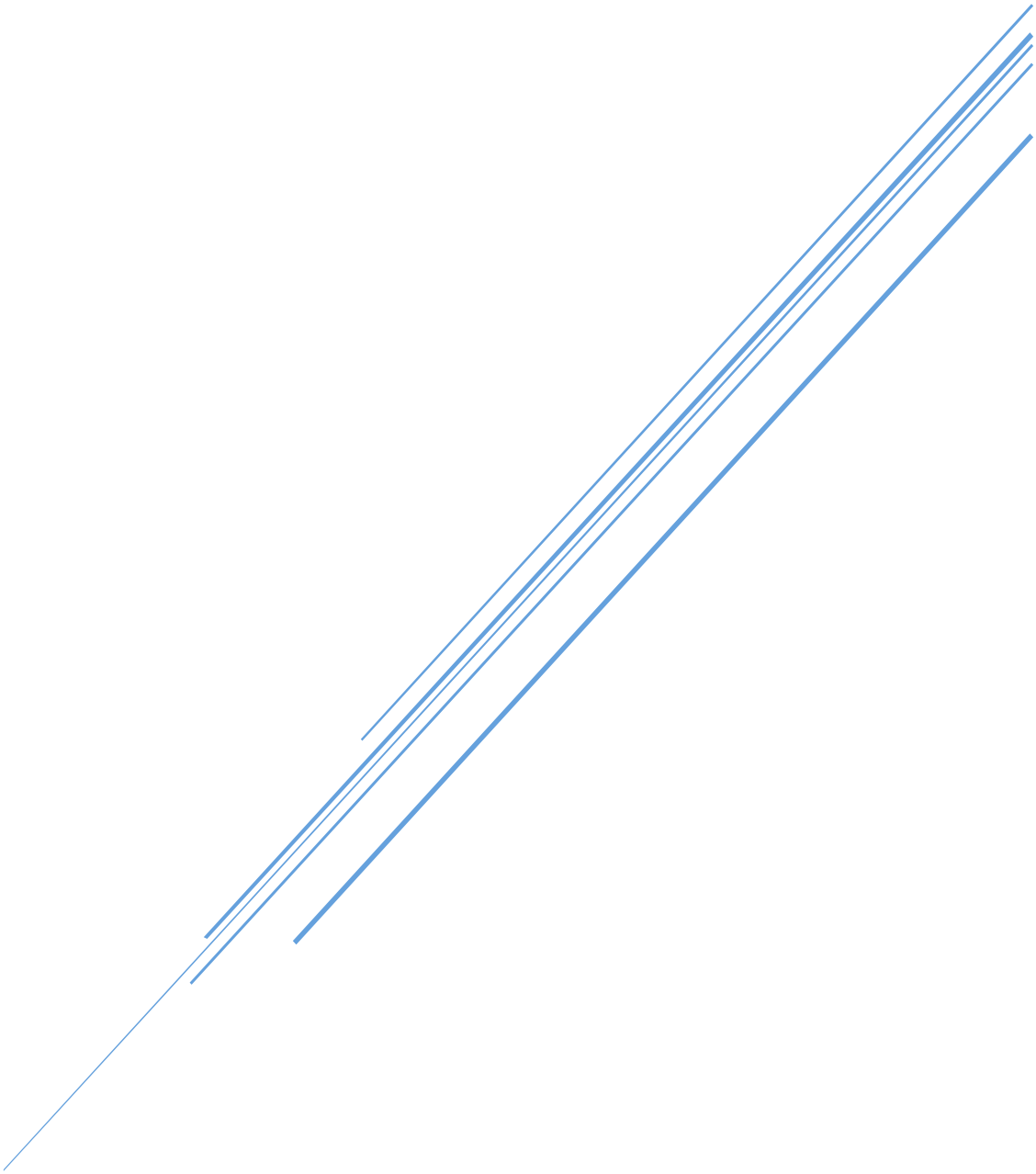
SAMENVATTING INFORMATIEMANGEMENT

Docenten: M. De Backer, L. Lemeire, J. Moons

Student: Vanden Berghe M.



Handelswetenschappen UGent
2016-2017

Inhoudstafel

1 Beleidsinformatiesystemen in de 21ste eeuw

1.1 Inleiding en motivatie

Informatiesystemen hebben een steeds prominentere aanwezigheid gekregen in de dagelijkse werking van organisaties. Maar de ontwikkeling van deze informatiesystemen brengt vaak een aantal problemen met zich mee.

- ⇨ Vaak moet men vaststellen dat er een soort 'Berlijnse muur' bestaat tussen business en IT: bedrijfsmensen hebben vaak een aantal verwachtingen en eisen & informatici hebben de neiging om zich op de technische aspecten te concentreren, maar de technologisch beste keuze is niet altijd de beste keuze vanuit bedrijfsorganisatorisch perspectief.

Business-ICT allignment: de mate van overeenstemming tussen bedrijfsstrategie en informaticastrategie

- ⇨ Krijgt de laatste jaren steeds meer aandacht (het juiste gebruik van informatiesystemen vs het verkeerde gebruik)
- ⇨ Het ontwikkelen van een ICT-strategie gebeurt best in samenspraak met de bedrijfsmensen

Een goede communicatie en samenwerking tussen bedrijfsmensen en informatici en een goede afstemming op de bedrijfsstrategie zijn meer bepalend voor het succes van een investering in informatiesystemen dan de technologie zelf.

1.1.1 Informatietechnologie heeft de wereld veranderd

- ⇨ Macro-economisch niveau

Thomas Friedman 'The world is flat': de wereld is door 3 globaliseringsfasen gegaan

- / *Globaliseringsfase 1.0*: omvang van de wereld is gekrompen van groot tot middelgroot
  - ⇨ Concurrentie op niveau van de landen
  - ⇨ Bepalende factoren: spierkracht, paardenkracht & windkracht (+ stoomkracht)
- / *Globaliseringsfase 2.0*: omvang van de wereld is gekrompen van middelgroot tot klein
  - ⇨ Concurrentie op niveau van multinationale ondernemingen
  - ⇨ Door dalende vervoers- en communicatiekosten
- / *Globaliseringsfase 3.0*: omvang van de wereld is gekrompen van klein tot uiterst klein
  - ⇨ Samenwerking en competitie op het niveau van het individu
  - ⇨ 'vlakke wereldplatform' (10 flatteners)
    - / Val van de Berlijnse muur
    - / Opkomst van het internet
    - / Opkomst van Workflow software en van XML
    - / Mogelijkheid om te uploaden
    - / Outsourcing
    - / Offshoring
    - / Supply-Chaining
    - / Insourcing
    - / Informing
    - / De steroïden

Alle flatteners zijn betrokken in een drievoudige convergentie

- / Ze versterken elkaar
- / Ze induceren in een wereldwijde verandering in gewoontes
- / Maken de 'flat world' toegankelijk voor mensen die voordien uitgesloten waren

1.1.2 De productiviteitsparadox

⇨ Micro-economisch niveau

Productiviteit is de hoeveelheid output die geproduceerd wordt met een bepaalde hoeveelheid input.

⇨ Zullen bedrijven die veel investeren in IT een hogere productiviteit hebben dan bedrijven die dat niet doen?

Solow stelt dat 'computers are found everywhere but in the productivity data' (**Solow productivity paradox**)

⇨ Aan de hand van deze uitspraak kon men argumenteren dat, hoewel informatietechnologie de werld verandert, het toch niet van significant belang is omdat het de productiviteit nauwelijks beïnvloedt.

Nicalos Carr argumenteert in zijn paper 'IT doesn't matter' dat zelfs indien de invoering van informatietechnologie zou leiden tot of een verklaring zou zijn voor een productiviteitswinst, dan is dit slechts op macro-economisch niveau en niet relevant voor het individuele bedrijf.

⇨ Iedereen heeft op gelijke manier toegang tot informatietechnologie en dus kan deze technologie geen basis zijn voor differentiatie en competitie.

3 richtlijnen:

- Minder investeren in IT
- Wachten tot andere het nut van een nieuwe technologie bewezen hebben
- Infrastructuurvoorzieningen moeten betrouwbaar zijn, concentratie op zwakten en niet op de kansen

In de vergelijking van informatietechnologie met infrastructuurvoorzieningen worden 2 fouten gemaakt, namelijk:

- Het rendement van informatietechnologie is heel sterk afhankelijk van hoe de technologie wordt ingezet
- Een deel van de technologie kan gecatalogeerd worden als basisinfrastructuur

Terwijl Carr zijn redeneringen zeker opgaan voor het infrastructuurgedeelte van de IT-investeringen, gaat zijn redenering niet op voor dat deel van de investeringen die betrekking hebben op de strategisch belangrijke toepassingen.

Sinds het produceren van de productiviteitsparadox, hebben vele onderzoekers getracht de paradox te bevestigen, te verklaren of te ontkrachten

⇨ Recente studies convergeren tot het besluit dat investering in IT wel degelijk een impact heeft op de performantie van ondernemingen, maar dat de feitelijke gerealiseerde performantieverbeteringen sterk verschillen van onderneming tot onderneming

Tatcher en Pingry tonen aan dat het effect van investeringen afhangt van:

- Het doel van de investeringen
- De marktstructuur
- Het soort product dat het bedrijf maakt
- De manier waarop je output meet

Intuïtieve verklaringen voor de productiviteitsparadox:

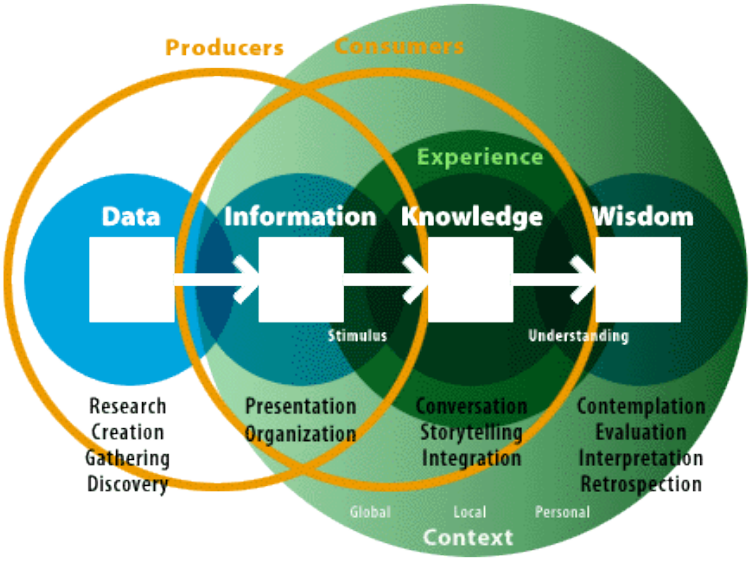
- Fundamenteel verschil tussen het inzetten van een machine ter vervanging van handenarbeid (automatiseren in het industriële tijdperk) en het inzetten van een computer ter vervanging van intellectuele arbeid (automatiseren in het informatietijdperk)
  - ⇨ Informatiesystemen zullen zelden mensen vervangen, maar zorgen er wel voor dat er meer informatie beschikbaar is wat heel wat opportuniteiten creëert
  - ⇨ Er zijn vaak meer mensen nodig om deze nieuwe/extra informatie te interpreteren
- De manier waarop productiviteit (niet) gemeten wordt
  - ⇨ Productiviteit meten adh van de ratio input/output maar in geval van informatiesystemen is deze ratio veel moeilijker te kwantificeren.
  - ⇨ Automatisatie heeft een aantal neveneffecten die moeilijk te kwantificeren zijn
  - ⇨ Soms ook eerder ene kwaliteitsgroei dan een productiviteitsgroei
  - ⇨ '**technology lag**': het duurt tijd vooraleer mensen vlot kunnen omgaan met de nieuwe manier van werken
  - ⇨ Het is heel moeilijk om bij automatisering een balans te vinden tussen het aanbieden van meer intelligentie en controle enerzijds en het waarborgen van flexibiliteit anderzijds

