Effect van de Crisis
Op de Organisatie van IT

Ronald Paans

vrije **Universiteit** ***amsterdam***

29 april 2009

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

File: Crisis en Organisatie van IT

DOEL VAN AUDIT

- **Het geven van Assurance, namelijk het verminderen van onzekerheid bij belanghebbenden**

Hebben wij als beroepsgroep hieraan voldaan?

- **Financiële crisis: toch uitgebroken ondanks regulation en audits**
- **IT: Mijn persoonlijke mening**
  - **Er wordt teveel gevinkt en nauwelijks echte Assurance gegeven**
  - **Auditors doen best goed werk door op de werkvloer verbeteringen voor te stellen, maar die zijn (te) klein**
  - **Auditors hebben onvoldoende oog voor grote risico's vanuit de bedrijfsprocessen en markten**

RULE BASED
VERSUS
PRINCIPLE BASED
REGULATION AND AUDIT

Congressional Oversight Panel

January 2009

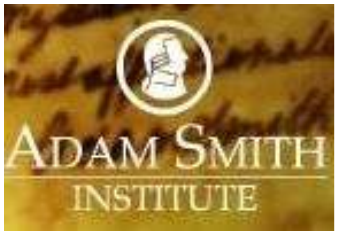
SPECIAL REPORT ON REGULATORY REFORM

Modernizing the American Financial Regulatory System: Recommendations for Improving Oversight, Protecting Consumers, and Ensuring Stability*

CONGRESSIONAL OVERSIGHT PANEL, JANUARY 2009, SPECIAL REPORT ON OVERSIGHT REFORM

1. Private financial markets do not always manage risk effectively. The current crisis is the product of a profound failure in private risk management, combined with an equally profound failure in public risk management
2. There is a range of proposals to regulate, reregulate and overregulate
3. The essential debate is not between deregulation and re-regulation, but instead between wise regulation and counterproductive regulation
4. Wise regulation helps make markets more competitive and transparent, empowers consumers with effective disclosure to make rational decisions, effectively polices markets for force and fraud, and reduces systemic risk
5. Counterproductive regulation hampers competitive markets, creates moral hazard, stifles innovation, and diminishes the role of personal responsibility in our economy. It is also procyclical, passes on greater costs than benefits to consumers, and needlessly restricts personal freedom

THE FINANCIAL CRISIS: IS REGULATION CURE OR CAUSE?



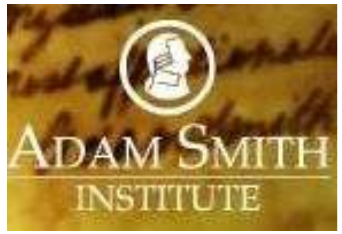
1. Regulation: indirectly fomented the crisis by providing the illusion of control
2. Government stoked the credit boom, since voting intentions are influenced more by spending than earnings. A classic bubble and believe the good times would last forever. Built up high levels of personal debt
3. Government regulation and Financial Service Authority (FSA) would guarantee financial security. It was an illusion and indirectly helped the fatal bubble to grow

Quality problems

4. Conventional wisdom: increase the size of the rule book and number of quality inspectors. However, quality is inversely proportional to inspectors. Having more quality inspectors actually reduces quality
5. Regulation incorporates a mass, if not a mess, of rules and regulations that amount to micro-management of the way firms are structured and carry on their business. This is generally referred to as "compliance"
6. They convince themselves that their overall business management and models have been validated. That is clearly not the case

http://www.adamsmith.org/briefings/economy/the-financial-crisis:-is-regulation-cure-or-cause?-200811272506/

