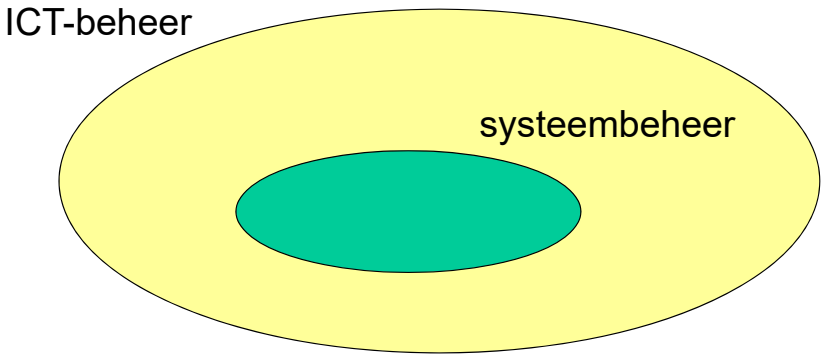
Les 10: Systeembeheer

"In 2031, lawyers will be commonly a part of most development teams."
– *Grady Booch*

best10-1

In deze les hebben we het over systeembeheer, dit is het geheel van handelingen en methoden die tot doel hebben om een computerinfrastructuur zo efficiënt en zo effectief mogelijk te beheren. Het systeembeheer zal steeds streven naar de technisch beste oplossingen.

Systeembeheer



het geheel van processen en procedures om ICT zo optimaal mogelijk te laten bijdragen tot de doelstellingen van een bedrijf of instelling

best10-2

Het systeembeheer is een onderdeel van het ICT-beheer, dit is het geheel van processen en procedures om ICT zo optimaal mogelijk te laten bijdragen tot de doelstellingen van een bedrijf of een instelling. Hierbij wordt de vraag gesteld wat de bijdrage van ICT is tot de uiteindelijke bedrijfsresultaten. Het ICT-beheer zal steeds streven naar de economisch beste oplossingen. Zo kan het voor een bedrijf goedkoper zijn om te investeren in een extra systeembeheerder om een verouderde applicatie operationeel te houden, dan om de applicatie volledig opnieuw te laten ontwikkelen.

Waarom management van ICT?

- Toenemende afhankelijkheid van ICT
- Toenemende risico's (aanvallen)
- Hoge kosten van ICT
- Zeer veel mogelijkheden

⇒ ICT moet professioneel beheerd worden
⇒ ICT bestuur (governance)
⇒ Bv. COBIT: Control Objectives for Information and related Technology

best10-3

ICT management is voor moderne bedrijven zeer belangrijk, en wel om de volgende redenen:

- De bedrijven zijn in toenemende mate afhankelijk van ICT. Hierbij gaat het niet louter om banken, ziekenhuizen of verzekeringsmaatschappijen, maar ook om KMO's die van hun computersysteem afhankelijk zijn voor bestellingen, leveringen en facturatie. Zeker met de opkomst van e-commerce en verkoop via het Internet is dit essentieel.
- De afhankelijkheid van ICT creëert bijkomende risico's. Gegevens kunnen gemakkelijk vernietigd worden, websites kunnen gekraakt worden, het computersysteem kan defect gaan, enz. De beveiliging van de ICT-infrastructuur moet dan ook professioneel aangepakt worden en kan niet aan het toeval overgelaten worden.
- De ICT-afdeling is verantwoordelijk voor een aanzienlijk deel van de uitgaven van een bedrijf (infrastructuur en personeel). Daarom moet men een duidelijke kijk hebben op de kostenstructuur van ICT en op de impact van ICT op de bedrijfsresultaten.
- Tenslotte moet men zich ook realiseren dat de ICT-infrastructuur een zeer grote impact kan hebben op het rendement van een bedrijf en dus de bedrijfsresultaten. Het is dus van het grootste belang dan de leiding van het bedrijf de ICT-ontwikkelingen en de kansen die ze kunnen creëren op de voet volgt.

Samenvattend kan gesteld worden dat ICT-beheer een essentiële pijler is in de moderne bedrijfsvoering, en dat een bedrijf het ICT-gebeuren onder controle moet houden. In het Engels spreekt men over ICT governance (ICT bestuur). Er werden raamwerken

uitgewerkt om deze doelstelling te helpen realiseren. Eén ervan is COBIT: Control Objectives for Information and related Technology.

Overzicht

- Kwaliteitsmodellen
- ICT-beheer
- Productieprocessen

best10-4

Kwaliteitsborging

Vijf verschillende niveaus

(CMM: capability maturity model)

- Basis: ad hoc, iedereen doet zijn best, maar geen garanties.
- Herhaalbaar: het huis op orde, prestaties zijn herhaalbaar, dupliceer successen.
- Gedefinieerd: processen zijn gedefinieerd, gestandaardiseerd, geïntegreerd, alles is doorzichtig.
- Beheerd: continue meting ter verbetering van de kwaliteit. Feedback naar management.
- Geoptimaliseerd: optimalisatie van de processen. Evaluatie van nieuwe technologie, continue verandering.

best10-5

In de literatuur over kwaliteitsborging bestaan er verschillende raamwerken die verschillende niveaus van kwaliteitsborging beschrijven. Eén ervan is het CMM-model (Capability Maturity Model). Het CMM-model wordt geregeld gebruikt in een ICT-omgeving. Men onderscheidt een vijftal niveaus.

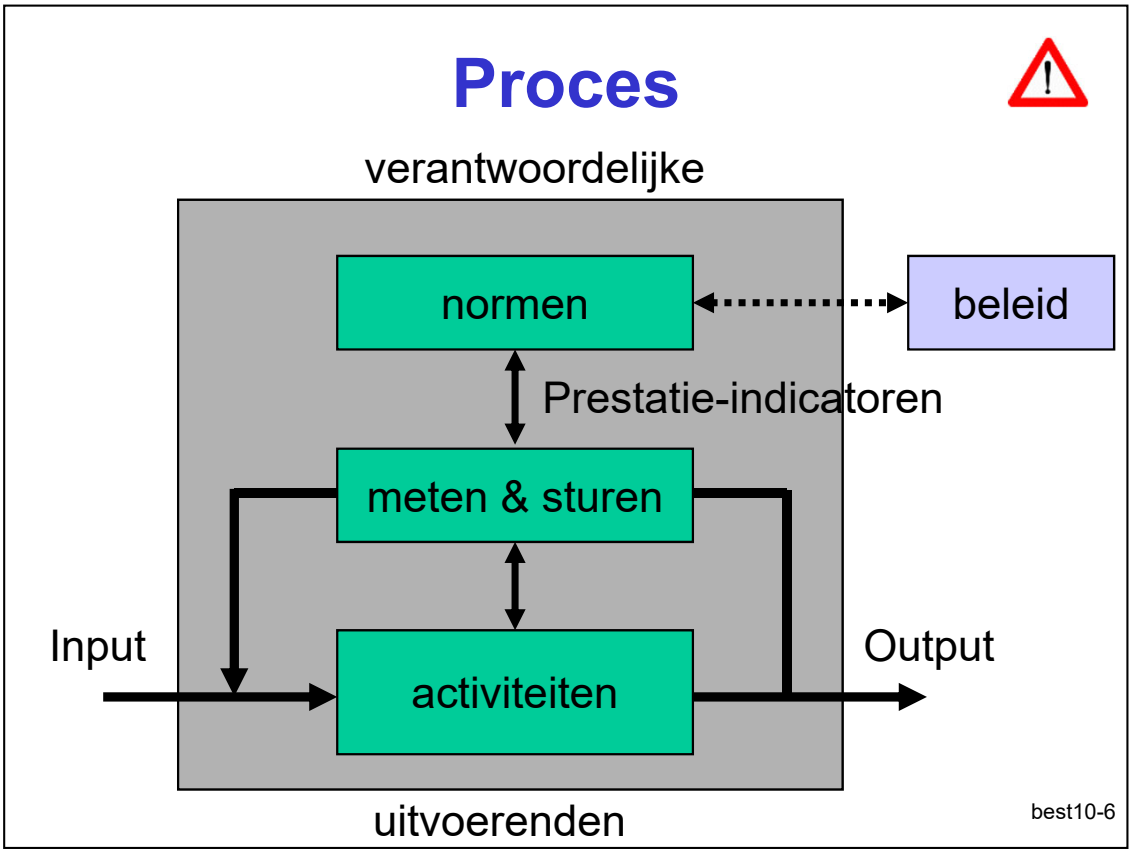
CMM-1: Basis (initial): ad hoc, iedereen doet zijn best, maar de kwaliteit van het resultaat is afhankelijk van de personen die betrokken zijn bij de taak. Haalt men de persoon weg, dan is er geen garantie dat de kwaliteit behouden blijft. Er zijn bijna geen processen gedefinieerd, acties zijn steeds een reactie op incidenten. Er is geen planning.

CMM-2: Herhaalbaar (repeatable): het huis op orde, succesvolle dienstverlening is herhaalbaar, acties maken deel uit van projecten; projecten kunnen gepland en begroot worden. Men leert uit ervaring.

CMM-3: Gedefinieerd (defined): processen zijn gedefinieerd, gestandaardiseerd, de activiteiten van management en productie zijn geïntegreerd. Men denkt na over de individuele processen.

CMM-4: Beheerd (managed): continue meting van alle prestatie-indicatoren ter verbetering van de kwaliteit van de dienstverlening. Processen opereren binnen vastgestelde normen met een zo klein mogelijke variantie. Continue meting van de kwaliteit van de dienstverlening. Het doel is het tijdig detecteren van gebreken.

CMM-5: Geoptimaliseerd (optimizing): de organisatie optimaliseert bewust de inrichting van de processen om de kwaliteit van de dienstverlening te verbeteren, een nieuwe technologie in te zetten of om diensten te ontwikkelen. Het doel is het voorkomen van gebreken.