De 3 richtlijnen die Carr geeft zijn in zekere mate correct maar hij ziet toch een aantal zaken over het hoofd (IT kan wel leiden tot strategische voordelen)

- De nood aan veranderingsmanagement
  - ⇨ Om voordelen te halen uit ICT investeringen, moet de manier van zakendoen aangepast worden
  - ⇨ Het zijn de gebruikers die bepalen hoe software gebruikt wordt
  - ⇨ '**magic bullet theory**': IT het gedrag van mensen en van organisatie automatisch aanpast doordat die technologie hen de mogelijkheid biedt om dingen te doen die men vroeger niet kan doen en door te voorkomen dat men op een oude, onproductieve manier blijft werken (deze theorie is vaak niet geldig)
- De nood aan alignering
  - ⇨ De technologie die geïnstalleerd wordt, moet naadloos aansluiten bij de manier waarop het bedrijf zaken doet
  - ⇨ '**mindfull decision making**': eerst selectieve en grondige testen doen alvorens een technologie te implementeren
    '**mindless decision making**': investeren op basis van succesverhalen van anderen
- Kopiëren is niet altijd eenvoudig of zinvol
  - ⇨ Richtlijnen om competitieve voordelen te behalen
    - Bouw op bestaande IT middelen
    - Bouw op/aan complementaire, gespecialiseerde middelen
    - Kies nauwkeurig je IT projecten
    - Zorg dat je een lock-in krijgt (verscheidene soorten omschakelingskosten creëren voor de klanten waardoor je de klanten vastbindt aan het bedrijf)

1.2 Wat is een beleidsinformatiesysteem?

1.2.1 Wat is informatie?



Data/gegevens zijn opgeslaan in datacenters in het binair stelstel. Het zijn ruwe gegevens (overdraagbaar en objectief) en vormen de basis voor informatie. Door deze gegevens in een context te plaatsen, kunnen ze geïnterpreteerd worden en zo worden omgevormd tot informatie.

Informatie heeft iets te maken met 'meer weten', moet kennis toevoegen maar wat voor de ene mens nietszeggend is, kan voor een ander zeer informatief zijn (niet overdraagbaar en subjectief). Uit deze informatie wordt kennis gegenereerd.

Soorten informatie

- Harde informatie: makkelijk te verwerken door informatiesystemen
  Zachte informatie: moeilijk te verwerken door informatiesystemen

- Interne informatie: binnen een onderneming
  Externe informatie: buiten een onderneming (uit de omgeving)

- **Meta-informatie**: informatie over informatie
  - ⇨ Dublin core: een algemeen aanvaarde manier om elektronische bronnen te beschrijven om op die manier efficiënter documenten te kunnen terugvinden
  - ⇨ Waarom zo belangrijk?
    - Informatie meer verstaanbaar maken voor mensen en computers
    - Doet de waarde van de informatie stijgen
    - Men kan de informatie steeds begrijpen of gebruiken nadat het van eigenaar verandert is
    - Maakt het gemakkelijker om informatie te delen
    - Verhoogt de veiligheid van data

1.2.2 Wat is een systeem?

⇨ Een verzameling van elementen waartussen verbanden bestaan en die met een bepaald doel zijn samengebracht

Concepten van een systeem

- Welke **elementen** zitten in een systeem?
- Hoe staan die elementen met elkaar in **relatie**?
- Wat is het **doel**?

Systemen vervullen een functie in hun omgeving, maken deel uit van een groter geheel. Om een systeem te bestuderen, heeft men een beschrijving van dat systeem nodig.

⇨ Hiërarchie van systemen: alle elementen van een systeem hangen samen, maar systeem bestaat ook uit een aantal subsystemen. Via de subsystemen kunnen we het algemeen systeem bekijken vanuit verschillende perspectieven. (cfr. Het lichaam)

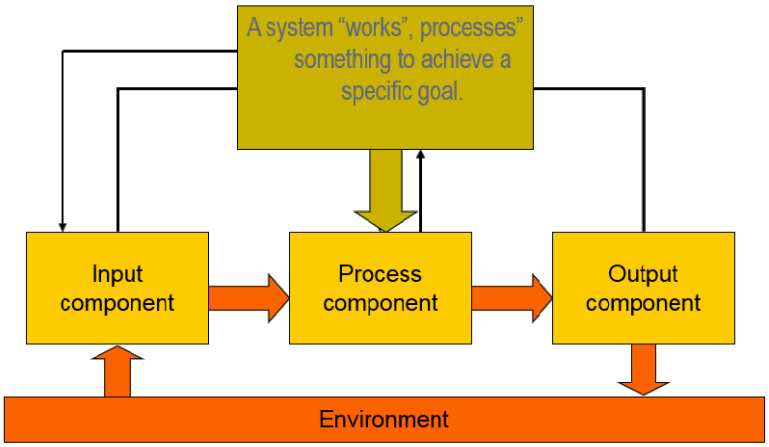
Soorten systemen:

- Abstracte systemen: een idee, een ontwerp. Alle systemen zijn eerst abstracte systemen en worden daarna fysieke systemen
  Fysieke systemen: zijn fysiek aanwezig in de werkelijkheid

- Open systemen: oefent invloed uit op zijn omgeving en ondergaat invloeden uit zijn omgeving
  Gesloten systemen: er zijn geen omgevingsinvloeden

- Statische systemen: verandert niet
  Dynamische systemen: de elementen, verbanden en/of doelen veranderen doorheen de tijd

- Formele systemen: de elementen en hun verbanden liggen duidelijk vast
  Informele systemen: minder duidelijk omschreven

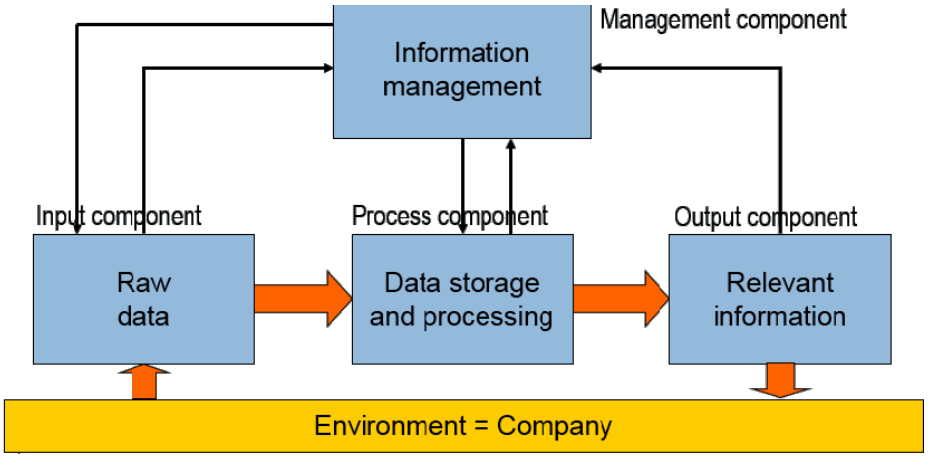


De **invoer- en uitvoercomponenten** zorgen voor de interactie met de omgeving (in het geval van open systemen). De **procescomponent** vervult de eigenlijke functie van het systeem en de **beheerscomponent** zorgt voor de afstemming van de processen op het beoogde doel.

1.2.3 Wat is een informatiesysteem?

⇨ Een informatiesysteem is formeel, open, dynamisch & fysiek!

Ook informatiesystemen zijn gekenmerkt door de 4 basis systeemcomponenten. De **systeeminput** bestaan uit een aantal ruwe gegevens. Het **systeemproces** transformeert deze gegevens in bruikbare informatie en het **systeembeheerelement** controleert de tijdigheid, nauwkeurigheid, … etc. van de verkregen informatie. Het bedrijfssysteem fungeert als omgeving voor een informatiesysteem.



Informatiesystemen verschillen in 2 belangrijke aspecten van bedrijfssystemen

- / Eerste opmerking heeft betrekking op de vele varianten die zich kunnen voordoen bij het produceren van informatie
- / Tweede opmerking heeft betrekking op de problemen die men ontmoet bij het definiëren van informatie als eindproduct (elke onderdeel/stukje informatie dient als nieuwe input voor andere onderdelen/informatie)

In vele bedrijven probeert men aan de hand van een zo volledig mogelijke registratie van gegevens en gebeurtenissen in het bedrijf, in het informatiesysteem een soort '**carbon copy**' of spiegelbeeld te creëren van de realiteit.

Het onderscheid tussen werkelijkheid en informatiesystemen wordt steeds vager (in beide richtingen)

- ⇨ **Virtuele realiteit**: de informatisering gaat zo ver dat het informatiesysteem de werkelijkheid is, de gegevens en gebeurtenissen worden dan enkel nog geregistreerd in het informatiesysteem en bestaan enkel daar. (vb. spaarboekje)
- ⇨ **'augmented reality'**: men probeert informatie en functionaliteit aan de realiteit toe te voegen (vb. de camera van je smartphone op een gebouw richten en informatie krijgen over dat gebouw)

Doordat informatiesystemen weerspiegelingen zijn van bedrijfssystemen, omvat de studie van informatiesystemen veel meer dan enkel de technologie, het omvat ook de mensen die met de systemen moeten werken

- ⇨ Organisatorische en management aspecten
  - / Organisatorische aspecten hebben betrekking op de te ondersteunen bedrijfsfuncties, op het beschrijven van de functionele processen en welke taken daarin ondersteund moeten worden en op het bepalen van hoe verschillende processen met elkaar kunnen geïntegreerd worden
  - / Management aspecten hebben betrekking op het bepalen van de informatiebehoeften voor de besluitvorming op strategische niveau, voor het tactische niveau en voor het operationele niveau

Soorten bedrijfssystemen

- ⇨ In bedrijven kunnen vele subsystemen onderscheiden worden (2 indelingen)
  - / Indeling geïnspireerd op de functionele domeinen die aan de basis kunnen liggen van de afbakening van informatiesystemen ('Isolated Silos')
  - / Indeling geïnspireerd op de niveaus van leidinggeven die algemeen worden onderscheiden: het operationele systeem & het management systeem (tactisch en strategisch)

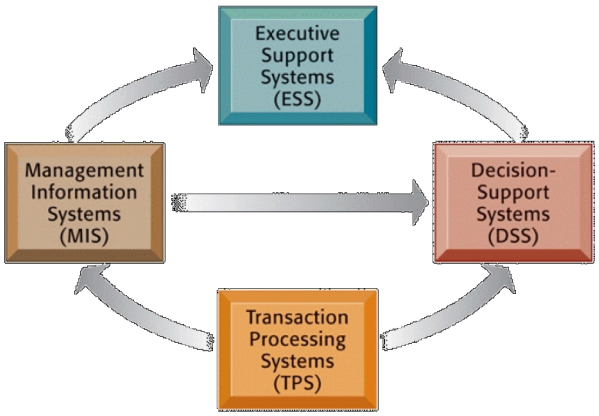
Soorten informatiesystemen

- ⇨ Weerspiegelen de indeling van de verschillende soorten bedrijfssystemen
  - / *Operationeel informatiesysteem* verstrekt informatie over en aan de operationele processen van het bedrijf (**Online Transaction Processing**)
  - / *Management informatiesysteem* verstrekt informatie over de besturingsprocessen van het bedrijf
    - ⇨ Beslissingen op tactisch niveau (MIS & DSS)
      - / Betreffen de middellange termijn
      - / Komen minder vaak voor en hebben minder routinematig karakter
      - / Gaan gepaard met een grotere onzekerheid en/of risico
    - ⇨ Beslissingen op strategisch niveau (ESS)
      - / Betreffen de lange termijn
      - / Hebben een incidenteel karakter
      - / Gaan gepaard met een grote mate van onzekerheid en/of risico

Management Information Systems (MIS) richten zich vooral op toegang tot de bedrijfsgegevens en routine rapporteringen.

