Enterprises

Wouter Jelmer Aziz Pieter Bart

17-03-2005

Contents

Centralise or not?

Definition

Centralization

- 1 : to bring to a center : CONSOLIDATE <centralize all the data in one file>
- 2 : to concentrate by placing power and authority in a center or central organization

Definition

Decentralization

- 1 : the dispersion or distribution of functions and powers; specifically : the delegation of power from a central authority to regional and local authorities
- 2 : the redistribution of population and industry from urban centers to outlying areas

Centralization

- Focus of control
- Improve efficiency

Decentralization

- Improve speed
- Flexibility
- Redundancy

Guidelines

- Understand your motivation
- Know the specific problem which you want to solve
- Centralize as much as makes sense for today, with an eye to the future
- The more centralized, the more customization or special features

- When a service becomes a commodity, consider centralization
- Be circumspect about unrealistic promises
- It's like rolling out a new service
- Listen to customers concerns
- You only have one chance to make a good first impression
- Listen to customers, but remember management has control

Design thoughts: Basic thinking

- Company has policies, missions, specific goals etc
- Environmental influence, competitors, budget constraints
- Understanding technological background of users / systems
- Create a complete picture

Centralization vs Decentralization

- Interconnections needed?
- Many factors to be considered
- No checklist available
- How to ensure effectiveness with many linked components?
- Classification needed: ideal or nonideal (real)

Ideal situation

- Design system from scratch
- No cost limit
- no resistance from earlier scratches / infrastructures

Non-ideal situation

- Limited (financial) resources
- Staf (re)training
- Legacy problems
- Company policies which do not fit anymore

Candidates for Centralization

- Might be cost saving
- Less overhead than the sum of the individual overheads of each decentralized item
- Can create simpler architecture
- Reliability through simplicity
- Succeed centralization by picking the right services

- Consolidate services on fewer hosts
- Consolidate expertise over the organization
- Outsourcing

Candidates for decentralization

- Does not automatically improve speed
- Often to democratize control
- Fault tolerance (failover)
- Compartmentalization

Example 1

- TomTom

Example 2

Online learning environments

- Becoming ubiquitous, example: Cisco CCNA, A+ etc.
- How to design a infrastructure worldwide which is suitable

Conclusion

- Neither is always better, politics and management are involved.

ITIL

Background

- Developed in the late 80's
- Central Computer & Telecommunications Agency (CCTA)
- World wide defacto standard in the mid 90's

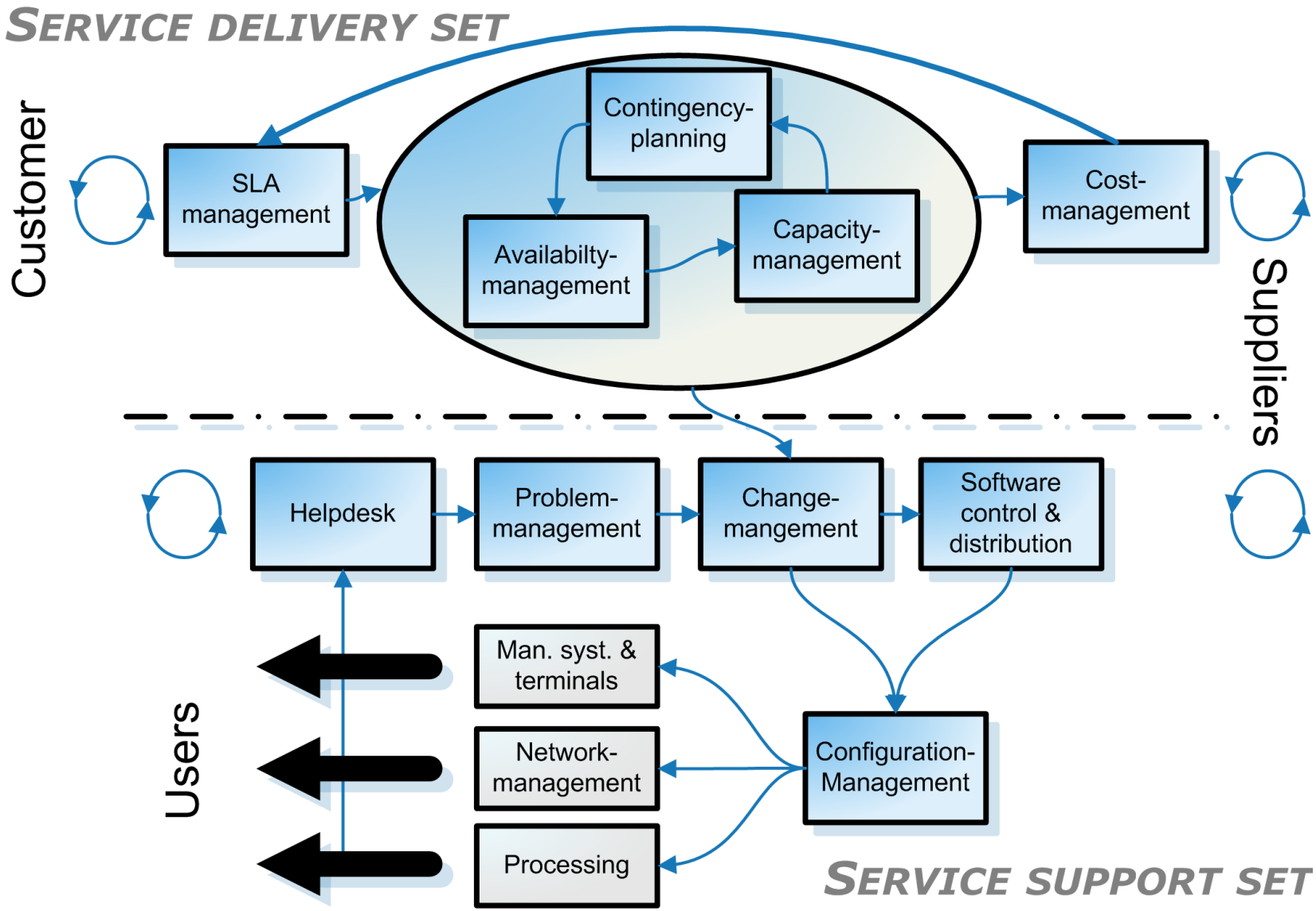
What is it?