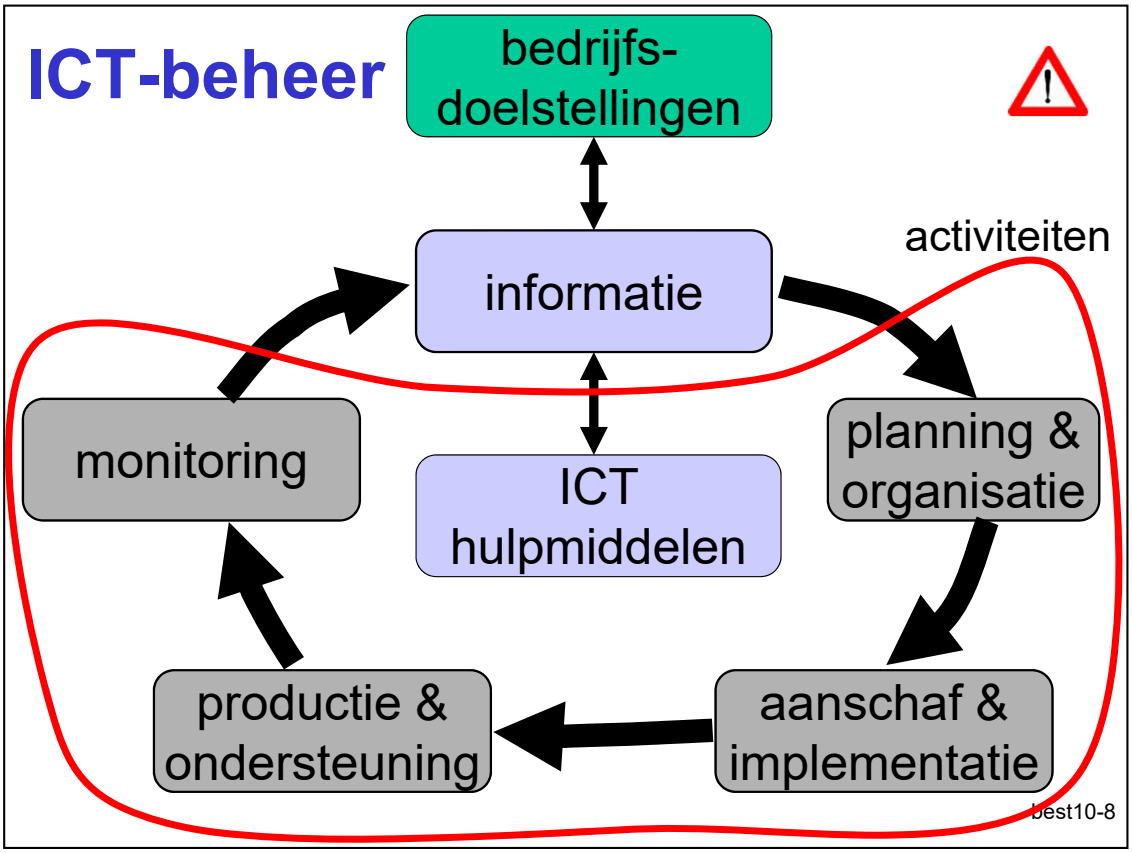
Om aan kwaliteitsborging te kunnen doen moet men de dienstverlening opdelen in een aantal processen waarvoor men een verantwoordelijke aanduidt, een aantal activiteiten definieert, de uitvoerenden aanduidt en prestatie-indicatoren definieert samen met de normen voor die prestatie-indicatoren.

Zo kan men een reservekopieproces definiëren. Men duidt de reservekopieverantwoordelijke aan. Hij of zij is verantwoordelijk voor de organisatie van het proces. De activiteiten zijn: het wekelijks nemen van een volledige reservekopie, het nemen van een dagelijkse incrementele reservekopie, het bijhouden van de reservekopietapes, het terugzetten van bestanden van de reservekopietape, enz. De uitvoerenden zijn de reservekopieoperators die zullen instaan voor de dagelijkse reservekopieën. Tijdens de vakantieperiode van een reservekopieoperator zal iemand anders zijn of haar activiteit moeten overnemen. Opdat dit mogelijk zou zijn zonder kwaliteitsverlies moeten de handelingen van de reservekopieoperator goed beschreven staan, evenals een aantal scenario's voor als het fout gaat. Een mogelijke prestatie-indicator kan het aantal gelukte reservekopieën per jaar zijn, of de maximale tijd die verstrijkt tussen twee reservekopieën. De norm kan zijn dat er minstens 300 reservekopieën per jaar moeten genomen worden en dat de maximale tijd tussen twee opeenvolgende reservekopieën niet meer mag bedragen dan b.v. 30 of 60 uur (indien er tijdens het weekend geen reservekopieën genomen worden). Het is de taak van de reservekopieverantwoordelijke om ervoor te zorgen dat de normen van de prestatie-indicatoren gehaald worden. Hiervoor zal hij of zij de nodige middelen (apparatuur en personeel) moeten inzetten. Het proces moet effectief (doeltreffend) en efficiënt (doelmatig) zijn zodat het beste resultaat bereikt wordt met de inzet van zo weinig mogelijk middelen. De werking van een proces wordt schematisch voorgesteld in de afbeelding.

Overzicht

- Kwaliteitsmodellen
- ICT-beheer
- Productieprocessen

best10-7



Eén van de belangrijke opdrachten van de ICT-afdeling van een bedrijf is het produceren van informatie voor het management. Deze informatie is essentieel bij het nemen van managementbeslissingen, en is dus cruciaal voor de realisatie van de bedrijfsdoelstellingen.

Informatie

Moet voldoen aan de volgende criteria:

- Effectiviteit “doeltreffendheid”
- Efficiëntie “doelmatigheid”
- Confidentialiteit
- Integriteit
- Beschikbaarheid
- Conformiteit
- Betrouwbaarheid

best10-9

Opdat ze voor dit doel bruikbaar zou zijn moet de informatie voldoen aan de volgende criteria, de zgn. informatiecriteria:

- Ze moet **effectief** (doeltreffend) zijn, d.w.z. dat de informatie relevant en pertinent moet zijn m.b.t. de bedrijfsprocessen, en ze op een bruikbare (tijdig, correct, consistent) manier ter beschikking moet gesteld worden.
- Ze moet **efficiënt** (doelmatig) zijn, d.w.z. dat de informatie op een optimale manier geproduceerd werd (met zo weinig mogelijk middelen).
- Ze moet **confidentieel** zijn, d.w.z. dat ze niet ongewild aan derden beschikbaar mag gesteld worden.
- Ze moet voldoen aan de voorwaarde van **integriteit**, dit wil zeggen dat de informatie accuraat en volledig moet zijn. In het bijzonder mag de informatie zelf geen contradicties bevatten (b.v. het totaal moet de som van de delen zijn).
- Ze moet **beschikbaar** zijn op het ogenblik dat men de informatie nodig heeft, en niet uitsluitend aan het einde van de maand of van het kwartaal. Dit kan repercussies hebben op de hoeveelheid middelen die men moet reserveren om aan dit criterium te voldoen: b.v. het dagelijks bijwerken van de informatie, i.p.v. éénmaal per week of per maand.
- Ze moet **conform** zijn met de geldende regels en gewoonten, waaraan de bedrijfsprocessen moeten voldoen. Zo zal de maandelijkse BTW-aangifte tegen een vastgestelde dag beschikbaar moeten zijn.
- Ze moet **betrouwbaar** zijn, d.w.z. dat het management deze informatie kan

gebruiken om het bedrijf te runnen, en aan al zijn rapporteringsverplichtingen te voldoen.

ICT-hulpmiddelen

- Gegevens
- Applicaties: programma's + manuele procedures
- Technologie: hardware, OS, DBMS, netwerk
- Faciliteiten: gebouwen, energie
- Mensen: werknemers, know-how

best10-10

De doelstelling van het ICT-beheer is om informatie te produceren die voldoet aan de zeven informatiecriteria. Om dit doel te bereiken kan de ICT-organisatie beschikken over de ICT- hulpmiddelen.

Deze hulpmiddelen moeten op de meest efficiënte manier ingezet worden om de informatiecriteria te realiseren.

Vier domeinen

- Planning en organisatie
- Aanschaf en implementatie
- Productie en ondersteuning
- Monitoring

best10-11

De activiteiten van het ICT kunnen ingedeeld worden in een viertal domeinen.

Planning en organisatie

- PO1: definieer een strategisch ICT-plan
- PO2: definieer de informatiearchitectuur
- PO3: bepaal het technologisch beleid
- PO4: definieer de ICT-organisatie en de relaties
- PO5: beheer de ICT-investeringen
- PO6: communiceer de beleidskeuzes
- PO7: beheer het menselijk potentieel
- PO8: garandeer conformiteit met de buitenwereld
- PO9: onderzoek de risico's
- PO10: beheer de projecten
- PO11: beheer de kwaliteit

best10-12

Het domein planning en organisatie is geen zeer technisch domein. Het houdt zich bezig met de strategische en organisatorische aspecten van het ICT-beheer en bestaat uit de volgende processen.

PO1 definieer een strategisch ICT-plan, dit is het opstellen van een planning op lange termijn. Dit plan moet op geregelde tijdstippen vertaald worden naar plannen op middellange termijn en concrete doelstellingen op korte termijn.

PO2 definieer de informatiearchitectuur, dit is een model van alle informatie over de bedrijfsprocessen die men wenst te beheren, en de systemen om dit te kunnen doen.

PO3 bepaal het technologisch beleid, dit is een plan waarin de technologische richting bepaald wordt: evolutie van de huidige infrastructuur, observatie van toekomstige evoluties, uitwijkmogelijkheden, investeringsplannen.

PO4 definieer de ICT-organisatie en de relaties, dit een plan voor de personeelsbezetting, definitie van verantwoordelijkheden, functies, relaties tussen functies, enz.

PO5 beheer de ICT-investeringen, dit omvat begrotingen, ramingen, controle over de uitgaven, verantwoording van de uitgaven.

PO6 communiceer de beleidskeuzes, dit omvat de regels voor goed gebruik van de infrastructuur, de technologische keuzen, kwaliteitsnormen, beveiligingspolitiek, enz. Dit is van belang opdat eenieder zou weten in welke richting de infrastructuur zal evolueren en zijn eigen plannen daarop kan afstemmen.

PO7 beheer het menselijk potentieel, dit is een taak van de personeelsdienst die instaat voor aanwerving, bevordering, training van het personeel.

PO8 garandeer conformiteit met de buitenwereld, dit proces volgt de externe verplichtingen op, zoals de overgang naar de euro, bescherming van de privacy, de databankwet, enz.

PO9 onderzoek de risico's van ICT-afdeling. Dit betreft technologische risico's beveiliging, continuïteit, enz.

PO10 beheer de projecten. Projecten bestaan uit taken die elk hun mijlpalen hebben, en waarvoor personen verantwoordelijk zijn. Het dagdagelijkse beheer van deze projecten valt onder dit proces.

PO11 beheer de kwaliteit. Dit proces houdt zich bezig met de invoering en de opvolging van een systeem van kwaliteitsborging (b.v. CMM of ISO 900x).

Aanschaf en implementatie

- AI1: identificeer de mogelijke oplossingen
- AI2: aanschaf en onderhoud software
- AI3: aanschaf en onderhoud hardware
- AI4: ontwerp en onderhoud ICT-procedures
- AI5: installatie en aanvaarding van oplossing
- AI6: beheer de veranderingen

best10-13

Dit domein houdt zich in hoofdzaak bezig met de realisatie van nieuwe projecten: het uitwerken van oplossingen, het vergelijken van oplossingen die commercieel beschikbaar zijn, de aanschaf en het onderhoud ervan. Eenmaal de projecten gerealiseerd zijn, wordt de uitbatingsfase gerealiseerd door het domein productie en ondersteuning. Men maakt een onderscheid tussen de volgende processen.

AI1 identificeer de mogelijke oplossingen: dit is het proces dat de verschillende mogelijke technische oplossingen tegen elkaar afweegt, en confronteert met de eisen van de gebruikers en de bedrijfsvoering.

