Van "Rule based" naar "Principle based" IT Audit

En hoe leiden wij hiervoor op?

Ronald Paans
vrije* Universiteit *amsterdam

14 november 2006

Noordbeek B.V.
Ronald.Paans@noordbeek.com
www.noordbeek.com
Tel. 071 3414632

Inhoud

- **Wat verwacht de markt van de IT-auditor en een post graduate opleiding?**
- **Hoe ziet de collegestof er uit om daaraan te voldoen?**
  Inzoomen op het nieuwe tweede jaar
- **Wat zijn de moderne speerpunten?**
- **Klant versus leverancier + binnen leverancier: goed huisvader en heldere ontkoppelvlakken**
- **Gebruik van standaard normenkaders en maatregelenkaders**
  Vind niet zelf het wiel uit!

NOREA Beroepsprofiel

Een gekwalificeerde IT-auditor geeft onpartijdige oordelen en adviezen over de kwaliteitsaspecten van IT

De kwaliteitsaspecten zijn, mede vanwege de maatschappelijke relevantie, hoog en betreffen effectiviteit, efficiëntie, exclusiviteit, integriteit, controleerbaarheid, continuïteit en beheersbaarheid

De IT-auditor handelt in rechtstreekse opdracht van het (top)management, maar kan ook bijstand verlenen aan een (interne dan wel externe) accountant

De oordelen hebben betrekking op de volgende IT-objecten: informatiestrategie, management van informatie en informatietechnologie, informatiesystemen, technische systemen, processystemen en operationele ondersteuning.

Bron: Jaarboek 2006/2007 NOREA

Basiscompetenties

- **Het beroep van IT-auditor vereist deskundigheid op het gebied van informatietechnologie, bestuurlijke informatievoorziening en organisatiekunde**
- **Verder hebben IT-auditors kennis van methoden en technieken voor onderzoek, toetsing en risicoafweging**
- **Bovendien hebben zij ervaring op het gebied van IT-kosten en hebben zij specifieke deskundigheid van toepassingsgebieden**

Vereist opleidingprogramma

RP/VU
NOV/2006

NOREA eisen aan opleidingsprogramma, o.a.

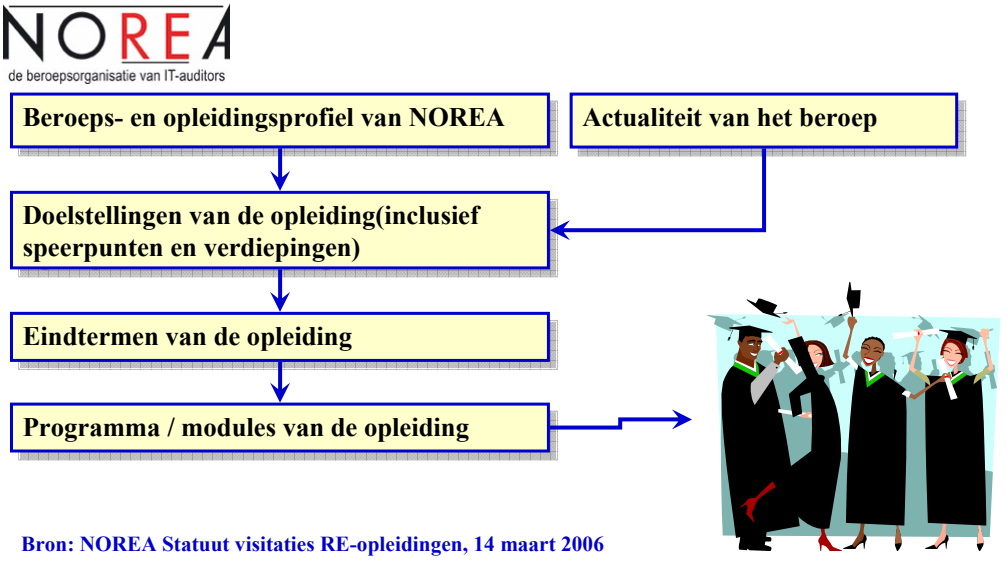
- Informatiestrategie en informatiemanagement
- Informatiesystemen
- Technische systemen
- Automatiseringsondersteuning

Aandacht dient te worden besteed aan

- De functionaliteit op operationeel, tactisch en strategisch niveau
- De daarin toegepaste technologie en procedures
- De beheersmaatregelen
- De (IT-)specifieke risico's en kwaliteitsaspecten
- De wijze waarop de maatregelen kunnen worden getoetst op bestaan en werking
- De (compenserende en aanvullende) controle- en beheersmaatregelen vanwege het advies aan de organisatie hieromtrent

Relatie naar opleiding

RP/VU
NOV/2006



Bron: NOREA Statuut visitaties RE-opleidingen, 14 maart 2006

VU Post Graduate IT Audit Opleiding

(geen Post Master, geen Post Initieel etc.)

