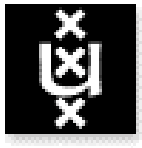


Enhanced Security Management

Informatiebeveiliging verankerd in een dynamische Business Alignment theorie

Scriptie in het kader van de Verkorte Opleiding bedrijfseconomie

aan de Universiteit van Amsterdam.

April 2002

Auteur: André Koot
Studentnr 9979050

Studierichting Information Management
Vak Informatie en Infrastructuren

1e Beoordelaar	2e Beoordelaar
Edo Roos Lindgreen	Guido Dedene

VOORWOORD

Dit document is deels de weerslag van een aantal jaren ervaring op het gebied van IT audit en het werken in een beveiligingsorganisatie en deels van de verdieping van mijn kennis, met name de theoretische onderbouwing van mijn vaktechniek, zoals ik die heb opgedaan tijdens mijn studie Bedrijfseconomie, variant Information Management. Een belangrijk deel van de theoretische onderbouwing werd mij aangereikt bij de keuzemodule 'Informatie en Infrastructuren'.

Al een aantal jaren ben ik zowel als IT auditor als in de functie van security manager actief binnen het vakgebied informatiebeveiliging. De postdoctorale opleiding EDP Auditing die ik enige jaren geleden heb afgerond, heeft de nodige bagage opgeleverd om dit vak uit te kunnen oefenen. IT-Audit houdt zich onder meer bezig met het beoordelen van de automatisering van een organisatie en de organisatie van de automatisering. Kortweg komt dat neer op zowel het beoordelen van de techniek van de automatisering en de processen die binnen een automatiseringsorganisatie bestaan als de relaties die bestaan tussen een IT organisatie en een bedrijfsorganisatie. Als security manager was ik verantwoordelijk voor het realiseren van het door de organisatie vereiste beveiligingsniveau.

In de praktijksituaties waarin ik werkzaam was, heb ik diverse knelpunten onderkend die het moeilijk maken om vast te stellen dat wat nodig is op het gebied van informatiebeveiliging, daadwerkelijk op een effectieve en efficiënte wijze wordt gerealiseerd. De wens ontstond om de in de praktijk ervaren knelpunten op te lossen met een model dat te onderbouwen is met enkele nieuwe wetenschappelijke denkbeelden. Dat onderzoek heeft geleid tot deze scriptie.

Het schrijven van deze scriptie heeft geleid tot een meer diepgaand onderzoek dan in eerste instantie de bedoeling was. De redenen waren verschillende. Niet in het minst speelde een rol dat gelijktijdig met het ontstaan van de denkbeelden ook binnen mijn werkomgeving de discussies rond de structurering van informatiebeveiliging speelden. De ontwikkeling van het besturingsmodel kan dan ook niet geheel los van deze herstructurering gezien worden.

MANAGEMENTSAMENVATTING

Het verkrijgen van inzicht in het bedrijfsbeleid lijkt voor een IT auditor een randvoorwaarde om een afgewogen audit naar het aspect informatiebeveiliging te kunnen uitvoeren. Als er beleid bestaat op dat gebied, zal dat ook kunnen ondersteunen in het op de juiste plek neerleggen van bevindingen die bij de audit naar voren komen, zodat deze meegenomen kunnen worden in de levenscyclus van bijvoorbeeld beveiligingsproducten.
Maar evenzogoed zal een IT auditor kunnen constateren dat de infrastructuur goed is beveiligd, terwijl van beleid terzake niets vastligt. Met name deze situatie komt in de praktijk voor: technisch is de beveiliging geregeld, maar van afstemming met de bedrijfsprocessen is niets gebleken. Het lijkt erop dat de beveiliging door de beheerders is ingericht om henzelf minder zorgen te geven: als de beveiliging goed is geregeld, hoeven de beheerders zich minder zorgen te maken over invloeden van buiten. Effectiviteit en efficiency zijn onvoldoende beoordeeld bij het realiseren van informatiebeveiliging.

Het Enhanced Security Management model geeft een verklaring voor dit fenomeen. Maar ook geeft het model aan hoe Security Management als proces ingericht kan worden om op een gestructureerde wijze het bedrijfsbeleid (de strategie) en de beveiligingsmaatregelen (techniek en organisatie) op elkaar af te stemmen. Het model is een uitwerking van het bekende ITIL Security Management proces waarin onder meer aandacht wordt geschonken aan de bedrijfsprocessen die leidend (zouden moeten) zijn bij de inrichting van de informatiseringsprocessen. Daarmee wordt de verantwoordelijkheid voor (het inrichten van) Security Management uit de techniek getrokken en ingebed in de totale bedrijfsvoering.

Voor alles dient er committent te bestaan. Het management van een organisatie dient de verantwoordelijkheid voor het op basis van het geformuleerde beleid normeren en toetsen van beveiliging over te dragen aan medewerkers binnen een betrekkelijk autonoom opererend proces.
Als na toepassing van de ontwerpregels van Enhanced Security Management ook deze voorwaarde is vervuld, dan moet de conclusie luiden dat informatiebeveiliging goed binnen de organisatie kan zijn verankerd.

Voorwoord

Managementsamenvatting

Inhoudsopgave

1. INLEIDING

De bedrijfsvoering binnen vrijwel elke grotere organisatie is in belangrijke mate afhankelijk van geautomatiseerde processen. De in de oude papieren wereld bestaande waarborgen voor de kwaliteit zijn daarbij vervangen door waarborgen binnen informatiesystemen. Waar voorheen de mogelijkheid bestond om bij een audit met behulp van de op papier vastgelegde audittrail vast te kunnen stellen dat bijvoorbeeld de noodzakelijke functiescheiding in de praktijk bestond, is dat door de complexiteit en de verwevenheid van geautomatiseerde systemen zonder een goede achtergrond kennis van zowel de bedrijfsprocessen als de IT en de specifieke IT auditkennis, niet meer echt mogelijk. De deskundige die over deze capaciteiten beschikt is een IT auditor.

Het beoordelen van de IT zonder kennis van de gerelateerde bedrijfsprocessen is echter ook niet zonder meer mogelijk. IT omvat bedrijfsproces ondersteunende processen en technieken. Het separaat beschouwen ervan kan weliswaar tot een oordeel van een IT auditor leiden, maar de waarde van het oordeel is beperkt, aangezien de waarde van de IT voor de bedrijfsprocessen een ander onderzoek, met name ook een risicoanalyse en weging vergt. Een IT auditor kan op basis van zijn professionele inzicht bijvoorbeeld constateren dat een firewall niet waterdicht is ingesteld, maar als de internetkoppeling die door de firewall wordt beschermd geen functie heeft in de bedrijfsvoering, zal het resultaat vermoedelijk zijn dat de aanbeveling niet opgevolgd zal worden.

Het verkrijgen van inzicht in het bedrijfsbeleid lijkt dan ook een randvoorwaarde voor een IT auditor om een afgewogen audit te kunnen uitvoeren. Als er beleid bestaat op het gebied van informatiebeveiliging zal dat bovendien kunnen ondersteunen in het op de juiste plek neerleggen van de bevindingen, zodat deze meegenomen kunnen worden in de levenscyclus van bijvoorbeeld de bewuste firewall.
Maar evenzogoed zal een IT auditor kunnen constateren dat een firewall zodanig is ingesteld dat de achterliggende infrastructuur van een organisatie prima beschermd is, terwijl van beleid terzake niets vastligt. Met name deze situatie komt in de praktijk voor: technisch is de beveiliging geregeld, maar van afstemming met de bedrijfsprocessen is niets gebleken. Het lijkt erop dat de beveiliging er alleen is om de beheerders minder zorgen te geven: als zo'n firewall goed is ingeregeld, hoeft de beheerder zich minder zorgen te maken over invloeden van buiten.

De vraag die opkomt is of het bestaan van beleid nu wel van vitaal belang is om een effectief en efficiënt niveau van beveiliging te bereiken.

1.1. PROBLEEMSTELLING

De vertaling van strategische eisen naar operationele maatregelen blijkt in de praktijk niet zo eenvoudig te maken als wel eens gedacht wordt. De gedachte dat een strategische uitspraak via een tactische vertaling resulteert in een operationele activiteit blijkt in de praktijk nauwelijks op te gaan. In de praktijk worden in het algemeen op strategisch niveau de eisen en normen op het gebied van beveiliging op een politiek correcte wijze verwoord. Gelijktijdig worden elders in een organisatie de politiek correcte technische maatregelen getroffen om het gewenste vertrouwen te scheppen dat het juiste niveau van beveiliging wordt gerealiseerd. Op grond waarvan nu dat vertrouwen gerechtvaardigd is, blijkt echter niet altijd evident te zijn.

Sterker nog, het blijkt vrijwel onmogelijk om met enige mate van zekerheid aan te tonen dat de eisen van het strategisch niveau op een effectieve en efficiënte wijze worden vertaald in alle noodzakelijke organisatorische en technische maatregelen. De strategische eisen zijn vaak zodanig verwoord, dat elke nadere uitwerking op tactisch of operationeel niveau wel is te vatten binnen de strategische eis. Of alle te treffen maatregelen daadwerkelijk gerealiseerd worden is hierdoor al niet vast te stellen. Evenmin valt vast te stellen of alle getroffen maatregelen daadwerkelijk noodzakelijk zijn. Toch is het gewenst om juist deze vertaalslagen te kunnen maken, aangezien het management gedechargeerd moet worden voor de effectiviteit en efficiency van het gevoerde beleid, ook op het gebied van informatiebeveiliging. De vraag is dan ook of het management adequaat heeft gereageerd door het treffen van de juiste maatregelen en of het operationeel management zich op de juiste wijze van haar taken heeft gekweten. Uiteindelijk gaat het er immers om vast te kunnen stellen dat het beoogde niveau van beveiliging is gerealiseerd.

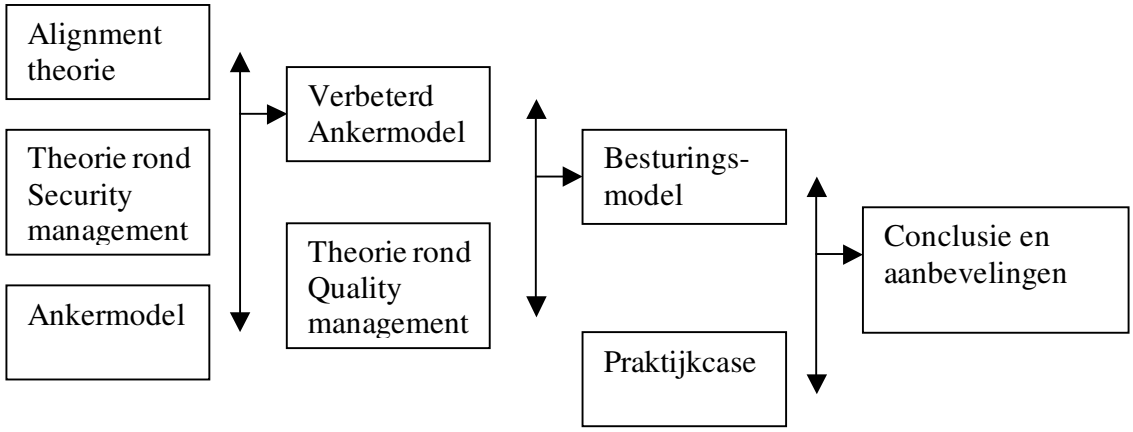
Deze vraagstelling is relevant, in het bijzonder in de relatie tussen een ICT leverancier en zijn klanten. In een Service Level Agreement (SLA) worden doelstellingen (lees normen en beoogde resultaten) gedefinieerd waarop de dienstverlening wordt ontworpen, ontwikkeld, ingericht en uitgevoerd. Ook wordt in de SLA vastgelegd op welke wijze terugkoppeling over de aan de klant geleverde diensten plaatsvindt. Daarbij worden onder meer de Key Performance Indicators (performance, beschikbaarheid, aantal wijzigingen) als verantwoordingsobjecten opgevoerd. Als geen overeenstemming bestaat tussen de aan de klant binnen de SLA overeengekomen criteria en de door de organisatie bereikte resultaten zoals die in de rapportage zijn opgenomen, dan lijkt een weinig effectieve sturing plaats te vinden. Deze kloof kan worden gemaskeerd door de norm KPI's betrekkelijk laag in te zetten. Het beloven van een beschikbaarheid van het mainframe van 95%, geeft bijvoorbeeld aan dat er eigenlijk op dit punt in het geheel geen sturing plaatsvindt: niet alleen zou een gemiddeld mainframe toch 99,999% beschikbaarheid waar moeten kunnen maken, er moeten ook nog aanvullende voorwaarden worden aangegeven, zoals een beoordelingsperiode, afspraken rond onderhoudsperioden etc. Een verwachtingenkloof leidt niet tot tevredenheid.
Kortom, het lijkt zinvol om te komen tot een aantoonbare afstemming tussen strategie en techniek.