- Set of best practices for high quality IT service management
- Customizable

Modules

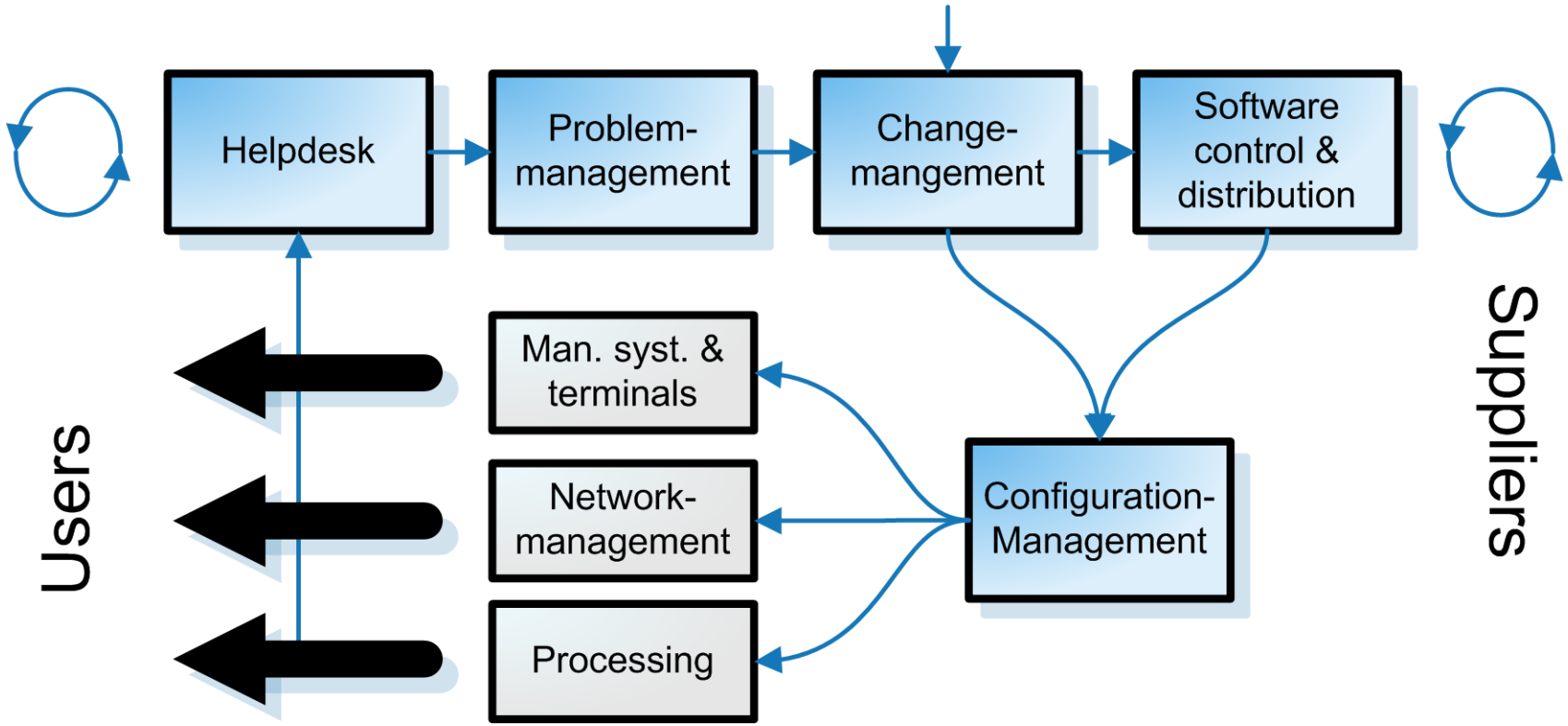
- Software support, Managers & Networks set
- Computer operations & Environmental management set
- Environmental stratagy & Office Environment set
- **Service support** & **Service delivery set**

