
- Ontwikkelen lijst van bedreigingen en risico's (kans van optreden en kosten van gevolgen)
- Inmiddels bezig met pilots
- Scriptieonderwerpen en mogelijk een promovendus

Bruto risicoanalyse voor telecombedrijf met vaste lijnen (voorbeeld)

Bedreiging (bijv.)	Gevolg	Kans	Kosten
Lage klanttevredenheid	Verlies aan markpositie en omzet	H	H
Technologie	Klanten stappen over op mobiel	H	H
Grondverzakkingen	Kwaliteit kabels loopt terug door rek, kabels breken, onderhoud is moeilijker	H	M
Aardbevingen	Opstijgpunten vallen uit	M	M

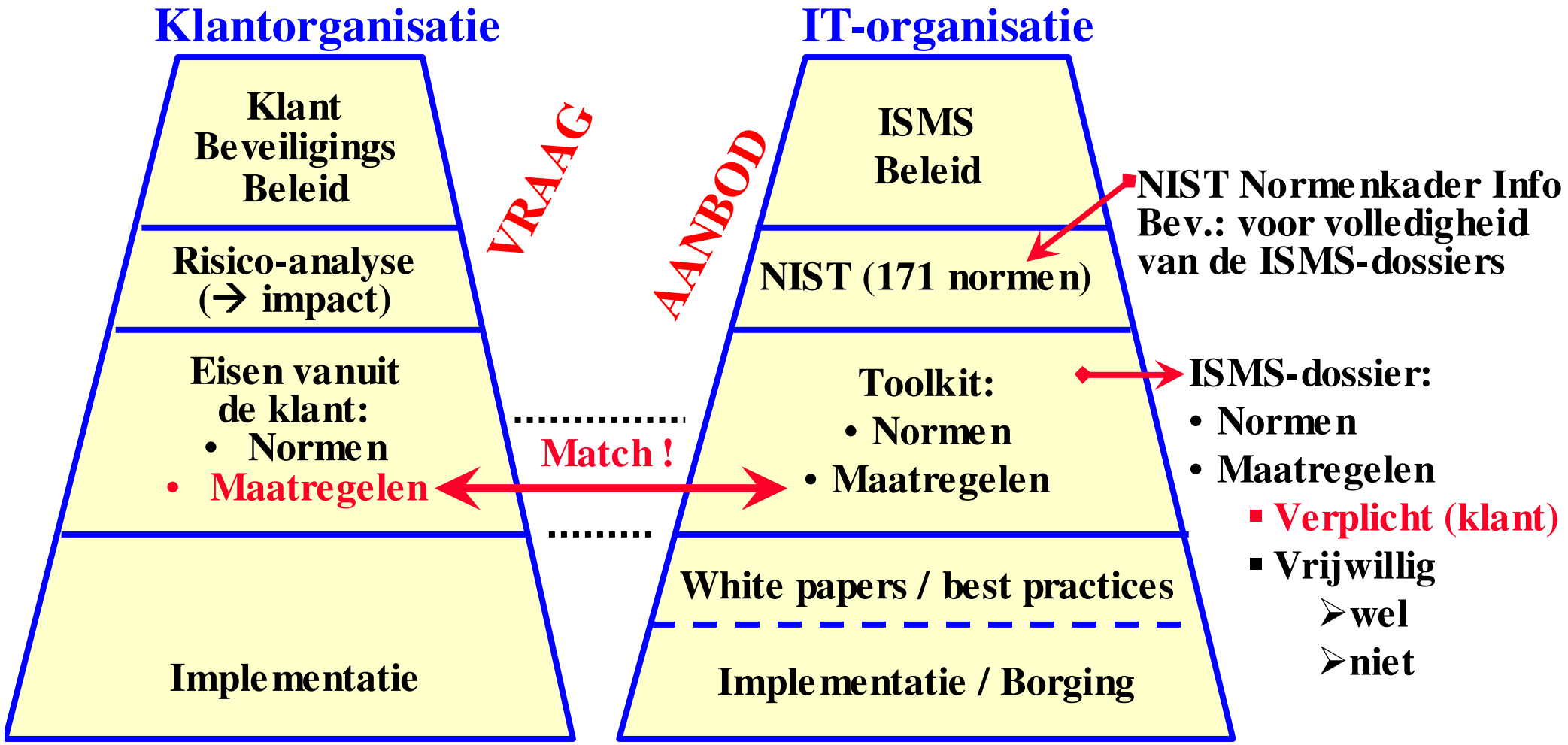
Kans van optreden	Kans
vaker dan 1 per jaar	Hoog
1 per jaar tot 1 per 10 jaar	Midden
minder dan 1 per 10 jaar	Laag