De centrale vraagstelling die in dit onderzoek aan de orde wordt gesteld, is welk besturingsmodel in staat is om de gewenste vertaling van strategie naar techniek in de praktijk mogelijk te maken. In het onderzoek zal moeten worden nagegaan welke modellen voorhanden zijn en welke eisen er aanvullend specifiek vanuit de praktijk van informatiebeveiliging gesteld worden.
Eén van de modellen die getoetst wordt, is het Ankermodel. Dit zelf ontwikkelde model werd eerder in de praktijk ontwikkeld om te visualiseren dat er een mechanisme moet bestaan om de afstemming tussen de ontwikkeling van strategische doelen en de ontwikkeling van technische maatregelen mogelijk te maken. Het model wordt toegelicht in paragraaf 2.2 van dit rapport.

1.2. ONDERZOEKSAANPAK

Het onderzoek is gestart vanuit een eerder in de praktijk ontwikkeld model (het ankermodel), waarmee getracht werd aan te geven dat het ontwikkelen van beveiliging niet zuiver vanuit de strategie te realiseren is, aangezien ook de gehanteerde techniek faciliterend of blokkerend is voor het te realiseren niveau van beveiliging (het realiseren van een hoog niveau van beveiliging is met bijvoorbeeld een operating system als Windows95, door het ontbreken van afdoende functiescheiding, niet mogelijk [bang2001]).

Om de validiteit van het model te toetsen en het model te verbeteren is een onderzoeksmethodiek gehanteerd die mede als structureringshulpmiddel toepasbaar kon zijn.
Het onderzoek is zo veel mogelijk gestructureerd conform de onderzoeksmodel van Verschuren en Doorewaard [pvhd2000]. In de onderstaande figuur is de structuur weergegeven, waarbij gelijktijdig het chronologisch perspectief is weergegeven.



Figuur 1-1 Onderzoeksmodel

De centrale vraagstelling die in dit onderzoek aan de orde wordt gesteld, is welk besturingsmodel in staat is om de gewenste vertaling van strategie naar techniek in de praktijk mogelijk te maken. In het onderzoek zal moeten worden nagegaan welke modellen voorhanden zijn en welke eisen er aanvullend specifiek vanuit de praktijk van informatiebeveiliging gesteld worden.

Eén van de modellen die getoetst wordt, is het Ankermodel. Dit model is eerder door mij ontwikkeld om te visualiseren dat er een mechanisme moet bestaan om de afstemming tussen de ontwikkeling van strategische doelen en de ontwikkeling van (technische) maatregelen mogelijk te maken. Door de ontwikkeling van het Ankermodel werd duidelijk gemaakt dat er met name een frictie bestaat doordat er een verschil in procescyclus op strategisch en operationeel niveau. Het model wordt toegelicht in paragraaf 2.2 van dit rapport.

1.3. LEESWIJZER

Aangezien dit rapport beoogt een visie op informatiebeveiliging te geven, wordt in hoofdstuk 2 eerst een inleiding informatiebeveiliging gegeven.
Uit literatuurstudies kwam naar voren dat er een relatie lijkt te bestaan met de alignment theorie. Vandaar dat in dit rapport uitvoerig wordt stilgestaan bij dit onderwerp (hoofdstuk 3).
In hoofdstuk 4 wordt getracht het originele ankermodel, dat werd ontwikkeld om een verklaring te geven voor het verschijnsel dat er blijkbaar geen rechtstreeks verband tussen de strategische doelen en de technische maatregelen bestaat, te verbeteren door de theorie rond procesontwerp en kwaliteitsmanagement te analyseren en toe te passen.
Hoofdstuk 5 omvat de praktijkcase Belastingdienst. Hierbij wordt geanalyseerd of het ontwikkelde besturingsmodel toegevoegde waarde bezit. In hoofdstuk 6 staan conclusies en aanbevelingen.
De in de tekst vermelde referenties worden in appendix 1 uitgewerkt.

2. INLEIDING INFORMATIEBEVEILIGING

2.1. INLEIDING

Informatiebeveiliging is in veel organisaties een hot item. Op alle hiërarchische niveaus is men zich bewust van de noodzaak tot het beveiligen van de eigen informatiesystemen. Met name de toenemende noodzaak om als organisatie aanwezig te zijn op het Internet, heeft organisaties er bijvoorbeeld toe gebracht om de inbraakdreiging om te zetten in daden, zoals het plaatsen van een firewall ([isma2002], [ernst2002], [kpmg2001], [fbi2002]). Maar te constateren valt dat de rechtstreekse vertaalslag van strategische besluitvorming ("wegnemen van de angst voor het onbekende") naar technische maatregelen ("plaats dit apparaat") niet de oplossing voor het probleem ("onveiligheid") is. Nog steeds wordt beveiliging vanuit de techniek opgezet en (vaak) geaccepteerd op grond van strategische ondeskundigheid op het vakgebied, waardoor feitelijk alleen maar sprake is van symptoombestrijding [erns2002]. Het lijkt erop dat een rechtstreeks verband tussen strategie (de normen en doelstellingen) en techniek (de maatregelen) ook niet bestaat. Er zijn verschillende redenen aan te voeren voor het ontstaan van deze lacune. In deze verhandeling zullen ze in een volgend hoofdstuk aan de orde komen.

Alvorens de speurtocht naar een effectieve methode om de vertaalslag te kunnen maken uit te voeren, is het zinvol om stil te staan bij het vakgebied Informatiebeveiliging. In deze en de volgende paragrafen worden in het kort de kwaliteitscriteria, aspecten en kenmerken van Informatiebeveiliging toegelicht, zodat het kader waarbinnen de speurtocht zich afspeelt, in de volgende hoofdstukken niet verder uitgewerkt hoeft te worden.

2.2. RISICO MANAGEMENT

Een ICT-dienstverlenende organisatie zal in het contract met de klant, dat ten grondslag ligt aan de dienstverlening, duidelijk trachten aan te geven welke kwaliteit wordt geboden en hoe die kwaliteit meetbaar wordt gemaakt. Zo worden in een Service Level Agreement (SLA) afspraken gemaakt omtrent beschikbaarheid (uitgedrukt in het aantal 9' s[1]), performance en servicetijden. Een van de kwaliteitscriteria is ook het niveau van beveiliging. Nu is beveiliging een moeilijk meetbaar te maken criterium. Wanneer is sprake van *sterke* beveiliging, in welk geval is beveiliging onvoldoende, kan beveiliging met een '7' worden gewaardeerd en zo ja, is dat dan niet te laag?
Wanneer het gaat om het begrip beveiliging wordt in de meeste gevallen impliciet uitgegaan van de aanname dat een hoger niveau van beveiliging meer zekerheid biedt en dat geen inbreuk wordt gemaakt op het afgesproken niveau van beveiliging. Wat nu als een hoog niveau van beveiliging moet worden geclassificeerd, is in veel gevallen niet duidelijk, met name door het ontbreken van meetbare grootheden. Het dogma lijkt te zijn dat toepassing van dure technologie (toepassing van PKI en Intrusion Detection Systemen), automatisch leidt tot een hoger beveiligingsniveau [isma2002]. Los van de vraag of dat juist is, kan de vraag gesteld worden of de continuïteit van het beveiligingsniveau ook niet in de beoordeling betrokken moet worden: is beveiliging ingebed in de overige ontwikkeld- en beheerprocessen?

[1] Beschikbaarheid wordt gemeten in de bedrijfsduur van een component, waarbij rekening wordt gehouden met gepland onderhoud. Een beschikbaarheid van 99,999% ('5 negens') wordt voor bedrijfskritische systemen wenselijk geacht.

In veel organisaties wordt getracht om informatiebeveiliging te professionaliseren. Het aspect wordt dan ook vaak meegenomen in het bedrijfsproces Risico Management[2] en er vindt ook meer en meer certificering van het proces plaats.

2.3. KWALITEITSCRITERIA BEVEILIGING

2.3.1. Beschikbaarheid

Beschikbaarheid is het kwaliteitscriterium dat ziet op de mate waarin gegevens of functionaliteit op de juiste wijze beschikbaar zijn voor de gebruikers [pols2000]. Dit criterium is gericht op het waarborgen dat wordt voldaan wordt aan de klantwensen op het gebied van de ongestoorde dienstverlening gedurende de overeengekomen gebruiksduur van de technische infrastructuur. Bovendien wordt onder dit aspect verstaan de mogelijkheid om een verstoring van de dienstverlening tijdig te kunnen herstellen of het gegevensverlies ten gevolge van een verstoring te beperken. Een rechtstreeks verband met informatiebeveiliging is te leggen doordat verlies van gegevens in het algemeen als beveiligingsrisico wordt beschouwd. Bovendien zijn er verschillende externe aanvallen gericht op het tenietdoen van de dienstverlening (bijvoorbeeld de veelvuldig voorkomende 'Distributed Denial of Service' aanvallen op het internet), waardoor aanvullende beveiligingsmaatregelen getroffen moeten worden. Of waardoor in de Service Level Agreements terzake een disclaimer opgenomen zou moeten worden: de beschikbaarheid is in voldoende mate gewaarborgd, maar omtrent de *bereikbaarheid* wordt alleen een inspanningsverplichting aanvaard. De relatie met het proces Service Level Management is nog niet overal gelegd…

2.3.2. Vertrouwelijkheid

Vertrouwelijkheid is de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn [pols2000]. Bevoegd zijn personen op grond van de door, of namens, de rechtmatige eigenaar van dat object verstrekte toegangsrechten. Kenmerkend is dus dat een objecteigenaar uitdrukkelijk bepaalt wie welke rechten op een object mag uitoefenen.
De waarborgen dat de beoogde exclusiviteit daadwerkelijk wordt geboden, worden gerealiseerd door op een aantal gebieden technische en organisatorische maatregelen te treffen.
Daar waar de eigenaar zelf niet kan toezien op het verstrekken van de toegangsrechten, wordt in de organisatie of in de infrastructuur van de gebruiker gevraagd zich te identificeren en zich te authenticeren. Na deze activiteiten, waarmee de nodige zekerheid omtrent de identiteit wordt verkregen, worden de bij de identiteit behorende rechten verstrekt, het autorisatieproces. Deze drie activiteiten worden ook wel IAA genoemd.
IAA wordt toegepast ten behoeve van bijvoorbeeld fysieke beveiliging (toegang tot een bedrijfspand na het tonen van een pasje) of logische toegangsbeveiliging (na het intoetsen van een user-id en een wachtwoord, waarna een operating system bepaalt wat de gebruiker daadwerkelijk mag.

De IAA maatregelen trachten te voorkomen dat ongeautoriseerd toegang wordt verkregen tot

[2] Risico Management omvat het beheersen van risico's op het gebied van financiële waarden, fysieke infrastructuur en integriteit van medewerkers.

bijvoorbeeld gegevens. Toch bestaat de mogelijkheid ongeautoriseerd gegevens te benaderen, bijvoorbeeld door een netwerkverbinding af te luisteren. Daarmee wordt de exclusiviteit geschonden. Als extra maatregel kunnen dan cryptografische technieken worden toegepast om gegevens te versleutelen, waardoor de kans op afluisteren aanzienlijk verminderd wordt.

2.3.3. Integriteit

Het kwaliteitscriterium Integriteit (ook wel betrouwbaarheid genoemd) is de mate waarin gegevens of functionaliteit juist ingevuld zijn [pols2000]. Betrouwbaarheid wordt verder onderverdeeld in de kernbegrippen juistheid, volledigheid, tijdigheid en geautoriseerdheid (JVTA).
Net als bij exclusiviteit is er geen absoluut niveau van integriteit. Integriteit is met name van belang waar het gaat om transactieverwerking. Het is vervelend als gegevens op een website onterecht worden gemuteerd, maar de potentiële schade van ongeautoriseerd aanbrengen van wijzigingen in personeelssystemen of betalingssystemen kan wel eens groter zijn, al valt dat de buitenwereld misschien niet zo snel op. In deze redenering wordt er natuurlijk wel ervan uitgegaan dat de website geen bedrijfskritische gegevens bevat of als e-commerce portaal wordt gebruikt. Deze beperking geeft meteen al de relativiteit van beveiligingseisen aan. Daar wordt later in deze beschouwing op doorgeredeneerd, onder andere in paragraaf 3.1.1 wanneer wordt gesproken over classificatie van bedrijfsprocessen en gegevens.
Aangezien van belang is vast te stellen dat een mutatie geautoriseerd is, ligt er een rechtstreeks verband met het begrip exclusiviteit. De IAA-maatregelen (IAA staat voor identificatie, authenticatie en autorisatie) zijn namelijk ook de waarborgen voor de integriteit.
Een belangrijke inbreuk op integriteit wordt onder andere gevormd door het optreden van virussen. Dergelijke programmatuur kan (door een gebruiker onopgemerkt) als geautoriseerd proces door een gebruiker gestart worden en daarmee met de rechten van die gebruiker wijzigingen aan gegevens of de infrastructuur te weeg brengen.