AI2 aanschaf en onderhoud software: dit behelst de definitie van de verschillende vereisten en een implementatieplan: configuratie, testen, acceptatie, documentatie.

AI3 aanschaf en onderhoud hardware: dit behelst de evaluatie van de hardware en systeemsoftware, installatie, beveiliging, enz.

AI4 ontwerp en onderhoud ICT-procedures, dit omvat alle procedures die moeten gevolgd worden door de gebruikers, de handleidingen, de training, enz.

AI5 installatie en aanvaarding van oplossing: dit omvat de overgang van de oude naar de nieuwe configuratie, met overdracht van gegevens, testen, accreditatie, en opvolging.

AI6 beheer de veranderingen: dit behelst alles wat nodig is om veranderingen op een goede manier door te voeren: bepalen van de prioriteit, het verkrijgen van de toestemming om een verandering door te voeren, het effectief doorvoeren van de verandering.

Productie en ondersteuning

- DS1: definitie dienstverleningsniveaus
- DS2: beheer diensten van derden
- DS3: beheer prestatie en capaciteit
- DS4: garandeer beschikbaarheid
- DS5: garandeer beveiliging
- DS6: identificeer kostenstructuur
- DS7: training gebruikers
- DS8: advies en bijstand van de gebruikers
- DS9: beheer de configuratie
- DS10: beheer incidenten en problemen
- DS11: beheer data
- DS12: beheer faciliteiten
- DS13: beheer de operaties

best10-14

Dit is voor wat betreft het systeembeheer (technisch luik) het belangrijkste domein. Hier bevinden zich de processen waarvoor technische know-how vereist is om ze met succes te kunnen uitvoeren. Deze lijst van processen werd overgenomen uit het COBIT raamwerk. Verder in deze les wordt een meer uitgebreide lijst uit het ITIL raamwerk behandeld.

Monitoring

- M1: Monitor de processen
- M2: Onderzoek de doeltreffendheid van de processen
- M3: Laat onafhankelijk nagaan of de doelstellingen en kwaliteit gehaald worden
- M4: Onafhankelijke audit om na te gaan of er volgens ‘best practice’ gewerkt wordt

best10-15

Dit domein is van groot belang voor de kwaliteitsborging en voor de bijsturing. Hier zullen de verschillende processen geobserveerd worden. Deze informatie kan dan gebruikt worden om deze processen bijkomend te gaan sturen door b.v. de normen voor de prestatie-indicatoren bij te stellen.

M1 Monitor de processen, dit is nodig om de effectiviteit van de processen te kunnen nagaan (nagaan of de normen voor de prestatie-indicatoren gehaald worden).

M2 Onderzoek de doeltreffendheid van de processen, t.t.z. dat men tracht na te gaan of de juiste prestatie-indicatoren en normen gebruikt worden.

M3 Laat onafhankelijk nagaan of de doelstellingen en kwaliteit gehaald worden. De bedoeling van deze controle is de klanten van de ICT-afdeling meer vertrouwen te geven in de doeltreffendheid van de organisatie. Daarom wordt er beroep gedaan op een extern bureau.

M4 Onafhankelijke audit om na te gaan of er volgens `best practice‘ gewerkt wordt. De bestaande processen en procedures kunnen zeer nauwgezet gevolgd worden, maar dit betekent nog niet dat ze de beste manier van werken inhouden. Een audit kan een aantal suggesties ter verbetering aanbrengen.

Overzicht

- Kwaliteitsmodellen
- ICT-beheer
- Productieprocessen

best10-16

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-17

In wat nu volgt zullen de productie- en ondersteunende processen in detail besproken worden. Hiervoor zullen we gebruik maken van het raamwerk ITIL: Information Technology Infrastructure Library. Dit raamwerk bevat een beschrijving van de `best practice' op allerlei terreinen van ICT. De indeling die gebruikt wordt in dit hoofdstuk is iets fijner dan de indeling die bij COBIT gebruikt wordt. De processen die hier beschouwd worden zijn:

Dienstverleningsniveaubeheer

- Beheer van service levels
  - Welke kwaliteit men kan men verwachten (objectief en meetbaar)
  - Tegen welke afgesproken prijs
- Link tussen leverancier en klant
- In de taal van de klant (bedrijfsdoelstelingen)
- Vastgelegd in SLA: Service Level Agreement

best10-18

Het dienstverleningsniveau (service level) is eigenlijk het contract met de gebruiker (of klant) van de ICT-afdeling. Hierin wordt duidelijk omschreven welke kwaliteit hij of zij kan verwachten tegen welke afgesproken prijs. Hierbij moet men de kwaliteit op een objectieve en meetbare manier kunnen specificeren. B.v. twee opeenvolgende reservekopieën zullen nooit meer dan 30 uur uit elkaar liggen, een bestand zal van de reservekopietape gehaald worden binnen het uur. Bij dit laatste kan bijkomend afgesproken worden dat dit enkel zo zal zijn tijdens de kantooruren. Daarbuiten kan dit ook, maar de prijs voor een dergelijke dienstverlening zal uiteraard een stuk hoger liggen. Het feit dat de kwaliteit meetbaar moet zijn, is van belang bij betwistingen.

Het is verder van groot belang dat het dienstverleningsniveau uitgedrukt wordt in de taal van de klant, en niet in de taal van de ICT-afdeling. Eerder dan te specificeren dat de reservekopieën online beschikbaar moeten zijn, en dat er tijdens de kantooruren een reservekopieoperator stand-by moet zijn, is het beter om te stellen dat een bestand tijdens de kantooruren binnen het uur teruggezet kan worden. Hoe men dat dan intern realiseert is voor de klant van geen belang, en laat de ICT-afdeling toe om indien dit zinvol is, van werkwijze te veranderen zonder dat de overeenkomst moet herzien worden.

De dienstverleningsniveaus worden vastgelegd in een dienstverleningsniveauovereenkomst of SLA: Service Level Agreement. Over een SLA wordt onderhandeld tussen de ICT-afdeling en het management van de gebruikers, niet met de gebruikers zelf. Dit betekent dat in geval van klachten van de gebruikers over de SLA, deze gebruikers kunnen doorverwezen worden naar hun eigen management.

Beheer diensten van derden

- Soms via een SLA (indien het diensten betreft)
- Soms confidentialiteitsovereenkomst vereist (NDA: Non Disclosure Agreement)
- Waarborg na aankoop
- Onderhoudscontracten
- Speciaal geval: outsourcing

best10-19

De ICT-afdeling zal voor bepaalde dienstverlening op haar beurt afhankelijk zijn van leveranciers (b.v. de communicatie met de buitenwereld, de leverancier van de computerhardware, enz.). Indien een ICT-afdeling in de SLA met haar klant afspreekt dat de computerinfrastructuur 99% van de tijd beschikbaar zal zijn (maximaal 3.65 dagen niet beschikbaar per jaar), dan zal zij minstens dezelfde garanties moeten eisen van haar leveranciers (b.v. dat de communicatie met de buitenwereld niet meer dan 24 uur per jaar onbeschikbaar mag zijn, en dat de computerhardware b.v. binnen de drie uur moet kunnen hersteld zijn). Zoniet kan de ICT-afdeling niet garanderen dat ze de SLA met de gebruikers zal kunnen nakomen.

De overeenkomst met de leveranciers zal er vaak ook uitzien als een SLA waarbij de ICT-afdeling nu als klant optreedt. Indien de leverancier voor het uitvoeren van zijn SLA toegang moet krijgen tot gevoelige informatie van het bedrijf kan men vragen dat er een confidentialiteitsovereenkomst (NDA: Non Disclosure Agreement) ondertekend wordt. Hierbij verbindt de leverancier er zich toe dat hij geen misbruik zal maken van de gevoelige informatie die hij kan inzien.

Een overeenkomst met een leverancier voor het onderhoud van hardware (maar ook van software) wordt vaak een onderhoudscontract (maintenance contract) genoemd. Bij hardware zal men vaak afspreken binnen welke periode na een defect de hardware opnieuw operationeel zal zijn. Voor software valt onder een onderhoudscontract soms bijstand via een helpdesk, en meestal ook de upgrades van de software.

Een bijzonder geval van onderhoudscontract is de waarborg na verkoop. Soms kan men vragen dat deze waarborgperiode uitgebreid wordt. Het dienstverleningsniveau dat men in de context van een waarborg kan vragen is doorgaans echter beperkter dan wat men kan vragen in een echt onderhoudscontract.

Outsourcing

- Overdracht van complete processen naar een derde partij
  - vaak met overname van eigen personeel
  - met een duidelijke SLA
- Outsourcing soms noodzakelijk als gevolg van de steeds sneller veranderende technologie
  - medewerkers worden aangeworven voor een periode van 30 jaar
  - een computergeneratie duurt een stuk minder lang
  - een drastische omschakeling is voor oudere medewerkers niet steeds evident

best10-20

Soms kan een ICT-afdeling beslissen om bepaalde processen integraal te laten verzorgen door derden. Dit wordt outsourcing genoemd. Voorbeelden hiervan zijn aanschaf, installatie en onderhoud van de hardware of van het netwerk. Het dienstverleningsniveau dat men verwacht, wordt ook in dit geval vastgelegd in een SLA. Indien de processen die men wenst te outsourcen voordien reeds door de ICT-afdeling zelf verzorgd werden, is het gebruikelijk dat de personeelsleden mee ge-outsource-t worden, d.w.z. dat zij overgenomen worden door het bedrijf dat voortaan dit proces zal realiseren. Een dergelijke operatie kan de oorzaak zijn van sociale onrust in het bedrijf. Anderzijds zijn het vaak processen die mank lopen die ge-outsource-t worden, waardoor een overname voor die werknemers kan betekenen dat zij hun werk op een meer professionele manier zullen kunnen uitvoeren en op meer technische ondersteuning zullen kunnen rekenen.

Outsourcing is soms noodzakelijk als gevolg van de steeds sneller veranderende technologie. Medewerkers worden aangeworven voor een periode van 30 jaar maar dit is veel langer dan een generatie van de technologie. Voor oudere werknemers is het niet steeds evident om over te schakelen naar een totaal nieuwe technologie. Outsourcing (weliswaar zonder overname van de oudere werknemers) kan in dit geval een oplossing zijn. Een voorbeeld is een KMO die sinds jaren met een minicomputer werkt (computer met terminals), en de overstap wil maken naar een client-server architectuur met thin client + de koppeling met het Internet en een eerste aanzet tot e-commerce. De verschillen met de bestaande architectuur zijn zo groot, dat het soms beter is om er niet zelf aan te beginnen, zeker indien ICT niet behoort tot de kernactiviteit van het bedrijf.

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-21

Capaciteitsbeheer

- De juiste capaciteit aan middelen voor de huidige en toekomstige behoeften
- Hangt af van voorspelbaarheid van de toekomstige vraag
- Gebaseerd op trends in de belastings-monitoring

best10-22

De wet van Moore stelt dat de rekenkracht van computersystemen om de 24 maanden verdubbelt. Een empirische vaststelling is dat in hoeveel systeemmiddelen men ook voorziet, deze binnen de kortste keren steeds opgebruikt geraken. In ieder geval is het van belang om de evaluatie in de capaciteit nauwkeurig op te volgen om tijdig te kunnen ingrijpen. Dit is van groot belang in organisaties waar men de budgetten die men voor de uitbreiding nodig heeft een lange tijd op voorhand moet reserveren (b.v. in een begroting). Het is niet ongewoon om uitbreidingen ruim een jaar op voorhand financieel te moeten plannen.