Kosten per incident	Kosten
> 10 M€	Hoog
> 1 M€ en < 10 M€	Midden
< 1 M€	Laag

Bruto risico: manifest worden van bedreiging terwijl er nog geen mitigerende maatregelen zijn getroffen (dat is volgende stap)

OVERSTAP

- In kader van de spreektijd: wij slaan de overige aspecten over van wat de IT-auditor moet betekenen bij de bestuurders, bedrijfsprocessen en risicomanagement
- Vervolgens:
  - Formuleren van de eisen vanuit de gebruikers, gesteld aan de IT, in termen zoals: functionaliteit (contract en specs), kwaliteit (SLA) en controls voor borging CIAA
  - Nieuw: specificeren geëiste controls in termen herkenbaar voor zowel de klant als de IT
  - Vereist: een gemeenschappelijke taal om controls te beschrijven


Klantorganisatie
IT-organisatie
Klant Beveiligings Beleid
Risico-analyse (→ impact)
Eisen vanuit de klant:
• Normen
• Maatregelen
Implementatie
VRAAG
AANBOD
Match !
ISMS Beleid
NIST (171 normen)
Toolkit:
• Normen
• Maatregelen
White papers / best practices
Implementatie / Borging
NIST Normenkader Info Bev.: voor volledigheid van de ISMS-dossiers
ISMS-dossier:
• Normen
• Maatregelen
▪ Verplicht (klant)
▪ Vrijwillig
➢ wel
➢ niet
Vanuit belangen van de klant:
• verplichte maatregelen
Invulling via risico-management

EISEN AAN DE LEVERANCIER VAN DE IT-DIENSTEN

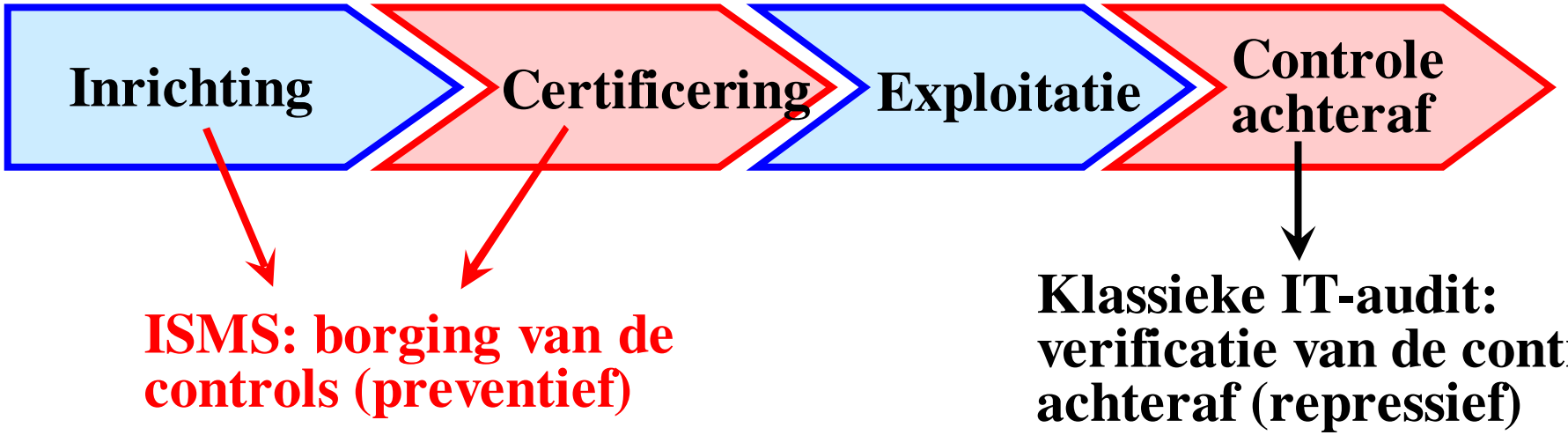
1. Goed huisvaderschap: ook zonder te vragen moet de IT als een goed huisvader een baseline aan maatregelen bieden
2. Invullen specifieke, verplichte eisen van de klant

AANTOONBAARHEID

- Nu komen wij op het cruciale punt, de rol van de IT-auditor
- Deze moet naar de markt of klant aantonen dat vertrouwen terecht is
- Hiervoor moet deze weten welke maatregelen (controls)
  - Zijn verplicht door de klant
  - Zijn getroffen vanuit goed huisvaderschap
  - Niet zijn getroffen en waarom (kosten / baten)

WAAR HEEFT DE MARKT BEHOEFTE AAN?