2.3.4. Controleerbaarheid

Controleerbaarheid wordt gevraagd om aan te kunnen tonen dat de overige criteria gerealiseerd zijn. Controleerbaarheid wordt onder meer mogelijk gemaakt door het registreren van handelingen met betrekking tot het benaderen van gegevens. Deze registratie heet logging. Naast de registratie moet ook de mogelijkheid bestaan om een analyse van de logging te maken, dus ook controleerbaarheid is een eis die gesteld wordt aan de infrastructuur.

2.4. BEVEILIGINGSMAATREGELEN

Om het gewenste beveiligingsniveau te kunnen bereiken, moeten maatregelen worden getroffen. Dergelijke maatregelen kunnen zowel van technische als van organisatorische aard zijn. Technische maatregelen zijn bijvoorbeeld toepassing van infrastructurele componenten, organisatorische maatregelen hebben bijvoorbeeld betrekking op inrichten van een beheer- en beveiligingsorganisatie. In het algemeen wordt de volgende onderverdelingen gemaakt als het gaat om de structurering van de maatregelen en de keuze voor implementatie [pols2000]:

2.4.1. Preventieve maatregelen

Dit zijn de maatregelen die worden getroffen om te voorkomen dat een onderkende bedreiging

manifest wordt. Een preventieve maatregel van technische aard is bijvoorbeeld installatie van anti-virus software.

2.4.2. Repressieve maatregelen

Dergelijke maatregelen worden getroffen om bij manifest worden van een bedreiging de negatieve gevolgen zo veel mogelijk te beperken. Een technische maatregel is het plaatsen van een noodstroomvoorziening, die in geval van stroomuitval (de bedreiging) het mogelijk maakt ene systeem gecontroleerd uit te schakelen.

2.4.3. Detectieve maatregelen

Detectieve maatregelen worden getroffen om tijdig vast te kunnen stellen dat een bedreiging manifest is geworden. Een detectieve maatregel van technisch aard is het installeren van een Intrusion Detection systeem (een inbraak alarm op bijvoorbeeld een firewall).

2.4.4. Correctieve maatregelen

Wanneer een bedreiging manifest is geworden zal door toepassing van correctieve maatregelen herstel plaats kunnen vinden. Dat houdt in dat de bedreiging wordt teniet gedaan en dat herstel van diensten en (zo mogelijk) gegevens kan plaatsvinden. Dit speelt bijvoorbeeld wanneer na een calamiteit moet worden uitgeweken naar een secundaire locatie van waaruit de productie tijdelijk wordt voortgezet.

Opgemerkt moet hierbij worden dat wanneer een maatregel om bijvoorbeeld organisatorische of financiële redenen niet te treffen is, de mogelijkheid bestaat om compenserende of aanvullende maatregelen te treffen.
Een compenserende maatregel is in staat om een risico dat bestaat doordat een andere maatregel niet kan worden getroffen, af te dekken. Als bijvoorbeeld functiescheiding in het beheer niet kan worden gerealiseerd, zou aanvullende logging van beheerhandelingen plaats kunnen vinden.
Een aanvullende maatregel kan getroffen worden als onvoldoende zekerheid over of inzicht bestaat in de restrisico's die blijven bestaan na het treffen van de noodzakelijk geachte maatregelen.

2.5. RESUMÉ BEVEILIGING

Het realiseren van een adequaat niveau van beveiliging betekent het op basis van risico analyses implementeren van een groot scala aan technische en organisatorische beveiligingsmaatregelen. Dit betekent dat in een situatie van een dynamische omgeving met een grote diversiteit aan technische componenten en in toenemende mate externe verbindingen met een onvertrouwde omgeving, het van groot belang is zicht te hebben op het daadwerkelijk gerealiseerde niveau van beveiliging. Het planning en control proces moet om die reden ook op het gebied van beveiliging ingericht te worden. En dat betekent weer dat niet alleen op het gebied van de techniek inzicht moet bestaan in het beveiligingsniveau.
Op grond van dit inzicht kan geconcludeerd worden dat er verschil bestaat tussen het inrichten van beveiliging, namelijk het treffen van preventieve en repressieve organisatorische en technische maatregelen, en het beheren van beveiliging, het treffen van detectieve en correctieve

organisatorische en technische maatregelen. Het beheren van beveiliging omvat daarnaast het inrichten van de beheerprocessen om ervoor zorg te dragen dat op elk moment zich bestaat op het niveau van beveiliging. Het een en het ander zijn niet per definitie aan elkaar gerelateerd: het is mogelijk om op enig moment een hoog niveau van beveiliging gerealiseerd te hebben, zonder het beheerproces ingericht te hebben. Helaas betekent dat wel dat er geen enkele zekerheid bestaat dat een volgend moment ook het beoogde resultaat gehaald wordt. Ook is het mogelijk om het beveiligingsbeheer proces ingericht te hebben en niet het beoogde niveau van beveiliging gerealiseerd te hebben. In dat geval zal echter wel bekend zijn waar en waarom afgeweken wordt van het norm niveau.

In het vervolg van deze verhandeling wordt ingegaan op ontwikkeling en inrichting van het beheersingsinstrument dat noodzakelijk is om met name de tweede situatie (het realiseren van een beveiligingsbeheer proces) te bereiken

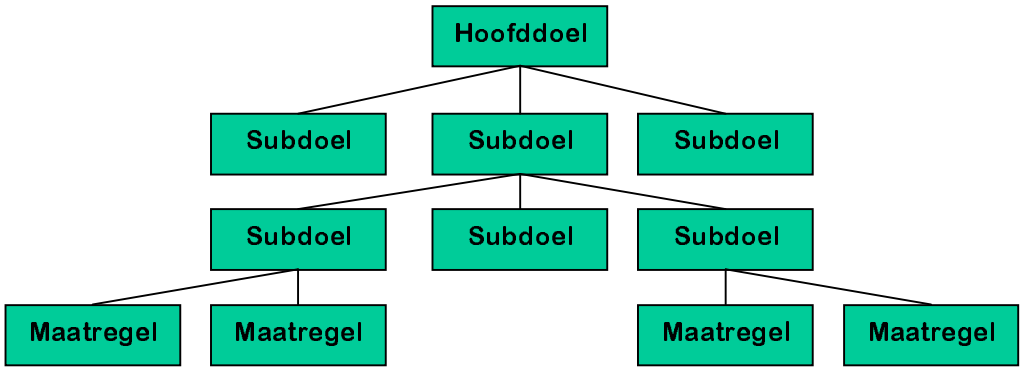
3. ALIGNMENT PROBLEMATIEK

3.1. ALIGNMENT THEORIE

3.1.1. Aanleiding

Om vast te stellen of het management voldoet aan de doelstellingen wordt in het algemeen door een externe auditor een onderzoek ingesteld. De auditor tracht aan de hand van een (door de opdrachtgever aangeleverd, of als dat niet aanwezig is, geaccordeerd) normenkader te toetsen of de doelstellingen in de praktijk worden gerealiseerd. Daarbij is een eenduidige relatie tussen normen en maatregelen van belang, waarbij een maatregel op een hoog niveau zelf weer een doelstelling ten opzichte van een lager niveau is.

Door deze methodiek te volgen ontstaat een doelstellingenboom, waarin elke doelstelling volledig door maatregelen wordt gedekt en elke maatregel te koppelen is aan een doelstelling. Kortom, wanneer elke maatregel op het laagste niveau als boomblad wordt beschouwd, zijn er geen kale takken en liggen er evenmin losse blaadjes (maatregel zonder achterliggende doelstelling) aan de voet van de boom.

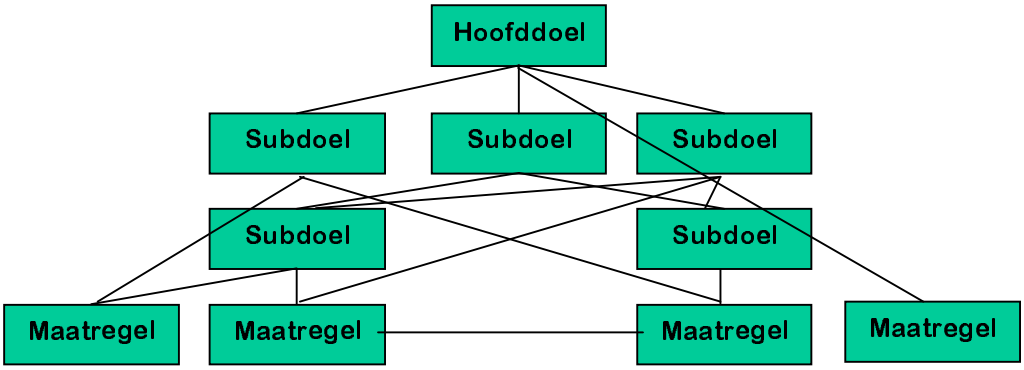


Figuur 3-1 Doelstellingenboom

Wanneer van elke doelstelling op een adequate wijze kan worden vastgesteld dat er afdoende maatregelen zijn getroffen om de doelstelling te realiseren, kan de auditor met een gerust hart verklaren dat voldaan is aan de doelstelling.

Vanuit de optiek van Informatiebeveiliging is hier dan ook de ideale structuur weergegeven: het hoofddoel is het bereiken van een afdoende beveiligingsniveau (dit wordt hier nu niet verder gedefinieerd, maar te denken valt aan het op basis van risicoanalyse en classificatie van processen en gegevens treffen van de noodzakelijke maatregelen, of bepalen van de gewenste doelstellingen). Dit hoofddoel kan worden uitgesplitst naar onderliggende doelstellingen zoals het realiseren van Integriteit, exclusiviteit en Beschikbaarheid. Elk van deze kwaliteitscriteria, kan vervolgens weer verder uiteengerafeld worden, totdat een technische of organisatorische maatregel bedacht kan worden waarmee de boom terug afgelopen kan worden. Uiteindelijk kan vervolgens door het scoren van de getroffen maatregelen het beveiligingsniveau gewaardeerd worden.

Het grote probleem is echter dat er in de praktijk maatregelen zijn die meerdere doelstellingen gelijktijdig (soms op verschillende niveaus in de boom) afdekken en dat er maatregelen zijn die geen enkele doelstelling van een hoger niveau lijken dienen. Er is dus geen sprake van een hiërarchische structuur, maar van een netwerkstructuur. Daarmee is de eenduidige relatie tussen Doelstelling en Maatregel niet meer aanwezig.
De volledigheid en juistheid van de maatregelen kan niet meer zonder meer worden vastgesteld.



Figuur 3-1 Doelstellingennetwerk

Dit vaststellende, is het voor een auditor derhalve niet eenvoudig om de volledigheid en juistheid van de getroffen maatregelen vast te stellen.

De wens om te komen tot afstemming tussen strategie en techniek is niet voorbehouden aan de audit discipline of aan het vakgebied informatiebeveiliging. Ook een proces als Service Level Management wil bijvoorbeeld een rapportage van technische resultaten (bijvoorbeeld het beschikbaarheidspercentage) hanteren om aan te tonen dat de dienstverlening voldoet aan de afgesproken niveau's.