- Filosofie: bouwstenen informatie in eerste jaar (BIV, auditing) en tweede jaar (techniek, audit van techniek, beheer), integratie in het derde jaar
- Eerste jaar is reeds gemoderniseerd
- Opzet tweede jaar wordt geheel herzien in dit collegejaar 2006/2007
- Herstructurering derde jaar is afgerond
- Examinering is vervangen door een scriptie
- Visitatie en accreditatie door NOREA is afgerond
  - Titel: Executive Master in IT Auditing
  - (MSc accreditatie is nog niet mogelijk doordat de wetgever nog bezig is met het Post Graduate Onderwijs)

STRUCTUUR

Eerste jaar (januari – juni)

- Primair de inrichting van de administratieve organisatie en interne controle. Komt overeen met de betreffende modules in de post graduate opleiding voor registeraccountant

Tweede jaar (september – mei)

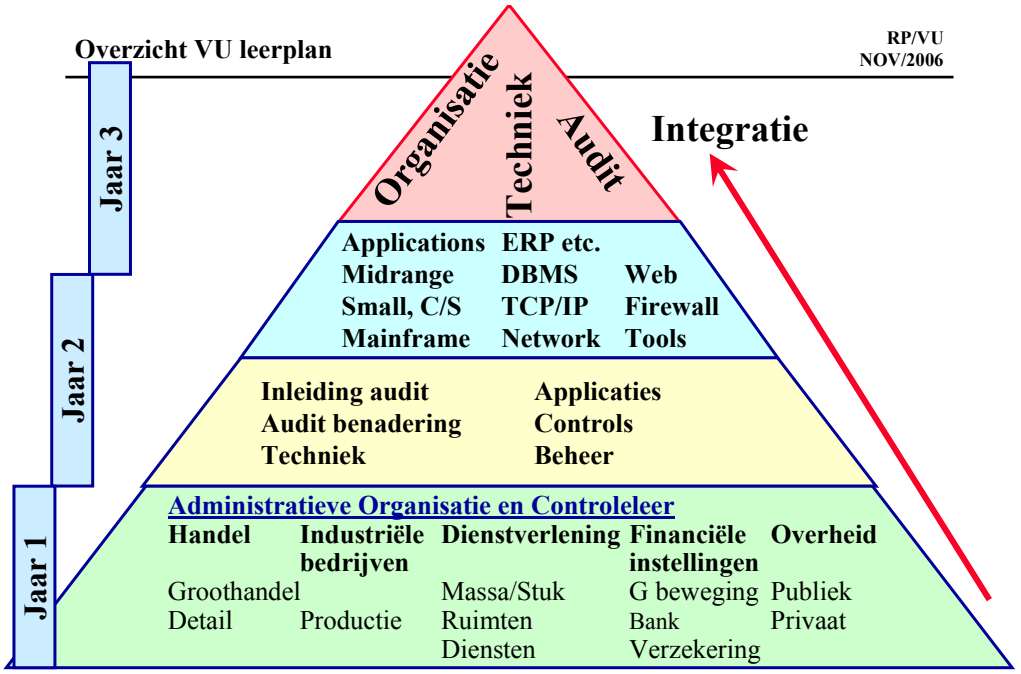
- Technische vaardigheden en beheer van IT, c.q. kennis die IT auditor zich eigen moet maken voor beroepsuitoefening

Derde jaar (september – mei)

- Samenbrengen van de verschillende competenties die tot dan toe zijn opgedaan
- Leerdoelstelling: integratie tussen de bestuurlijke informatie verzorging, auditing, techniek en het praktische kader van de beroepsuitoefening van de IT auditor

Overzicht VU leerplan

RP/VU
NOV/2006



Tweede jaar

RP/VU
NOV/2006

Module 2.1 (5)
Introductie IT audit

Module 2.2 (11)
Techniek en audit van platformen
- Hardware base
- Operating system
- Logical security
- XP/2003 + case
- Middleware C
- Unix + case
- i5/OS = AS/400
- Physical security

Module 2.3 (11)
Techniek en audit van datacommunicatie
- OSI model C
- Netwerk architecturen
- Cryptografy
- LAN, TCP/IP
- Firewall
- Wireless, email, VOIP
- Web architecturen
- Security beheer
- Casus C

Module 2.4 (11)
Inrichting en audit van IT beheer
- CobiT
- ITIL
- Tactical processes: SLM, costing and charging, security
- Operational processes: change, incident and problem management C
- Project risk management
- Information system development
- Application controls
- Sourcing, SOx and SAS 70
- Case: Outsourcing
- Risk management