De mogelijkheid om te plannen hangt natuurlijk in sterke mate af van de voorspelbaarheid van de toekomstige vraag. Hierbij moet rekening gehouden worden met de normale evolutie (b.v. toename van de schijfcapaciteit met 20 GB per maand), en met minder voorspelbare evoluties (b.v. het binnenhalen van een belangrijk contract of een belangrijke verandering in bepaalde bedrijfsprocessen zoals het voortaan inscannen van alle binnenkomende facturen). De evolutie van de capaciteit over de laatste 5 jaar geeft vaak een goede indicatie over toekomstige evoluties. Om aan een goede capaciteitsplanning te kunnen doen moet de capaciteit en de prestatie van de infrastructuur voortdurend gemonitord worden (zie ook het domein monitoring).

Beschikbaarheidsbeheer

- Beschikbaarheid
  - 99%: 3,65 dagen per jaar onbeschikbaar
  - 99,9%: 9 uur per jaar onbeschikbaar (1 werkdag)
  - 99,99%: <1 uur per jaar onbeschikbaar
  - 99,999%: 5 min per jaar onbeschikbaar
- Betrouwbaarheid: beschikbaarheid zonder de aangekondigde onbeschikbaarheid

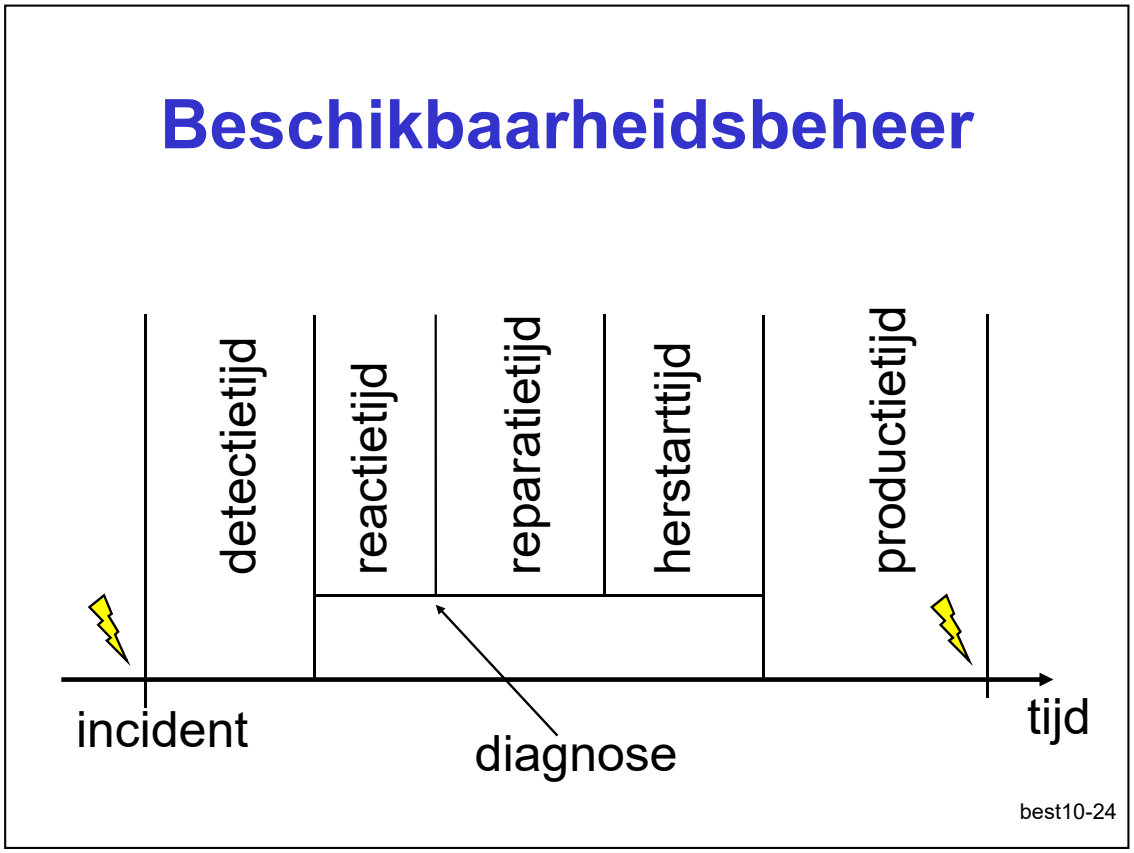
best10-23

Het beschikbaarheidsbeheer houdt zich bezig met het maximaal beschikbaar houden van de infrastructuur.

Om een idee te geven wat dit precies betekent, wordt beschikbaarheid uitgedrukt in ‘aantal negens’. 5 negens betekent een onbeschikbaarheid van maximaal 5 min per jaar. Hierbij moet men zich realiseren dat 5 minuten voor een server nauwelijks meer is dan de tijd om het systeem te bootstrappen. Het mag dus duidelijk zijn dat men om een dergelijke beschikbaarheid te realiseren, aanzienlijke investeringen in redundantie zal moeten plannen.

Men maakt een onderscheid tussen beschikbaarheid en betrouwbaarheid. Beschikbaarheid slaat op de fractie van de tijd dat het systeem beschikbaar is. Betrouwbaarheid slaat op de tijd dat het systeem beschikbaar is, zonder de aangekondigde onbeschikbaarheid. De betrouwbaarheid kan stukken hoger liggen dan de beschikbaarheid.

Windows is niet goed bruikbaar voor systemen die een hoge beschikbaarheid moeten hebben, al was het maar omdat het systeem herboot moet worden na elke niet-triviale aanpassing aan de configuratie (b.v. installatie van sommige softwarepakketten).



Hierboven worden de verschillende tijden aangegeven waarmee men rekening moet houden bij het optreden van een probleem. De som van de detectietijd, de reactietijd, de reparatietijd en de herstarttijd is de totale onbeschikbare tijd.

Reservekopie

- Om de M dagen een volledige reservekopie (volledige reservekopie) die langere tijd bewaard wordt
- Tussendoor dagelijks een incrementele reservekopie (bevat alle bestanden die veranderd werden sinds de laatste volledige reservekopie)
- Reservekopieën worden niet meteen overschreven, maar geroteerd

best10-25

Beschikbaarheid gaat echter verder dan de beschikbaarheid van de hardware of van de systeemsoftware. Ook de gegevens moeten beschikbaar zijn. De beschikbaarheid van gegevens kan verbeterd worden door b.v. het nemen van reservekopieën.

Men maakt een onderscheid tussen een zgn. volledige reservekopie en een incrementele reservekopie. Een volledige reservekopie is een reservekopie van alle bestanden op het systeem. Een volledige reservekopie wordt normaal gezien gedurende langere tijd bewaard. Tussen twee volledige reservekopieën hoort men incrementele reservekopieën te nemen, dit zijn reservekopieën die alle bestanden bevatten die veranderd werden sinds de laatste volledige reservekopie. Deze reservekopie is normaal gezien een grootteorde kleiner dan de volledige reservekopie.

Reservekopietapes

- Moeten geëtiketteerd zijn
- Mogen niet meer dan N keer gebruikt worden
- Moeten centraal, maar op een andere plaats bijgehouden worden (kluis?)
- Moeten tijdens de daluren aangemaakt worden
- Moeten gecontroleerd worden

best10-26

De gemaakte reservekopieën worden niet dagelijks overschreven, maar moeten gedurende een zekere tijd bewaard worden. Zo kan men b.v. voor de incrementele reservekopieën 7 tapes gebruiken, één per dag van de week. De volledige reservekopieën worden b.v. gedurende twee maanden bewaard alvorens de tapes te hergebruiken.

De reservekopietapes moeten duidelijk geëtiketteerd worden en de datum van de laatste reservekopie moet duidelijk op de reservekopietape vermeld worden. reservekopietapes hebben een eindige levensduur. Dit wil zeggen dat ze niet vaker dan het door de fabrikant aangegeven aantal keren mogen hergebruikt worden. De gemaakte reservekopieën moeten op een veilige plaats bewaard worden, liefst op een plaats die fysiek een eind van de computer verwijderd is. Dit is belangrijk om te vermijden dat bij een calamiteit (overstroming, brand) zowel de originele gegevens als de reservekopie zouden verloren gaan. Verder moeten reservekopietapes op een beschermde plaats opgeslagen worden om te vermijden dat ze in handen van derden vallen. Deze reservekopietapes bevatten immers dezelfde gevoelige informatie als de computersystemen zelf. Een kluis is toch wel de minimumbescherming.

Reservekopie

- Streef steeds naar unattended back-up, hetzij door
  - te kopiëren op 1 tape
  - een kopieerrobot te gebruiken
- Probeer het maken van reservekopieën te doen vanaf 1 machine
- Hou de inhoud van de tapes bij door de lijst met gekopieerde bestanden in een bestand op te slaan

best10-27

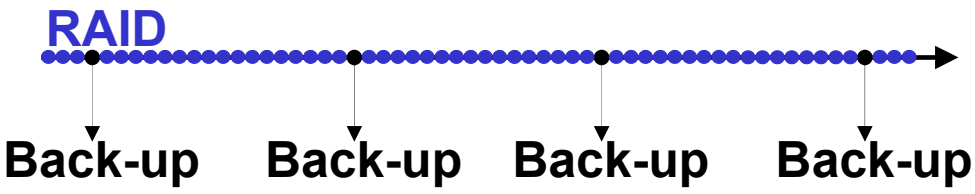
Om te vermijden dat bij het maken van een reservekopie een operator aanwezig moet zijn, moet men streven naar een oplossing van unattended back-up, hetgeen wil zeggen dat de reservekopie zonder menselijke tussenkomst kan gebeuren. Voor kleine systemen betekent dit dat de reservekopietape 's avonds klaargezet wordt, en 's ochtends gecontroleerd en opgeborgen wordt. Voor grote systemen zal dit betekenen dat men een kopieerrobot moet aankopen om 's nachts de tapes te verwisselen. Verder verdient het ook de aanbeveling om de reservekopie op 1 enkele machine te doen, om te vermijden dat men langs verschillende toestellen moet gaan om de tapes te verwisselen, en dat men verschillende tapes moet controleren.

Reservekopieën moeten 's nachts aangemaakt worden om de normale werking van de computerinfrastructuur zo weinig mogelijk te belasten. De reservekopieën moeten steeds gecontroleerd worden. Bij een fout tijdens het kopiëren is het immers mogelijk dat er maar een gedeeltelijke, of helemaal geen reservekopie gemaakt werd. Deze situatie kan gedurende weken of maanden onopgemerkt voorbij gaan, met dramatische gevolgen van zodra een schijf werkelijk defect gaat. Verder moet men ook op geregelde tijdstippen nagaan of men van een gelukte reservekopie wel een bestand kan terugzetten. De ervaring leert dat dit niet steeds eenvoudig is door incompatibiliteiten tussen het programma om de reservekopie te maken en het programma om bestanden terug te zetten.