3.1.2. Traditionele zienswijze

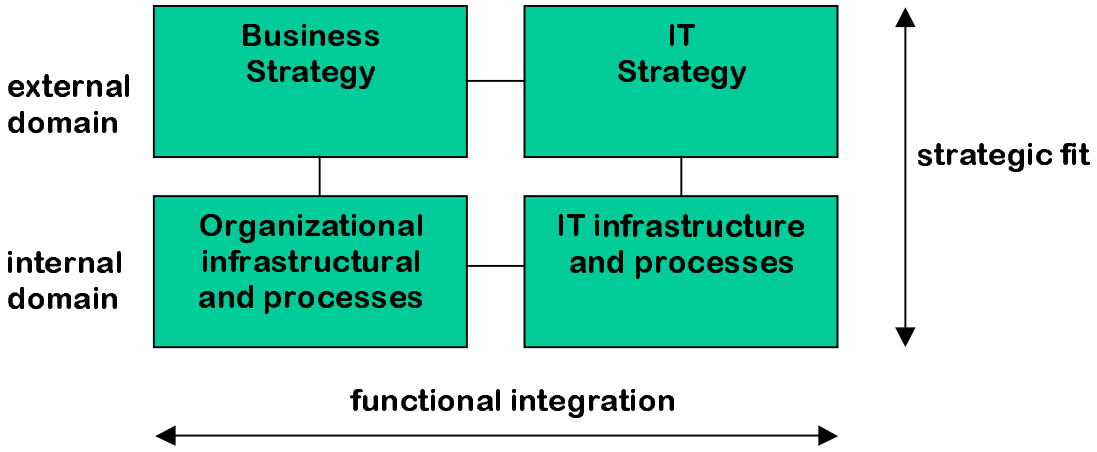
In de management literatuur is veel aandacht besteed aan de alignment problematiek. Daarbij is de focus komen te liggen op de wens om de afstemming tussen de business en IT te kunnen waarborgen. De gedachtegang daarachter is dat de IT de business moet faciliteren, immers wat heeft IT voor nut wanneer de IT de primaire processen van een organisatie niet ondersteunt.
Het drijven van een onderneming is niet hetzelfde als het realiseren van een adequate IT-ondersteuning ten behoeve van die onderneming: daar kan en wil een business manager niet verantwoordelijk voor zijn. De reden daarvoor is onder meer dat er een verschil in cultuur bestaat tussen de business en de IT. Om de IT in goede banen te leiden is er dan ook in veel gevallen een hoofd van de automatiseringsafdeling (CIO, Chief Information Officer). [grin1995].

In de management literatuur wordt ervan uitgegaan dat er een overeenstemming bestaat tussen de business strategie en de ICT strategie. Uit diverse onderzoeken is gebleken dat het bereiken van deze afstemming tot de grootste uitdagingen en zorgen hoort van het IT management [keen1991, grin1995].

Daarbij is een aantal theorieën gangbaar. In [keen1991] wordt aangegeven dat alignment met name afgedwongen wordt door economische overwegingen. Het kostenaspect van de IT (hoe kunnen de totale IT-kosten stijgen terwijl de IT componenten in kostprijs dalen?) noopt tot een vergaande afstemming tussen het management van het bedrijf en het management van de IT afdeling. Alignment is een 'relationeel' probleem.

Vanuit de Harvard management school is de alignment theorie onder meer vervat in het werk van Weill en Broadbent. Zij hebben vastgesteld dat het management de noodzaak heeft toe te zien op de afstemming van de IT op de business [cibo2000].

De onderzoekers Henderson en Venkatraman hebben de relatie tussen business en IT uitgewerkt door een niveau verschil te introduceren. De alignment heeft niet alleen te maken met het verschil tussen de business strategie en de technologische ontwikkeling, maar er is ook een hiërarchische alignment te onderkennen. De schrijvers hebben het model als volgt weergegeven [maes1999]:



Figuur 3-2 Strategical Alignment

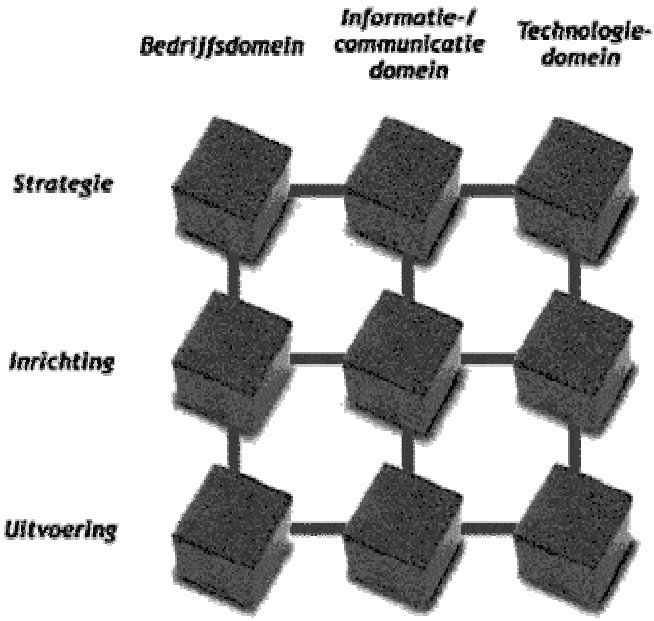
Dit model toont een betrekkelijk rechtlijnig verband tussen de business strategie en de IT strategie. Er blijkt een afhankelijkheid te bestaan, de één beïnvloedt de ander, waarbij vanuit de optiek van de onderzoekers (zie ook [keen1991], Weill en Broadbent) de business leidend is.
Daarnaast wordt verondersteld dat er een rechtstreeks verband bestaat tussen de strategie van een organisatie en de organisatorische en technische inbedding van deze strategie.

Uiteindelijk leidt deze modellering tot de constatering dat elke strategische uitspraak rechtstreeks gevolgen heeft voor de infrastructuur en processen in een operationele organisatie.

3.1.3. 9-Vlak

Dit model is niet het enige model waarmee de relatie tussen strategie en techniek kan worden weergegeven. Het Amsterdamse 9-vlak is een andere recente poging om inzicht te verschaffen in de krachten die spelen op het vakgebied Informatie Management [maes1999]. Het model Henderson - Venkatraman is op een eenvoudige wijze aangepast: de ontwikkelaars hebben niet alleen een hiërarchisch niveau, namelijk het tactische niveau, op de verticale as tussengevoegd, ook is de verdeling in het horizontale vlak uitgebreid met een nieuwe functie, namelijk de functie

Informatiemanagement.



Figuur 3-3 Het (Amsterdamse) 9-vlak

Het resultaat is dat het nu mogelijk is om enkele extra vertaalslagen te verklaren. De hiërarchische alignment van strategie via tactiek naar operatie is nu duidelijk geworden en ook de organisatorische functie van informatiemanagement als vertaler van business naar IT en vice versa is concreet vormgegeven. Midden in de nieuw ontstane matrix bestaat nu opeens een geheel nieuw vakgebied, dat in het kort als architectuur is te kenschetsen: dit is de functie die oplossingen ontwerpt.

Bovendien blijkt dat het nu inzichtelijk is dat er meerdere vertaalslagen mogelijk zijn. Dat lijkt triviaal, maar het effect is dat er daarmee een vorm van onafhankelijkheid wordt gecreëerd. Een wijziging van de strategie (business richting) leidt tot een wijziging van de nevengeplaatste vlakken, die zelf weer een reactie tot gevolg heeft. Er is echter geen rechtstreeks verband tussen de strategische besluitvorming en de feitelijk getroffen technische maatregelen (uitvoering techniek in de terminologie van het 9-vlak).

3.2. ANKERMODEL

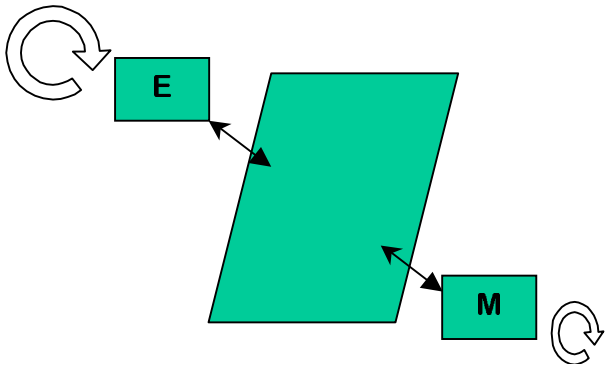
Een poging tot het vinden van een verklaring voor het missen van het rechtstreekse verband tussen strategie en techniek, is gedaan in de ontwikkeling van het Ankermodel. In dit model wordt ervan uitgegaan dat zowel de eisen, als de technische maatregelen vaststaan, verankerd zijn:

- De beveiligingseisen zijn verankerd omdat ze betrekkelijk statisch zijn in de tijd. De eis van integriteit is vermoedelijk al een decennium aanwezig en zal nog wel een decennium gelden. Er zullen vermoedelijk wel in beperkte mate nieuwe eisen gesteld worden, maar die zijn vooral het gevolg van de technology push. Te denken valt aan nieuwe eisen op het gebied van draadloze communicatie, telewerken en de toepassing van internettechnologie.

- De technische maatregelen staan grotendeels vast, omdat ze zijn verankerd in de technische infrastructuur. Daarmee is meteen vastgesteld dat ze niet zo statisch zijn als de eisen, want de technische infrastructuur is betrekkelijk veranderlijk. De veranderlijkheid is niet zonder meer eenduidig, maar een periodiciteit van 2 tot 4 jaar is wel gebruikelijk. Er bestaan weliswaar infrastructuur componenten die enkele tientallen jaren betrekkelijk onveranderlijk zijn, denk aan CICS-Cobol[3] applicaties op een mainframe platform, maar in de regel is een korte termijn eerder regel.

Uit het feit dat de periodiciteit van verandering zo sterk afwijkend is, blijkt dat er een frictie moet bestaan. De flexibiliteit van de veranderende techniek moet in overeenstemming worden gebracht met de vastigheid van de eisen.

Uitgaande van deze beide ankers moet er een instrument bestaan om te waarborgen dat in ieder geval de strategische eisen een plek krijgen en dat ook de noodzakelijke operationele maatregelen op hun plaats terechtkomen.



Figuur 3-4 Ankermodel

(E=strategische eisen op strategisch niveau, M=technische en organisatorische maatregelen op operationeel niveau).

In het ankermodel wordt de rechtstreekse relatie tussen eisen en maatregelen doorbroken door een nieuw grensvlak. De inrichting van dit grensvlak dient te waarborgen dat de frictie tussen eisen en maatregelen wordt opgeheven. Bovendien moet in dit grensvlak gewaarborgd worden dat zowel de strategische eisen tot hun recht komen richting techniek, alsook dat er ruimte is voor een juiste afweging van de te treffen maatregelen, vanuit technisch perspectief.

Om te waarborgen dat met name dit laatste aspect niet los van de strategische en tactische doelstellingen wordt beschouwd, is het noodzakelijk om naast de top-down benadering een structuur te vinden waarin de bottom-up benadering tot zijn recht komt. Met name dit aspect is in de traditionele alignment theorie niet goed uitgewerkt. In het ankermodel zijn de relaties tussen de verschillende niveau's wederkerig. Dat lijkt logisch gezien de wens te komen tot de afstemming tussen de verschillende niveau's. Het tekenen van pijltjes is echter nog geen methodiek die in een organisatie zomaar ingebed kan worden. Om die reden lijkt het zinvol om aan recycling te doen: de relaties tussen de verschillende niveau's kunnen wellicht beter procesmatig ingericht worden:

[3] CICS-Cobol is de onderliggende technologie die wordt gebruikt voor informatiesystemen op het mainframe platform

3.3. DIS-ALIGNMENT THEORIE

Opmerkelijk is dat hoezeer deze alignment blijkbaar gewenst wordt, de praktijk anders uitwijst. Het lijkt erop dat alignment niet altijd haalbaar, of zelfs maar gewenst is. Uit diverse onderzoeken blijkt dat de haalbaarheid (en zelfs wenselijkheid) vaak discutabel is [cibo2000].

Een van de knelpunten die optreden, is dat de alignment automatisch wordt opgevat vanuit de visie dat de business strategie leidend is en dat derhalve de ICT strategie (en implementatie) volgend [keen1991, bere2001].

Daarbij kunnen we meteen de volgende kanttekeningen plaatsen:
Alignment is geen eenrichtingsverkeer. Er zijn strategische ICT keuzes denkbaar die onmiskenbaar gevolg hebben voor de business strategie. Als voorbeelden kunnen genoemd worden de invoering van een ERP pakket als SAP of de invoering van Workflow Management technologie. Daarentegen kunnen de keuzes die in het verleden gemaakt zijn dermate ingrijpend zijn dat het niet voor de hand ligt om een verandering in de business strategie ook een verandering van de ICT omgeving door te laten voeren. Dit speelt met name op het gebied van de ICT infrastructuur. Er zijn nog steeds veel informatiesystemen die vele jaren geleden ontwikkeld zijn (wellicht bestond voor dat systeem op het moment van ontwikkeling een sterke mate van alignment) maar die nog steeds ten dienste staan van een organisatie die zelf verder ontwikkeld is, los van deze infrastructuur, waardoor de alignment niet langer bestaat. Hiermee is dus niet gezegd dat het ontbreken van alignment ineffectief en inefficiënt is [cibo2000]. De veranderlijkheid van de ICT mag wel spreekwoordelijk heten: de ontwikkeling van vandaag is morgen al achterhaald. Maar de technologie van vandaag kan evenwel meteen ook een kans voor de business voor morgen zijn.