Totaal 37 dagen

C = Tentamencasus uitwerken

Rode lijn in tweede jaar

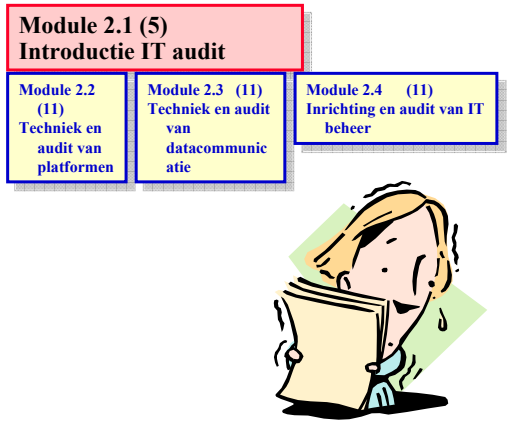
- Code voor Informatiebeveiliging (Code of Practice, ISO 17799 / ISO 27002) voor maatregelen
- US standard NIST 800-53 "Recommended security controls for federal information systems" voor normen
- Module IT audit: aanpak van audit en rapportage
- Module Platformen: matrix benadering en het faciliteren van applicaties als doelstelling
- Module Datacom: hoe ziet de moderne web wereld er uit en hoe vorm je daar een oordeel
- Module Inrichting en audit van beheer: CobiT, ITIL, (project) risk management, applicatie ontwikkeling, applicatieve controls, outsourcing

Module: IT Auditing

- Studenten hebben weinig ervaring met opdrachtuitvoering en rapportage

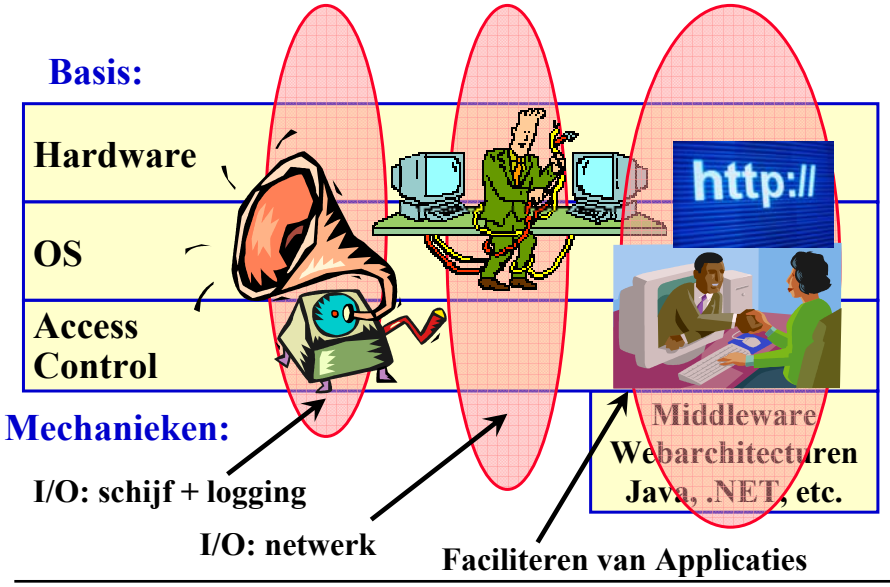
5 weken aan begin 2de jaar

- Basisbegrippen
- Workshop
  - Intake en opdrachtformulering
  - Normenkader
  - Bevindingen omschrijven
  - Concept rapport
  - Afstemmen met auditee
  - Eindrapport



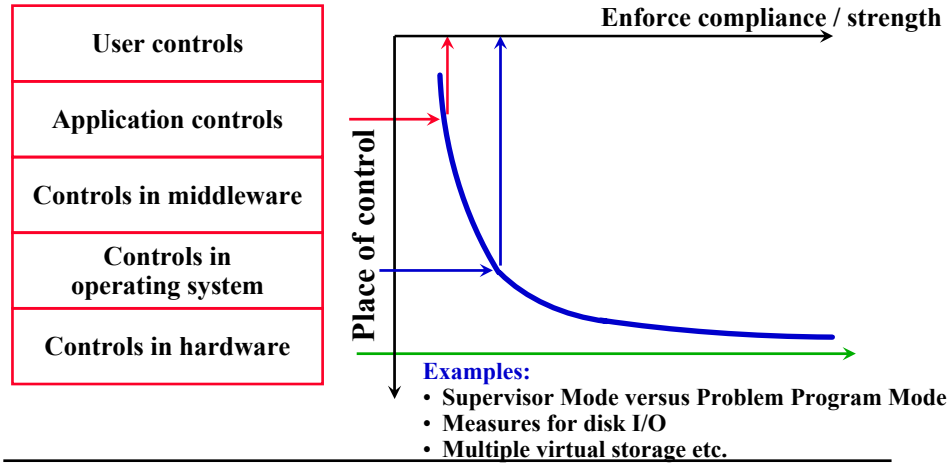
Leerdoelstelling: Het klassieke ambachtelijke werk aanleren van scope, kwaliteitsaspecten, normen opstellen, toetsen, negatieve en positieve bevindingen vastleggen, risico's inschatten en aanbevelingen opstellen