Om gemakkelijk met gegevens van de reservekopie te kunnen werken is het handig om de inhoud van een reservekopietape op de computer te bewaren zodat men snel kan zoeken op welke tape het te herstellen bestand zich bevindt. Dit bestand kan meteen gebruikt worden om te controleren of de reservekopie wel degelijk gelukt is.

Maatregelen tegen defecten

- Reservekopie (niet continu, b.v. 1x per dag)
- RAID/Mirroring (continu)



best10-28

Back-up is een methode voor de verhoging van de beschikbaarheid die maar eens per dag een redundante kopie maakt. Indien men gegevens zonder onderbreking redundant wil opslaan, kan men zijn toevlucht nemen tot een RAID-systeem. In die gevallen zal het falen van één schijf geen gegevens verloren laten gaan.

Voor een volledige reservekopie van een schijf verdient het de aanbeveling om gebruik te maken van ‘disaster recovery’. Dit is een optie bij het kopiëren die niet enkel een reservekopie oplevert, maar tevens een set van diskettes of CD die gebruikt kunnen worden om de volledige reservekopie terug te zetten. Indien men dit niet heeft is het moeilijk om een schijf te herstellen: indien de schijf corrupt is en de computer niet meer opstart kan men ook het restore-programma niet opstarten, en zelfs indien de computer wel opstart zal het besturingssysteem doorgaans niet toelaten dat de systeembestanden overschreven worden terwijl ze in gebruik zijn. Het terugzetten van een systeemschijf wordt dus wel bijzonder moeilijk. Bij disaster recovery is dit geen probleem omdat de computer opstart van floppy of CD en de schijf dan volledig beschikbaar is.

Archivering

- Dit is te beschouwen als de laatste reservekopie vooraleer de gegevens van de schijven gewist worden
- Medium
  - tape
  - DVD
- Tijdig archiveren is belangrijk om de schijfcapaciteit beter te benutten

best10-29

Doorgaans zal de hoeveelheid gegevens op een computersysteem steeds maar blijven toenemen. Gelukkig neemt de capaciteit van de schijven ook toe, maar toch is het belangrijk om van tijd tot tijd ongebruikte gegevens van de schijf weg te halen. Indien men de gegevens blijvend wil bewaren moet men deze archiveren. De reservekopie alleen volstaat niet omdat reservekopietapes na verloop van tijd opnieuw gebruikt zullen worden. Archivering is te beschouwen als een finale en permanente reservekopie. Als medium kan tape gebruikt worden, maar tegenwoordig kiest men steeds vaker voor optische media. Tijdig archiveren is belangrijk om de schijfcapaciteit beter te benutten. Voor het archiveren is het van belang zich de vraag te stellen hoelang het medium nog leesbaar zal blijven (10, 20 jaar?) Men verwacht dat optische media (i) de gegevens gedurende een langere periode betrouwbaar kunnen opslaan, en (ii) dat de leestoestellen de bestaande formaten langer zullen kunnen blijven lezen (o.a. doordat het formaat van de DVD ook door videoapparaten gebruikt wordt).

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-30

Continuïteitsbeheer

- Herstarten na een calamiteit (brand, bomaanslag, aardbeving, stroomuitval, waterschade, enz.)
- Opties
  - Niets doen, we zien wel
  - Terug naar pre-computer tijdperk
  - Uitwijken: andere bedrijven, uitwijkcentrum
- Continuïteitsbeheer vereist een continue aandacht voor deze aspecten

best10-31

Met continuïteitsbeheer wordt bedoeld het verder zetten van de dienstverlening na een calamiteit zoals brand, ontploffing, aardbeving, stroomuitval, waterschade, enz. Het herstarten van de dienstverlening is in deze gevallen verre van eenvoudig, en vereist speciale aandacht en voorbereiding in de periode die de calamiteit voorafgaat.

Een bedrijf kan op een aantal verschillende manieren omgaan met continuïteitsbeheer:

1. Het kan het probleem gewoon negeren, ervan uitgaande dat de kans dat er zich een calamiteit voordoet eerder gering is, en dat gevolgen van de calamiteit zich wellicht niet zullen beperken tot de ICT-afdeling alleen. Men opteert ervoor om het probleem op te lossen op het ogenblik dat het zich zal voordoen, en niet te investeren in de oplossing van een probleem dat zich hopelijk nooit zal voordoen.
2. Het bedrijf opteert ervoor om in geval van een calamiteit in de ICT-afdeling terug te keren naar het pre-ICT tijdperk en de manuele procedures terug in te voeren. In die gevallen waar dit mogelijk is, kan dit een zinvolle optie zijn.
3. Het bedrijf opteert ervoor om in geval van een calamiteit de activiteiten zo snel mogelijk opnieuw op te starten. De moeilijkste opdracht is ervoor te zorgen dat de hardware opnieuw operationeel wordt. Hiervoor kan het bedrijf hetzij een overeenkomst afsluiten met een ander bedrijf dat over dezelfde infrastructuur beschikt, hetzij een overeenkomst afsluiten met een uitwijkcentrum waar men de benodigde apparatuur beschikbaar houdt, hetzij zelf een dubbele infrastructuur onderhouden. In dit laatste geval zal deze infrastructuur op twee verschillende locaties moeten opgesteld worden, en zal er ook een continue synchronisatie tussen de parallelle systemen moeten gebeuren (mirroring). De infrastructuur voor het continuïteitsbeheer kan dan ook ingeschakeld worden in geval van gewone

defecten of voor het uitvoeren van preventief onderhoud.

Beveiligingsbeheer

- Beveiliging = CIA
  - Confidentiality
  - Integrity
  - Availability
- Door
  - Authenticatie en afscherming
  - Beveiligde communicatie, cryptografie
  - Incidentbehandeling en rapportering
  - Virusdetectie
  - Firewalls
  - …

best10-32

Het beveiligingsbeheer garandeert confidentialiteit, integriteit en beschikbaarheid van een computersysteem en de gegevens door oog te hebben voor een doeltreffende authenticatie en afscherming, de communicatie op de verschillende niveaus te beschermen, incidenten te behandelen en erover te rapporteren, virussen tijdig te detecteren, en firewalls te gebruiken.

Beveiligingsbeheer

- Niet enkel de verantwoordelijkheid van de systeembeheerder, maar van de volledige organisatie.
  - Een beveiligingspolitiek moet afdwingbaar zijn ($\rightarrow$ ook het management moet erachter staan)
  - Beveiliging is ook de verantwoordelijkheid van de eindgebruikers

best10-33

De beveiliging is echter niet louter de verantwoordelijkheid van de systeembeheerder, maar van de volledige organisatie. Aangezien het ICT-departement hiërarchisch niet hoger staat dan de departementen waarmee het samenwerkt, kan het geen beveiligingspolitiek opleggen zonder medewerking van de departementshoofden. Vandaar dat men een beveiligingspolitiek meestal zal laten goedkeuren door het topmanagement waarna het via de gebruikelijke hiërarchische weg kan opgelegd worden aan de gehele organisatie.

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-34

Financieel beheer

- ICT is duur
- Opstellen kostenstructuur is belangrijk om te weten waar de kosten vandaan komen
- Het laat toe om de kosten door te rekenen aan de gebruikers

best10-35

ICT is duur: er zijn de hoge kosten van de infrastructuur, en ook de hoge kosten van personele omringing voor het operationeel houden van de infrastructuur en voor de ontwikkeling van nieuwe applicaties. Het is dan ook belangrijk om te weten te komen waar al het geld naartoe gaat. Dit is nodig om de uitgaven onder controle te houden, en om eventuele kosten door te kunnen rekenen aan de gebruikers.

Het moet b.v. mogelijk zijn om de prijs per geprint blad te berekenen. Deze is afhankelijk van (i) de aanschafprijs van de printer, (ii) de prijs van papier en inkt, (iii) de levensduur van de printer, (iv) onderhouds- en herstellingskosten, (v) het aantal uren interventie van een personeelslid om de printer te installeren en operationeel te houden. Indien men al deze factoren kent, kan men de prijs per afgeprint blad berekenen. Deze prijs kan als basis dienen voor een facturatie aan de gebruikers, of voor het opstellen van een budget voor de realisatie van een nieuw project. Het kennen van de kostenstructuur van de dienstverlening is hierbij essentieel.

Total Cost of Ownership (TCO)

- De totale kost van computerinfrastructuur: aankoop, installatie, onderhoud, enz. (Gartner 1988)
- PC's blijken zeer duur te zijn (tot 5 x aankoopprijs PER JAAR). Dus aankoopkost is slechts 20% van de totale kost per jaar.
- Gemiddelde levensduur = 3-4 jaar, nadien stijgt de kost

best10-36

In dit verband wordt vaak het concept van Total Cost of Ownership (TCO) gebruikt. Dit is de totale kost van het bezit van een ICT- component: aankoop, installatie, onderhoud, enz. Voor PC's worden bedragen genoemd van driemaal de aankoopprijs van de hardware. Hieruit blijkt dat de aankoopprijs niet het primaire criterium mag zijn bij de aankoop van ICT-materiaal. De kosten van onderhoud zijn doorgaans stukken hoger. Een duurder apparaat dat minder onderhoud vergt zal doorgaans op termijn goedkoper uitkomen. Een ander relevant gegeven is dat de gemiddelde economische levensduur van een PC drie jaar is. Naderhand stijgen de kosten voor onderhoud aanzienlijk, en beginnen deze toestellen ook functionele beperkingen te tonen (b.v. te traag om de meest recente software uit te voeren).

Bij het opstellen van een financiële planning is het niet enkel van belang om de huidige projecten te realiseren, maar moet men meteen ook in rekening brengen dat de infrastructuur moet onderhouden worden, en dat ze op termijn zal moeten vervangen worden.

Directe kosten TCO

- Hardware/software: aankoop, huur, onderhoud, reserveonderdelen, onderhoudscontracten, netwerkhardware, reservekopie,…
- Operations: systeembeheer, helpdesk, ingenomen vloeroppervlakte, meubilair, netwerkbeheer, …
- Administratie: aankoop, marktonderzoek, planning, training,

best10-37

Indirecte kosten TCO

- Eindgebruikers spenderen een deel van hun tijd met het zelf zoeken naar oplossingen…
- Downtime: b.v. bij preventief onderhoud, of bij defecten…

best10-38

Gebruikersbeheer

- Gebruikers hebben een persoonlijke account
- Gebruikers hebben een peter (hiërarchische overste)
- Gebruikers (en de peters) krijgen feedback over het gebruik van systeemmiddelen
- Gebruikers moeten getraind worden

best10-39

Technisch gezien wordt een gebruiker voorgesteld door een account. Elke gebruiker moet een individuele account bezitten. Het is geen goed idee om gebruikers een account te laten delen. Dit heeft o.a. te maken met het bepalen van de verantwoordelijkheid bij het optreden van problemen. Doordat een account persoonlijk is, kan bij het optreden van een probleem steeds verwezen worden naar de eigenaar van het probleemaccount.