Process connection


SERVICE DELIVERY SET
Customer
SLA management
Contingency-planning
Availabilty-management
Capacity-management
Cost-management
Suppliers
Helpdesk
Problem-management
Change-mangement
Software control & distribution
Users
Man. syst. & terminals
Network-management
Processing
Configuration-Management
SERVICE SUPPORT SET

ITIL - Service Support Set

Processes


Helpdesk
Problem-
management
Change-
mangement
Software
control &
distribution
Users
Suppliers
Man. syst. &
terminals
Network-
management
Processing
Configuration-
Management

Configuration Management - Goals

- Making the IT infrastructure manageble
  - Only authorized compontents
  - Changes have to be approved
- Providing information about the infrastructure
  - What, who, where, relations

ConfM - Items

- Hard- & Software, LAN
- Request for change
- Manuals
- Organisational Structure & Procedures
- SLA's

ConfM - Scope

- Services, applications, network, modem
- NOT: The copper of your telco

ConfM - Level of detail

The lowest level are the parts that are:

- essential for the service
- regularly installed, modified or removed

ConfM - Attributes

- Assetnumber (unique), Serialnumber
- Category, Status
- Version / model & type
- Location, owner, Supplier
- Comments

ConfM - Activities

- Identification
- Database maintenance & verification
- Lifecycle (planned, realised, tested, implemented, operational, maintenance, archive)
- Regular reports

ConfM - Conclusion

- Correct level of detail
- Procedures in absence of DB maintainer
- Be sure to have full support of all IT members
- Prevent an image that ConfM is a wast of time

Helpdesk - Goals

- Added value for business processes
- "Face" of the IT department for questions, complaints & suggestions
- Continuity of services

Helpdesk - Incident

- Failures / Interruptions
- Faulty procedures
- Unfamiliarity

But, within certain limits.

Helpdesk - Activities

- Communication & promotion
- Incident management
- Reports

Helpdesk - Incident management

- Detection & Registration
- Classification & Assign
- Diagnose & Solve
- Close

Helpdesk (IM) - Detection & Registration

- Monitor different domains (Central facilities, network, terminals, usage,. . .)
- Reactive $\Rightarrow$ Proactive
- Quick fixes are allowed (don't forget ConfM!)

Helpdesk (IM) - Classification & Assignment

- Priority (Impact, Urgency, Estimated effort)
- E.g: resetting a password

Helpdesk (IM) - Diagnose & Solve

- Second or higher line support (Escalation)
- Hierachical (authorization)
- Functional (competence)
- Helpdesk is still responsible

But first: inform the user, communication is *very* important!

Helpdesk - Reports

- Numbers categorized by service, impact, usergroup, problem
- Average outage
- Time spended (helpdesk, second line, suppliers)

Problem Control - Goal

- Solve (more serious) problems permanently

Problem Control - Activities - 1

- Indentification & registratrion
  - Incident(s) $\Rightarrow$ Problem $\Rightarrow$ Known error
- Classification
- Allocation of resources

Problem Control - Activities - 2

- Research & diagnoses (define, brainstorm, causality)
- Reports

Problem Control - Conclusion

- Problem Control should never be inferior to quick fixes/ad hoc solutions
- Gain and hold stability by "fixing things once" and forever

Program Management & Distribution

- Stadia: development, test, exploitation, archival
- Track versions $\Rightarrow$ Martijn
- Operational acceptance: design/specs, source/documentation, install procedure, known erros, manuals, testplan