Ervaring in 2006/2007: Meer individuele coaching nodig



Strength of controls

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

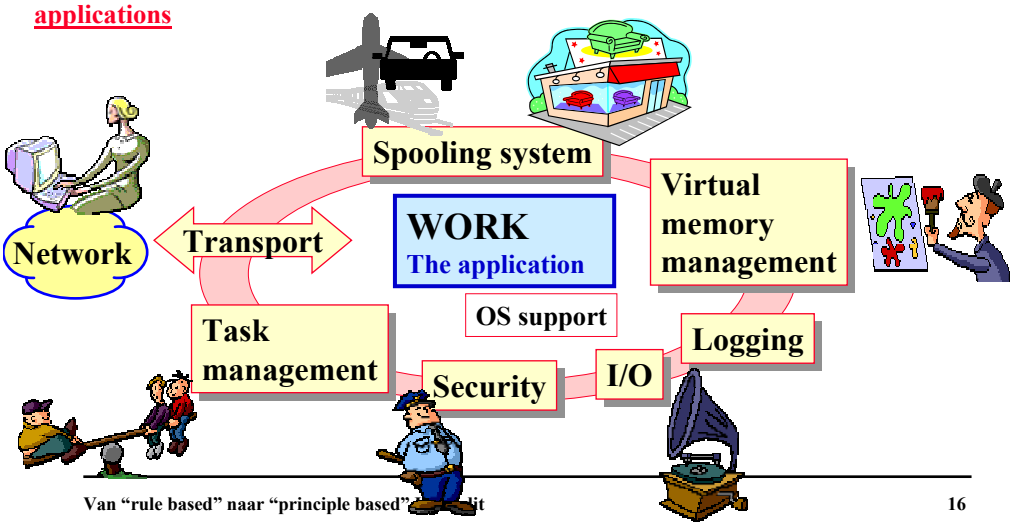


Internal controls voor jaarrekening RP/VU NOV/2006

The model for OS RP/VU NOV/2006

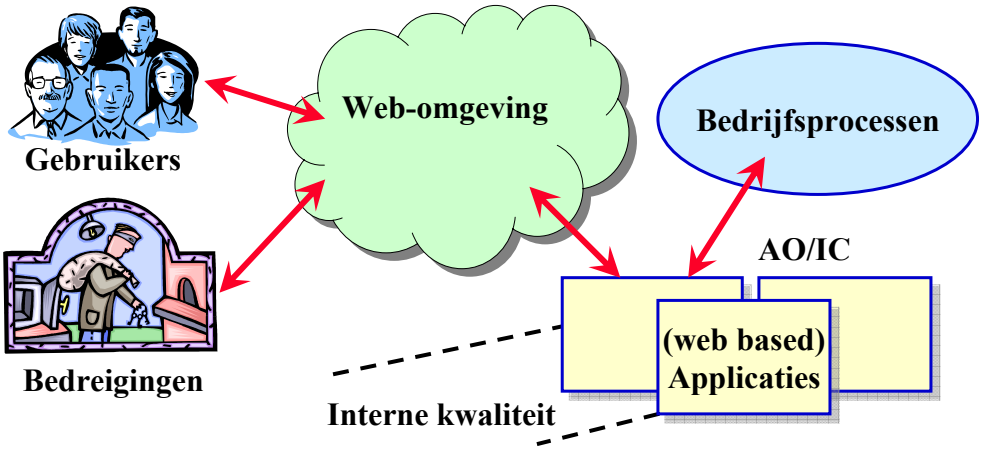
THE MODEL FOR THE OPERATING SYSTEM

The hardware and operating system provides all the functionality required to execute applications



Modules 2.3 en 2.4

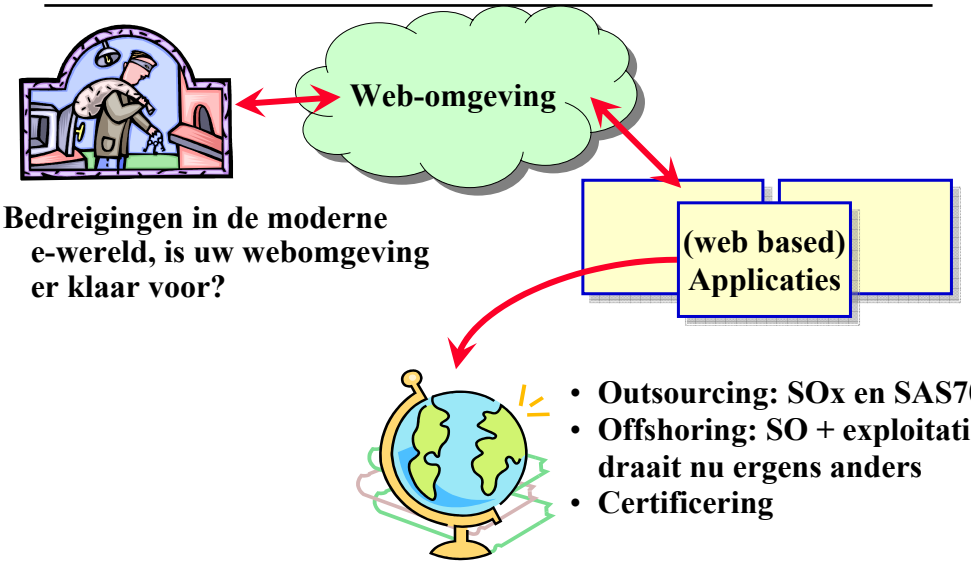
RP/VU
NOV/2006



- **Hoe beheerst men het: ITIL**
- **Hoe bouwt men het en welke controls zitten waar**
- **Wat kost het en wat levert het op (uit oogpunt IT Auditor)**