Decision Support Systems (DSS) richten zich vooral op data-analyse ten behoeve van beslissingen op management niveau, zullen de mogelijkheid bieden op interactieve wijze een antwoord te geven op specifieke vragen.

Executive Support Systems (ESS) dienen voor communicatie, analyse en informatievoorzieningen voor het strategische niveau



In een bedrijf kunnen zeer veel verschillende informatiesystemen aanwezig zijn, nochtans staan deze zelden los van elkaar. ERP (Enterprise Resource Planning) probeert alle soorten systemen te bieden in een uniform platform: zij ondersteunen in principe alle functionele domeinen op alle mogelijke niveaus.

De bovenste 3 (MIS, ESS, DSS) zijn samenvattend en gebaseerd op het TPS-systeem.

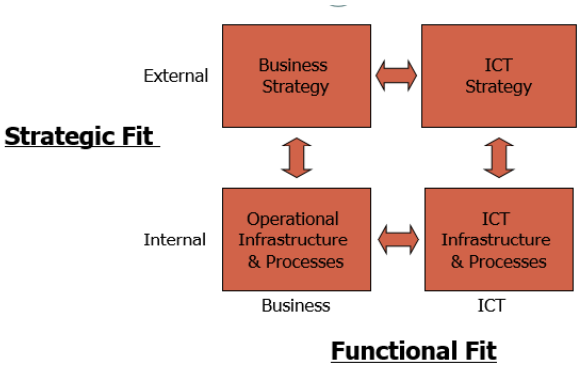
2 Enterprise Architecture (EA)

2.1 Enterprise Architecture

2.1.1 Waarom Enterprise Architecture?

Henderson en Venkatraman argumenteerden dat een van de belangrijkste redenen waarom het zo moeilijk is toegevoegde waarde te realiseren door het investeren in informatietechnologie is dat er vaak een groot gebrek is aan overeenstemming tussen de bedrijfsstrategie en de informatiestrategie. Deze afstemming is geen eenmalige oefening maar moet permanent bewaakt worden.

het Strategic Alignment model



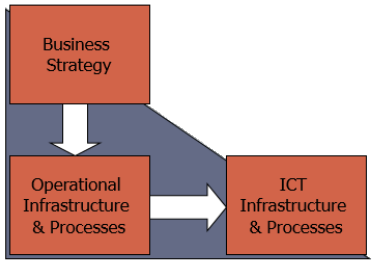
De **strategische fit** is de afstemming tussen het strategische niveau en het operationele niveau

⇨ Zorgt ervoor dat de strategie ook effectief wordt uitgevoerd op het operationele niveau

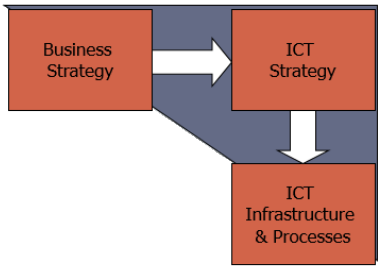
De **functionele fit** zorgt ervoor dat de informatiestrategie in lijn is met de bedrijfsstrategie, zowel op strategisch niveau als op operationeel niveau

4 paden van afstemming

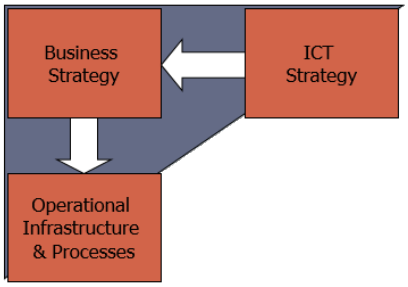
- Strategie-uitvoering
  - ⇨ De bedrijfsstrategie is de drijvende factor voor zowel het ontwerp van de organisatie als voor het ontwerp van de informatiesysteeminfrastructuur en de processen.



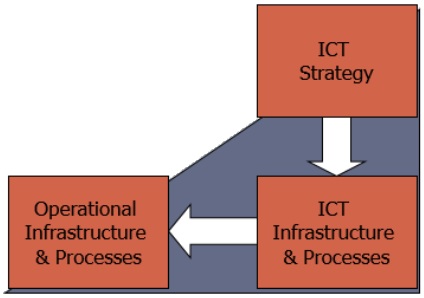
- Technologiepotentieel
  - ⇨ De bedrijfsstrategie is de drijvende factor, maar ook wordt ook een ICT-strategie geformuleerd om de gekozen bedrijfsstrategie te ondersteunen. Deze ICT-strategie is bepalend voor de informatiesysteeminfrastructuur en de processen voor de ontwikkeling van het informatiesysteem.



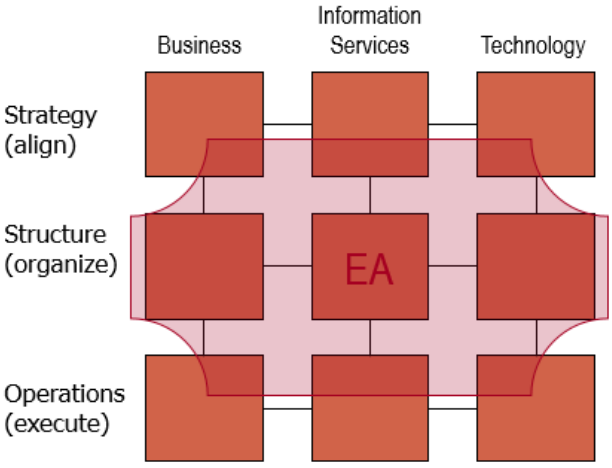
- Concurrentiepotentieel
  - ⇨ Heeft betrekking op het gebruik van nieuwe mogelijkheden geboden door ICT. Dit perspectief staat de wijziging van de bedrijfsstrategie toe via deze nieuwe mogelijkheden



- Serviceniveau
  - ⇨ Concentreert zich op hoe IT binnen een organisatie een eigen organisatie op zich kan worden. Het bepalen van ICT-strategie is niet meer zozeer in functie van de bedrijfsstrategie, maar eerder in functie van de "markt" van afnemers van ICT-services. (SOA, Service Oriented Architecture)



Maes actualiseert het raamwerk van Henderson en Venkatraman door het om te vormen naar een 3x3 raamwerk. Het is immers belangrijk een onderscheid te maken tussen de technologie en de toepassing van de technologie.



- De 1ste kolom beschrijft het zuivere bedrijfsperspectief
- De 2de kolom beschrijft het informatie(systeem)perspectief
- De 3de kolom beschrijft de technologische aspecten

- De 1ste rij beschrijft de strategie van de onderneming
- De 2de rij beschrijft hoe men zich wenst te organiseren om de gekozen strategie te bereiken

- De 3de rij beschrijft de operationele, dagelijkse uitvoering, met name hoe in de onderneming de dingen verricht worden

Strategische fit betekent dat de wijze waarop we onze organisatie inrichten, in overeenstemming moet zijn met de gekozen strategie en dat de dagelijkse uitvoering in lijn moet zijn met de gekozen wijze van uitvoering.

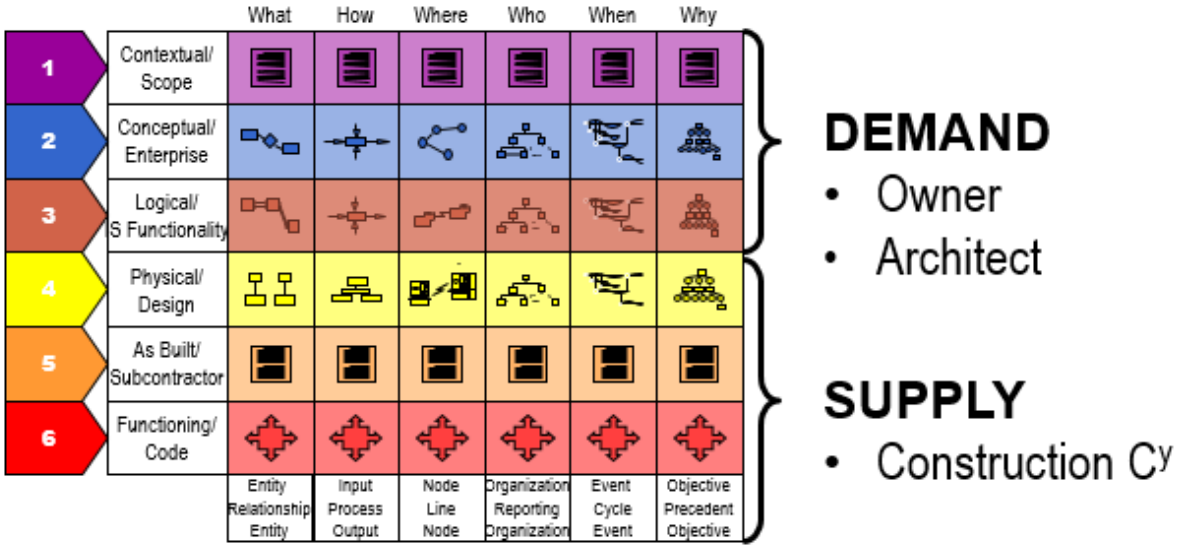
Functionele fit betekent dat de keuzes die men maakt op vlak van informatiesysteemondersteuning en op vlak van informatietechnologie in lijn moeten zijn met elkaar en met de bedrijfsvoering.

⇨ De projectmatige aanpak en het permanent aanpassen van systemen valt onder de noemer EA (Enterprise Architecture)

2.1.2 Het raamwerk van Zachman

⇨ Informatiesystemen kunnen verschillende voorstellingen of plannen hebben

Het raam werk van Zachman is een classificatieschema voor beschrijvende voorstellingen van complexe informatiesystemen. Het biedt de mogelijkheid om op een gestructureerde manier de systeemarchitectuur weer te geven.