Adam Smith Institute: Move to unsafe areas



Some of the contributing factors from regulation and the regulators

1. **Traditional business was over-regulated. This removed market opportunities and reduced profitability, inadvertently driving enterprise towards new, unregulated and unsafe areas. This migration of enterprise strained those parts of the system least able to withstand it**
2. **The over-regulation of traditional financial services shifted enterprise towards the complex financial engineering of packages unknown to, unseen by, and not understood by the FSA or UK Treasury**
3. **Even bank directors prided themselves for their inability to understand derivatives, Default Package Swaps and their like: "We have Cambridge PhDs for that, old boy"**
4. **Their only concerns were that they were legitimate means of raising funds off balance sheet, i.e. outside the traditional debt to capital controls, and that they generated positive earnings**

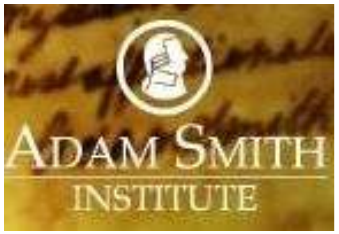
De financiële sector in USA was goed voor zo een 30% van de Corporate winsten

MODERNIZING REGULATION

The FSA has a legalistic, rules-based approach, preferring not blowing the whistle. It is like a policeman ignoring a burglary because the other side of the road is outside his patch

We need to distinguish here between "regulation" – creating a set of written, legalistic rules but not necessarily enforcing them – and "oversight", as once practiced by the Bank of England, where dubious practice was called into question whether the subject of written rules or not

1. **The more regulations there are, the more the FSA focuses on box ticking and compliance**
2. **Regulators should focus on a rethink of their regulatory procedures and objectives**
3. **Regulation should be much less oriented towards process and much more focused on principles and outcomes**
4. **Regulators should be more concerned about where we are going, and whether that place is a sensible place to be, not how we travel there"**



RECOMMENDATIONS

1. **FSA should be changed from "maintaining confidence in the financial system" to "ensuring that the financial system is worthy of confidence"**
2. **The FSA's legalistic, pedantic view of regulation should be replaced by "oversight", i.e. monitoring the business as a whole**
3. **Traditional markets had few regulations but wide latitude for the market supervisor to step in quickly to deal with malpractice, or dubious practice**
4. **The Bank of England and FSA should review the audits of the major banks and those financial institutions which the FSA highlights as having potentially non-viable business practices**

One Hundred Seventh Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Wednesday, the twenty-third day of January, two thousand and two

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Sarbanes-Oxley Act of 2002".

Requirements SOx act 404

Who

Corporate management, executives and financial officer

What

1. **A statement of management's responsibility for establishing and maintaining adequate internal control**
2. **A statement identifying the framework used by the management**
3. **An assessment of the effectiveness of the company's internal control**
4. **A written conclusion by management about effectiveness of the internal control including a conclusion about the effectiveness**
5. **Management is precluded from concluding internal control are effective if there are one or more material weaknesses**

INTENTIE SOx

Correctheid van de jaarrekening en het verstrekken van correcte informatie aan de markt en aandeelhouders + inlichten over de werkelijke risico's

Reporting via SAS 70

Q1 report of findings per object

Up to N reports per Q

Control activity
D / E / OE
Finding
Risk level
Action item

tracking

To local IT management
and QA of Service Organization

Consolidated Q1 report for User

Control activity
Per object:
D / E
Finding

Consolidated Q2 report for User

Control activity	
Q1	Q2
Per object:	
D / E	OE
Finding	Finding

Etc.

Q2, Q3 and Q4: ditto

- Each report of findings is issued to local IT management and QA
- Action item to be tracked by QA

Final report for User over 200X

Control activity			
Q1	Q2	Q3	Q4
Per object:			
D / E	OE	-	OE
Finding	Finding	-	Finding

Ervaring: rapporten worden zeer omvangrijk, bevatten veel feiten en falen aan te geven wat de werkelijke situatie is