Modules 2.3 en 2.4 …

RP/VU
NOV/2006

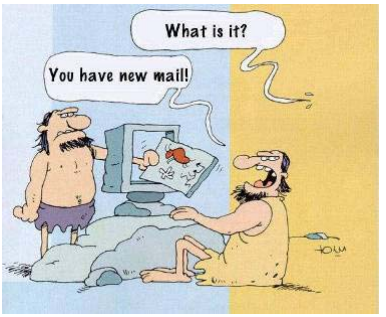


Motto: Van "rule based" naar "principle based"

- **IT Audit was van oudsher een ambachtelijk beroep, gebaseerd op gedegen normenkaders en lange werkprogramma's**
- **IT-audit-rapporten blonken uit door degelijkheid en omvang (en saaiheid)**
- **Wij leren onze studenten en juniors nog steeds deze aanpak**
- **Maar er moeten ook andere methoden zijn om tot een deugdelijke grondslag te komen voor de oordeelsvorming over de kwaliteit van IT**
- **Niet alleen moet het vak "leuk" blijven, maar ook efficiënt en effectief, leidend tot een helder oordeel over wat wel en wat niet goed is**

JURASSIC IT

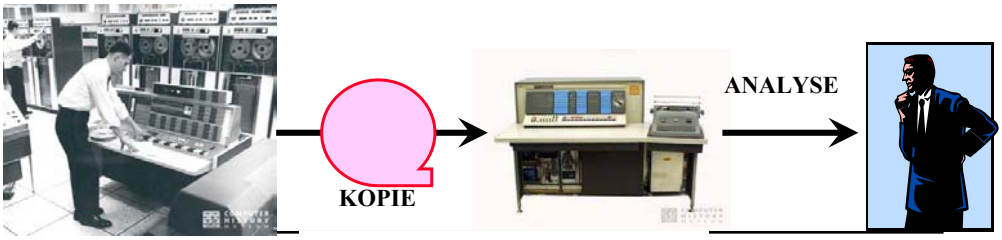
- **Mainframes: in 1950 was de verwachting dat één mainframe voldoende was voor Europa…**
- **Begonnen met de Closed Shop**
- **Toepassingen: administratie en wetenschappelijk berekeningen**
- **Integriteit en vertrouwelijkheid snel onder controle**
- **Beschikbaarheid was de belangrijkste zorg**



HISTORY:
IBM Model 1620 (1959)
- **Decimal variable word length**
- **No general registers, to sum numbers a table was used**
- **Memory 60 k**
- **Price: $ 64.000 (some 5.000 delivered)**

ONTSTAAN VAN IT AUDIT

- IT audit is langzaam gegroeid vanuit de accountancy
- Zij controleerden de boekhouding en AO/IC, en zagen die langzaam de computer inschuiven…
- Eerste poging begin 80er jaren: AC-accountant (AC = Accountant en Computer)
- Vooral kopiëren van bestanden uit het mainframe en op eigen computer met eigen software de boekhouding controleren



 Dit was de Jurassic IT Audit

De Nederlandsche Bank: Memorandum omtrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen

- 20 september 1988
- Bijna een normenkader:
  Sectie 5, B, 2.9: Beveiligen van gevoelige informatie tijdens transport tegen ongeautoriseerd raadplegen of veranderen (datatransmissie met behulp van communicatienetwerken, tape-transport, transport van PC-gegevensdragers enz.)

Ideaal hulpmiddel voor het "afvinken", en de basis voor vele DNB-gesprekken met bankdirecties, interne en externe accountants, en IT-auditors

In die tijd: alles werd uitgebreid uitgeschreven → soms werd dat vooral "papieren" veiligheid ("rule" based)

RULE BASED – in detail alles voorschrijven

Voorbeeld, NAVO standaard voor informatieclassificatie

Art. 34.0.3. Aangetekende brieven met aangegeven waarde mogen *niet* ter verzending worden aangeboden, indien

- het adres met potlood is geschreven
- het adres is opgeplakt
- het adres met de schrijfmachine is geschreven en door onderstreping een snee in het papier is ontstaan
- vensterenveloppen zijn gebruikt
- de postzegels en de op de postdienst betrekking hebbende stroken zonder enige tussenruimte naast elkaar zijn opgeplakt of over twee zijden van de verpakking zijn gevouwen
- de vermelding van het bedrag van de aangegeven geldswaarde met potlood of inktpotlood is geschreven etc.

RULE BASE versus PRINCIPLE BASED

- RULE BASED geeft geen ruimte voor eigen initiatief en eigen verantwoordelijkheid
- Alles wordt voorgeschreven, dus men wacht op instructies. Men pakt niets vooraf op, *"want het zal toch wel niet mogen volgens de regeltjes"*. Audit is hierbij vooral *"afvinken"*

Moderne aanpak voor Corporate Governance

- behaal op verantwoorde wijze de doelstellingen en/of winst en laat zien dat risico's goed worden afgewogen en men "in control" is

Moderne aanpak voor IT Governance

- zorg voor het leveren van de diensten met de afgesproken kwaliteit en laat zien dat dit op een verantwoorde wijze gebeurd

Dit geeft de leiding van IT de ruimte hun business kosteneffectief in te richten volgens hun eigen normen en standaarden

Belangrijk: zij moeten kunnen aantonen hoe zij het doen !