Het **scope-perspectief**: het perspectief van de planner van een project

⇨ Er wordt nagegaan op welke manier de organisatie efficiënter en effectiever kan worden gemaakt en welke beperkingen daarbij komen kijken
⇨ Het is de bedoeling dat de omvang van het organisatiesysteem dat moet worden ontwikkeld, contextueel duidelijk wordt afgelijnd
  - DATA-dimensie: welke objecten heeft de organisatie nodig?
  - FUNCTION-dimensie: lijst van processen die de organisatie nodig heeft om haar input om te zetten in output
  - NETWORK-dimensie: lijst van locaties waarin de organisatie actief is
  - PEOPLE-dimensie: lijst van personen/groepen die door de organisatie verantwoordelijk worden gesteld voor een bepaalde taak
  - TIME-dimensie: lijst van gebeurtenissen waarop de organisatie inspeelt
  - MOTIVATION-dimensie: lijst van bedrijfsdoelen die belangrijk zijn voor de organisatie
⇨ Het afbakenen van de scope gebeurt in de eerste fase van het project

Het **enterprise-model perspectief**: het perspectief van de eigenaar of van de opdrachtgever

- ⇨ Geeft een overzicht van de werking van de organisatie
- ⇨ De regelgeving, de gebruiksvoorwaarden en de beperkingen
  - ⁄ DATA-dimensie: welke objecten zijn belangrijk voor de organisatie?
  - ⁄ FUNCTION-dimensie: model van eigenlijke bedrijfsprocessen die plaatsvinden binnen de organisatie
  - ⁄ NETWORK-dimensie: geeft de locaties weer waar de organisatie actief is, samen met de verbindingen tussen die locaties en een beschrijving van hoe die locaties met elkaar communiceren.
  - ⁄ PEOPLE-dimensie: definieert de verantwoordelijkheden met betrekking tot taken in de organisatie, samen met specificaties van die taken
  - ⁄ TIME-dimensie: geeft een model weer van de bedrijfscycli
  - ⁄ MOTIVATION-dimensie: presenteert een businessplan

Het **system-model perspectief**: het perspectief van de ontwerper

- ⇨ Vertaalt de specificaties die door de eigenaar werden beschreven, naar technische specificaties van het informatiesysteem
- ⇨ De ontwerper dient rekening te houden met de beperkingen die de dagdagelijkse omgeving oplegt
  - ⁄ DATA-dimensie: die objecten in de organisatie waarover het informatie opneemt
  - ⁄ FUNCTION-dimensie: model van logische systeemimplementatie die de bedrijfsprocessen ondersteunt
  - ⁄ NETWORK-dimensie: in een logisch model wordt aangegeven welke systeemfaciliteiten en controlerende software zich op de knooppunten en verbindingen tussen die knooppunten bevinden
  - ⁄ PEOPLE-dimensie: een logische voorstelling van de workflow
  - ⁄ TIME-dimensie: de logische systeemspecificaties van bepaalde tijdstippen en tijdsperiodes
  - ⁄ MOTIVATION-dimensie: een logische voorstelling van de bedrijfsregels in termen van wat er moet bereikt worden en de beperkingen waarmee men rekening moet houden
- ⇨ Wanneer alle dimensies zijn overwogen, bekomt men een set van specificaties die in technische termen beschrijft wat er moet worden gebouwd om te voldoen aan de gebruikersnoden van de eigenaar, rekening houdend met de beperkingen beschreven door de planner

Een nadeel van architectuurraamwerken zoals dat van Zachman is dat er weinig informatie is over de graad van detail die men moet hanteren bij het concreet invullen van het raamwerk, noch in de volgorde waarin dit zou moeten gebeuren, of wie dit zou moeten doen.

- ⇨ **TOGAF** is een open *Architecture Governance* standaard die beschrijft welke stappen moeten/kunnen doorlopen worden en welke mensen betrokken moeten worden bij het uitwerken van een enterprise architecture

Een advies van TOGAF is dat wanneer het ontwikkelen van één groot raamwerk niet haalbaar is, er kan gewerkt worden met '**federated architectures**' (meerdere architecturen die op een of andere manier met elkaar geïntegreerd worden)

- ⇨ 2 basisprincipes
  - ⁄ De organisatie wordt opgesplitst in functionele domeinen en voor elk van de domeinen wordt een volledig raamwerk ontwikkeld
  - ⁄ Het raamwerk wordt opgesplitst per aspect en men ontwikkelt elk aspect apart

2.2 Informatiemanagement

2.2.1 De scope layer

In deze rij bepalen we welke informatie de organisatie nodig heeft en definiëren we zo welke informatie kan gebruikt worden in de verschillende processen.

2.2.2 Enterprise Layer: informatiemodellering

We geven aan welke informatie we juist willen bijhouden voor elk object en wat de verbanden zijn tussen de objecten

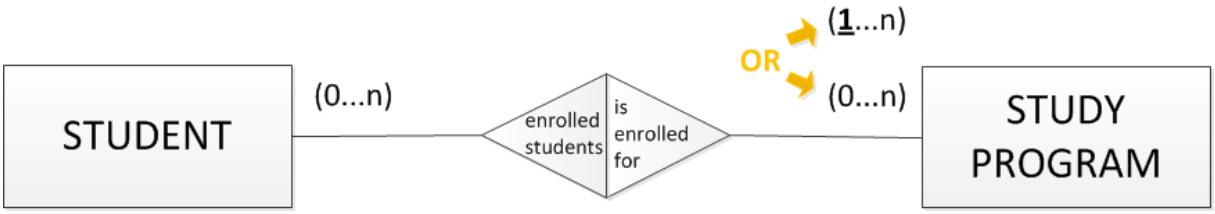
- ⇨ **Data model**: beschrijft de 'universe of discourse' maar kan ook dienen als blauwdruk voor de oplossing

2 niveaus van denken

Level 1	Het model niveau	⁄ Een persoon ⁄ Een programmajaar ⁄ Een opleidingsonderdeel
Level 0	Het voorbeeld niveau	⁄ Els, Jan, … ⁄ 1ste bach HW, 2e bach HW, …

Modelleren is abstraheren: de overgang maken van level 0 naar level 1. We modelleren door verzamelingen te definiëren, de eigenschappen van de elementen in een verzameling te beschrijven, verbanden tussen verzamelingen en hun elementen te definiëren, … etc.

Voor het neerschrijven van een model wordt een 'modelleringstaal' gebruikt, een verzameling van symbolen.



De getallen naast het relatietype (verband) geven weer hoeveel elementen uit de doelverzamelingen minimaal en maximaal kunnen verbonden zijn met een element uit de bronverzameling.

Het doel is een precieze definitie te geven van alle relevante entiteitstypen in het bedrijf en de geldende relatietypen.

- ⁄ Elementen = instanties of entiteiten
- ⁄ Verzameling = entiteitstype
- ⁄ Verbanden = relatietypen

2.2.3 Functionaliteit van het informatiesysteem

Op operationeel niveau heeft de ondersteuning door informatiesystemen in de eerste plaats betrekking op het registreren van gegevens (input), het verrichten van de basisverwerking van deze gegevens (data wordt informatie) en het rapporteren over geregistreerde gegevens, al dan niet na verwerking (output).

2.2.4 Kwaliteit van de ondersteuning door informatiesysteem

Het operationele informatiesysteem moet idealiter zorgen voor een goede weerspiegeling van het bedrijfssysteem.

- ⇨ 2 elementen van groot belang
  - / Het datamodel moet een correcte weergave zijn van de bedrijfsrealiteit: het moet de juiste en relevante entiteitstypen beschrijven en een correct weergave van de relatietypen zijn
  - / De registratie van gegevens in de databank moet correct verlopen, en de verwerking en rapportering over de gegevens moet van goede kwaliteit zijn

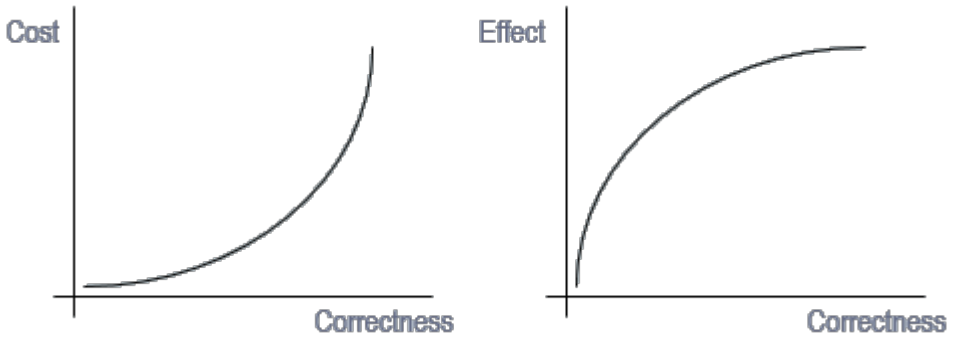
Kwaliteitsvolle informatie is een sleutelvereiste voor kwaliteitsvolle procesuitvoering (garbage in, garbage out). Het bewaken van de kwaliteit van gegevens en informatie is één van de sleutelelementen voor de succesvolle implementatie van informatiesystemen.

De **kwaliteit van het datamodel** moet in de eerste plaats bewaakt worden op het niveau van enterprise modelling. Het moet correct en volledig zijn.

- ⇨ *Correct*: dat het datamodel de werkelijkheid weerspiegelt
- ⇨ *Volledig*: dat het datamodel voorziet in de mogelijkheid tot registeren van alle relevante informatie

De ontvanger moet erop kunnen vertrouwen dat de informatie juist is. De juistheid van de uitvoer is afhankelijke van de juistheid van de invoer en van verwerking. De **juistheid van informatie** kan op verschillende manieren worden uitgedrukt. Welke maatstaf moet gebruikt worden, hangt af van het beschouwde geval.

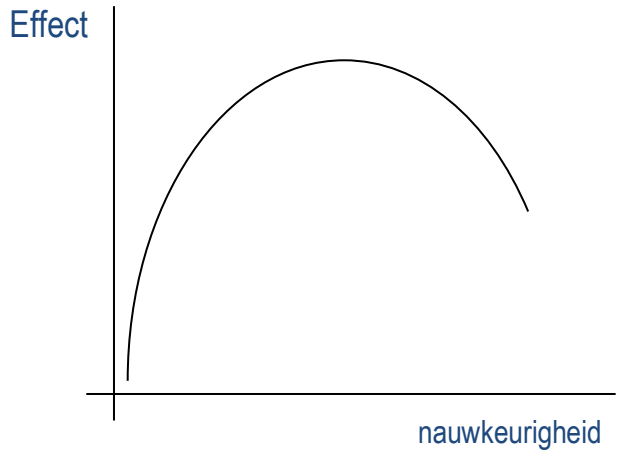
- ⇨ Een steeds verder doorgedreven juistheidgraad heeft een steeds kleinere invloed op het effect van de besturing. Het streven naar 100% juistheid van gegevens brengt vaak een hoge kostprijs met zich mee (zoeken naar balans).