D = Design OE = Operating effectiveness
E = Existence

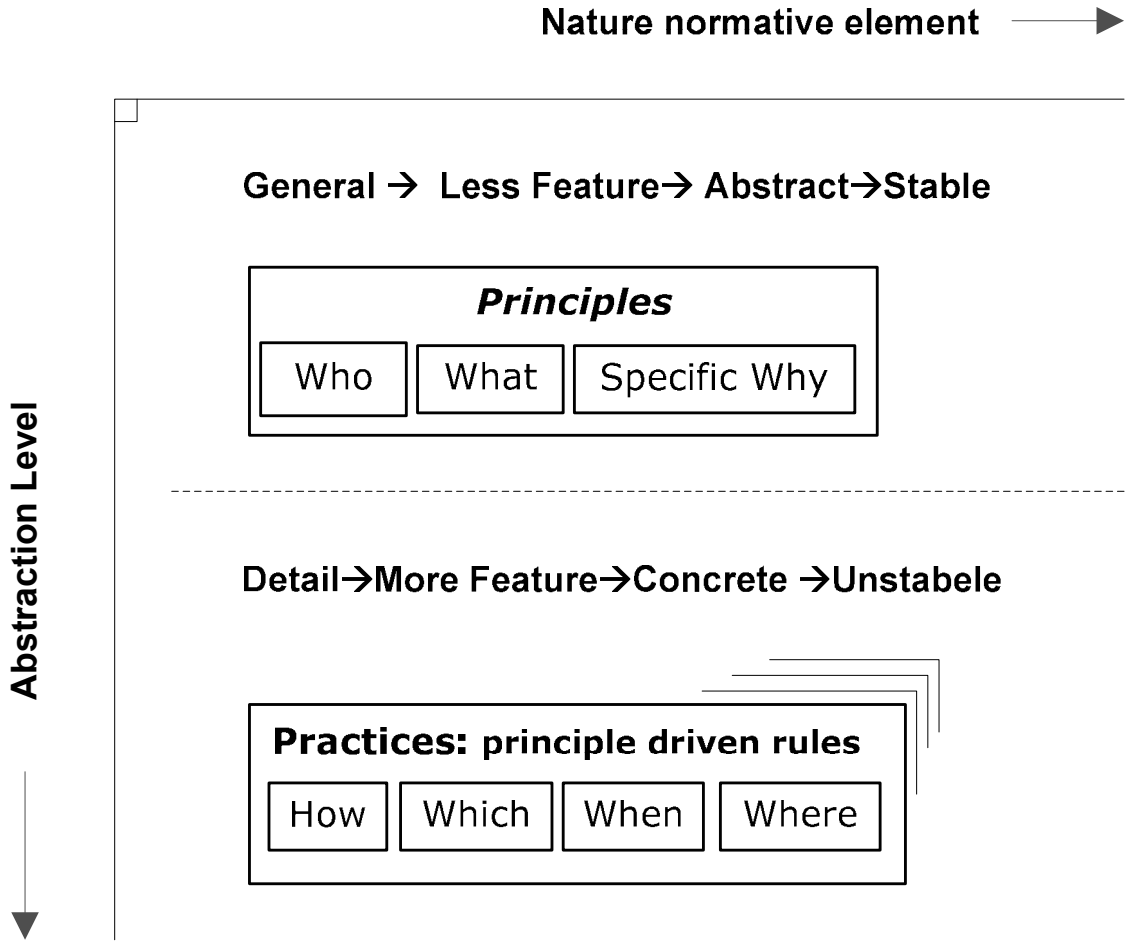
RULE BASED VERSUS PRINCIPLE BASED

- Wij als auditors moeten de regeltjes niet dicteren
- Geef de norm, en laat de auditee aantonen hoe aan de norm wordt voldaan
- De auditee runt de business. Wij controleren of dat verantwoord gebeurt. En wij controleren vanuit de belangen van de business
- Ons beroep is
  - Vaststellen of risico's goed en weloverwogen worden gemanaged
  - Vaststellen of men een werkend stelsel van maatregelen heeft geïmplementeerd, dat voldoet aan de eisen van de business