Change Management

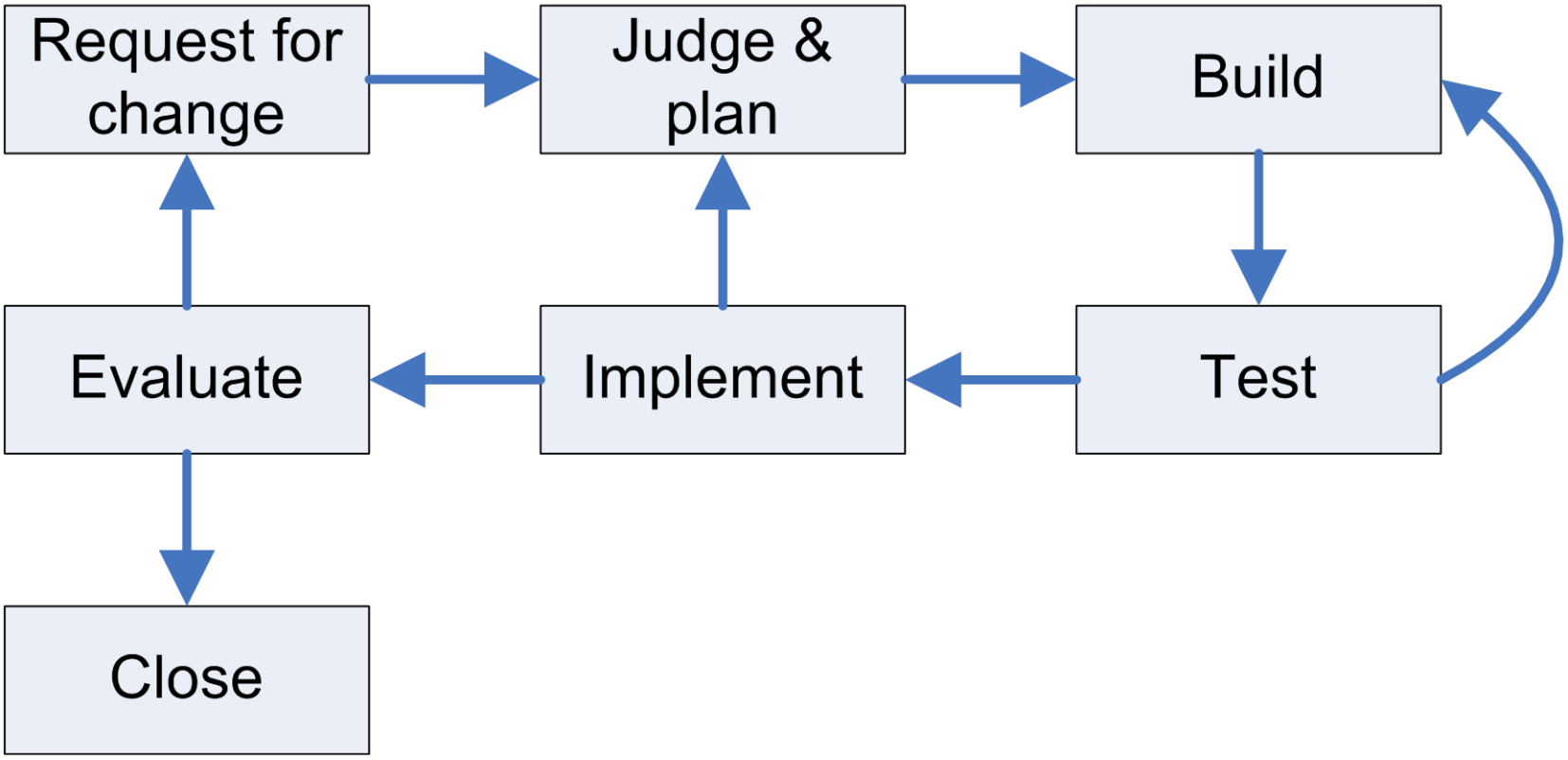
- Never ending
- Central in ITILs Service Support set
- Goal: keeping track of, managing and controling (requests for) changes

CM - The change

What is a *change*?

- NOT: mutations on data, resetting a password, personal settings
- changes that affect multiple users/services
- mostly: items covered by ConfM