Een tweede knelpunt is dat de veranderlijkheid van de bedrijfsstrategie een andere cyclus kent dan die van de ICT strategie of, sterker nog, dan de ICT technologie. Een voorbeeld vanuit de optiek van Security Management: de eis van integriteit van de gegevens bestaat al geruime tijd, stel 10 jaar. Bovendien zal deze eis de komende 10 jaar niet drastisch veranderen. Wellicht zullen er nieuwe technologieën worden ingevoerd (bijvoorbeeld invoering van e-commerce en ontsluiting van het internet) waar deze eis ook neergelegd wordt, maar de eis zelf blijft min of meer stabiel. Daar staat tegenover dat met de implementatie van nieuwe componenten ook nieuwe maatregelen getroffen moeten worden om te voorkomen dat een degradatie van het beveiligingsniveau optreedt. Het ankermodel geeft visueel weer dat deze afwijkende cycli door een buffer, een flexibele structuur, opgevangen moeten worden.

Deze fenomenen waarnemend, zijn er verschillende redenen op te noemen die nopen tot het accepteren van dis-alignment:

- verschillende gemaakte (strategische) keuzes hebben een zeer lange uitwerking tot gevolg. De beslissing voor een infrastructurele investering kan tot gevolg hebben dat de operatie gedurende vele jaren op deze infrastructuur gebaseerd zal zijn. Een volgende strategische keuze zal wellicht een andere uitwerking tot gevolg mogen hebben, maar de operatie zal in de meeste gevallen de nieuwe keuze niet kunnen volgen. Als voorbeeld: de keuze voor invoering van een ERP-pakket als SAP is bepalend voor de bedrijfsvoering van de komende jaren. Daarmee wordt een vorm van stabiliteit, of starheid, gecreëerd die strijdig kan zijn met andere ontwikkelingen. Sterker, de invoering van deze component kan leidend zijn voor de inrichting van de organisatie voor de komende jaren.
- De bedrijfscultuur kan het onmogelijk maken een gewenste aanpassing door te voeren.

Cultuur blijkt een grote impact op de bedrijfsvoering te hebben. De veranderlijkheid binnen bedrijven is beperkt, te denken valt aan de doorlooptijd van minimaal 4 jaar [grin1995]. Dat impliceert dat een strategiewijziging niet direct tot resultaat zal kunnen leiden. Met als logisch gevolg: er is sprake van dis-alignment.

- Snelle technische vooruitgang zou de bestaande bedrijfsstrategie (of zelfs de ICT-strategie) kunnen inhalen. Om dat mogelijk te maken moet er een flexibel verband bestaan om kansrijke ontwikkelingen niet in de kiem te smoren.

Ook de wenselijkheid van alignment is niet altijd helder te maken:

- Alignment leidt tot starheid, pas bij een afdoende afstemming tussen de business en de ICT is er ruimte voor een nieuw veranderingsproces [grin1995].
- De alignment zoals in de literatuur beschreven, gaat uit van een top-down afstemming, dat wil zeggen dat een wijziging van de strategie van de business voorrang heeft. Het zou wel zinvol kunnen zijn dat de technology push invloed heeft op de business strategie (te denken valt aan de ontwikkeling van de mogelijkheden van e-commerce.

Hiermee is niet gezegd dat alignment een ongewenst doel is, wel dat de huidige modellen in ieder geval niet altijd de oplossing bieden voor een effectieve en efficiënte werkwijze. Alignment kan dan ook niet een doel op zich zijn, het bereiken van alignment zou niet meer dan een middel tot realisatie van bedrijfsdoelstellingen moeten zijn.

3.4. ALIGNMENT EN BEVEILIGING

3.4.1. Vader van de gedachte

Vanuit de optiek van informatiebeveiliging zou het prettig zijn wanneer het alignment model in de praktijk toepasbaar en toetsbaar zou zijn. Wanneer dat het geval is, kan betrekkelijk eenvoudig een gedefinieerd beveiligingsniveau worden gerealiseerd. Elke strategische doelstelling kan bij een effectieve vertaling via de IT strategie of via de operationele organisatie in afdoende mate worden afgedekt door de noodzakelijke technische maatregelen te treffen. Bovendien wordt door deze "doelstellingenboom" [4] gewaarborgd dat er geen losse "blaadjes" rond dwarrelen, elke technische beveiligingsmaatregel dient een hoger beveiligingsdoel.

De pogingen om de noodzakelijke technische beveiligingsmaatregelen af te leiden uit de concrete (strategische) eisen en gebruik te maken van de vanuit het model blijkende relaties, zijn weinig kansrijk. Daarvoor zijn verschillende redenen aan te dragen:

- De strategische eisen worden in grotere organisaties afgeleid uit andere bestaande richtlijnen. Op het gebied van Informatiebeveiliging wordt in het algemeen niets anders vermeld dan hetgeen op grond van bestaande richtlijnen ([code2000], [vir1994]) is voorgeschreven. Deze richtlijnen worden al geruime tijd (circa 6 a 8 jaar) als normenkader gehanteerd. In de normen worden begrippen als integriteit en vertrouwelijkheid omschreven. De beschrijvingen blijven betrekkelijk abstract.
  Door de betrekkelijk abstracte beschrijving van de normen, zijn alle maatregelen eigenlijk wel zinvol, het juistheids aspect van de maatregelen is wel snel afgedekt. Het

[4] zie figuur 3-1

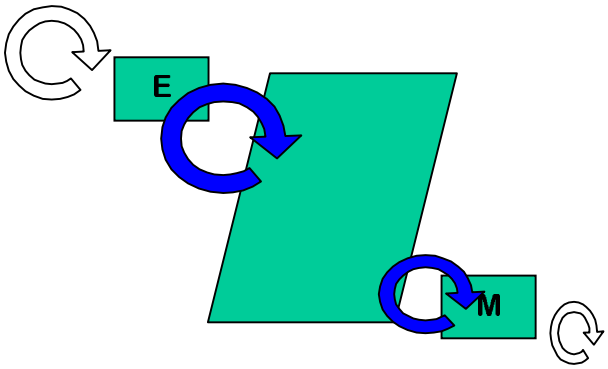
volledigheidsaspect blijft echter buiten beschouwing.

- Een eis als het waarborgen van de integriteit van gegevens behelst het uitwerken van verschillende gerelateerde kwaliteitscriteria. De integriteit is onder meer afhankelijk van het voorkomen van de mogelijkheden om buiten de gedefinieerde toegangspaden gegevens te kunnen benaderen en muteren. Deze toegangspaden worden onder meer gewaarborgd door het afdwingen van Logische Toegangsbeveiliging (LTB). En LTB staat weer onder hetzelfde regime van het waarborgen van de exclusiviteit van de gegevens, zoals daar zijn identificatie, authenticatie en autorisatie. Op dit punt is dan ook nog geen enkele eenduidige technische maatregel te definiëren: er is geen onderscheidend vermogen voor classificatie van de maatregelen. Elke te treffen maatregel zal zonder meer toegevoegde waarde voor het beveiligingsniveau hebben, maar of daarmee de juiste maatregelen getroffen worden is niet zeker.
  Ook kan een enkele technisch maatregel een heel scala aan strategische eisen afdekken. Denk aan de invoering van een PKI infrastructuur waarmee niet alleen exclusiviteit maar ook integriteit, onweerlegbaarheid en controleerbaarheid gerealiseerd kunnen worden. Een één op één vertaling is dus evenmin mogelijk.
- Een ander probleem voor het niet kunnen realiseren van een één op één relatie is dat de te treffen technische maatregelen vooral afhankelijk zijn van de technische infrastructuur die wordt toegepast.
  Er moet vaak louter op grond van technische beperkingen een autonome beslissing worden genomen met betrekking van het treffen van beveiligingsmaatregelen. De strategische uitgangspunten, of de eisen van de klant hebben hier dus geen enkele rechtstreekse relatie met de technische uitvoering van het beveiligingsinstrument.

Uit de constatering dat eenduidige alignment niet lijkt te bestaan, kan niet afgeleid worden dat informatiebeveiliging in de praktijk niet effectief is. De meeste technische maatregelen worden door de techniek afgedwongen. Maar er is, zoals aangegeven, geen rechtstreeks, controleerbaar verband met de strategische eisen. De centrale vraag is of het strategische management kan vertrouwen op deze ongecontroleerde inrichting van beveiliging, of dat er toch een betere structurering van het beveiligingsproces gewenst is.

3.4.2. Verbeterd ankermodel

In het onderstaande schema is het ankermodel in beperkte mate aangepast. De noodzaak hiertoe is gelegen in het feit dat in het ankermodel wel een erg eenvoudig communicatiemiddel aanwezig werd verondersteld: namelijk een actieve rol tussen de verschillende verantwoordelijkheden, waarbij elk niveau zelfstandig de andere niveaus informeert. Ook hier lijkt ook de wens de vader van de gedachte. In de praktijk blijkt dat de relaties niet altijd zo eenvoudig zijn. Elk niveau heeft eigen prioriteiten, waardoor onbaatzuchtig anderen ondersteunen niet voorop staat.
Door nu de afstemming tussen de verschillende niveaus procesmatig in te richten, is sprake van een structurele inrichting van het totale proces, waarbij de verantwoordelijkheid voor de afstemming op een meer eenduidige wijze binnen de organisatie belegd kan worden.



Figuur 3-5 Verbeterd Ankermodel

De sturing vindt plaats vanuit het hoger liggende niveau. Aanpassingen die in de lager liggende tactische of operationele niveau's worden doorgevoerd op grond van gebleken technische of organisatorische noodzaak, zouden een trigger moeten zijn voor aanpassing van normen of eisen op het bovenliggende niveau. Een aanpassing binnen het operationele niveau zou zo kunnen leiden tot ofwel een aanpassing van de normatiek op het tactische niveau, of tot de noodzaak om vanuit het tactische niveau de operatie aan te sturen (als blijkt dat op operationeel niveau een beoordelingsfout is gemaakt). Een norm aanpassing op het tactische niveau kan leiden tot een beoordeling door het strategische niveau, die kan leiden tot bijstelling van de strategische kaders of tot aansturing van het tactische niveau door het strategische niveau.
Natuurlijk moeten deze processen wel worden ingericht. Het meest pragmatisch is om de trigger functie bij het onderliggende proces te beleggen, zodanig dat een aanpassing van bijvoorbeeld technische normen of baselines (op operationeel niveau), leidt tot een interne beoordelingsslag op tactisch niveau. Evenzo zal een aanpassing van tactische normen leiden tot een toetsing door de strategische functie. Hiermee is dan enerzijds gewaarborgd dat de wenselijke aanpassingen vanuit de onderliggende niveau's niet veronachtzaamd worden en tevens wordt de juistheid en volledigheid van de gehanteerde normen ten opzichte van de bovenliggende niveau's gewaarborgd.

In het ankermodel is hiermee voorzien in een structureel verbeterproces. Het traditionele alignment principe (top-down) wordt gecomplementeerd door een feed-back mechanisme voor de relevante aanpassingen vanuit de onderliggende niveau's. Het koppelvlak is in dit model feitelijk het sturingsmechanisme.
Door nu de verantwoordelijkheid voor beide feedback processen te beleggen bij het tactische proces Security Management, immers verondersteld mag worden dat de specialisten op het gebied van informatiebeveiliging binnen dat proces werkzaam zijn, is er expliciet één belanghebbende voor het structureel inrichten van het proces opgesteld, zodat consistentie van inrichting en operatie is gewaarborgd.

Daarmee worden meteen verschillende eisen gesteld aan de inrichting van het tactische koppelvlak:

- inzicht in lange termijn strategie en de capaciteiten bezittend om dit inzicht te vertalen in eisen op tactische niveau;
- inzicht in de gehanteerde techniek en de capaciteiten bezittend om dit inzicht te vertalen in aanpassing van de eisen op tactische niveau;
- witte vlekken en doublures kunnen vaststellen en analyseren en deze vertalen in aanvullende tactische eisen;

- de op tactisch niveau gedefinieerde eisen af kunnen stemmen met strategisch en operationeel vlak;
- de capaciteiten bezitten om te kunnen omgaan met afwijkende planningscycli en -horizonnen.