Rule based versus Principle based …

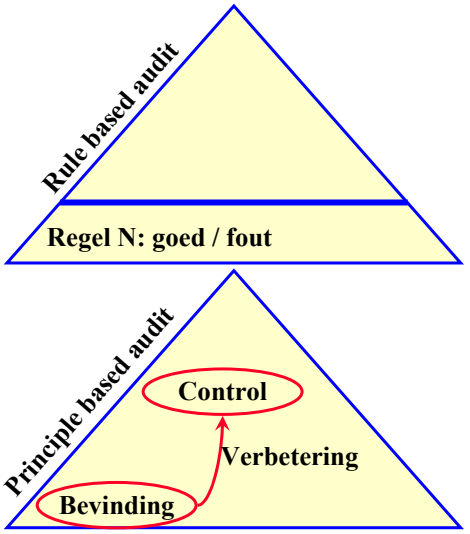
RP/VU
NOV/2006

Rule Based Audit

- Analytische decompositie tot de kleinste details
- Bevindingen blijven laag hangen in de organisatie

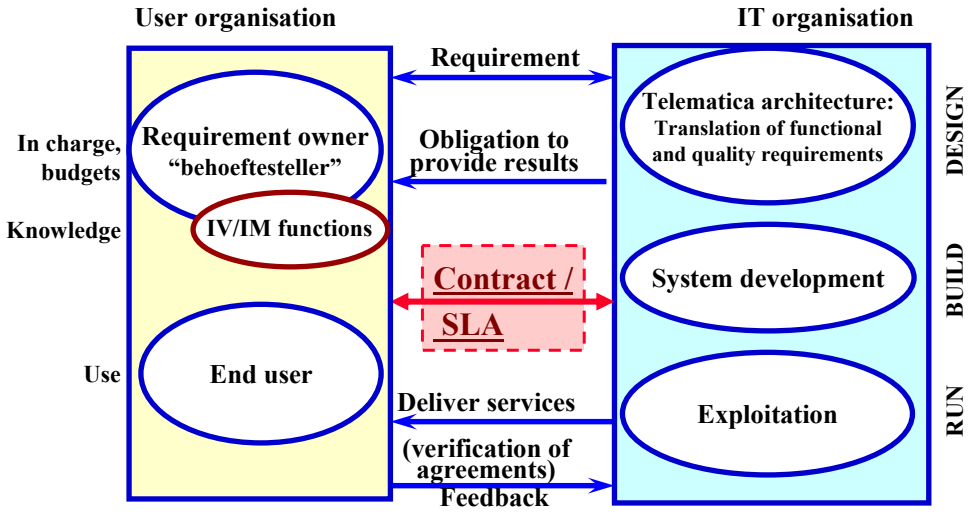
Principle Based Audit

- Meer synthese van detail-bevinding tot conclusies over wezenlijke problemen en oplossingen
- Verbeteringen liggen op hoger niveau binnen de organisatie
- Men verbetert de control