- Kijkend naar voorgaande, is de markt echt geholpen met een oordeel achteraf?
- NEEN
- De IT-auditor heeft unieke vaardigheden, namelijk redeneren vanuit bedrijfsprocessen en risico's, naar maatregelen en de effectiviteit van die maatregelen
- **Advies:** Gebruik die vaardigheden eerder in het traject, namelijk bij de inrichting
- **Voordeel:** Daarmee worden "aantoonbaarheid" en "vertrouwen" **vooraf** gecreëerd
- En krijgt men tevredener klanten en tevredener ITers



Doelstelling

- Fabriek specificeert kwaliteitssysteem en aan te bieden maatregelen
- Fabriek controleert zelf, signaleert manco's en stelt actieplannen op
- Als iets al bekend is en onderhanden is → geen rode kaart
- Directeur IT tekent dat is ingericht en dat is gecontroleerd binnen de fabriek ("certificaat van compliance met eigen regels")

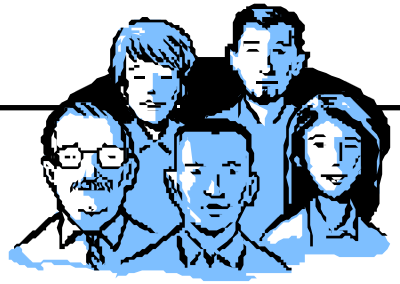
(dit is het idee van IT Governance en ook de basis van SOx)

DE AANPAK

- De IT-auditor heeft unieke vaardigheden en is als geen ander in staat de controls te doorgronden
- Controls zijn echter gebonden aan objecten

De aanpak is

- Opstellen van een beheeratlas, dat is een decompositie van de IT-organisatie en infrastructuur in samenhangende delen, op basis van beheerhandelingen ("opsplitsen in behapbare brokken")
- Per domein scope vaststellen, plus de daarvoor passende normen uit NIST 800-53
- Normen vertalen in maatregelen (controls)
- De lijn coachen bij het realiseren van de controls en het vervaardigen van de beheerdocumentatie
- Vervolgens opzet en bestaan vaststellen in twee stappen, namelijk als coach en, door een onafhankelijke IT-auditor, ter bevestiging