3 oorzaken voor onjuiste informatie

- / *Invoer van onjuiste gegevens*: hoe meer de gegevens getransformeerd worden vooraleer ze ingevoerd of verwerkt worden, hoe groter de kans op fouten.
  - ⇨ Oplossingen: 'self service', automatiseren van invoer & validiteitscontroles
- / *Het niet invoeren van gegevens*: leidt tot onvolledige of verouderde gegevens
  - ⇨ Oplossing: RFID-tags
- / *Verwerkingsproblemen*: ontstaan onder andere bij data transformaties en door toegang door niet geautoriseerde gebruikers
  - ⇨ Oplossing: locking en concurrency control

De **nauwkeurigheid van informatie** is niet het zelfde als de juistheid van informatie. Met betrekking tot de nauwkeurigheid kan worden opgemerkt dat meestal voorbij een zeker punt een verder doorgedreven nauwkeurigheid een negatieve invloed uitoefent op de besturing, omdat de informatie niet langer bruikbaar wordt.



Veiligheid van gegevens heeft te maken met het bewaren van de vertrouwelijkheid van gegevens (enkel die personen met bevoegdheid krijgen toegang tot de informatie) en met authenticiteit (zekerheid wordt verkregen door de oorsprong van de informatie).

Selectiviteit van informatie kan worden onderverdeeld in 3 deelaspecten

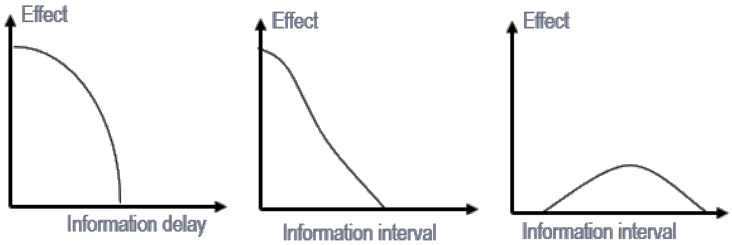
- De *detailgraad* heeft betrekking op de mate van gedetailleerdheid van het object waarover men wordt geïnformeerd. Deze wordt aangepast aan het niveau van leidinggeven.
- De *uitzonderingsgraad* is de mate waarin informatie enkel de toestand rapporteert van objecten waarvan de waarde vooropgestelde boven- of ondergrenzen heeft overschreden
  - ⇨ Management by exeption
- De *graad van relevantie* is het aandeel van relevante informatie op het geheel van de informatie die men krijgt
  - ⇨ Precision: het aandeel van relevante documenten op het geheel dat men krijgt
  - ⇨ Recall: het aandeel van relevante documenten die men kreeg op het aantal documenten dat men had willen krijgen

Informatie moet **tijdig** worden verschaft want het is aan tijd gebonden.

⇨ Hoe sneller de beschikbaarstelling, hoe duurder de informatie

Onder oogpunt van de factor tijd wordt een boodschap gekenmerkt door 3 parameters:

- De *informatievertraging*: de tijd die verloopt tussen het ogenblik waarop de informatie betrekking heeft en het ogenblik waar ze de beslissingnemer bereikt
- De *informatieperiode*: de tijdsperiode waarover informatie wordt verstrekt
- Het *informatie-interval*: de tijdsperiode die verloopt tussen 2 opeenvolgende mededelingen van informatie



Figuur 1 geeft aan dat een verhoging van de informatievertraging doorgaans een negatief effect op de besturing uitoefent.

Figuur 2 en 3 duiden aan dat naargelang het geval, de invloed van een verlenging van informatie-interval en informatie periode gelijkaardig kan zijn als deze van de informatievertraging ofwel dat soms een dergelijke verlenging eerst een gunstig en daarna een ongunstig effect kan hebben.

2.3 Business Process Management (BPM)

Naast informatie en data (wat?) bevatten organisaties een 2e belangrijke component: processen (hoe?). Zij zijn de fundamentele bouwblokken van elke onderneming.

⇨ Ondernemingen streven naar continue ontwikkeling en verbetering om van deze bedrijfsprocessen door hun zoektocht naar standaarden, tools en technieken om met uitmuntende processen die klanten aan zich te binden.

Het doel van business process management bestaat uit het ontdekken, ontwerpen en implementeren van de processen, alsook om deze te analyseren, op te volgen en te optimaliseren zodat deze in lijn blijven met de strategische doelstellingen van de onderneming.

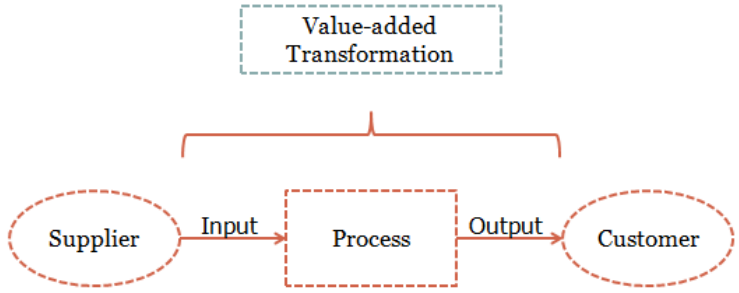
⇨ Via procesperformantie komen tot bedrijfsperformantie

2.3.1 De opkomst van business process management

Niet belangrijk

2.3.2 Bedrijfsprocessen: een definitie

Zairi (1997) "(1) Voorspelbare en definieerbare inputs, (2) een lineairen logische opeenvolging of stroom, (3) een groep van duidelijk definieerbare activiteiten, en (4) voorspelbare en gewenste outputs"



M. De Backer "een groep van (logische) gerelateerde taken (of activiteiten) die zijn uitgezocht door een onderzoek om een doel te bereiken om de objectieven van de organisatie te ondersteunen"

Niet elk proces binnen een onderneming is even belangrijk, doorgaans wordt er onderscheid gemaakt tussen:

- **Core**: deze processen staan in voor de ontwikkeling van diensten of producten en zijn meestal direct gelinkt aan (externe) klanten
- **Support**: deze processen ondersteunen de core-processen zodat deze hun doel kunnen bereiken
- **Management**: deze processen zijn verantwoordelijk voor corporate governance of strategische ontwikkeling in een onderneming

Een andere opdeling die vaak wordt gehanteerd is deze van

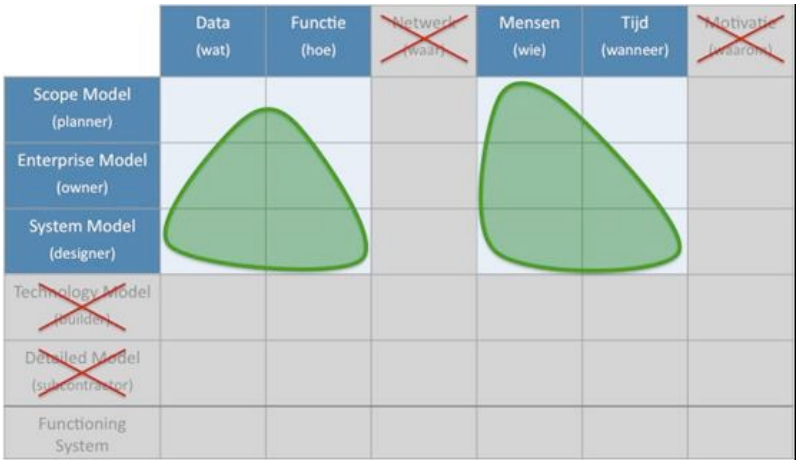
- **Gestructureerde** processen: de opeenvolging van stappen is duidelijk gedefinieerd en vastgelegd
- **Ongestructureerde** processen: de opeenvolging van stappen is onmogelijk op voorhand vast te leggen

Case-management zijn processen die doorgaans semigestructureerd zijn, waarbij enkel een startpunt en een proces doel wordt gedefinieerd.

2.3.3 Processen in het Zachman raamwerk

Indien men naar de definities van een bedrijfsproces kijkt, wordt duidelijk dat een bedrijfsproces een veel bredere focus heeft dan degene die wordt voorgesteld in de individuele cel van Zachman.

⇨ Een bedrijfsproces geeft ook aan welke specifieke input en output onderworpen worden aan de bedrijfsfuncties en welke resources deze functies uitvoeren.

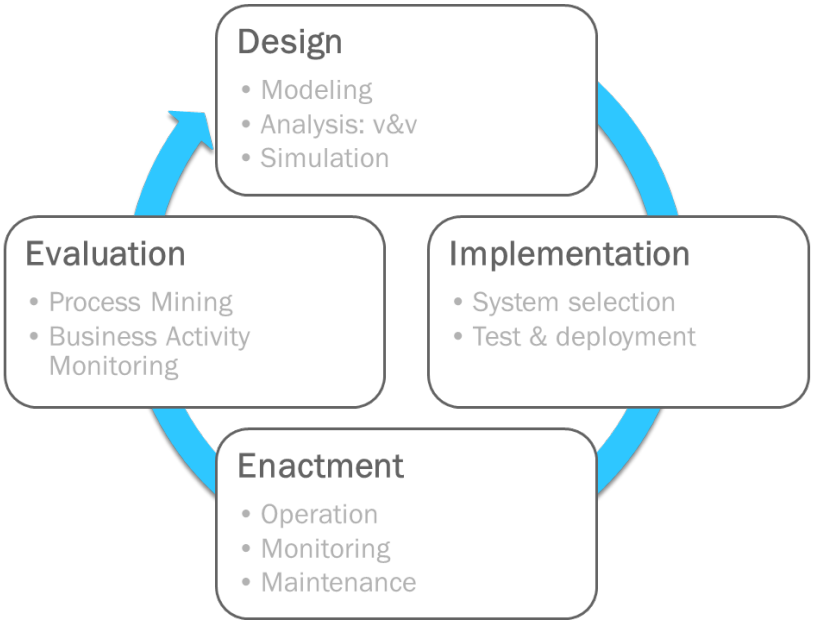


Een procesmodel kan dus 4 van de 6 dimensies weergeven, maar ook 3 van de 6 perspectieven.

Binnen de notie van procesmodellen zal het **scope niveau** dienen om zeer high level aan te geven welke bedrijfsprocessen binnen beschouwing vallen van de onderneming. Het **enterprise niveau** zal dan een kort overzicht geven van hoe deze bedrijfsprocessen intern opgebouwd zijn. Het **system niveau** zal een verder uitdieping van deze activiteiten inhouden, waarbij meer detail aan elk beschouwde aspect wordt toegevoegd.

2.3.4 Business Process Management

Het beheren van alle processen die instaan voor de dagelijkse werking van de onderneming (**business process management**) is een belangrijke taak binnen elke onderneming geworden.



Een visuele voorstelling van de componenten van een business process management raamwerk, ook wel de levenscyclus genoemd.