Moderne IT: ontkoppelvlakken

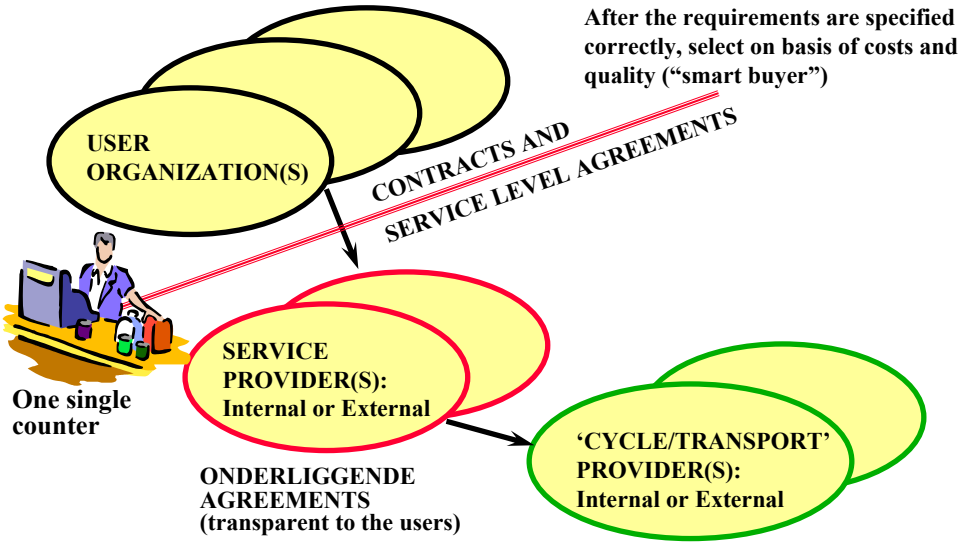
RP/VU
NOV/2006



IV/IM = Informatie Voorziening / Information Management

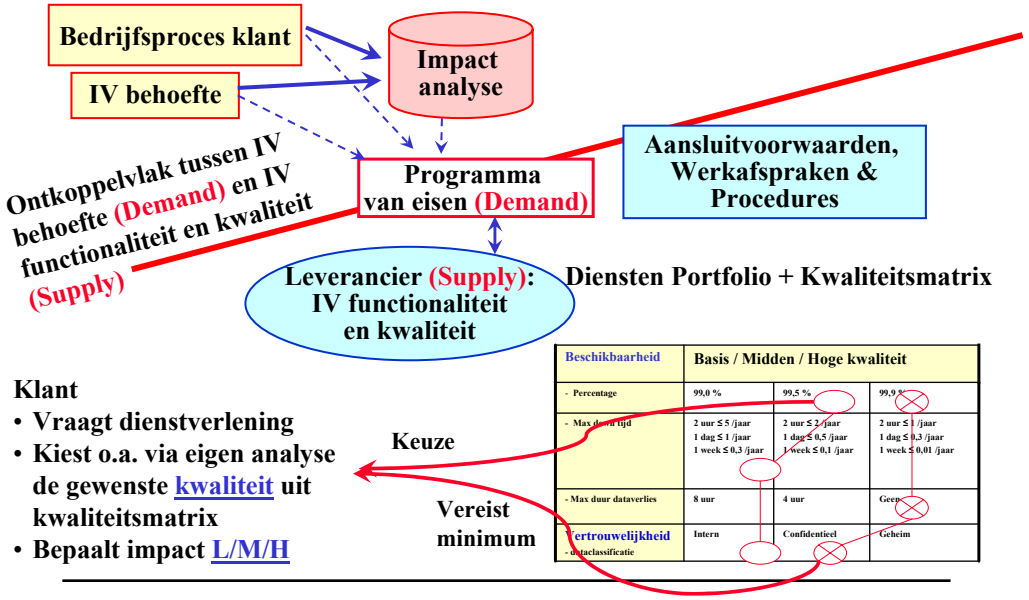
IT service provider (intern of extern)

RP/VU
NOV/2006



Ontkoppelvlak Demand en Supply

RP/VU
NOV/2006



DE IT AUDIT VANDAAG

- Complexe netwerk infrastructuur die vele bedreigingen kent
- Gedistribueerde verwerking met vele kopieën van gevoelige gegevens
- Complexe applicaties met hoge toegankelijkheid
- Bedrijfsprocessen die steeds meer afhankelijk worden van de IT
- Hinder van virussen, trojaanse paarden, spyware etc,
- Mondiale aanpak: waar staan uw gegevens en waar uw applicaties?
- De kosten van IT liggen "onder vuur"
- Meer aandacht van toezichthouders en wetgevers: DNB, AFM, Sarbanes Oxley, etc.
- Meer risico's voor accountants: claims, imago
- Krapte op de IT-audit markt: te weinig aanbod van echt ervaren IT-auditors → verhoging van de efficiëntie van het IT-audit-vak is dringend nodig

DE MODERNE AANPAK VAN IT AUDIT

- Laat het inrichten over aan de vakmensen binnen de IT. Het hoe is minder belangrijk
- Het principe voor de IT-er
  - Doe wat je zegt
  - Toon aan wat je doet
  - En doe het verantwoord
- Zij zijn in staat de complexe IT te runnen. Zij zijn ook in staat, mede aan de hand van vele boekjes, de zaak veilig in te richten (in feite het "principe" van een goed "huisvader")
- Laat hen een deugdelijk "systeem" van beveiliging en interne controle inrichten; geef hen de principes, niet de regeltjes
- Wij als IT auditors moeten toetsen of dat "systeem" werkt