Niet zomaar elke gebruiker kan een account krijgen. Een gebruiker moet voorgedragen worden door een hiërarchische overste (de zgn. peter). De gebruiker en de peter hebben recht op informatie over het gebruik van de computerinfrastructuur door de gebruiker (hoeveelheid cpu-tijd, pagina's geprint, enz.). De bedoeling hiervan is om misbruiken (door de gebruiker, maar ook door derden) van het account tegen te gaan. Indien een gebruiker gedurende 1 maand op vakantie is, maar er toch gewerkt werd, kan dit wijzen op een gecompromitteerd wachtwoord. Indien een gebruiker maar heel sporadisch hoeft te printen, en plotseling duizenden bladzijden geprint heeft, dan kan dit opnieuw wijzen op misbruik door de gebruiker of door derden.

Training

- Opleiding is zeer belangrijk
  - voor een optimaal gebruik van de beschikbare infrastructuur
  - om het aantal triviale interventies te beperken
  - om gevaren te leren herkennen
  - psychologisch: opleiding wordt vaak als 'beloning' beschouwd en werkt zeer motiverend ('er wordt in mij geïnvesteerd')

best10-40

Tenslotte moeten gebruikers getraind worden. Opleiding is zeer belangrijk voor een optimaal gebruik van de beschikbare infrastructuur, om het aantal triviale interventies door het systeembeheer te beperken, en om de gebruikers bewust te maken van de gevaren van het Internet en van het negeren van de beveiligingsmaatregelen.

Tenslotte kan training of opleiding ook als beloning gebruikt worden voor verdienstelijke personeelsleden. Dit is zeer zeker het geval indien de opleiding gecombineerd wordt met een aantal andere voordelen (opleiding in het buitenland, in een luxehotel, enz.).

Accountbeheer

- Accounts hebben een eindige levensduur
- Dode account = gevaarlijke account
- Accounts worden toegevoegd aan één of meerdere groepen
- Rechten en privileges worden toegekend aan groepen, niet aan gebruikers
- Elk account: minste privilege (cpu, opslag, uren van activiteit): quota-systeem

best10-41

Accounts moeten beheerd worden. Zij worden steeds toegekend voor een eindige tijd, maar kunnen uiteraard verlengd worden indien nodig. Een niet-gebruikte account is een potentieel beveiligingsprobleem. Misbruik van een dergelijk account kan lange tijd onopgemerkt blijven. Met accounts worden privileges en toegangsrechten geassocieerd. Toegangsrechten worden in de regel niet toegekend aan accounts, maar aan groepen. Een account verwerft een toegangsrecht door het lidmaatschap van een bepaalde groep. Om misbruiken te voorkomen hanteert men het principe van het ‘minste privilege’ hetgeen wil zeggen dat men aan een account niet méér toegangsrechten toekent dan deze die nodig zijn om een gebruiker zijn of haar taken te laten uitvoeren. Alle bijkomende toegangsrechten zijn overbodig en kunnen aanleiding geven tot misbruiken.

Accountbeheer

- Een gebruiker kan verschillende accounts hebben
- Paswoordbeheer centraal: single-sign-on
- Gebruikers moeten een verklaring van ‘correct gebruik’ ondertekenen bij de aanvaarding van hun account
  - geen paswoorden communiceren
  - account is strikt persoonlijk
  - geen inbreuk op de rechten van derden

best10-42

Accounts hebben slechts één eigenaar, maar één eigenaar kan wel verschillende accounts hebben. Het wachtwoordenbeheer voor al deze accounts gebeurt best centraal. Dit wil zeggen dat een gebruiker maar één wachtwoord heeft dat hij of zij voor de verschillende accounts kan gebruiken en dat een gebruiker het wachtwoord ook maar éénmaal hoeft in te geven (single sign on). Dit maakt het geregeld veranderen van wachtwoord heel wat gemakkelijker, waardoor het minder gemakkelijk zal uitgesteld worden.

De gebruikers moeten bij het openen van een eerste account een verklaring van ‘correct gebruik’ ondertekenen. Hierin staat de beveiligingspolitiek van het bedrijf vermeld: geen wachtwoorden communiceren, accounts zijn strikt persoonlijk, inbreuken op de rechten van derden zijn verboden, enz.

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-43

Helpdesk

- Afhandelen van vragen, klachten, en storingsmeldingen
- Afhandelen van dienstverzoek (b.v. restore van reservekopie, paswoord vergeten)
- Afhandelen van eenvoudige aanvragen tot wijzigingen (RFC's)
- Verspreiden van informatie onder de gebruikers

best10-44

De helpdesk is het aanspreekpunt voor de gebruikers. De voornaamste taken zijn

- Afhandelen van vragen, klachten en storingsmeldingen. Indien mogelijk zal er ogenblikkelijk hulp geboden worden. Indien dit niet mogelijk is, dan zal alles in het werk gesteld worden opdat het probleem zo snel mogelijk opgelost wordt.
- Afhandelen van een dienstverzoek (b.v. restore van reservekopie, wachtwoord vergeten). Strikt genomen gaat het hier dus niet over problemen of klachten, wel over een vraag voor een interventie waarvoor bijkomende rechten nodig zijn.
- Afhandelen van aanvragen tot wijzigingen. Gebruikers kunnen vragen om een bepaalde dienstverlening aan te passen. Het aanpassen van de dienstverlening valt buiten de bevoegdheid van de helpdesk en moet via een Request For Change (RFC) overgemaakt worden aan het veranderingenbeheer.
- Verspreiden van informatie onder de gebruikers. Doordat de helpdesk het aanspreekpunt voor de gebruikers is, is het ook het ideale doorgeefluik voor informatie van de ICT-afdeling naar de gebruikers.

De helpdesk fungeert als een soort van loket voor alle interacties met de gebruikers. Op die manier kan ervoor gezorgd worden dat de gebruikers op een correcte manier geholpen worden (de helpdesk heeft zijn eigen regels), rekening houdend met de precieze inhoud van de SLA. Op die manier verhindert men ook dat de gebruikers rechtstreeks contact opnemen met het gespecialiseerd personeel van de ICT-afdeling.

De helpdesk houdt een databank bij van vragen en antwoorden. Zo wordt een kennisdatabank opgebouwd waar alle helpdeskmedewerkers informatie kunnen uit

putten. Delen van deze databank kunnen als `veel gestelde vragen' (Frequently Asked Questions, FAQ) op de website van de helpdesk geplaatst worden.

Configuratiebeheer

- Bijhouden van de CMDB (Configuration Management Data Base)
- Identificatie en registratie van alle componenten in de ICT-infrastructuur

  Naam, installatiedatum, prijs, plaats, eigenaar, leverancier, type, serienummer, problemen, opmerkingen, onderhoudscontract, …
- Etiketteren van alle apparaten (ook netwerkpoorten)
- Ook documentatie en licenties bijhouden

best10-45

Een essentiële pijler in het systeembeheer is het configuratiebeheer, d.i. de inventaris van alle onderdelen van de ICT infrastructuur (hardware en software). Die informatie wordt bijgehouden in de CMDB (Configuration Management Data Base). Deze databank houdt per component van de ICT-infrastructuur o.a. de volgende gegevens bij: naam, installatiedatum, prijs, plaats, eigenaar, leverancier, type, serienummer, problemen, opmerkingen, onderhoudscontract, ... De CMDB bevat centrale informatie voor het financieel beheer, de strategische planning, enz.

Om de fysieke componenten op een gemakkelijke manier terug te kunnen vinden moeten alle apparaten duidelijk geëtiketteerd worden zodat identificatie gemakkelijk wordt. Niet enkel de hardware, maar ook de netwerkpoorten, documentatie en de software, licenties en onderhoudscontracten moeten op deze manier bijgehouden worden.

Aanschaf Software

- Commerciële software
  - op maat gemaakt
  - standaardpakket (COTS, Commercial Of The Shelf)
- Shareware
  - gratis, maar met beperkte functionaliteit tot betaling
- Public Domain/Freeware/Postware

best10-46

Er bestaan verschillende soorten software: commerciële software die hetzij op maat gemaakt kan zijn, hetzij Commercial Of The Shelf (COTS), dit zijn de standaardpakketten. Daarnaast bestaat er shareware met een beperkte gratis functionaliteit die kan uitgebreid worden door betaling (doorgaans vrij goedkoop). Tenslotte is er de software uit het publieke domein die zonder betaling kan gebruikt worden. Linux is hiervan het bekendste voorbeeld.

Indien mogelijk verdient het steeds de voorkeur om te onderzoeken of er degelijke standaardpakketten bestaan voor een bepaalde toepassing. Indien beschikbaar zal deze oplossing steeds goedkoper zijn dan het zelf ontwikkelen van een toepassing. Bovendien kan men verwachten dat deze software al door verschillende gebruikers uitgetest werd, en daardoor ook betrouwbaarder is dan software die men zelf ontwikkelt.

Ontwikkeling van Software

- Voor een niet-softwarebedrijf is de beste oplossing voor het realiseren van een niet-triviaal softwarepakket de uitbesteding met resultaatverbintenis aan een gespecialiseerde firma
- Het project moet opgevolgd worden door iemand van binnen het bedrijf, tenzij men hiervoor een consultant wil aanwerven

best10-47

Indien het echt nodig is om software op maat te ontwikkelen, is het voor een niet-softwarebedrijf beter om dit uit te besteden aan een gespecialiseerde firma, met een duidelijke resultaatsverbintenis. Tijdens de ontwikkeling kan het project opgevolgd worden door iemand van binnen het bedrijf, die naderhand kan instaan voor het onderhoud van de software. Deze taak kan eventueel ook door een consultant waargenomen worden.

Het zelf ontwikkelen van een niet-triviaal pakket is af te raden. Door gebrek aan ervaring zullen er in het begin wellicht fouten gemaakt worden, door gebrek aan voldoende ontwikkelaars zal de ontwikkeling langer duren dan nodig, indien het fout afloopt is er geen resultaatsverbintenis waarop men kan terugvallen, enz. De ontwikkelaar die hieraan begint loopt het risico dat een eventuele mislukking hem of haar voor de rest van zijn of haar carrière achtervolgt. In ieder geval moet de ontwikkelaar eisen dat hij of zij tijdens de ontwikkeling van het pakket vrijgesteld wordt van andere opdrachten. Het ontwikkelen van een applicatie is niet iets wat men zomaar even bij de andere taken bijneemt. Voor kleine opdrachten ligt dit natuurlijk anders.