CONCLUSIES OVER REGULATION

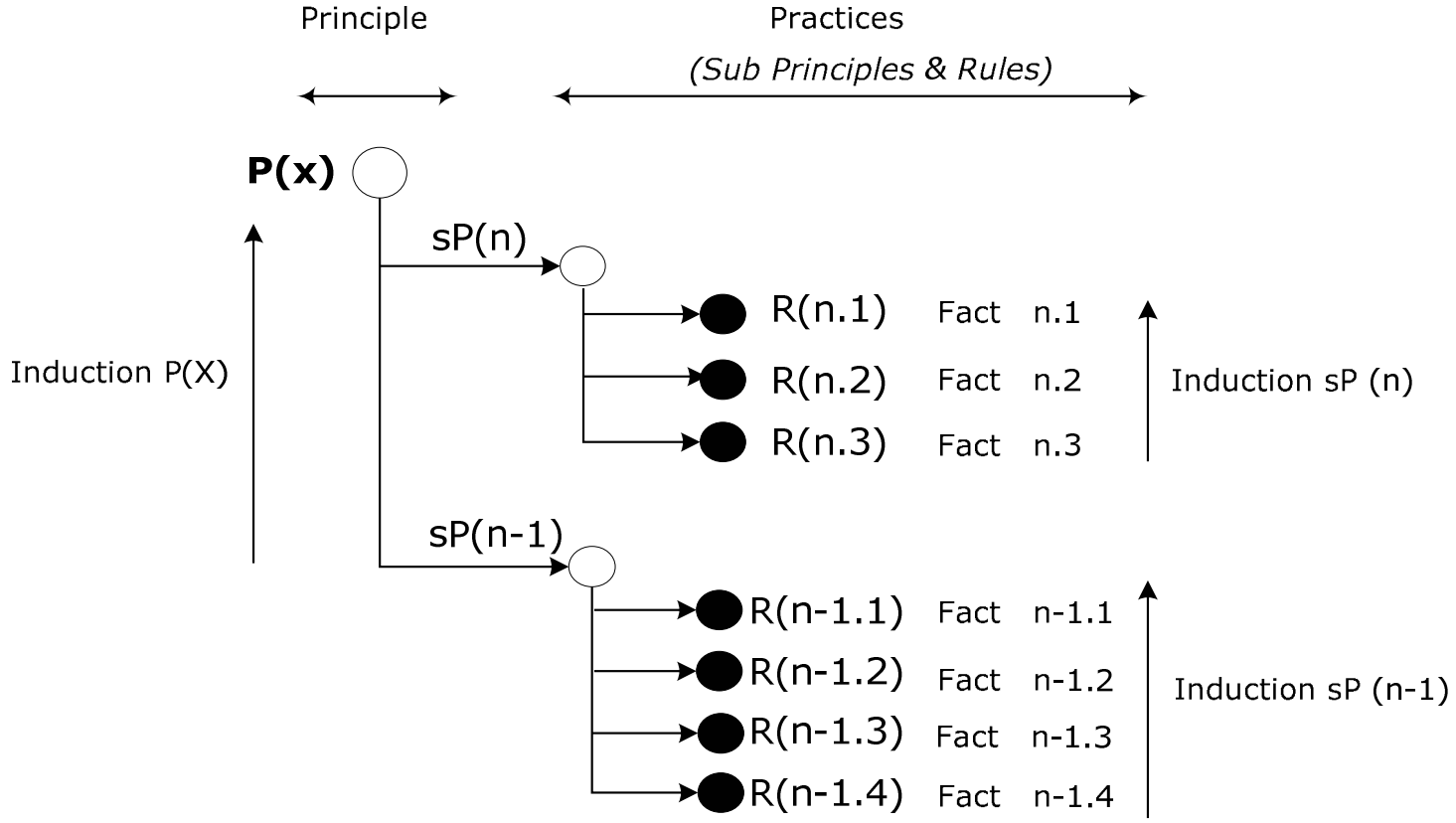
- De traditionele banken zijn overgereguleerd
- Om extra winst te maken is men overgestapt op (veel te) riskante producten
- Zelfs management overzag de risico's niet meer en gedroeg zich niet als bankier, maar als marketeer en verkoper
- In strijd met de intentie van SOx, wat stelt dat management zorgvuldig met risico's moet omgaan
- Regulation en SOx zijn vervallen tot het afvinken van regeltjes, zonder na te denken over de echte risico's
- De financiële crisis toont aan dat overheid en beroepsorganisaties verkeerd bezig zijn met regulation en audit
- Men moet terug naar PRINCIPLES en daarop toetsen