CM - Process

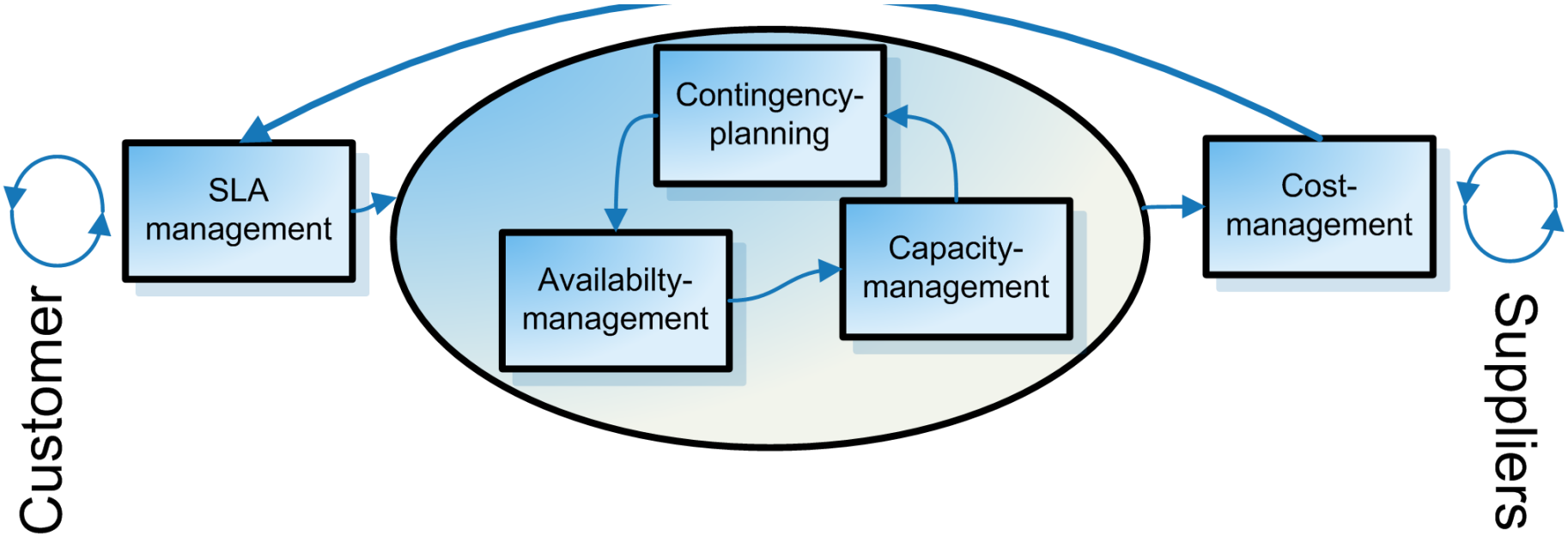

Request for change
Judge & plan
Build
Evaluate
Implement
Test
Close

CM - Reports

- (Succesful) changes per category
- Urgent changes
- Fallback & new problems
- Resources & costs
- Trends & future expectancies

ITIL (2)

Planning en beheersing



Planning en beheersing

Verwachtingen over de kwaliteit nemen constant toe.

Bepalend voor de kwaliteit:

- Beschikbaarheid
- Betrouwbaarheid
- Beveiliging
- Integratiemogelijkheden

- Toegankelijkheid
- Prestaties van informatiesystemen

Planning en beheersing

Klant wilt meer mensgerichte kwaliteitsaspecten:

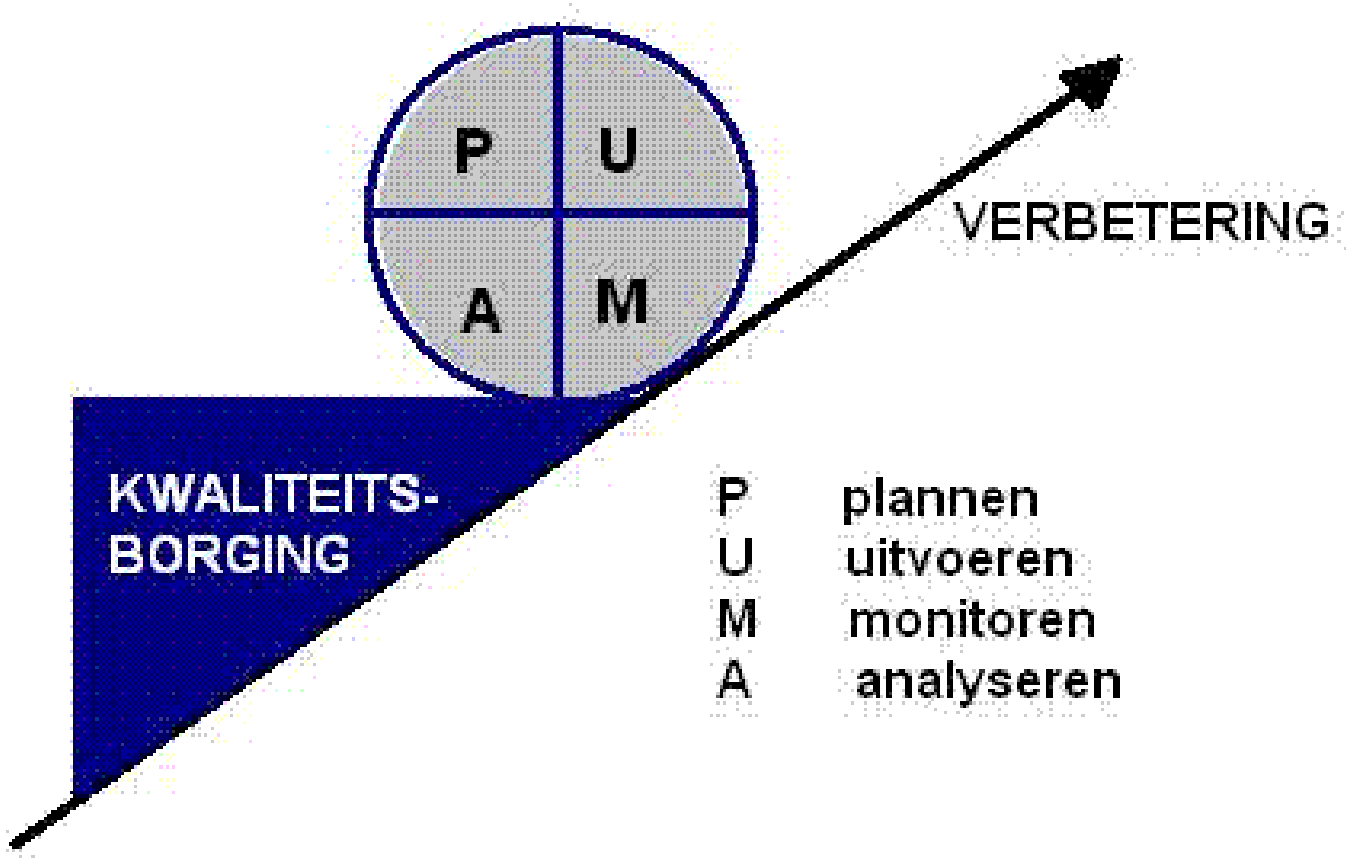
- Betrokkenheid
- Integriteit
- Professionaliteit (medewerkers & IT-dienstorganistatie)