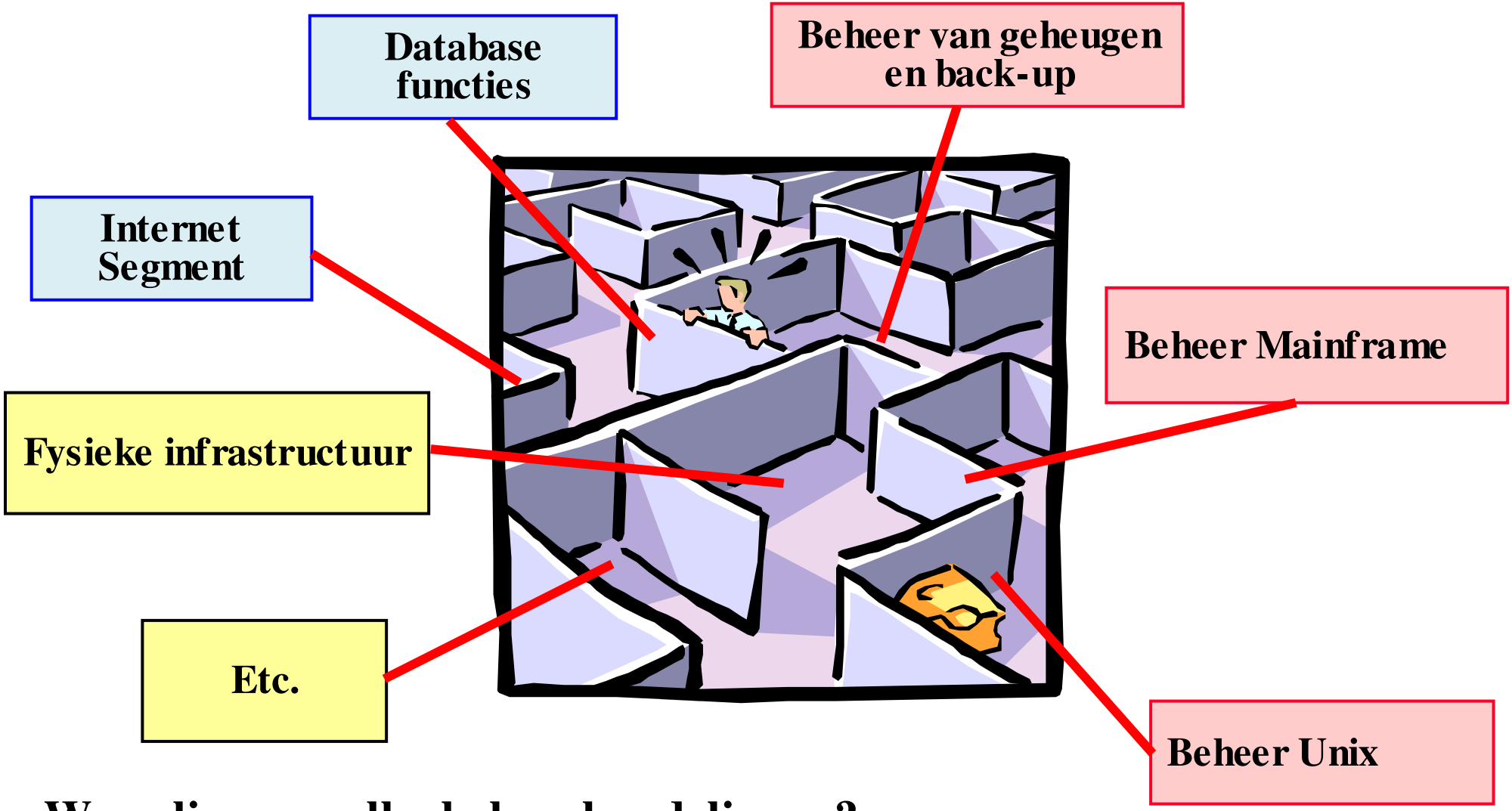


Definitie Beheerdomein

Een samenhangend geheel van een of meer componenten en beheerders gericht op een bepaalde verzameling aan functionaliteit, met één verzameling beheerdocumentatie, gericht op operationeel beheer

- **Beheer betreft personen die handelingen uitvoeren**
- **Beheerhandelingen zijn ondeelbaar en moeten altijd plaatsvinden, zoals**
  - **Als een kabel breek moet iemand de KPN graafploeg bellen**
  - **Kabels moeten worden bewaakt**
- **Een groep samenhangende beheerhandeling vormt een domein → daarvoor geldt een groep normen en maatregelen**

De beheerdomeinen binnen een IT-fabriek



Waar liggen welke beheerhandelingen?

PER BEHEERDOMEIN

Op basis van de kennis en kunde van de IT-auditor

- **Stel vast welke bedreigingen werkelijk relevant zijn voor de componenten en processen binnen dit domein**
- **Doe dat samen met een groep personen met ervaring, zoals architecten, beheerders, lokale kwaliteitsmedewerkers, interne controle functionarissen, interne IT-auditors etc.**
- **Zorg voor voldoende deskundigheid en strak geleide workshops, waarbij iedereen vooraf zich oriënteert en voor adequate input zorgt**
- **Zorg voor tussenposes zodat iedereen tussenrapportages kan lezen en er nogmaals over na kan denken**
- **Het resultaat is een weloverwogen inschatting van risico's**