Bescherming van software

- De gebruikte methode moet zowel de rechten van de maker (betaald worden voor zijn product), als de rechten van de rechtmatige gebruiker (het gebruiken van het programma) vrijwaren.
- In de praktijk betreft het steeds een compromis: het programma kan gekraakt worden en de gebruiker heeft last van de bescherming.

best10-48

Software is een product van de creativiteit van de ontwikkelaars of een bedrijf waarvoor zij uiteraard vergoed willen worden. Dit gebeurt aan de hand van de verkoop van licenties. Een licentie moet zowel de rechten van de maker (betaald worden voor zijn product), als de rechten van de rechtmatige gebruiker (het gebruiken van het programma) vrijwaren. In de praktijk betreft het steeds een compromis: ongeacht de methode die men gebruikt zal het programma kunnen gekraakt worden en de gebruiker zal steeds op de één of andere manier last hebben van het beschermingsmechanisme.

Licenties

- Individuele licenties
- Netwerklicenties (floating licenties)
- Site-licenties (departementale licenties)
- Campuslicenties

best10-49

Er bestaan verschillende soorten licenties. De individuele licentie laat de installatie op maximaal 1 computer toe. Het programma kan wel van één computer afgehaald worden, en op een andere computer geïnstalleerd worden. Een dergelijke licentie laat ook toe dat verschillende personen gebruik maken van die ene computer. Er mag ook een reservekopie gemaakt worden van de geïnstalleerde software, maar deze mag niet gebruikt worden om een tweede (simultane) installatie mee uit te voeren. Sommige licenties dwingen het individuele gebruik af door de aanwezigheid van een hardwaresleutel te eisen (zgn. dongle).

Naast de individuele licenties zijn er ook netwerklicenties (floating licenties). Hierbij maakt men gebruik van een zgn. licentieserver. De software mag zo vaak geïnstalleerd worden als men maar wil. Bij het opstarten maakt het pakket contact met de licentieserver om te onderzoeken hoeveel simultane gebruikers er zijn. Indien het totale aantal niet overschreden is, dan wordt het programma opgestart, zoniet wordt de melding gegeven dat alle licenties in gebruik zijn. Een eventuele hardwaresleutel zal nu aanwezig moeten zijn op de server.

Site-licenties (departementale licenties) zijn licenties voor ongelimiteerd gebruik binnen een bepaalde organisatie. In veel gevallen kan het IP-subdomein van de organisatie gebruikt worden om de toegang tot de software te regelen. Campuslicenties zijn vergelijkbaar met site-licenties maar voor het onderwijs. Soms laten campuslicenties toe dat studenten en personeel de software ook thuis kunnen gebruiken zonder bijkomende kosten.

Problemen met licenties

- Reservekopieën
- Weghalen code na verstrijken van de licentie
- Defecte machines bij eenmalig installeerbare licenties
- Carry-in herstelling

best10-50

Licenties veroorzaken vaak ongemakken. Zo is er het probleem van de reservekopie, en het herstellen van de reservekopie. Op een tweede computer mag het niet, maar indien de originele computer defect is, moet het wel kunnen op een tweede computer. Indien het een licentie voor een bepaalde periode is, dan hoort men in principe de programma's weg te halen van de computer (en van de reservekopieën) na het verstrijken van de licentieperiode.

In de praktijk is dit bijna niet afdwingbaar. Sommige pakketten zijn bij wijze van bescherming slechts éénmaal installeerbaar. Bij het defect gaan van de bewuste computer creëert dit heel wat problemen. Verder heeft men maar weinig controle over een licentie indien men een defecte computer naar een hersteller brengt. In dat geval kan men niet garanderen dat de software niet gekopieerd of gekraakt wordt.

Niet enkel om deze reden, maar voornamelijk om de confidentialiteit van de gegevens op een harddisk te garanderen, verdient het de aanbeveling om bij de herstelling van een computer de harddisk tijdelijk te verwijderen zodat de gegevens op de schijf geen risico lopen.

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-51

Incidentenbeheer

- Incident: elke gebeurtenis die niet tot de standaardoperatie van een dienst behoort en een onderbreking of vermindering van de kwaliteit ervan veroorzaakt
- Dienstverzoek: verzoek van een gebruiker om informatie, advies of documentatie

best10-52

Het incidentenbeheer is verantwoordelijk voor de behandeling van de incidenten. Een incident is een gebeurtenis die niet tot de standaardoperatie van een dienst behoort en een onderbreking of vermindering van de kwaliteit ervan veroorzaakt. Een incident is verschillend van een dienstverzoek, dit is een verzoek van een gebruiker om informatie, advies of documentatie, zoals de creatie van een bijkomende gebruiker, het terugzetten van een bestand van de reservekopie, enz.

Incidentenbeheer

- Een incident heeft een
  - Urgentie, afhankelijk van de hinder die de storing veroorzaakt bij de gebruiker
  - Impact, afhankelijk van de hinder die de storing veroorzaakt in het systeem
- Urgentie x impact = prioriteit die maat is voor de hoeveelheid middelen die men zal inzetten om het incident op te lossen.

best10-53

Een incident heeft een urgentie en een impact. De urgentie is afhankelijk van de hinder die de storing veroorzaakt bij de gebruiker. Zo zal een klacht over een soms wat minder goed werkend toetsenbord doorgaans minder urgent zijn dan de vraag om een gecrashte schijf te vervangen. In het eerste geval zal de gebruiker wellicht verder kunnen werken, in het tweede geval is hij of zij misschien wel technisch werkloos.

De impact is afhankelijk van de hinder die de storing veroorzaakt in het systeem, of met andere woorden op hoeveel gebruikers het een invloed heeft. Zo zal het uitvallen van het netwerk een grote impact hebben, het uitvallen van één toetsenbord heeft dit duidelijk niet.

De prioriteit waarmee een incident moet aangepakt worden is het product van de urgentie en de impact. De prioriteit is de maat voor de hoeveelheid middelen die men zal inzetten om het incident op te lossen. Indien de prioriteit zeer hoog is, zal men alles proberen doen om het incident zo snel mogelijk op te lossen.

Incidentenbeheer

- Registreert de storingen
- Kent een prioriteit toe
- Probeert de dienstverlening zo snel mogelijk te herstellen, in functie van de prioriteit
  - Bij een storing wordt er eerst naar een oplossing gezocht in de databank
  - Zoniet wordt er naar een oplossing gezocht, eventueel met de hulp van specialisten (oplosteam voor deze storing)

best10-54

De taak van het incidentenbeheer is om de incidenten (i) te registreren, (ii) ze een prioriteit toe te kennen, en (iii) de dienstverlening zo snel mogelijk opnieuw te herstellen, in functie van de prioriteit. Dit wil zeggen dat de incidenten met de hoogste prioriteit eerst aangepakt worden.

Het incidentenbeheer zal bij het optreden van een storing eerst op zoek gaan naar een oplossing in de databank van incidenten (en oplossingen). Indien er geen gekende oplossing voor de storing gevonden wordt, dan wordt er naar een oplossing gezocht, eventueel met de hulp van een aantal specialisten. Per storing kan er een speciaal oplosteam samengesteld worden om de storing op te lossen. Dit team wordt samengesteld door het incidentenbeheer.

Problemenbeheer

- Moet oplossing zoeken voor structurele fouten (aangebracht door incidenten-beheer)
- Een probleem waarvan de oorzaak bekend is wordt een ‘gekende fout’
- Dient ‘aanvraag voor verandering’ in bij het veranderingsbeheer om de gekende fout te verwijderen

best10-55

Het problemenbeheer moet oplossingen zoeken voor structurele fouten die door het incidentenbeheer aangebracht worden. Indien een serverapplicatie driemaal per week dienst weigert, en het incidentenbeheer deze storing enkel maar kan oplossen door de applicatie te herstarten, dan is er sprake van een structureel probleem dat een nader onderzoek vereist. In dit geval zal het incidentenbeheer dit dossier doorsturen naar het problemenbeheer. Het problemenbeheer zal op zoek gaan naar de oorzaak van dit gedrag. Het kan veroorzaakt worden door onstabiele hardware, sporadische netwerkfouten, een fout in de serverapplicatie, een probleem in het besturingssyteem, enz. Na verloop van tijd zal de grondoorzaak bekend zijn, en spreekt men van een gekende fout. Het problemenbeheer dient dan een `aanvraag voor verandering' bij het veranderingenbeheer. Het problemenbeheer mag zelf geen niet-triviale veranderingen met grote impact aan het systeem aanbrengen omdat elke verandering terug de oorzaak van andere instabiliteiten kan zijn. Veranderingen moeten op een gecontroleerde manier aangebracht worden door het veranderingenbeheer.

Veranderingsbeheer

- “Niet elke verandering is een verbetering, maar elke verbetering is een verandering”
- Aanvragen voor veranderingen worden geaccepteerd en geklasseerd
- Veranderingen met de hoogste prioriteit worden uitgevoerd
- Niet alle aangevraagde veranderingen moeten uitgevoerd worden

best10-56

Voor veranderingen geldt dat niet elke verandering is een verbetering is, maar elke verbetering wel een verandering is. Daarom moeten veranderingen met de grootste omzichtigheid aangebracht worden. Aanvragen voor veranderingen die binnenkomen worden geaccepteerd en geklasseerd. Hierbij geldt dat de veranderingen met de hoogste prioriteit meteen doorgestuurd worden naar het vrijgavebeheer dat zal instaan voor de implementatie van de verandering. Niet alle voorgestelde veranderingen moeten effectief doorgevoerd worden. Daarom is het belangrijk dat het problemenbeheer en het veranderingenbeheer best niet bij dezelfde personen berust. Indien dit wel zo is, dan is het gevaar reëel dat alle voorgestelde veranderingen ook effectief doorgevoerd worden.

Vrijgavebeheer

- Distributie en ingebruikname van hardware en software
- Procedures voor de distributie
- Communicatie omtrent updates
- Bijhouden van moederkopieën van alle software en configuratieparameters

best10-57

Het vrijgavebeheer is verantwoordelijk voor de distributie en de ingebruikname van de hardware en de software, rekening houdend met alle aspecten die hierbij van belang zijn (zoals de continuïteit van de dienstverlening). Het vrijgavebeheer beheert de procedures die bij de distributie gebruikt worden, organiseert de communicatie omtrent de aanpassingen (zodat de gebruikers op de hoogte gebracht worden van wijzigingen die hen aanbelangen), en bewaart de moederkopieën van alle software en configuratieparameters. Dit is essentieel om bij problemen identieke configuraties te kunnen opzetten, of te kunnen terugkeren naar een vorige configuratie.

Vrijgavetypes

- Full release (volledige pakket)
- Delta release (enkel gewijzigde delen)
  - Service packs (windows)
  - Service releases (office)
- (Emergency) fixes. Dringende aanpassing voor een gekende fout.

best10-58

Het vrijgavebeheer zal de veranderingen groeperen in zgn. releases. Hierbij maakt men een onderscheid tussen een full release die het volledige pakket bevat, delta releases die enkel maar de gewijzigde delen bevat, en (emergency) fixes die dringende aanpassingen voor gekende fouten bevatten. Delta releases worden soms ook service packs of service releases genoemd.