Principles in the context of IT auditing can be seen as basic elements or the source for reasoning, observation or evaluation of actions and states



Proefschrift Wiekram Tewarie, UWV en VU PGO IT Audit

Principles versus practices



Legend:

Non- Terminal Nodes (Abstract Principle)

Terminal Nodes (Concrete sub Principles or Rules)

Source: Model Akoka et al., 1996

Wat geeft de meeste Assurance?

Regeltjes uit een normenkader

- Scheid elektriciteitsleidingen naar spanning en frequentie
- Scheid elektriciteitsleidingen van communicatiekabels
- Spoor het personeel aan om de locatie netjes te houden
- Zorg voor schone aarde uit de buurt van de centrale aarde van de computerruimte
- Alle gegevensdragers tonen de hoogste classificering van de informatie op het medium

Principe

- Beheer het datacenter zorgvuldig
- Laat zien welke risico's u wilt voorkomen met uw maatregelen
- Laat zien dat uw stelsel van maatregelen voldoet in dit kader

Assurance

- Is het verantwoord dat ik mijn systemen laat draaien in uw datacenter?
- Kan ik er op vertrouwen dat u zorgvuldig met mijn belangen omgaat?

Het vinken van de regeltjes draagt hier weinig toe bij !

GOVERNANCE OF SOURCING RELATIONS

Knokkende juristen - of het WIJ-gevoel van partners ?

EFFECT OP ORGANISATIE VAN IT

- IT is een bedrijfsmiddel en geen doel
- Risicomanagement is een hulpmiddel en geen doel
- In detail controleren van de controls vermindert onzekerheid, maar is geen doel

WAT IS ONS DOEL?

- IT moet effectief en efficiënt de bedrijfsprocessen ondersteunen
- Wij als (IT) Auditors moeten vanuit de belangen van de klant en leverancier redeneren, kijken naar de echte risico's en aangeven of datgene wat management doet verantwoord is
- Dit is veel breder dan "vinken"
- Als Auditors zijn wij het geweten van de samenleving

Quint White Paper

SOURCING STRATEGIE WORDT KERNACTIVITEIT

- **Geïmplementeerd door onder andere het Ministerie van Defensie, Bedrijfsgroep IV en Technologie (BG IVENT, voorheen DTO)**
- **Heldere definitie van rollen**