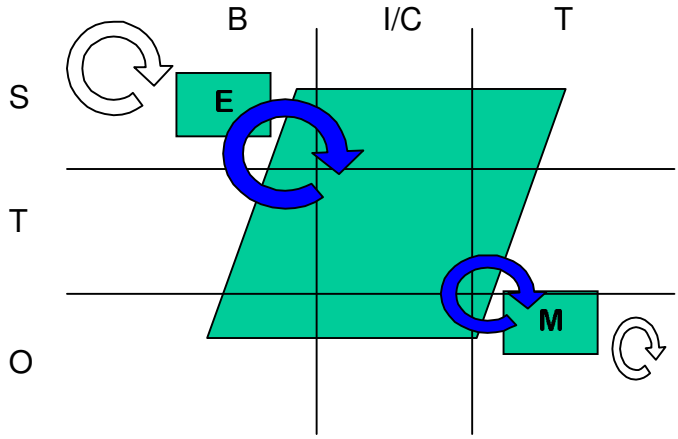
Al deze eisen zijn noodzakelijk om de bufferfunctie, de flexibele structuur, tussen strategie en techniek op te kunnen vullen. Deze functie creëert de noodzakelijke versnelling of vertraging tussen de strategische lange termijn planningscyclus en korte termijn technische realisatiecyclus.

4. PROBLEEMANALYSE EN -OPLOSSING

4.1. PROBLEEMANALYSE

Het verbeterde ankermodel biedt van zichzelf al de mogelijkheid om te verklaren dat er (onder andere door de verschillende procescycli) geen rechtstreeks verband bestaat tussen strategie en techniek en dat er blijkbaar een mechanisme moet bestaan om de dientengevolge bestaande frictie op te vangen. De taak, functie en plaats van dit mechanisme is echter niet meteen uit dit model af te leiden.

Op dit punt aangekomen lijkt het zinvol om het ankermodel te projecteren op het ten tonele gevoerde 9-vlaks model.



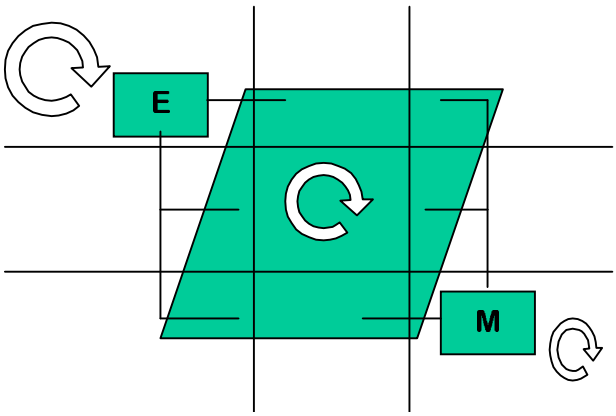
Figuur 4-1 Verbeterd Ankermodel op z'n Amsterdams

Uit deze projectie blijkt dat deze buffer een bijzondere plaats inneemt in het negenvlak. In eerste instantie wordt de diagonaal van het 9-vlak afgedekt. Maar daarnaast wordt de buffer ook een plaats gegeven in de overige 6 vlakken. Dat is niet alleen een tekentechnische aardigheid, er zijn verschillende argumenten aan te dragen om het instrument zodanig vorm te geven:

- Verantwoordelijkheid voor afstemming: twee vlakken vormen de input voor het proces. Om autonoom de verantwoordelijkheid te kunnen dragen moet vanuit de bufferfunctie invloed op de andere vlakken uitgeoefend kunnen worden
- Om te voorkomen dat zuilvorming plaatsvindt (feitelijk is dat verzuiling binnen elke cel van het 9-vlak) moet een overkoepelend proces bestaan om de coördinatie uit te voeren. De coördinatie met de beide externe relaties is in het concept voorzien middels de 1 op 1 relaties (de regelkringetjes tussen de cellen).

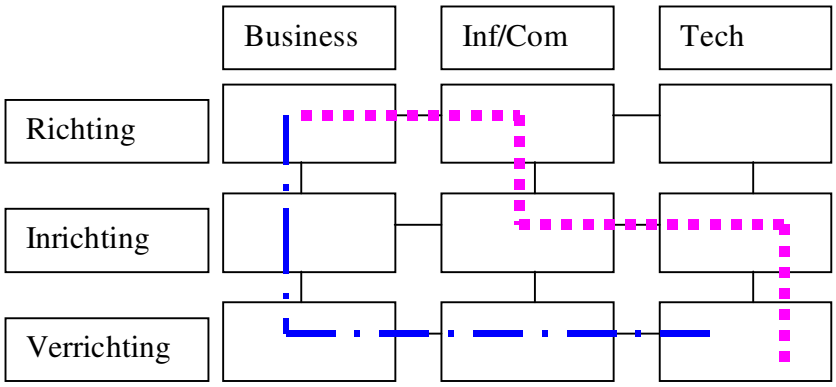
In paragraaf 3.4.2 is een aantal inrichtingseisen met betrekking tot deze bufferfunctie beschreven. Met name de laatste eis is interessant. Om te kunnen omgaan met cyclusverschillen lijkt het voor de hand te liggen dat een cyclische inrichting wordt gekozen.

Aangezien sprake is van een buffer tussen twee vlakken met een afwijkende dynamiek, moet eveneens sprake zijn van een dynamische verschijningsvorm, die een eigen autonomie kent. De vorm die voor de hand ligt, is die van een proces, dat zich afspeelt op tactisch niveau (inrichting) en dat zich vooral ook afspeelt op het gebied van informatie- en communicatiemanagement (met name planning en control).
Kortom: de vertaling van Strategische Eisen naar Technische Maatregelen dient procesmatig plaats te vinden, waarbij (door de verschillen in tijdshorizon) er verschillende procescycli gelijktijdig, maar gestructureerd, in uitvoering zijn.
In de onderstaande figuur wordt binnen de projectie van het Ankermodel op het 9-vlak de procesinrichting vormgegeven.



Figuur 4-1 Communicatielijnen

Zoals geschetst raakt de buffer meerdere vlakken en vindt de vertaalslag plaats conform de communicatiestromen zoals die binnen het 9-vlak zijn gedefinieerd, met dien verstande dat de concrete vertaling op een autonome wijze, geheel transparant (of wellicht geheel ondoorzichtig) binnen de buffer plaatsvindt. Er is sprake van een onafhankelijkheid tussen strategie en techniek. Maar ondanks deze onafhankelijkheid bestaat toch de mogelijkheid om, weliswaar op een indirecte wijze, een gewenste vertaalslag tussen strategische eisen en technische maatregelen te maken. Het tactische proces bepaalt welk coördinatiemechanisme wordt gehanteerd. In de onderstaande figuur worden twee mogelijke procesgangen weergegeven:



Figuur 4-2 Procesflow

Hoewel sprake is van een autonome verantwoordelijkheid voor het tactische bufferproces, moet dit proces wel in staat zijn aan te geven op welke wijze een invulling is gegeven aan de verantwoordelijkheid en kan moet het proces ook in staat zijn te verantwoorden op welke gronden de verschillende keuzes en afwegingen zijn gestoeld. Het eindresultaat mag in bovenstaande situatie min of meer hetzelfde zijn, de boodschap zal afhankelijk van de procesgang op een andere manier verwoord moeten worden. Ook dat hoort tot de autonome verantwoordelijkheid van het proces.

4.2. BEVEILIGING ONDER CONTROLE?

Het probleem van de ontbrekende, maar toch gewenste afstemming tussen de strategische bedrijfseisen en de technische beveiligingsmaatregelen lijkt nu in afdoende mate opgelost. Het nieuwe model heeft de kracht om het aspect informatiebeveiliging te adresseren. Voor de concrete invulling ervan moet nu alleen nog getracht worden het aspect beveiliging procesmatig in te richten. Voor deze inrichting volstaat het om aan te sluiten bij het binnen ITIL beschreven proces Security Management. Dit proces is als laatste boekwerk binnen de ITIL documentatiereeks opgenomen. Het proces is binnen ITIL als tactisch proces gepositioneerd. Als vastgesteld kan worden dat de procesbeschrijving voldoet aan de in het model gestelde eisen zou getoetst kunnen worden of deze theoretische beschouwing in de praktijk toegepast kan worden.

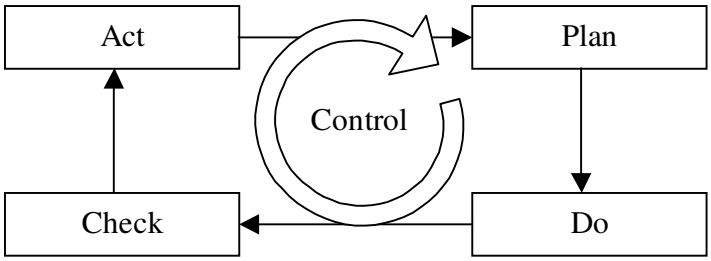
4.3. ITIL

De IT Infrastructure Library omvat een verzameling boekwerken waarin de *best practices* voor het exploiteren van een ICT beheer organisaties staan beschreven. Deze best practices zijn opgesteld door in de praktijk van grotere ICT organisaties het beheer te analyseren en de succesfactoren in beeld te brengen. Kenmerkend voor de ITIL beschrijvingen is dat alle beheeractiviteiten zijn onderverdeeld in processen. Het op deze wijze in kaart brengen van alle beheeractiviteiten moet dan ook gezien worden in de ontwikkeling van ICT organisaties van de traditionele rekencentra, waarin het beheer zeer geformaliseerd was en alle activiteiten door specialisten werden uitgevoerd, naar ICT dienstverlenende organisaties, die ten behoeve van de klanten een veelheid aan infrastructuren en diensten op een beheerste manier, maar met beperkte middelen moeten leveren. Deze ontwikkeling loopt gelijk met de verandering van de centrale automatisering via de client server architecturen naar de netwerk omgevingen waarin de PC een prominente plaats inneemt en door de groter wordende betrokkenheid van de eindgebruikers de invloed van de specialist (de baas van de machine) kleiner wordt. Om in deze veranderende situatie de beheersing te kunnen blijven garanderen, moet het beheer op een andere wijze worden ingericht. Het INK-model (zie Appendix 2) kent ook deze kanteling, van de activiteiten gerichte organisatie naar de procesgerichte organisatie. Ook de volgende INK-fase (van de procesgerichte naar de ketengerichte organisatie) doet overigens al opgeld, hierover in het kort meer in de casusbeschrijving in hoofdstuk 5.

Binnen ITIL worden processen onderkend op zowel het Strategische, als het Tactische en het Operationele niveau. ITIL zelf kent feitelijk nog geen best practices op strategisch niveau. De processen op tactisch en operationeel niveau zijn wel al (grotendeels) beschreven.
Kenmerkend voor de operationele processen is dat sprake is van een procesbeschrijving die in een werkstroom uitmondt. Ofwel er is sprake van het input → verwerking → output model, waarbij de output van de ene processtap input voor de volgende processtap kan zijn. Elk proces wordt door een proceseigenaar ingericht. De verschillende operationele processen kennen een logische volgorde,

waarin (het is immers een best practice) bij voorkeur geen proces wordt overgeslagen. Voorbeelden van operationele processen zijn het Helpdesk proces, Incident Management en Change management. Het Operations Management proces is het ultieme operationele proces, aangezien daarin feitelijk een opdracht wordt uitgevoerd. In appendix x wordt een visuele weergave van de procesgang gegeven.

De tactische processen zijn enigszins complexer van aard. Het standaard model is dat van de regelkring volgens de Deming Circle (zie [smbg1996] en Appendix 3). Daarbij is sprake van een iteratief proces, waarin de processtappen achtereenvolgens doorlopen worden. De Deming Circle kent 4 processtappen:



Figuur 4-3 Deming Circle

De eerste fase, de planning fase, omvat het opstellen van kaders/richtlijnen. In de tweede fase worden deze richtlijnen geëffectueerd. Vervolgens wordt gecontroleerd of aan de richtlijnen is voldaan, waarna, in de 4e fase, besloten kan worden tot ingrijpen. Dat houdt in dat ofwel de kaders gewijzigd dienen te worden of dat in de implementatie moet worden ingegrepen.

Teneinde de procesgang te bewaken moet er wel een coördinerend subproces bestaan, aangezien een proceseigenaar niet verantwoordelijk kan zijn voor een logische, planbare, werkstroom. Om die reden wordt een vijfde subproces toegevoegd, het Control proces. Dit proces ligt over de 4 andere subprocessen heen en is onder meer verantwoordelijk voor de feitelijke inrichting en de sturing.

De processen Capacity Management (gericht op het waarborgen van het gewenste serviceniveau op het gebied van performance en capaciteit) en Security Management zijn voorbeelden van processen die op deze wijze kunnen worden ingericht.

Doordat dergelijke processen Tactische processen zijn, ontstaat van nature een coördinatieprobleem. Deze processen moeten ingrijpen in de operationele processen, die feitelijk voor de operatie verantwoordelijk zijn. Een wijziging in de infrastructuur die bijvoorbeeld opgelegd wordt door het proces Capacity Management, moet via de reguliere change procedure uitmonden in een daadwerkelijk wijziging. Deze wijziging wordt feitelijk door het Operations Management proces doorgevoerd en wordt binnen het Configuration Management proces vastgelegd. De output van het ene operationele proces is de input voor het volgende.