Preventief omgaan met controls binnen een beheerdomein

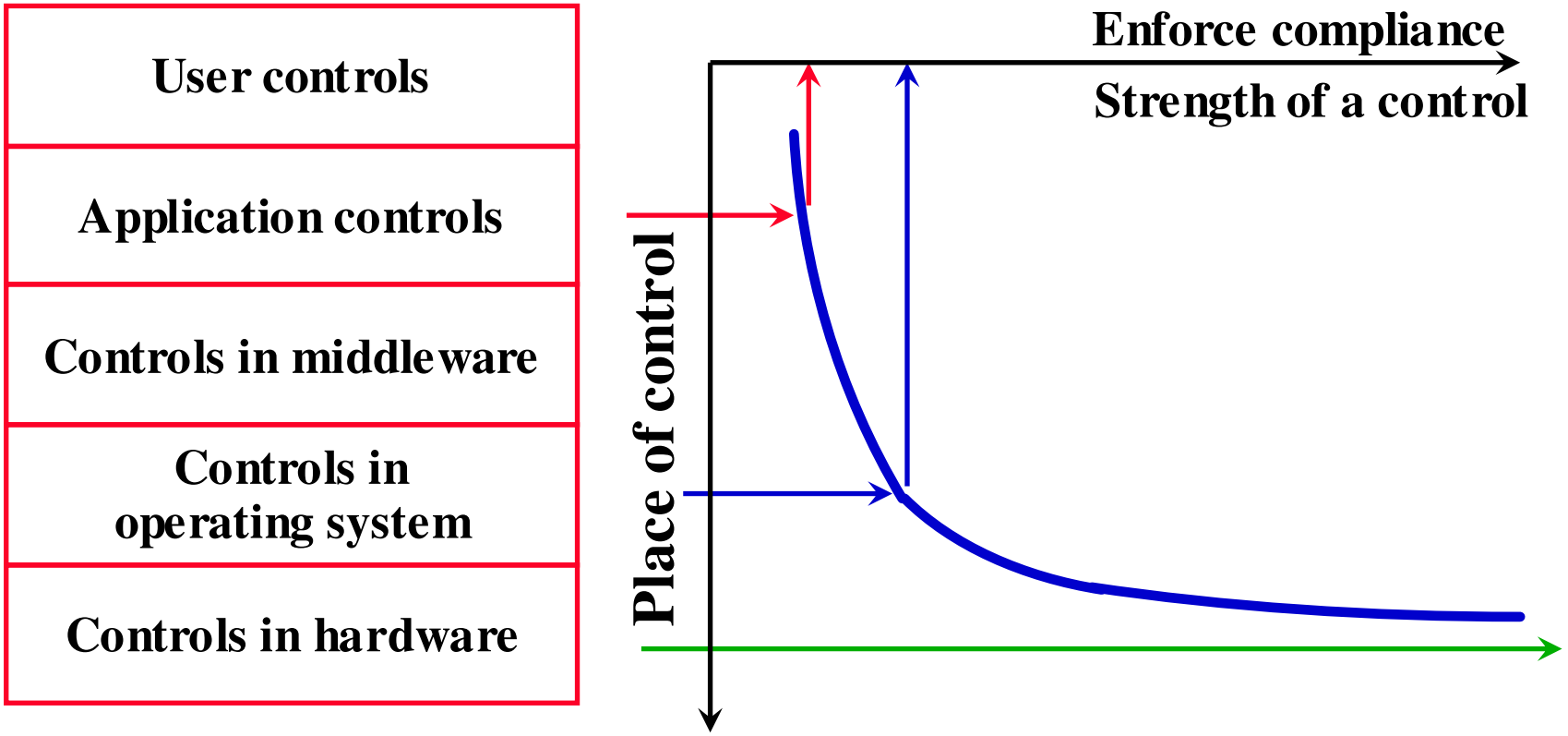
Proces	Doel	Resultaat
1. Intakeworkshop	• Vaststellen scope • Bruto risicoanalyse • Vaststellen eisen CIAA	Afbakenen en inkaderen
2. Risicoworkshop	• Vaststellen normen	Ontwerpen controls
3. Validatieworkshop	• Vaststellen maatregelen	
4. Beheerdocumentatie	• Verantwoordelijkheid lijn • IT-auditor coachend	Inrichten controls
5. Verificatietoetsing	• Vaststellen netto risico (en restrisico)	Toetsen controls
6. Certificatietoetsing	• Bevestiging restrisico	
7. Certificering IT-dir		