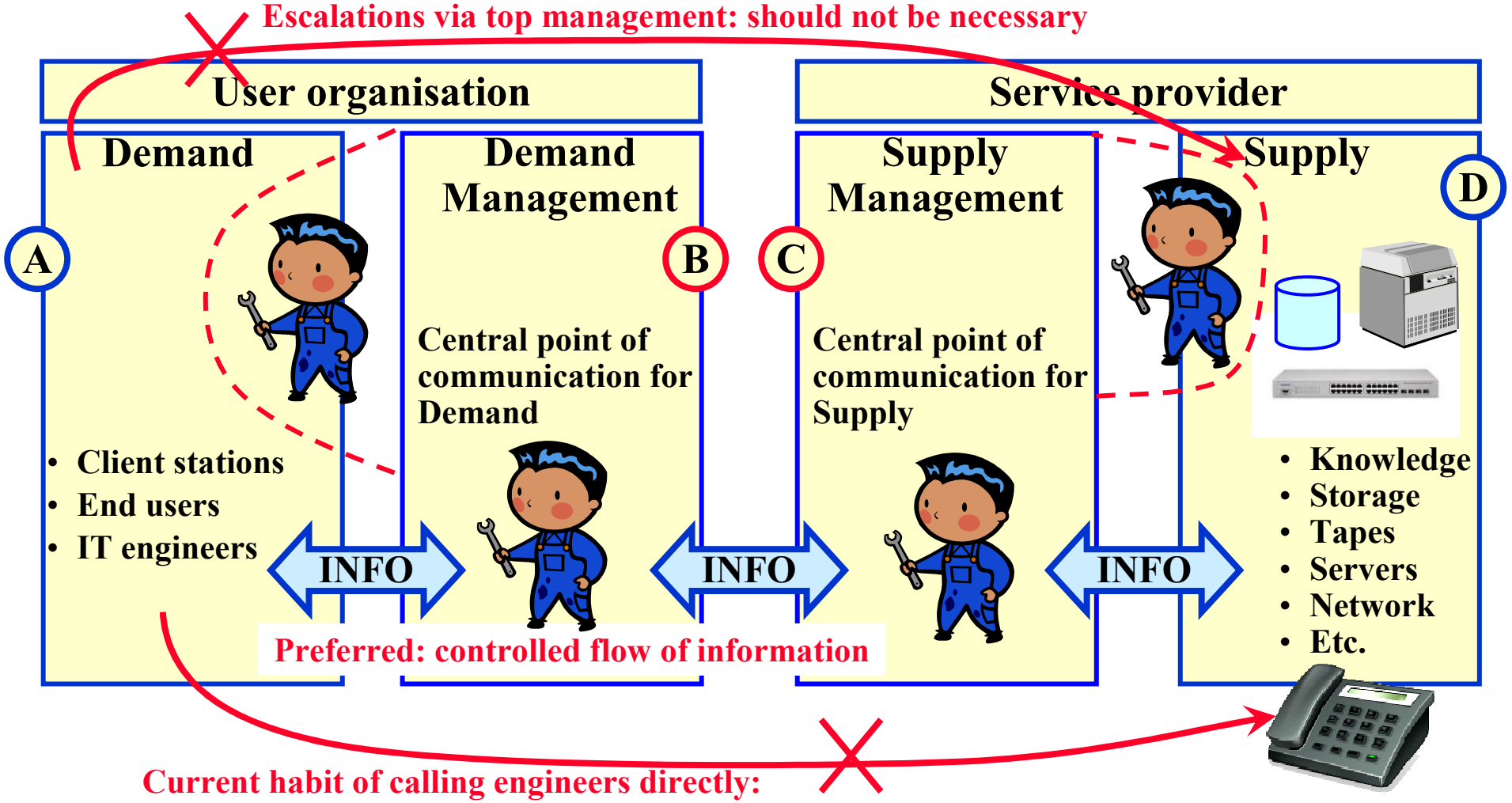
A. **Demand**

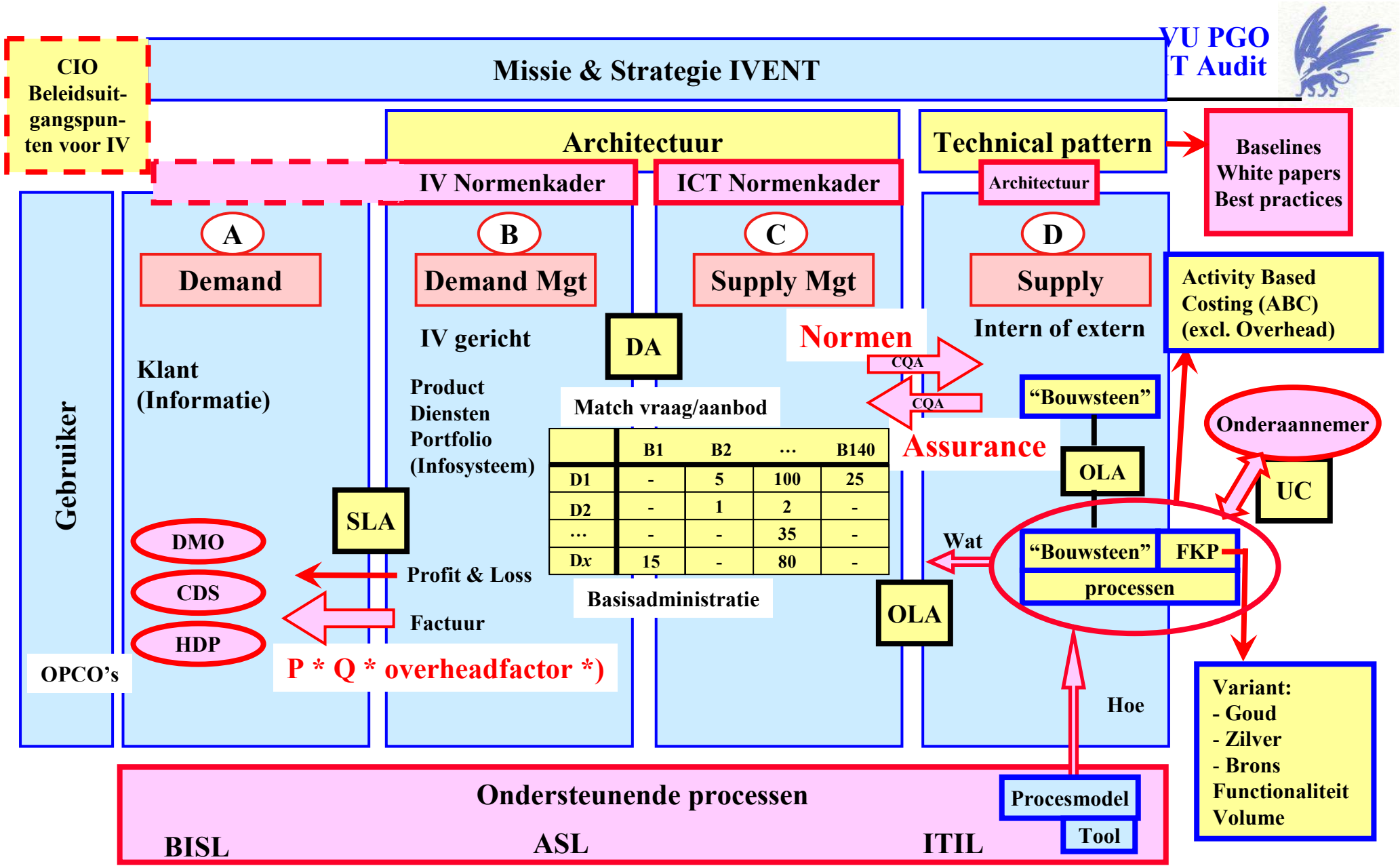
B. **Demand Management: de regierol vanuit de gebruikersorganisatie**