2.3.4.1 Design

Het **design** heeft als doel een zo realistisch mogelijke en correcte beschrijving van het real-life bedrijfsproces te bekomen (ontwerpen, modelleren, analyseren, simuleren)

- ⇨ De bedrijfsprocessen worden (her)ontworpen
- ⇨ Er worden verschillende Business Process Modeling technieken gebruikt waarbij een conceptueel model van het bedrijfsproces wordt opgemaakt

Procesmodellering start steeds met een *analyse* van de huidige situatie en de huidige werkwijze binnen de organisatie (⇨ AS-IS modellen). De resultaten van deze analyse leiden doorgaans tot verbeteringen en werkwijzen worden gestandaardiseerd overheen afdelingen en optimalisaties.

- ⇨ Deze nieuwe bedrijfsprocessen worden ook wel TO-BE bedrijfsprocessen genoemd.

De *validatie* van een bedrijfsproces houdt het voorleggen van het ontwerp aan belanghebbenden binnen de organisatie in. Zij zullen oordelen of alle belangrijke aspecten van het bedrijfsproces zijn opgenomen in het model.

Nadien kan het proces *gesimuleerd* worden, waarbij de interne opbouw van het proces wordt nagekeken om te vermijden dat het ongewenst gedrag vertoond. Eventuele afwijkingen worden dan opgelost.

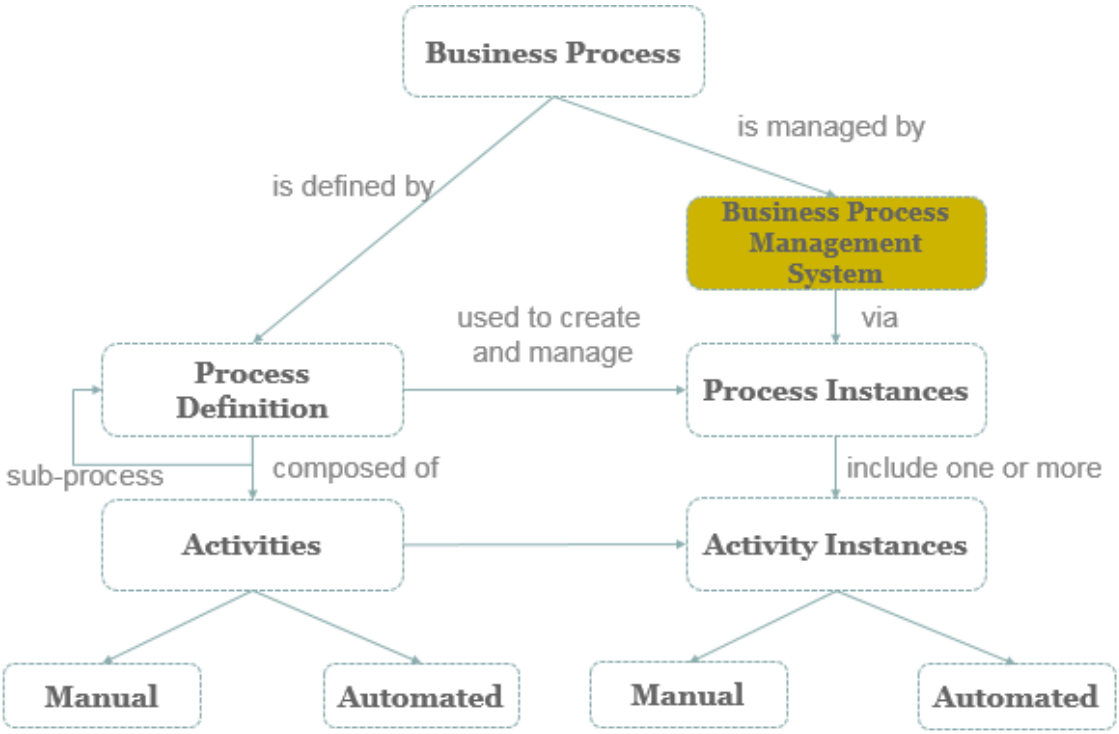
Als laatste stap wordt een *verificatie* uitgevoerd van het bedrijfsproces binnen beschouwing.

Om een bedrijfsproces volledig en in detail te bespreken, moeten de volgende dimensies van bedrijfsprocessen in kaart gebracht worden:

- / Procescontext
- / Gedragsdimensie
- / Taken in een bedrijfscontext
- / Data perspectief
- / Analyseperspectief
- / Regels binnen de organisatie
- / Implementatie perspectief
- / Service component

2.3.4.2 Implementatie

De **implementatie** kijkt naar een aantal mogelijkheden en alternatieven die er bestaan om de bedrijfsprocessen te implementeren in een informatiesysteem



Bovenaan wordt het bedrijfsproces weergegeven zoals de bedrijfsmensen het in de organisatie uitvoeren.

Linkerzijde van de figuur	Rechterzijde van de figuur
Wanneer we van het bedrijfsproces een model gaan bouwen, of een *procesdefinitie*, dan ontwikkelen we een beschrijving van het bedrijfsproces. Elk procesmodel wordt opgebouwd uit een verzameling activiteiten en deze activiteiten kunnen onderverdeeld worden in manuele en geautomatiseerde taken.	*BPMS* is een software dat in staat is om het procesmodel uit te voeren, op te volgen en te beheren Telkens een proces opgestart wordt, zal er een *procesinstantie* aangemaakt worden. Deze procesinstantie bestaat op zijn beurt uit verschillende *activiteitinstanties*. De activiteitinstanties kunnen onderverdeeld worden in manuele en geautomatiseerde taken

De implementatie van bedrijfsprocessen heeft doorheen de jaren een ware revolutie doorgemaakt.

- **Processen in de hersenen** (jaren 1990): de mensen waren de belangrijkste uitvoerders van de bedrijfsprocessen. De taken werden ondersteund door informatiesystemen maar het was de bediende zelf die besliste in welke volgorde de taken werden uitgevoerd.
- **Work flow systemen** (1993) waren in staat om herinneringen te versturen over het werk dat nog gedaan moest worden
- (1996) Het systeem ondersteunde niet meer enkel de gebruiker maar kon ook de taken van een proces overheen verschillende personen distribueren.
- **Service Oriented Architecture** (SOA): bood de mogelijkheid om informatie van welke plaats dan ook te consulteren

2.3.4.3 Enactment

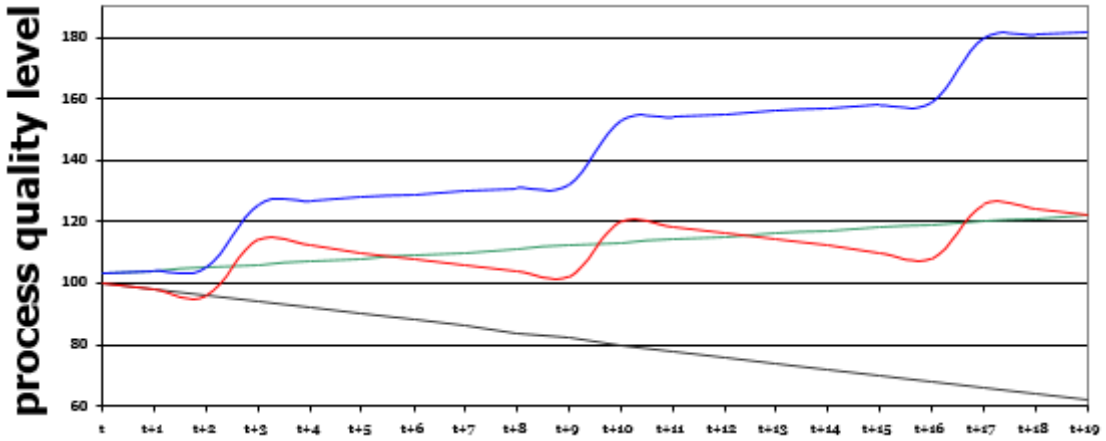
De **enactment** is de werkelijke uitvoering van de processen zoals deze geïmplementeerd werden in de organisatie of in die informatiesystemen.

Het BPMS zal al de instanties controleren en begeleiden naar de correcte personen of systemen voor het uitvoeren van de manuele en geautomatiseerde activiteitinstanties.

2.3.4.4 Evaluatie

De **evaluatie** is cruciaal en geeft het continue verbeteringsaspect dat verbonden is aan BPM duidelijk weer.

Al de informatie over de procesuitvoeringen wordt geëvalueerd en gebruikt om procesverbeteringen door te voeren.



Bij de implementatie van een proces zullen alle medewerkers zich mooi aan de regels houden maar na verloop van tijd zullen er steeds meer mensen hun eigen regels gebruiken. Een onderneming heeft 2 mogelijkheden om deze negatieve trend tegen te gaan.

- **Business Process Improvement**: er worden op projectbasis verbeteringen aangebracht zodat deze doorheen de tijd steeds gealigneerd blijft met de realiteit
- **Business Process Management**: de proceseigenaar zal de kwaliteit van het proces continu opvolgen.

De optimale oplossing kan bekomen worden indien de continue business process management methode wordt aangevuld met periodieke improvement projecten.

2.3.5 Business Process Oriëntatie

Om van alle voordelen van BPM te kunnen genieten moeten ondernemingen een volledige transformatie ondergaan van functionele organisatie naar een procesgerichte organisatie.

- ⇨ Elk departement begint intern aan BPM te doen
- ⇨ De verschillende processen van de departementen worden aan elkaar gekoppeld zodat de volledig interne organisatie op elkaar afgestemd kan worden

Ook de cultuur en structuur in de onderneming dienen procesgericht te worden.

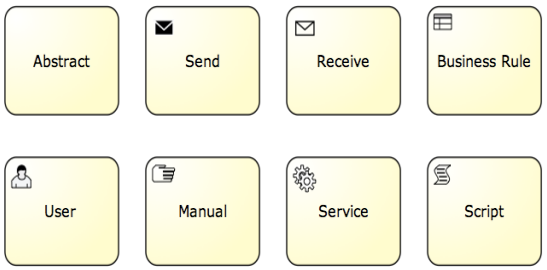
2.3.6 BPMN

⇨ Business Process Modelling Notation

BPMN is een grafische modelleringstaal die een specificatie van de wijze waarop elk element dient uitgevoerd te worden in een informatiesysteem of business process engine bevat.

De belangrijkste elementen van BPMN, ofwel de 'flow objecten', zijn beperkt tot 3:

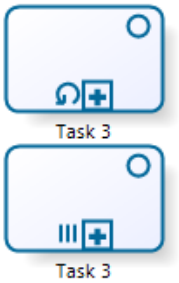
- Sequence flow: geeft de opeenvolging weer van activiteiten, events en gateways in één proces
- Message flow: geeft weer hoe en wanneer het proces communiceert met externe partijen
- Association: een connector waarmee bijkomende informatie aan de flow objecten kan worden toegevoegd



Een **activiteit** wordt voorgesteld door een rechthoek met afgeronde hoeken en verwijst naar iets dat door de onderneming wordt uitgevoerd. BPMN bevat 2 soorten activiteiten: **subprocessen** verwijzen naar een niet opdeelbare eenheid van werk en een samengestelde groep van taken en een **taak** verwijst naar de kleinste eenheid van werk die in een bedrijfsproces kan gemodelleerd worden.