Installatie

- Installatie van software is veel eenvoudiger in een homogeen computerpark
  - Installatie vanaf een netwerkschijf
  - Klonen van schijven
- Het homogeen houden van een installatie is een belangrijke taak van de systeem-beheerder (zowel applicaties als OS)
- Massale installatie: roll-out (ontplooien)

best10-59

De installatie van software is aanzienlijk eenvoudiger in een homogeen computerpark. Het homogeen houden van de infrastructuur is een belangrijke taak van de systeembeheerder (hardware maar ook software). In een homogene infrastructuur is het gemakkelijker om installaties te laten gebeuren vanaf een netwerkschijf, of de installaties zelfs te `klonen'. Dit wil zeggen dat men de software éénmaal installeert op een schijf, en men deze schijf dan gewoon dupliceert per bijkomende installatie. Hiervoor bestaat speciale software (b.v. Norton ghost). Het massaal invoeren van nieuwe hardware of software wordt ook `roll-out' genoemd.

De-installatie

- De installatie van niet-triviale pakketten verandert zoveel systeemparameters en bestanden dat het manueel volledig ongedaan maken van een installatie quasi onmogelijk is
- Er dient de voorkeur gegeven te worden aan een O.S. met de-installatiefaciliteiten

best10-60

Het installeren van een softwarepakket geeft meestal niet zo heel veel problemen. Het volledig weghalen van een softwarepakket is echter heel wat moeilijker. De installatie van een niet-triviaal pakket verandert immers zoveel systeemparameters en bestanden dat het manueel volledig ongedaan maken van een installatie onbegonnen werk is. Daarom dient men de voorkeur te geven aan besturingssystemen en applicaties die faciliteiten aanbieden voor deïnstallatie.

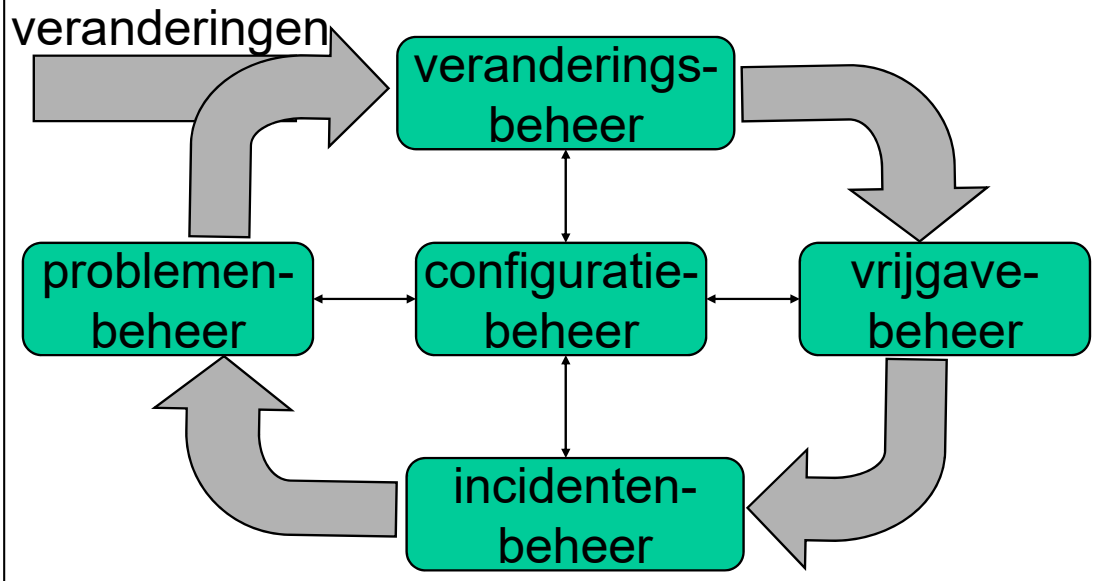
Upgrade + reservekopie

- Voor de installatie van software: volledige reservekopie
  - Indien installatie mislukt, kan men snel terug
- Na een installatie van software: volledige reservekopie
  - Sommige installatiebestanden kunnen zeer oud zijn, volledige reservekopie is de enige manier om ze met zekerheid te kopiëren.

best10-61

Een manier om zelf voor deïnstallatie te kunnen zorgen is om vóór de installatie van nieuwe software een volledige reservekopie te nemen. Indien de installatie mislukt dan kan men steeds terug naar de vorige toestand (indien men disaster recovery heeft kan men zelfs terug indien het echt grondig fout zou lopen). Na de installatie verdient het ook de aanbeveling om een volledige reservekopie te nemen omdat sommige bestanden zeer oud kunnen zijn en de reservekopieattributen van de bestanden verkeerd kunnen ingesteld staan. Een volledige reservekopie zal een effectieve oplossing bieden voor al deze mogelijke problemen.

Relatie tussen processen



best10-62

Processen van productie en ondersteuning

- dienstverleningsniveaubeheer (service level mgmt)
- beheer diensten van derden (vendor relationship mgmt)
- capaciteitsbeheer (capacity mgmt)
- beschikbaarheidsbeheer (availability mgmt)
- continuïteitsbeheer (continuity mgmt)
- beveiligingsbeheer (security mgmt)
- financieel beheer (financial mgmt)
- gebruikersbeheer (customer relationship mgmt)
- advies en bijstand van de gebruikers (helpdesk)
- configuratiebeheer (configuration mgmt)
- incidentenbeheer (incident mgmt)
- problemenbeheer (problem mgmt)
- veranderingsbeheer (change mgmt)
- vrijgavebeheer (release mgmt)
- databeheer (data mgmt)
- logistiek beheer (facilities mgmt)
- organisatiebeheer (operations mgmt)

best10-63

Databeheer

- De applicatiegegevens moeten ook beheerd worden
- Inhoudelijk: databankbeheerder
- Systeemniveau: reservekopie, RAID, enz.

best10-64

De gegevens waarover de ICT-afdeling de hoede heeft (databanken) moeten uiteraard ook beheerd worden. Onder het databeheer valt de belangrijke taak van de databankbeheerder die beslist welke gegevens er in de databank opgenomen worden, en op welke manier. Verder kunnen onder het databeheer ook een aantal systeemtaken vallen zoals het beheer van de reservekopieën en de RAID-systemen.

Logistiek beheer

- Beheer van de lokalen, gebouwen
- Betrouwbare energievoorziening
- Gestructureerde bekabeling
- Koeling
- Fysieke toegangscontrole
- Branddetectie

best10-65

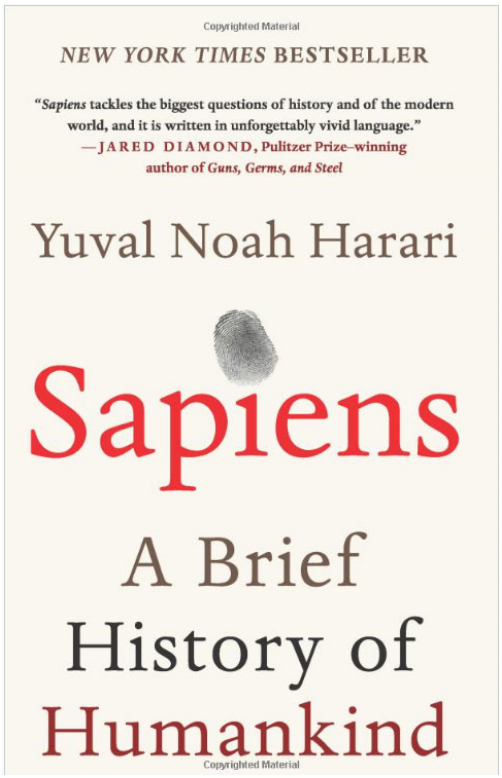
Een ICT-afdeling leeft niet van bits alleen, maar heeft ook nood aan lokalen, energie, enz. Onder het logistiek beheer vallen het beheer van de lokalen en gebouwen, een betrouwbare energievoorziening, de zorg voor een goed gestructureerde bekabeling, de verwarming en de koeling, de toegangscontrole, branddetectie, enz.

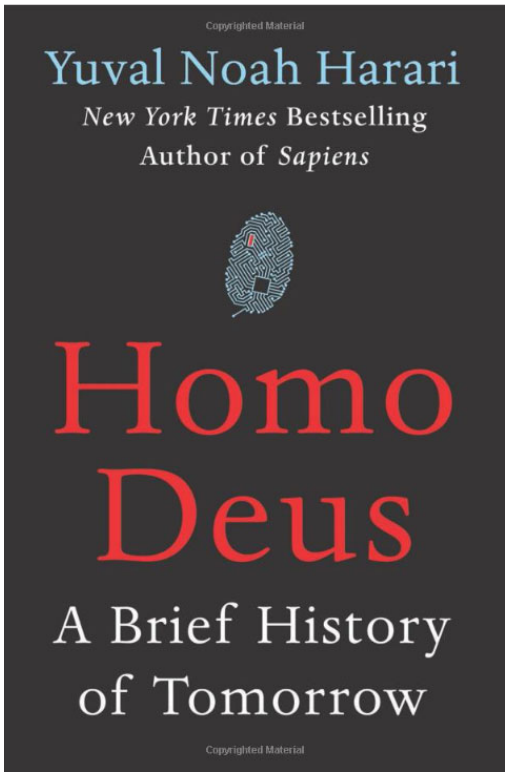
Organisatiebeheer

- Toewijzing van verantwoordelijken voor processen
- Opzetten van ploegen voor 24/7 werking
- Opzetten van overlegstructuren voor het overleg tussen de verantwoordelijken van de verschillende processen

best10-66

Een ICT-afdeling kan niet werken zonder dat ook de human resources (personeel) optimaal ingezet en gemotiveerd worden. Dit luik houdt zich bezig met het toewijzen van verantwoordelijken voor de verschillende processen. Merk trouwens op dat er in dit hoofdstuk zeer veel processen gedefinieerd werden, en dat het niet noodzakelijk is dat al deze processen verschillende verantwoordelijken hebben. In zeer kleine organisaties zal het wellicht zelfs zo zijn de ICT-verantwoordelijke verantwoordelijk zal zijn voor alle processen, en ook voor de uitvoering van alle activiteiten van alle processen. In dit geval zal er dan geen 24/7 werking mogelijk zijn. In grote organisaties zal dit wel mogelijk zijn, en zal het beheer van de operaties verantwoordelijk zijn voor het opzetten van een ploegensysteem. Indien er voor de verschillende processen verschillende verantwoordelijken zijn, dan zullen er ook overlegstructuren tussen de verantwoordelijken van de verschillende processen moeten opgezet worden.


Copyrighted Material
NEW YORK TIMES BESTSELLER
"Sapiens tackles the biggest questions of history and of the modern world, and it is written in unforgettably vivid language."
—JARED DIAMOND, Pulitzer Prize–winning author of Guns, Germs, and Steel
Yuval Noah Harari
Sapiens
A Brief History of Humankind
Copyrighted Material


Copyrighted Material
Yuval Noah Harari
New York Times Bestselling Author of Sapiens
Homo Deus
A Brief History of Tomorrow
Copyrighted Material

best10-67