C. **Supply Management: regie over de middelen**

D. **Supply: de middelen, namelijk systeemontwikkeling, OTAP en het datacenter met het netwerk**

Preferred information flow

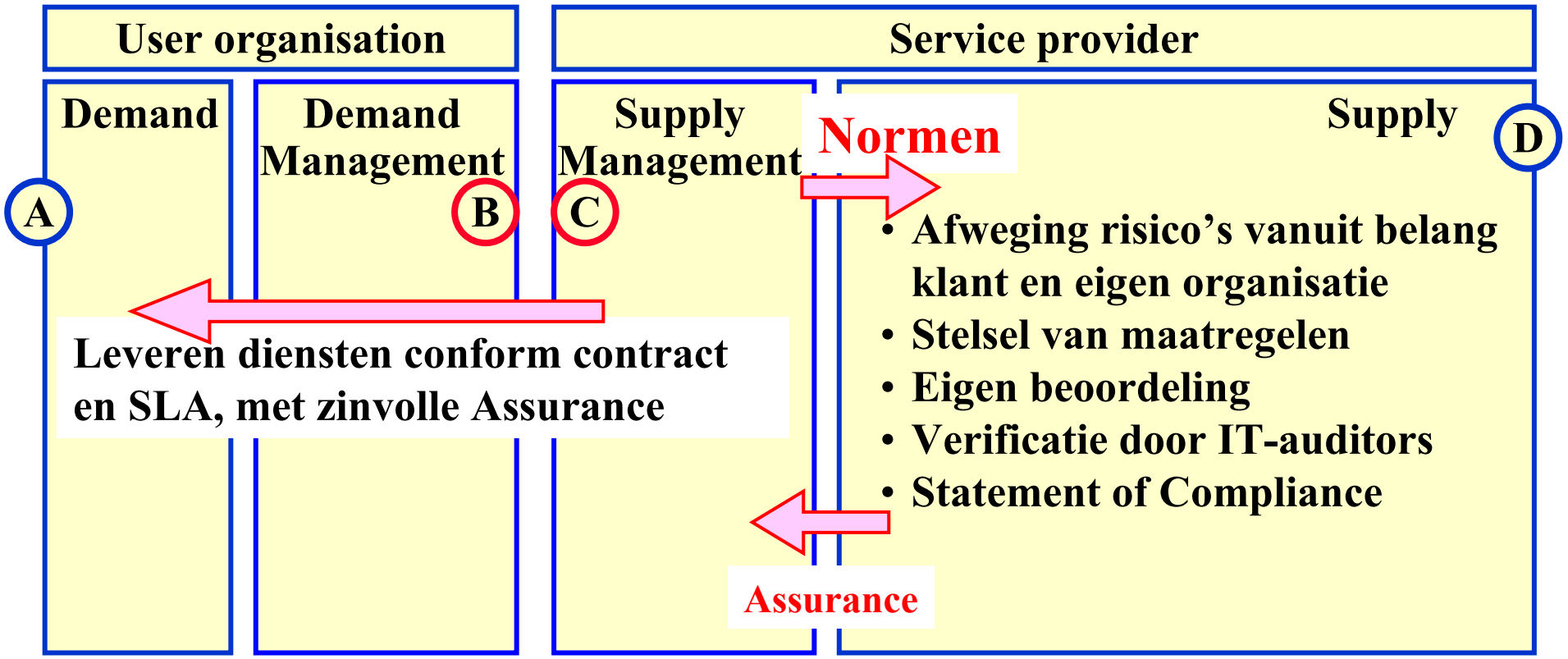




	B1	B2	…	B140
D1	-	5	100	25
D2	-	1	2	-
…	-	-	35	-
D*x*	15	-	80	-

Basisadministratie

*) Prijs per kwaliteit(=variant) * kwantiteit * overhead



NIST 800-53 uitgebreid met procesnormen

Implementatie volgens best practices, zoals ISO 20000 en 27002, en ITIL

Normen

- Moeten in lijn zijn met zakelijke belangen van de gebruikersorganisatie en ook met die van de leverancier
- Normen moeten maatregelonafhankelijk zijn: zeg **wat** er moet gebeuren, niet **hoe**
- Laat de leverancier zelf de maatregelen selecteren op basis van de voorziene risico's, die controleren en daar een mededeling over afgeven
- Auditors moeten de waarheid achter de mededeling verifiëren
- Zo voldoen wij aan de intentie van SOx en hebben wij als beroepsgroep toegevoegde waarde