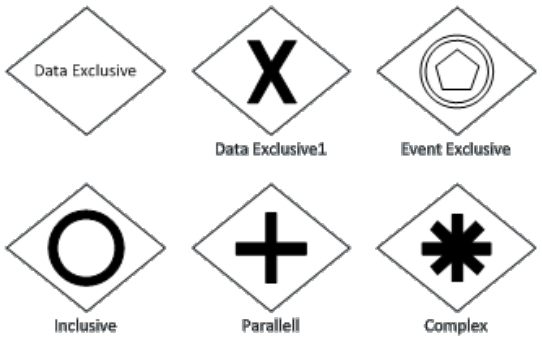
BPMN kent 2 constructen die het mogelijk maken om herhalende delen van een bedrijfsproces op een correcte wijze te modelleren

- De **loop** wordt gebruikt indien men op geen enkele wijze op voorhand kan afleiden hoeveel keer een subproces moet worden uitgevoerd (op basis van een conditie); verloopt altijd sequentieel
- De **multi-instances** worden gebruikt wanneer men op voorhand wel kan bepalen hoeveel keer een subproces moet worden uitgevoerd; verloopt altijd parallel



In realistische bedrijfsprocessen komen complexe volgordebeperkingen voor een BPMN voorziet daarvoor in een aantal specifieke constructen om de divergentie (opsplitsing) als de convergentie (samenvoeging) van de sequence flow aan te duiden

⇨ Gateways



Een vaak voorkomende situatie in een bedrijfsproces is wanneer er steeds één pad gekozen wordt uit verschillende alternatieve paden. De beslissing van het te kiezen pad is gebaseerd op een conditie die kan worden uitgevoerd.

⇨ **Datagebaseerde, exclusieve gateway**

Dit wordt meestal intern in het proces besloten, wanneer de beslissing extern genomen wordt, wordt er gebruik gemaakt van de **eventgebaseerde exclusieve gateway**.

Het komt vaak voor dat er geen echte volgordebeperking is. Een dergelijke situatie kan gemodelleerd worden adhv een parallelle gateway. Er bestaat nog een derde manier om de paden in een procesmodel op te splitsen, nl. de **inclusieve gateway**. De condities zullen bepalen of er 1 of meerdere paden parellel

moeten worden opgestart. De **complexe gateway** kan gebruikt worden om complexe synchronisatie patronen uit te tekenen.

Gebeurtenissen, activiteiten en gateways worden met elkaar verbonden dmv 'verbindingsobjecten/ connectoren'.

- Sequence flow
- Message flow
- Association

Een gebeurtenis of **event** verwijst naar een gebeurtenis die ene invloed heeft op het bedrijfsproces.

- Start event: geeft de start van een (sub)proces weer en bevat meestal een trigger die aangeeft hoe een proces start
  - ⇨ None: een lege trigger die betekent dat de trigger niet gespecifieerd werd
  - ⇨ Message: het proces wordt opgestart na het ontvangen van een bericht van een externe partij
  - ⇨ Timer: het proces wordt opgestart op een bepaald moment

- Intermediate event: er zijn 12 verschillende triggers voor intermediate events en de betekenis kan variëren naargelang het gaat over een event van het type 'throwing' of van het type 'catching'.
  - ⇨ Catching: wanneer een lege trigger wordt gebruikt
  - ⇨ Throwing: wanneer een volle trigger wordt gebruikt

  Kan ook gekoppeld worden aan een activiteit (listening)

  - ⇨ Listening: het proces zal luisteren naar het event en wanneer het event wordt gehoord zal deze verwerkt worden
- End event: geeft weer waar een pad in het proces ten einde loopt. Ook hier wordt er gebruik gemaakt van triggers
  - ⇨ None: het einde van een pad in het proces
  - ⇨ Message: er wordt nog een bericht verstuurd naar een andere partij
  - ⇨ Terminate: is in staat om ook parallelle paden in het proces te stoppen
  - ⇨ Error: wanneer er zich in het proces een probleem heeft voorgedaan
  - ⇨ Escalation: een persoon heeft tijdens het proces een probleem ontdekt

Er zijn in BPMN nog andere elementen aanwezig die gebruikt kunnen worden om bijkomende informatie aan het procesmodel toe te voegen

- ⇨ **Artefacten**

3 Netwerkbeveiliging

3.1 Potentiële aanvallers van netwerken

3.1.1 Extern

⇨ 3 hoofdcategorieën

- *Hacker*: persoon die veel kennis heeft over computers en die dikwijls tracht die kennis op een illegale manier te testen
  Hebben niet altijd kwade bedoelingen
  - ⇨ **Penetration testing**: ondernemingen huren hackers in om hun bestaande netwerkbeveiliging te testen door te proberen toegang te verschaffen tot specifieke netwerken
- *Cracker*: een kwaadwillige hacker
- *Script kiddie*: maakt vooral gebruik van bestaande 'hacking tools' die door crackers ter beschikking worden gesteld via het internet.

3.1.2 Intern

Schade aangericht door externen is kleiner dan schade aangebracht door (ex-)medewerkers.

⇨ 3 categorieën

- *Niets vermoedende medewerker*: vaak herleidbaar naar het feit dat werknemers zich onvoldoende bewust zijn van de gevaren die hun gedrag (veiligheidsmaatregelen vergeten of negeren) met zich meebrengt.
- *Misnoegde medewerker*: de gevaarlijkste groep; zijn uit op wraak en hebben tot doel om schade aan te brengen
- *Nieuwsgierige medewerkers en "snoops"*: snoops zijn medewerkers die aan spionage doen (vaak in opdracht van)
  Soms gebeurt het ook dat werknemers puur uit nieuwsgierigheid op zoek gaan naar bepaalde informatie

3.2 Manieren van externe aanvallen

(1)Een **virus** is een reeks code die zo gemaakt is dat ze zichzelf kopieert en probeert andere computers te infecteren met deze code

- *File virussen*: maken zich vast aan een programma
- *Boot(sector) virussen*: bevinden zich in de bootsector van een diskette, USB-stick of harde schijf
- *Macrovirussen*: infecteren databestanden via scripts

Een virus kan enkel een netwerk binnen komen en aantasten, wanneer het van buitenaf is binnengebracht.

De kosten die gepaard gaan met het afhandelen van een virus kunnen hoog oplopen en het kan heel tijdrovend zijn.

Computernetwerken kunnen op verschillende manieren geïnfecteerd worden

- Via het internet
- Via e-mail
- Floppy disks, cd's, dvd's, …etc.
- Documenten en/of spreadsheets
- Computerprogramma's

(2)**Hoaxen** kunnen meldingen zijn van virussen die eigenlijk niet bestaan. Deze 'valse alarmen' kunnen veel tijd en geld kosten voor een organisatie. Hoaxen kunnen ook gebruikt worden om een bedrijf aan te vallen ⇨ overbelasting

(3)Een **worm (worms)** is een programma dat zichzelf kan vermenigvuldigen en dat zich via het netwerk verspreid maar kan zich niet aan een ander programma vastmaken (in tegenstelling tot een virus). Het maakt gebruik van fouten in het besturingssysteem of de servers om zo binnen te komen op het netwerk.

(4)Een **trojaans paard** is een bedrieglijk programma dat zijn ware aard verbergt. Eens het programma wordt geactiveerd door de gebruiker kan het verschillende soorten schade aanrichten. Het kan pas op het netwerk binnen komen als het van buitenaf wordt geïmporteerd.

(5)Een '**blended threat**' is een aanval waarbij gezocht wordt naar de schadelijkste en snelste manier om een netwerk aan te vallen. Er wordt gebruik gemaakt van een combinatie van eigenschappen van bv worms en virussen, terwijl mijn misbruik maakt van bepaalde veiligheidslekken.

(6)'**Bufferoverflow**' is een aanvalstype waarbij de aanvaller misbruik maakt van fouten in de software.

(7)Wanneer een organisatie over een website beschikt kan deze kwetsbaar zijn voor '**defacing'**. Dit houdt in dat men zonder toestemming een website vervangt, verandert of vernielt. Dit gebeurt onder andere dmv DNS-aanvallen (Domain Name Service). Wordt ook wel pharming genoemd.

(8)**Spoofing** houdt in dat men zich voordoet als iemand om op deze manier mensen en informatiesystemen te misleiden

- IP-spoofing ⇨ aanvaller kan een bericht doen verschijnen alsof het van een geldig IP-adres komt
- ARP-spoofing ⇨ (Address Resolution Protocol) wordt gebruikt om een IP-adres op te zetten naar een overeenkomstig MAC-adres op Ethernet-niveau.
- DNS-spoofing (zie defacing)
- E-mail spoofing ⇨ er wordt misbruik gemaakt van de onwetendheid van de gebruiker om belangrijke gegevens te ontfutselen

(9)Een **backdoor** is een niet-gerapporteerde manier van toegang krijgen tot een programma of besturingssysteem. Kan ook gebruikt worden door crackers die het informatiesysteem zijn binnengeraakt. Zij creëren voor zichzelf een manier om snel terug toegang te krijgen.

(10)**verkennende aanvallen** zijn aanvallen waarbij de aanvaller op zoek gaat naar informatie over het netwerk om dan later, via de gevonden gaten in de beveiliging, het netwerk aan te vallen.

- Sniffers ⇨ een programma om het dataverkeer over het netwerk in beeld te brengen
- Scanners ⇨ in beeld brengen van de zwakheden van het netwerk waardoor de hacker een idee kan krijgen over de plaatsen die het gemakkelijkst uit te buiten zijn om het netwerk aan te vallen

(11)Een **password cracker** werd oorspronkelijk ontworpen om te gebruiken wanneer een werknemer zijn wachtwoord zou vergeten zijn. Een andere aanval waarbij wachtwoorden worden achterhaald is via 'dictionary attacks'

(12) Het doel van een **DoS** (Denial of Services) is het netwerk onbeschikbaar maken zodat geautomatiseerde gebruikers geen gebruik meer kunnen maken van één of meerdere diensten die het netwerk aanbiedt.

- Consumptie van gelimiteerde resources: houdt in dat men de bandbreedte, hard disk, CPU tijd enzo. zo zal trachten te benutten dat het maximum wordt overschreden waardoor de netwerkconnectie het begeeft. (gebruik van meerdere computers = DDos)
- Vernietiging of wijziging van configuratie informatie: belemmeren dat men gebruik kan maken van een bepaalde computer of het hele netwerk
- Fysieke vernieling of wijziging van netwerkcomponenten

(13) **Spam** bestaat vooral uit het ontvangen van ongevraagde commerciële berichten.

(14)**Spyware** komt meestal binnen op het netwerk doordat het wordt geïnstalleerd wanneer men bepaalde websites bezoekt of bepaalde gratis software binnenhaalt.

Aanvallen op een draadloos netwerk is gemakkelijker dat een traditioneel netwerk want draadloze netwerken maken gebruik van radiogolven. Men dient er dus op toe te zien dat bij de installatie de toegangspunten correct worden geconfigureerd.

Men hoeft geen technische middelen te gebruiken om binnen te geraken in een netwerk ⇨ **social engineering**

3.3 Technische maatregelen ter beveiliging van een netwerk

3.3.1 Preventie

3.3.1.1 Toegangscontrole

Via toegangscontroles moeten de bevoegde personen binnengelaten worden en alle andere buiten. Het staat dus in voor het vaststellen van de identiteit of de authenticiteit van een persoon.