Wat is kwaliteit?

Planning en beheersing

- Volgens ISO (International Organization for Standarization):
- Kwaliteit is het geheel van eigenschappen en kemerken van een product of dienst dat van belang is voor het voldoen aan vastgelegde of vanzelfsprekende behoeften
- ISO 8402

Illustratie


P
U
A
M
VERBETERING
KWALITEITS-
BORGING
P plannen
U uitvoeren
M monitoren
A analyseren

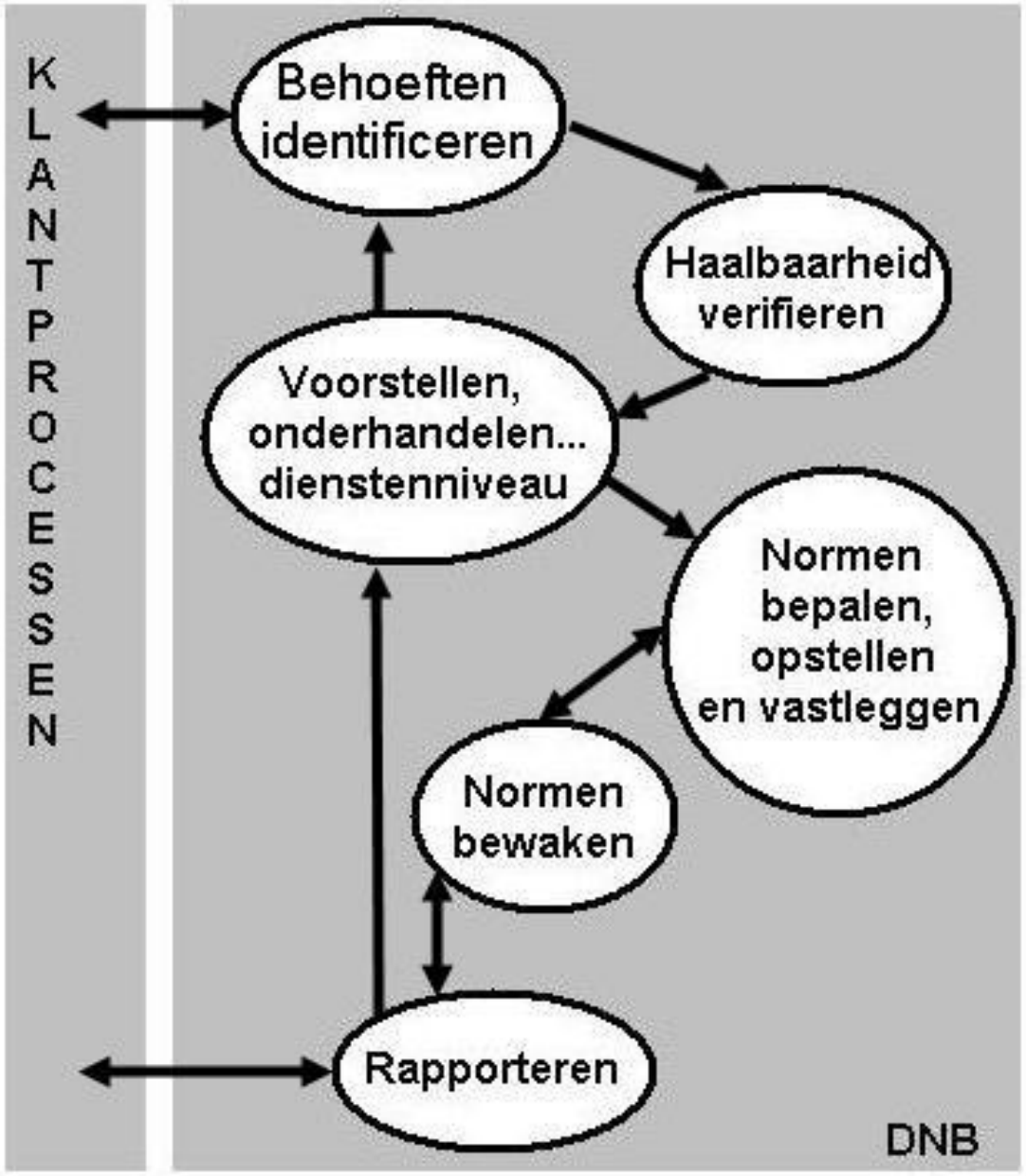
Dienstniveaubeheer

- Wat is dienstniveaubeheer?
- Afspraken over kwaliteitsniveau en hoe zij tot stand komen.
- Het proces dat, door een goed samenwerkingsverband tussen aanbieder en afnemer, zorg draagt voor het overeenkomen en bewaken van een optimaal niveau van IT-dienstverlening.

Dienstniveaubeheer

- SLA (DNO, Dienstniveau-overeenkomst):
- Een SLA specificeert de betreffende diensten, het overeengekomen dienstenniveau, de omstandigheden waaronder de diensten geleverd worden en de partijen die hierbij betrokken zijn.
- SLA-catalogus:
- Een complete en uitgebreide overzicht van alle IT-diensten die een aanbieder te bieden heeft.

Dienstniveaubeheer


KLANTPROCESSEN
Behoeften identificeren
Haalbaarheid verifieren
Voorstellen, onderhandelen... dienstenniveau
Normen bepalen, opstellen en vastleggen
Normen bewaken
Rapporteren
DNB

Dienstniveaubeheer

De fundamenten die worden gelegd voor dienstniveaubeheer:

- Capaciteitsbeheer
- Beschikbaarheidsbeheer
- Calamiteitenbeheersing
- Financieel beheer

Capaciteitsbeheer

- Capaciteitsbeheer is het proces dat zorgt draagt voor een optimale inzet van IT-middelen
- Optimaal wil zeggen: juiste plaats, juiste moment, juiste hoeveelheid en tegen gerechtvaardigde kosten

Capaciteitsbeheer

- Constant monitoren van prestaties en het gebruik van het systeem
- Goed capaciteitsbeheer resulteert in optimale systeemprestaties, kostenbesparingen en een verlaging van risico's

Capaciteitsbeheer

- Aandachtspunten:
- Monitoren legt beslag op systeemcapaciteit. Dit beinvloedt de prestaties van het systeem
- Een tekort aan capaciteit komt vaak pas aan het licht op het moment dat zich performance-problemen voordoen