CONTROLS

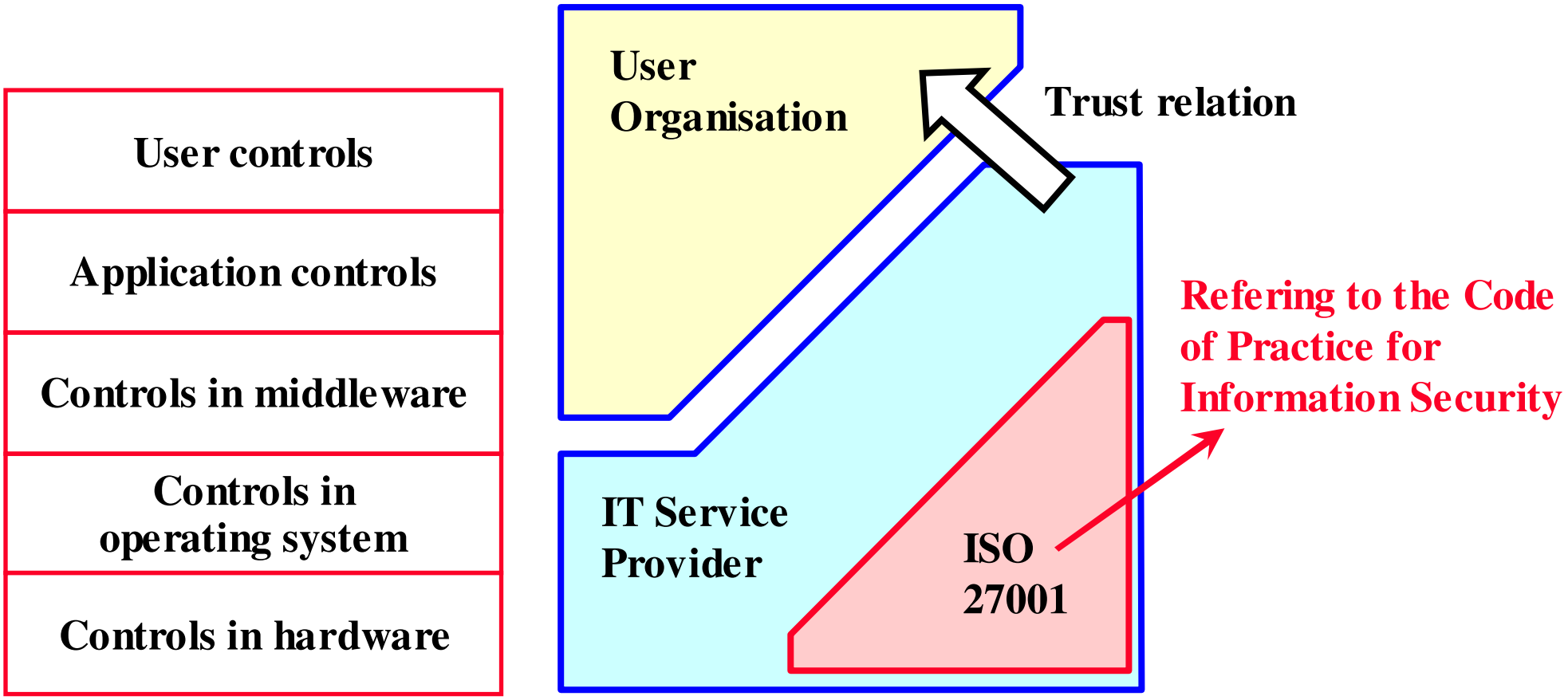
- In feite een vaag begrip binnen de IT
- Accountants zijn veel verder, maar hun theorie past niet bij de IT
- Dan maar uitgaan van wat bekend is uit de AO/IC: gebruikers controls, ondersteund door applicatieve controls en General IT Controls
- Een control is een maatregel of een verzameling aan samenhangende maatregelen, sommige onvervangbaar, andere compenserend
- IT-audit kent wel de maatregelen: ISO 27001/2, ITIL, CRAMM etc., allen voortkomend uit best practices en zijn facultatief

Strength of controls

Controls form a column. When the control is located lower, it is more effective and has more strength



Scope of responsibilities



An ISO 27001 certificate is only a partial solution. However, it provides a foundation for trust. It shows the trustee is paying attention to security

ONDERZOEK BIJ PGO IT AUDIT

- Ontwikkelen methode voor het opdelen van de IT in disjuncte beheerdomeinen, vanuit oogpunt IT-auditing
- Ontwikkelen methode voor het alloceren van normen en maatregelen aan specifieke domeinen
- Inmiddels bezig met pilots (met deels CRAMM voor maatregelen)
- Scriptieonderwerpen en mogelijk een promovendus

TOT SLOT

- De IT-auditor heeft een hoge toegevoegde waarde in een preventieve rol, namelijk vooraf de ITers vertellen wat belangrijk is vanuit het bedrijfsproces
- Het “audit-gereed” maken van de IT borgt de controls, hetgeen veel belangrijker is dan het achteraf aangeven wat mis is
- Wij moeten afstand nemen van regeltjes en ons richten op de echte risico’s
- NIST 800-53 blijkt prima te voldoen als overkoepelend normenkader, als hulpmiddel om de volledigheid van de controls te borgen
- De "taal" voor het specificeren van de maatregelen is een nog op te lossen probleem

De stukken waarnaar is verwezen tijdens deze presentatie zijn:

- **http://csrc.nist.gov**
- **NIST = National Institute of Standards and Technology, U.S. Department of Commerce**
- **NIST SP 800-30 "Risk management guide for information technology systems"**
- **NIST SP 800-53 “Recommended security controls for federal information systems”**