Het ideaal van de IT-auditor

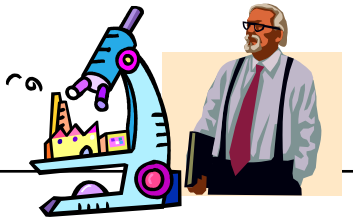
RP/VU
NOV/2006

Van het gegevensgerichte vinken

Naar een geolied systeem met check and balance

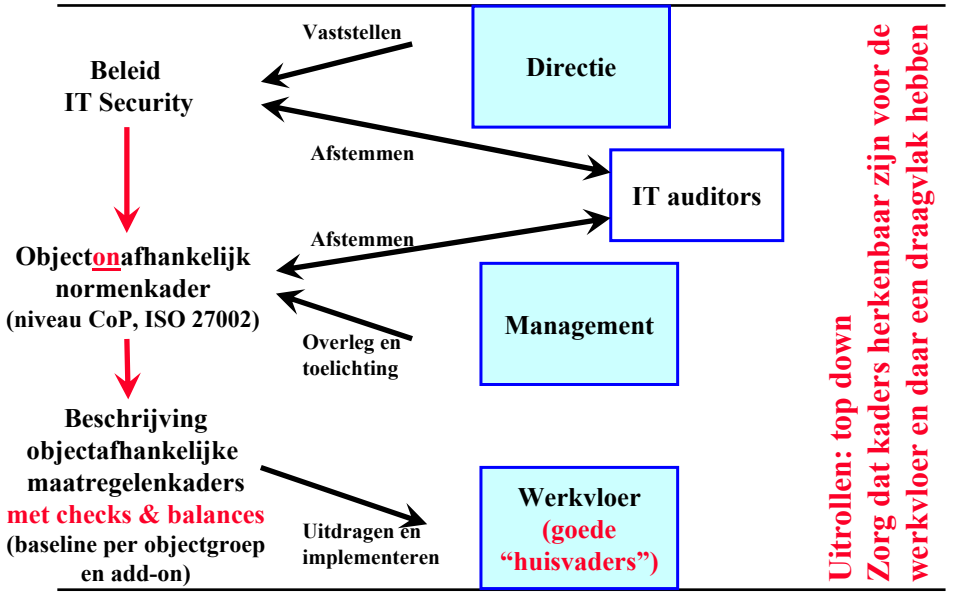
Via goed "huisvaderschap" van de ITers

Waar wij ons oordeel over vormen



Uitrollen IT Security

RP/VU
NOV/2006



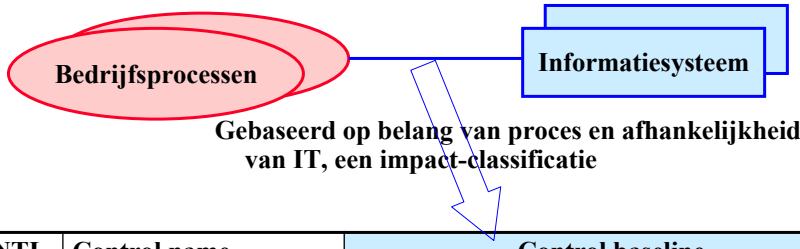
Objectonafhankelijk normenkader

- **Waarom zelf opstellen, als er goed materiaal op Internet staat (gratis)**
- **NIST 800-53 "Recommended security controls for federal information systems"**
- **NIST = National Institute of Standards and Technology, US Department of Commerce**
- **Deze standaard is een bundeling van Code of Practice (ISO 17799), militaire US Standard DoD 8500.2 etc.**
- **Pragmatische aanpak, heldere indeling**
- **Gaat uit van risico / impact-analyse: hoe kwetsbaar is het ondersteunde bedrijfsproces en wat zijn de gevolgen van verstoringen, resulterend in driedeling high, moderate en low impact**
- **Normen: baseline plus een impact-afhankelijke delta**
- **Voordeel: men hoeft niet zelf het normenkader te ontwerpen en het onderhoud wordt daar gedaan**

http://csrc.nist.gov

Indeling normenkader

RP/VU
NOV/2006



CNTL NR	Control name	Control baseline		
		Low impact	Moderate impact	High impact
Group	Access control			
AC-1	Access control policies and procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (Delta's)	AC-2 (1) (2) (3) (4)

Groups of controls

RP/VU
NOV/2006

NIST 800-53 Groups of Controls

1. Access control
2. Awareness and training
3. Audit and accountability
4. Certification, accreditation and security assessments
5. Configuration management
6. Contingency planning
7. Identification and authentication
8. Incident response
9. Maintenance
10. Media protection
11. Physical and environmental protection
12. Personnel security
13. Risk Assessment
14. System and services acquisition
15. System and communications protection
16. System and information integrity

Schriftelijk slotexamen

- Er was een theoretisch gedeelte van het slotexamen over de gehele scope van het vakgebied. Dit was tot 2004/2005 een schriftelijk open boek examen
- Dit is vervangen door de 4 + 3 tentamencasussen in het 2de en 3de jaar als toetsmomenten tijdens de modules

Slotexamen Casus

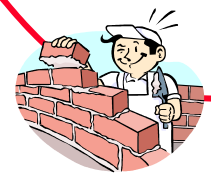
- Er was een klassieke slotexamencasus tot 2005/2006: een casusuitwerking van ongeveer 3 uur in de vorm van een schriftelijk examen
- Deze is vervangen door een scriptie naar eigen keuze, op academisch niveau. Hierbij wordt een praktijkcasus uitgewerkt door 1 of 2 studenten onder begeleiding van een bedrijfsinterne coach en een VU docent

Mondeling slotexamen

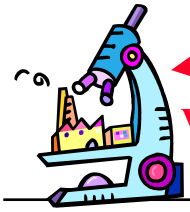
- Slotexamen van 1 uur met scriptie als uitgangspositie en verder over collegestof en vakgebied
- De kandidaat dient individueel blijk te geven van vaardigheden en inzicht in het vakgebied van de IT-auditor

VAN regels opstellen door IT auditors

NAAR principes opleggen en ITers zelf hun eigen regels laten opstellen en invullen



EN laten aantonen dat het juist is



VIA principle based IT Audit