Uit deze analyse blijkt overigens dat het traditionele alignment probleem, ofwel de kloof die bestaat tussen de business en de IT, voor dergelijke tactische processen niet lijkt te bestaan. Doordat op allerhande vlakken communicatie moet bestaan (wat wil de business, wat kan de techniek nu

bieden, wat biedt de markt), ontstaat er een vorm van alignment over het business aspect en het IT aspect heen. Deze alignment is noodzakelijk om een effectieve werking van het proces te waarborgen. Het proces zelf is dus het alignment mechanisme.
Met deze constatering is het alignment probleem zelf niet opgelost, maar de zoektocht naar een besturingsmodel kan beperkt blijven tot de initiële vraag naar de hiërarchische alignment. Misschien dat business alignment ook procesmatig op te lossen is, maar het vinden van een antwoord op die vraag wordt in dit onderzoek niet beoogd…

De relaties tussen tactische en operationele processen zijn complex. Om te voorkomen dat monopolisering van procesrelaties plaatsvindt (ofwel dat een proces een hogere prioriteit dan andere processen heeft en dat dit proces zich onttrekt aan de invloed van de overige processen), kan gesteld worden dat de tactische processen aspectsturing op de operationele processen uitvoeren. Om coördinatieproblemen binnen de procesketen te onderdrukken worden procesafspraken tussen de tactische en operationele processen gemaakt. In matrixvorm ziet dat er bijvoorbeeld als volgt uit (in dit schema wordt op geen enkele wijze juistheid of volledigheid gepretendeerd):

Tactische processen en aspecten	Operationele processen			
	Incident Mgt	Problem Mgt	Change Mgt	Config Mgt
Capacity Mgt	Monitoring	Escalatie	Baselines	Meting
Security Mgt	Classificatie van beveiligingsincidenten	Autorisatie richtlijnen	Baselines	Classificatie
… etc.				

Tabel 1Aspect sturing

Er bestaat wel een zwakheid van een organisatievorm waarin aspectsturing plaatsvindt:
Hoe is de onderlinge functionele sturing tussen de aspecten gewaarborgd, ofwel hoe kan (bijvoorbeeld) Security Management het proces Capacity Management aansturen ten aanzien van het aspect beveiliging? Deze vraag wordt in dit onderzoek niet uitputtend beantwoord, maar in de casusbeschrijving blijkt dat er in onderlinge procescontracten wel concrete afspraken gemaakt kunnen worden.

4.4. TOTAL QUALITY MANAGEMENT

Op dit punt aangekomen kan wellicht een verdere verbetering aan het model worden aangebracht om (bezien vanuit de kwaliteitsgedachte) een nog meer structurele en logische inbedding te realiseren. Binnen de theorie van Total Quality Management (TQM, zie appendix 3) wordt onderkend dat een procesmatige inrichting (onder andere door waarnemen en experimenteren) leidt tot een kwaliteitsverbetering. Daarbij worden verschillende soorten processen onderkend. In [smbg1996] wordt een modelmatige uitwerking van TQM beschreven, die wellicht voor het onderhavige vraagstuk een oplossing biedt.

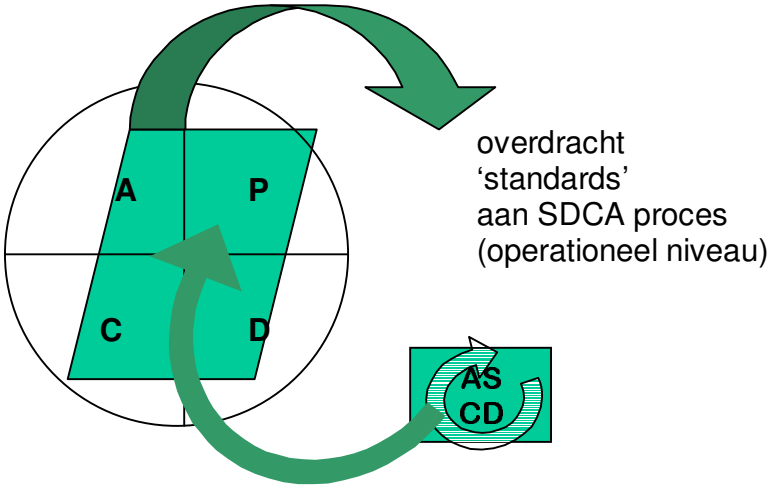
Naast de al genoemde Deming Circle van de variant Plan-Do-Check-Act (PDCA), wordt ook een proces van de variant Standard-Do-Check-Act (SDCA) gedefinieerd. Het verschil is dat het SDCA proces op operationele activiteiten betrekking heeft, terwijl PDCA als een kwaliteitsverbeterproces wordt benut. De Standard die wordt benoemd, heeft alles te maken met de te hanteren kaders, ofwel normen, werkinstructies en richtlijnen. De Do-fase betekent in dit proces: voer de werkzaamheden uit conform de Standard. Ook de Act is enigszins afwijkend, in die zin dat reactief een aanpassing in

de operatie wordt doorgevoerd als dat nodig mocht blijken op grond van de uitgevoerd Checks.

Het PDCA procestype komt overeen met het in de voorgaande paragraaf gedefinieerde model, met dien verstande dat de Act-fase betekent dat een Standard gedefinieerd wordt. Deze standard komt tot stand na de gePlande oplossing (de normen/kaders), die in een proefsituatie (Do) geanalyseerd en getest zijn (Check), te formaliseren.

Als dit model wordt gepositioneerd naast het ITIL procesmodel, blijkt dat er een proceshiërarchie is beschreven. Het PDCA proces levert de standaarden die binnen het SDCA proces worden gehanteerd. Binnen deze proceshiërarchie wordt ook een feedback mechanisme onderkend. Enerzijds moeten beide processen natuurlijk gestart worden, anderzijds moeten er ook standaard uitwegen ('traps') in een proces zijn om te voorkomen dat op een onjuist ingeslagen weg wordt voortgegaan. In zo'n trap wordt op enig moment gedurende een operationeel proces gewacht op aanvullende of nieuwe Standards. Hierbij is het operationele proces de trigger voor het tactische proces. De vraag is of en zo ja, welk proces leidend is wordt in dit onderzoek niet uitgewerkt.
Binnen het TQM model maakt dat niet heel veel uit, aangezien zowel proactieve als reactieve kwaliteitsverbetering bestaat. In proactieve zin wordt vanuit het PDCA proces een aanpassing van standards doorgevoerd. In het reactieve model levert het operationele proces de trigger tot kwaliteitsverbetering, die zal leiden tot aanpassing van de Standards.

De aanpassing van een deel van het Anker-model op basis van de TQM inzichten worden in de volgende figuur weergegeven. Het PDCA proces levert vanuit de Act-fase de standards op die in het operationele SDCA proces worden gehanteerd. Daarbij zal vanuit de Check/Act fase in het SCDA proces waar nodig een uitstapje richting PDCA proces gemaakt moeten worden



Figuur 4-4 TQM communicatielijnen

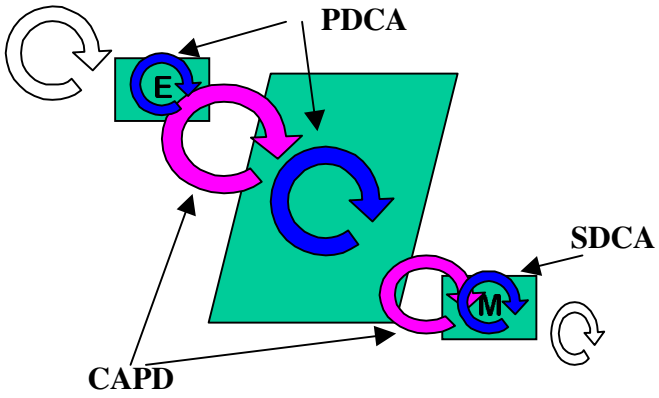
In dit schema ontbreekt nog het strategische niveau. Ook op dat niveau zou een PDCA proces moeten worden gedefinieerd. De plaats van dat proces is niet zeer belangrijk, wel relevant is dat de output van dat strategische proces een trigger is voor de start van het PDCA proces. De resultaten van dit PDCA proces (de door het tactische proces gedefinieerde Standards die in het SDCA proces worden gehanteerd) moeten permanent worden getoetst aan de strategische kaders.

Binnen TQM wordt een derde procescyclus onderkend. Naast PDCA (de ontwikkelcyclus) en SDCA (de operationele onderhoudscyclus), wordt ook een CAPD cyclus beschreven. Deze cyclus wordt ook wel de verbetercyclus genoemd. Het lijkt erop dat we met name deze verbetercyclus kunnen inbedden in het model om daarmee het besturingsmodel te beschrijven dat in staat is om de gewenste vertaalslag tussen strategisch en operationeel niveau te realiseren.

4.5. ENHANCED SECURITY MANAGEMENT

4.5.1. Ontwerp ESM

Op grond van deze verworven inzichten lijkt het mogelijk om het verbeterde ankermodel in een beperkte mate aan te vullen. Geconstateerd kan worden dat op het operationele niveau feitelijk allen sprake kan zijn van een SDCA procesmodel. Op dit niveau vindt de operatie plaats conform de door het tactisch niveau ontwikkelde normen en richtlijnen (lees PDCA). Het tactische niveau is verantwoordelijk voor het stellen van kaders op grond van de door het hogere strategische niveau gedefinieerde richtlijnen/normen. Op dit tactische niveau zijn deze strategische normen als Standard te beschouwen. Dat houdt dus in dat op strategische niveau ook (zij het wellicht onbewust) een PDCA proces wordt uitgevoerd.
Het herziene, verbeterde ankermodel ziet er nu als volgt uit:



Figuur 4-5 Besturingsmodel

Kenmerkend in dit model is met name het onderscheid tussen de inrichting van het strategische en tactische niveau. Vanuit deze verschillende processen (zowel planning en realisatie) wordt de output geleverd die het verbeterproces (CAPD) activeert. De verantwoordelijkheid voor dit CAPD proces is belegd bij het tactische proces.
Hiermee is gewaarborgd dat niet alleen de top-down en bottom-up koppelingen tussen de opeenvolgende niveaus zijn gerealiseerd, maar dat ook een structurele overall beoordeling van het gehele beveiligingssysteem plaatsvindt. Dat impliceert dat sprake moet zijn van een autonome verantwoordelijkheid voor de inhoud van het proces. In het kader van de eisen vanuit het aspect Security Management zou daarmee een voorwaarde vervuld zijn. En daarmee is het gewenste besturing van het Security Management proces een feit.
En weinig weerhoudt ons ervan om dit besturingsmodel Total Security Management te noemen

(naar analogie van de Hoshin TQM terminologie, zie Appendix 3). Maar omdat niet zeker is dat er geen beter besturingsmodel te ontwikkelen is, komt de term 'Enhanced Security Management' eerder in aanmerking.

4.5.2. Inrichting ESM

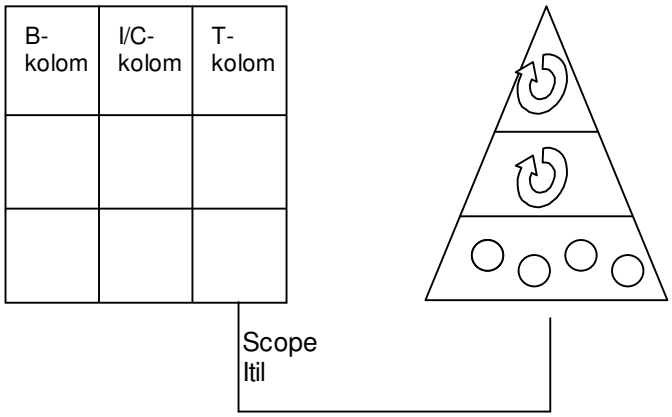
Gegeven het model van Enhanced Security Management, wat is dan de relatie tussen het besturingsmodel en de daadwerkelijk organisatievorm?
Deze vraag is eigenlijk niet zonder meer te beantwoorden. Toepassing van bijvoorbeeld de ITIL structureringsmethodiek betekent dat de modellen volledig op de eigen organisatie moeten worden toegesneden, er is niet een standaard blauwdruk voorhanden [bere2001].