Beschikbaarheidsbeheer

Beschikbaarheidsbeheer is het proces dat de juiste inzet van middelen, methoden en technieken waarborgt

Beschikbaarheidsbeheer

Beschikbaarheidsbeheer wordt uitgedrukt in een beschikbaarheidsprecentage:

$$\text{Beschikbaarheidsbeheerprecentage} = \frac{\text{o. openstellingsduur} \;\; \text{storingsduur}}{\text{o. openstellingsduur}} \text{ X } 100\ \%$$

Beschikbaarheidsbeheer

- Beschikbaarheidsbeheer wordt geborgd door:
- betrouwbaarheid
- onderhoudbaarheid
- veerkracht

Calamiteitenbeheersing

Een calamiteit is een ongeplande situatie waarbij verwacht wordt dat de duur van het niet beschikbaar zijn van een of meer IT-diensten afgesproken drempelwaarden zal overschrijden

Calamiteitenbeheersing

- Calamiteit:
- Organistatie bepaalt zelf wanneer er sprake is van een calamiteit
- Een calamiteit is het gevolg van een of meer ernstige storingen

Calamiteitenbeheersing

Calamiteitenbeheersing is het proces dat zorg draagt voor afdoende technische, financiele en organisatorische voorzieningen bij calamiteiten

Calamiteitenbeheersing

Activiteiten binnen calamiteitenbeheersing zijn o.a.

- risico-analyse
- risicobeheersing

Calamiteitenbeheersing

Risico-analyse richt zich op het kwantificeren van bedreigingen waraan IT-middelen bloot staan, alsmede de mate van kwetsbaarheid van deze middelen.

```
Gebruikte formule:
K(ans) x S(chade) = R(isico)
Niet alle soorten schade zijn meetbaar
```

Calamiteitenbeheersing

Risicobeheersing Het identificeren en selecteren van tegenmaatregelen waarmee risico's tot een acceptabel niveau worden gereduceerd.

- Voorbeelden:
- dubbel uitvoeren van netwerkcomponenten
- uitwijkmogelijkheden

Conclusie

Security

Enterprise info sec.

What's the difference between Enterprise info sec. and normal, day-to-day info sec?

- Day-to-day info sec. focuses on technicalities
- Enterprise info sec. comprises a lot more
- An enterprise is big, it's security important
- Money, politics, laws involved

Enterprise security: what's at stake?

Why does one need enterprise IT security?