⇨ steunt hoofdzakelijk op 3 principes

- Adhv iets dat men weet ⇨ wachtwoord
- Adhv iets dat men bezit ⇨ smartcard
- Adhv iets dat men is ⇨ biometrie

  Voldoen aan 5 voorwaarden:

  Uniekheid
  Universeel
  Meetbaarheid
  Duurzaamheid
  Gebruiksvriendelijkheid

3.3.1.2 Encryptie

⇨ het uitvoeren van allerlei wiskundige berekeningen op een bepaald pakket gegevens, zodat die gegevens onleesbaar worden

3 belangrijke vormen

- Symmetrische encryptie ⇨ 1 encryptiesleutel
- Asymmetrische encryptie ⇨ 2 sleutels: private en publieke
- Hybride systemen ⇨ 2 versleutelingen: 1 symmetrische & 1 asymmetrisch

3.3.1.3 Firewall

⇨ heeft als doel om 2 of meerdere netwerken van elkaar af te schermen

Op deze manier kan ongewenste en niet-geautoriseerd dataverkeer tegengehouden worden. Kan ook gebruikt worden om binnen 1 LAN een aantal delen van elkaar los te koppelen.

2 types regelen mogelijke voor de configuratie van een firewall: exclusieve firewall en de inclusieve firewall

Regels kunnen gedefinieerd worden op 4 niveaus

- Packet-filtering gateways
- Toepassingsproxies
- Circuit leven gateways
- Dynamic packet-filtering firewall

3.3.1.4 Anti-virus software

⇨ kan virussen detecteren, toegang weigeren tot geïnfecteerde bestanden of zelfs virussen verwijderen.

- On-demand scanners
- On-access scanners

3.3.1.5 Anti-spamfilters

Verschillende soorten

- Filteren op basis van de afzender (Blacklist)
- Filteren op basis van de inhoud
- Whitelisting
- Anti-spam authentication

3.3.1.6 Virtual Private Network (VPN)

⇨ veilige verbinding maken over het publieke netwerk.

Op deze manier kan gevoelige informatie toch centraal bewaard blijven en eventueel van op afstand benaderd worden op een veilige manier.

2 belangrijke protocollen

- SSL (Secure Sockets Layer) is een transportprotocol en wordt gebruikt om een beveiligd communicatiekanaal op te zetten tussen 2 applicaties
- IPSec is een netwerkprotocol die het IP-protocol uitbreid met de nodige beveilingsdiensten om een VPN te bouwen

3.3.1.7 Intrusion Prevention Systems (IPS)

Een IPS kan een bedreiging detecteren nog voor ze het netwerk kan bereiken alsook kan ze onmiddellijk reageren.

IPS treedt in werking wanneer een potentiële bedreiging wordt opgemerkt.

3.3.2 Detectie

3.3.2.1 Intrusion Detection Systems (IDS)

Het doel van IDS is dat onbevoegde gebruikers of indringers worden ontdekt wanneer ze ongeautoriseerd toegang hebben verkregen op het netwerk. Ze is echter niet in staat tot actie over te gaan wanneer een aanval zich voordoen en er is dus nood aan menselijke opvolging.

De detectiemethode die aangewend wordt door een IDS kan onderverdeeld worden in 2 categorieën:

- Knowledge based detection systems ⇨ gebaseerd op gekende inbraaksenario's en technieken die gebruikt kunnen worden
- Anomaly detection ⇨ gebaseerd op een refentiemodel dat een bepaald gedrag als 'normaal' definieert
    - ⇨ NIDS (Network-based Intrusion Detection Systems)
    - ⇨ HIDS (Host-based Intrusion Detection Systems)
    - ⇨ Hybrid IDS

3.3.2.2 Honeypots

⇨ men installeert een server die geïsoleerd is van het bedrijfsnetwerk. Ze is zo geïnstalleerd dat de aanvaller denkt dat het om een deel van het bedrijfsnetwerk gaat.

2 soorten

- Low-interaction honeypots (wordt vaak gebruikt voor productiedoelen)
- High-interaction honeypots (wordt vaak gebruikt voor een onderzoek)

3.3.3 Reactie

Een **patch** is een tijdelijke oplossing voor en bug in een softwareprogramma.

3.4 Het informatiebeveiligingsproces

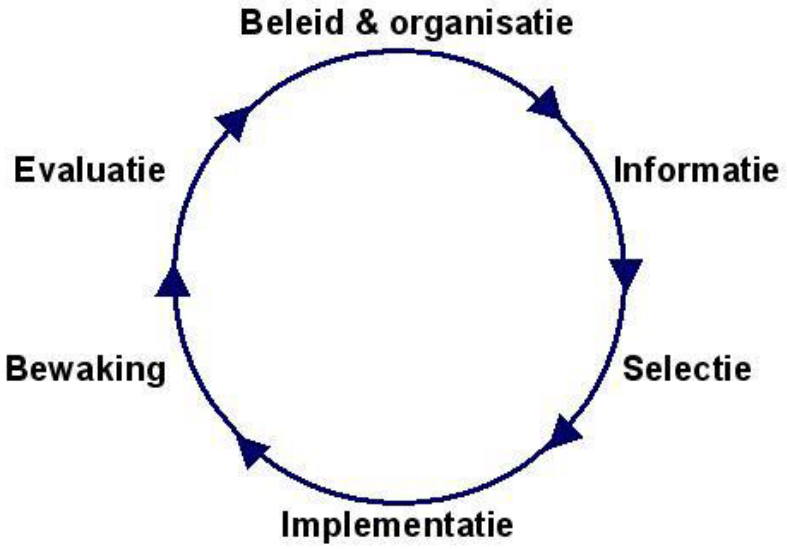
3.4.1 De BS7799-norm

⇨ een information security management standaard en omvat een soort checklist met elementen die in de policy kunnen worden opgenomen.

10 hoofdcategorieën

- Informatiebeveiligingsbeleid voor de organisatie ⇨ houdt in dat men de ondernemingsdoelstellingen begrijpt en het belang en de afhankelijkheid van de organisatie ten aanzien van informatiebeveiliging kent
- Creatie van informatiebeveiligingsinfrastructuur
- Classificatie en controle van de middelen ⇨ inventariseren van de IT-bezittingen in de onderneming
- Personeel/menselijke factor
- Fysieke beveiliging
- Systeem- en netwerkbeheer ⇨ er dient ervoor gezorgd te worden dat de uitgevaardigde procedures goed gedocumenteerd zijn en dat de informatiesystemen operationeel blijven
- Toegangsbeveiliging tot informatie en IT-middelen ⇨ toegang tot informatie en bedrijfsprocessen zijn voorzien van de nodige beveiligingsmaatregelen
- Systeemontwikkeling en –onderhoud
- Continuïteitsbeheer
- Toezicht

3.4.2 Opstellen van een informatiebeveiligingsproces



In eerste instantie dienen beveiligingseisen en –randvoorwaarden te worden gespecifieerd die uiteindelijk zullen leiden tot het informatiebeveiligingsbeleid. In een volgende stap dienen de bedreigingen te worden bepaald die tot onacceptabele risico's leiden. Op basis van deze informatie kan uiteindelijk een pakket van maatregelen worden geselecteerd en geïmplementeerd. In een volgende fase wordt geëvalueerd of het geselecteerde pakket maatregelen nog steeds aan de beveiligingsvereisten en –randvoorwaarden voldoet.

3.4.2.1 Inventarisatie en classificatie van de assets

Vooraleer men een beveiligingsbeleid kan beginnen uitwerken dient men eerst een beeld te krijgen van welke middelen er in de organisatie aanwezig zijn.

Nadat de inventaris is gedaan, is het ook belangrijk om te kijken welke assets voor de onderneming van zeer groot en minder groot belang zijn.

⇨ classificatie van de graad van belangrijkheid adhv 4 criteria

- Herstelbaarheid
- Misbaarheid
- Betrouwbaarheid
- Belang

Het is ook de graad van belangrijkheid die zal bepalen of het al dan niet nodig is om een grondige risicoanalyse te doen.

De informatie die volgt uit de inventarisatie en classificatie van informatie en informatiesystemen vormt de basis van het op te stellen beveiligingsbeleid.

3.4.2.2 Informatie risicoanalyse

Men heeft een beeld nodig van waar de risico's zich bevinden die de vertrouwelijkheid, integriteit en beschikbaarheid van informatie(systemen) in het gedrang kunnen brengen.

Een risicoanalyse gebeurt best door een onafhankelijke (externe) auditor en baseert zich op 4 pijlers:

- Informatieanalyse
- Dreigingsanalyse
- Schadeanalyse
- Waarschijnlijkheid

3.4.2.3 Selectie van beveiligingsmaatregelen

De te nemen beveiligingsmaatregelen kunnen volgens hun werkwijze in volgende categorieën worden onderverdeeld:

- Organisatorische maatregelen ⇨ hebben betrekking op het bedrijf als geheel
- Procedurele maatregelen ⇨beschrijven hoe diverse maatregelen uitgevoerd moeten worden. De procedures laten toe dat de personen in de organisatie waten wat hen in welke situatie te doen staat en tot welke personen zij zich mogelijks doen te wenden.
  Er zijn 5 categorieën van procedures:
  - ⇨ Gebruikersbeheer procedures
  - ⇨ Systeembeheer procedures
  - ⇨ Incident responsprocedures
  - ⇨ Procedure voor configuratiebeheer
  - ⇨ Rampenplannen (DRP)
- Fysieke maatregelen ⇨ de keuzen van de maatregelen hangt in eerste instantie af van de risico's die ze moeten beperken en het belang van de te beveiligen informatie(systemen)
- Technische maatregelen

3.4.2.4 Implementatie van beveiligingsmaatregelen

Bij de implementatie dient men erop toe te zien dat alle betrokkenen de nodige opleidingen krijgen en voldoende worden geïnformeerd.

⇨ **security management**

3.4.2.5 Bewaking van de naleving vd beveiligingsmaatregelen

Er dient een continue opvolging plaats te vinden en men dient erop toe te zien dat werknemers steeds de juiste werkwijze hanteren en de procedures juist blijven volgen

3.4.2.6 Evaluatie

⇨ zodat het management zich een beeld kan vormen of de geselecteerde maatregelen op een correcte wijze zijn geïmplementeerd en of de werknemers daarbij de juiste werkwijze volgen. Verder wordt er ook geëvalueerd of de maatregelen de relevante risico's voldoende en op ene kostenefficiënte wijze reduceren.

3.4.3 De menselijke factor

De mens, en vooral de eindgebruiker, wordt steeds weer als zwakste schakel binnen de beveiliging aangeduid. De beveiliging staat of valt namelijk met de houding van de gebruiker, de manier waarop hij met de beveiliging omgaat.

Fouten in onbewust gedrag

- Uitglijders
- Afdwalingen

Fouten in bewust gedrag

- Vergissingen
- Overtreding

De beste manier om een organisatie te behoeden voor dergelijke fouten in het menselijke gedrag gebruik te maken van bewustwordingsprogramma's en opleidingen voor het personeel.