- Infrastructure important for business
- Competitors want the enterprise's information
- Criminals are out after enterprise's money
- Kids seek enterprise's diskspace/bandwidth
- Insiders like a bit of extra pay

Enterprise security: what's at stake?

Security incidents cost money:

- System/network downtime: lost revenues
- Incident response
- Loss of reputation
- Liability

Enterprise security: what's at stake?

Security incidents cost money. Some statistics from securitystats.com:

- BBC: Computer hacking 'costs billions'
- CSI/FBI: Losses of $377 million
- 1997: I-CAMP I, 30 incidents: over $1,000,000
- 2000: I-CAMP II, 15 incidents totalling $59,250

A multi-dimensional approach

Security has long been approached single-dimensionally:

- No or only a small security group
- Some groups kept out of the loop
- Only simple, single-layer technical defenses
- No monitoring, auditing and forensics

A multi-dimensional approach

Enterprises are too big and complex beasts to use a single-dimensional approach.

- Multigroup involvement
- Multilayer defense: prevention, detection and response

Multigroup involvement

Everybody in an enterprise has to be in-the-know about security, otherwise it just won't work. Four groups of people which need consideration:

- Security team (with real ultimate power)
- Users
- Management

Multilayer defense

By using a multi-layered approach on the technical level, intrusions can be avoided.

- Prevention: Security policy/awareness, access controls, authentication, firewalling
- Detection: Firewalls, IDS, scanning, auditing
- Response: procedure, IPS, disaster recovery, forensics

Setting up an enterprise security architecture

How would you go about setting up information security architecture for an enterprise?

Use the six-step process:

- Initiation: begin with the effort, both technically as well as business-wise
- Describe the current security status

- Describe the desired level of security
- Plan how to reach that level
- Execute the plan(!)
- Maintain the effort

Initiation

The security effort has to be started, the company as a whole has to be prepared and talked into it.

- All groups inside the company have to be motivated
- They need to know what the stakes are
- And how they can help security
- Or rather: what's expected from them

Plan the change

To be able to improve security, there have to be things changed.

- Describe where you are
- Describe where you want to be
- Plan the change

Execute the plan

Actually changing security practices is a daunting task.

- Get security into the processes
- Update the plans
- Keep it all going

Keep the initiative alive

Things change, the security world doubly so. The enterprise itself will change, too.

- Keep up with security threats
- Reevaluate security practices, adapt
- Stay in power

Conclusion

A multi-layered approach, both on the business level as well as the technical level is needed to ensure some degree of security in an enterprise.

TCO

TCO?

- What is it?
- What does it do?
- Why?

In Short

Simply stated, TCO consists of the costs, direct and indirect, incurred throughout the life cycle of an asset, including acquisition, deployment, operation, support and retirement.

History

- Bill Kirwin, 1987 - Gartner

Gartner

- LAN's
- Client/Server software
- Distributed Computing
- Telecommunications
- Mainframe data centers
- Windows CE & Palm OS handhelds

Companies

- http://www.solutionmatrix.com/
- http://www.robbinsgioia.com/
- http://www.1000ventures.com/

How is TCO calculated? (1)

- Direct costs
- Indirect costs

How is TCO calculated? (2)

- Direct costs:
  - Hardware & Software
  - Operations
  - Administration

How is TCO calculated? (3)

- Indirect costs:
  - End user operations
    - Support
    - Futz Factor
  - Downtime
  - Training

Value of using TCO

- Framework for IT analysis
- Baseline for IT costs
- Widespread understanding

Symptoms

- Cheeseslicer method
- Price-quality complains
- No insight, lack of registration basic information
- Transparency costs of service

ABC

- Activity Based Costing

Advantages

- Easy overview
- Cost reduction
- Supplier - cost vs. quality
- Benchmark
- Outsourcing . . . ?

Disadvantages

- Time-consuming
- Research $$$

Conclusion

- Not only costs
- Me or You
- To do or not to do

Wanna try

- www.solutionmatrix.com

Questions

Research - TCO for Linux in the Enterprise

- Windows
- Linux
- Solaris

What?

- OS
- Webserver
- Processors
- Period

4 area's

- software purchase costs
- hardware purchase & maintenance prices
- software maintenance & upgrade prices
- administrative costs

Licenses

- Windows
- Linux

Software Costs

OS	Up front	Year2	Year3
Linux	$400	$0	$0
Solaris	$27.500	$0	$0
Windows	$5.320	$1.330	$1.330

Hardware Costs

OS	Purchase	Year2 Maint.	Year3 Maint.
Linux	$37.511	$252	$252
Solaris	$345.400	$21.083	$21.083
Windows	$38.524	$258	$259

Support & Administration

OS	Ex. Support Admin.	Administrator Salary costs.
Linux	<$10	$12.010
Solaris	$19.309	$29.509
Windows	$1.520	$46.360

Questions