Vanuit het ESM model kunnen we wellicht wel een aanzet geven tot het integreren van het proces binnen een organisatie. Dat op het gebied van de al genoemde tactische processen sprake is van standaardisatie van (primaire) processen en producten (namelijk die welke het resultaat zijn van de PDCA processen) leidt namelijk tot de conclusie dat daarmee ook een effectieve organisatievorm vastgesteld kan worden.
In de managementtheorie wordt door Mintzberg een model aangereikt dat aansluit bij de ESM procesinsteek. In zijn boek Structures in Fives [mint1983] beschrijft hij een vijftal basisfuncties in organisaties. Naast de lijnorganisatie (top management, lijnmanagement en het operations proces) definieert hij de ondersteunende en de technocratische afdelingen. Deze laatste afdelingsvorm is bij uitstek het organisatieonderdeel dat de standaardisatie ten behoeve van de primaire processen uitvoert. Dat omvat met name het voorschijven van directieven, waarmee de staf feitelijk de functionele aansturing van de overige organisatieonderdelen verzorgt.
Vanuit deze visie, ligt het voor de hand om de beveiligingsdeskundigheid buiten de hiërarchische organisatie te plaatsen. Vanuit de functionele eis vanuit informatiebeveiliging wordt daarmee gelijktijdig de gewenste onafhankelijk positie gewaarborgd.
De uiteindelijke verantwoordelijkheid voor het aspect beveiliging hoort echter uitdrukkelijk binnen de hiërarchie te zijn belegd.

4.5.3. En de relatie met ITIL

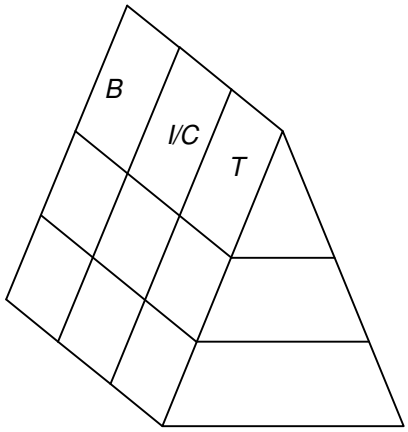
De vraag komt op wat nu eigenlijk het wezenlijke verschil is met de ITIL structuur: ook ITIL beschrijft de procesmatige inrichting van Security Management op het tactische vlak.
Het ESM model bouwt grotendeels op dat model als het gaat om de inrichting op tactisch niveau. Waar het model verder gaat, is dat feitelijk een derde dimensie aan het ITIL model wordt toegevoegd. Daar waar ITIL zich richt op het beschrijven van de processen in een ICT-diensten verlenende organisatie, voegt het ESM model de relatie met de 'business'toe. Daarmee kan dan niet alleen het ankermodel worden geplaatst in het kader van het 9-vlak, maar is ook het ITIL model te relateren aan deze structuur. Het is nu duidelijk dat Security Management deel uitmaakt van het totale bedrijfsbeleid op het gebied van informatiebeveiliging (zie ook het model van Berends [bere2001])

De beide relevante modellen naast elkaar:



(omwille van de eenvoud is de scope van ITIL beperkt tot de laatste kolom: ITIL beschouwt echter ook een deel van de I/C kolom, aangezien ITIL niet alleen betrekking heeft op de technische component, maar ook de inrichting en verantwoording ten opzichte van de bedrijfsprocessen onderkend (bijvoorbeeld de relatie met Service Level Management).

Dat leidt tot het volgende model, waarbij het voorstel deel van de piramide het ITIL beschouwingsgebied is:



Het ESM model maakt het mogelijk een integraal beveiligingsbesturingsmodel te onderkennen, waarin zowel het alignment model als de inrichting van het tactische proces Security Management een plaats vinden..

5. CASE STUDY BELASTINGDIENST

5.1. AUTOMATISERING IN HET GROOT

De Belastingdienst behoeft als organisatie nauwelijks enige toelichting. De organisatie is binnen het departement van Financiën verantwoordelijk voor de primaire processen Heffing, Inning van belastinggelden en het uitvoeren van Controle op de door de Belastingplichtigen op de juiste wijze voldoen aan de verplichtingen die de verscheidene wetten hen opleggen. Ook de Douane maakt onderdeel uit van de Belastingdienst en is binnen de organisatie met name verantwoordelijk voor de heffing van invoerrechten en accijnzen. Bij de Belastingdienst zijn circa 30.000 medewerkers in dienst.
Het beveiligen van informatie is voor de Belastingdienst niet alleen een interne doelstelling. Als overheidsorgaan is de Belastingdienst op het gebied van informatiebeveiliging gehouden aan overheidsbrede regelgeving, namelijk het Voorschrift Informatiebeveiliging Rijksdienst 1994 [vir1994].

De Belastingdienst is op grote schaal geautomatiseerd, vrijwel alle productieprocessen vinden geautomatiseerd plaats. De mate van automatisering van bijvoorbeeld het heffingsproces is zo hoog, dat circa 70% van de aangiften niet meer handmatig door een Belastingdienstmedewerker worden beoordeeld.

De automatisering van de verschillende processen wordt door de Belastingdienst nagenoeg volledig in eigen beheer uitgevoerd. Vanuit de oogpunten van effectiviteit en efficiency, zijn nagenoeg alle ICT georiënteerde activiteiten in één organisatie ondergebracht, namelijk het Belastingdienst/centrum voor ICT (het B/CICT). Voor 1 januari 2002 werd een aantal ICT-gerelateerde processen uitgevoerd door enkele beheerorganisaties binnen de Belastingdienst. Het betrof met name functionele beheer taken [looi2000] en delen van het ontwikkelproces (met name de fase van informatieanalyse). Deze casus beschrijft grotendeels de situatie van voor 1 januari 2002, toen het rekencentrum opereerde onder de naam Belastingdienst Automatiseringscentum (het B/AC). Vandaar dat in deze casus hoofdzakelijk over het B/AC wordt geschreven.

In de case study wordt in eerste instantie het model getoetst aan de situatie binnen het B/AC. Vervolgens wordt het B/CICT procesontwerp geconfronteerd aan het model.
Opgemerkt wordt wel dat deze casus niet representatief is voor de gemiddelde interne ICT-afdeling van een organisatie. Zowel de absolute omvang als bijvoorbeeld het feit dat de Belastingdienst in de volle maatschappelijk belangstelling staat, maakt dat er relatief beduidend meer middelen beschikbaar zijn om informatiebeveiliging grootschalig op te zetten. De opgedane ervaringen zijn echter wel voldoende relevant om als casus te presenteren.
Ook is deze case study niet geheel dekkend voor het ESM model. De reden daarvoor is dat het nauwelijks mogelijk is om voor deze grote organisatie het volledige vakgebied Informatiebeveiliging te beschrijven, de nadruk ligt op Security Management.

5.2. BELASTINGDIENST AUTOMATISERINGSCENTRUM

Het rekencentrum van de Belastingdienst (B/AC) is gevestigd in Apeldoorn. Het is met ruim 3000

medewerkers een van de grootste rekencentra in Nederland. Het B/AC kent verschillende sectoren. De grootste zijn de sector Systeemontwikkeling (circa 1200 medewerkers die zich bezig houden met de ontwikkeling van informatiesystemen), de sector Systeemintegratie (200 medewerkers, die betrokken zijn bij de ontwikkeling en levering van ICT-Infrastructuur) en de sector Beheer en Exploitatie (ook 1200 medewerkers). De sector Beheer en Exploitatie (BE) is verantwoordelijk voor het op een effectieve en efficiënte wijze beheren en exploiteren van de infrastructuur en applicaties van de Belastingdienst.

In 1996 is binnen de sector BE begonnen met het op een gestructureerde wijze inrichten van de beheerprocessen. Daarbij werd ingehaakt op de initiatieven van de Nederlandse Kwaliteitsprijs [ink1993]. In het INK model wordt de groei van een onderneming van productgericht naar Totale Kwaliteit beschreven[5].
De sector BE van het B/AC verkeerde voor 1996 in het productgerichte stadium. Elk platform en elke component werd op een eigen wijze beheerd. De doelstelling was dan ook om binnen het voorziene groeimodel eerst te komen tot een procesgerichte organisatie. De structurering die daarbij voor organisaties in de ICT branche een gangbare is, wordt geboden door de documentatie van ITIL.

5.2.1. Procesgericht werken

Binnen de Sector Beheer en Exploitatie van het Rekencentrum van de Belastingdienst wordt sedert enkele jaren procesgericht gewerkt, waarbij ITIL in eerste instantie leidend is geweest. Ook het tactische proces Security Management is opgezet conform de (in paragraaf 3.3) beschreven procesgang. De vijf vermelde subprocessen zijn overgenomen, waarbij echter wel een essentiële aanpassing heeft plaatsgevonden. Het proces is (net als in de ITIL modellering) als tactisch proces gepositioneerd, maar ook de inbedding heeft uitsluitend op tactisch niveau plaatsgevonden. Dat houdt in dat de procesmanager slechts een tactische verantwoordelijkheid heeft. En dat komt er weer op neer dat de feitelijke uitvoering (de implementatie van de kaders, richtlijnen, baselines) door de operationele organisatie plaatsvindt. Daardoor is het proces Security Management (SeM) niet verantwoordelijk voor de feitelijk implementatie, maar voor het doen implementeren. Dat impliceert dat er een relatie moet bestaan tussen SeM en de operationele processen (te denken valt aan Operations Management).
Binnen het B/AC betekent dat zoveel dat er binnen de operationele processen procesmanagers ‘type 2’ worden gepositioneerd die verantwoordelijk zijn voor het behartigen van de belangen van de tactische processen. Deze procesmanager van het Type 2 maakt geen deel uit van het tactische proces, maar van het operationele proces. Hij is wel verantwoording verschuldigd aan de procesmanager van het Tactische proces (de ‘Procesmanager Type 1’).

Net zoals dat geldt voor het implementeren (Do) van de richtlijnen, geldt ook voor het evalueren (Check) dat de feitelijke uitvoering buiten de verantwoordelijkheid van het Tactische proces valt. SeM is derhalve verantwoordelijk voor het doen uitvoeren van de evaluatie, die feitelijk in gang wordt gezet door onder meer de Procesmanager Type2. Deze evaluatie wordt deels vorm gegeven in de Security Scans die zijn gebaseerd op de richtlijnen. Hiermee valt het Planning en Control proces ten behoeve van het tactische proces onder de verantwoordelijkheid van de PM1. De feitelijke uitvoering is de verantwoordelijkheid van het operationele proces.

[5] Het INK model onderkent de volgende fasen:
Productgericht, Procesgericht, Systeemgericht, Ketengericht en Totale Kwaliteit, zie appendix 2

Door deze subtiele aanpassing van het ITIL model is een natuurlijke functiescheiding gecreëerd die een aanvullende waarborg kan zijn voor het te bereiken kwaliteitsniveau.

5.2.2. Proces Security Management

Rollen

Het proces Security management wordt bemenst door verschillende beveiligingsexperts die ieder een eigen specialiteit hebben. Zijn voeren hun werkzaamheden op grond van hun functie uit vanuit beveiligingsrollen. Zo zijn er deskundigen op de gebieden Mainframe en Netwerken. Deze deskundigen worden beveiligingsbeheerder genoemd.
Binnen het proces zijn verschillende andere rollen gedefinieerd, zoals de beveiligingsmonitor, de beveiligingsarchitect.
Het proces zelf is een tactisch proces, hetgeen inhoudt dat de medewerkers binnen het proces zelf geen operationele taken uitvoeren. Aangezien de meeste activiteiten op het gebied van beveiliging operationele taken zijn, bestaat de behoefte om in de operationele processen en afdelingen ook beveiligingsrollen te definiëren. De belangrijkste binnen het proces gehanteerde rollen zijn die van Security Officer en Security Administrator. De Security Officer wordt functioneel door de Beveiligingsbeheerder aangestuurd. Zijn taak is het in de operationele processen en afdelingen toezien op het handhaven van het door de beveiligingsbeheerder gedefinieerde beveiligingsniveau. De security officer is een reguliere lijnfunctionaris.
De Security Administrator is de functionaris die het ontwerp van de beveiligingsregels vastlegt in de beveiligingsomgeving. De administrator definieert bijvoorbeeld de beveiligingsprofielen voor de logische toegangsbeveiliging van infrastructuurcomponenten (bijvoorbeeld een beveiligingspakket als RACF).

Subprocessen

Plan/kaderstellen
De planfase omvat het stellen van beveiligingskaders, die worden zichtbaar gemaakt in de Operationele Beveiligingsrichtlijnen. In deze richtlijnen vindt de vertaling van de tactische normen naar operationele maatregelen plaats. De Beveiligingsbeheerder is verantwoordelijk voor de vertaling van de redelijk abstracte normatiek naar concrete (meestal technische) maatregelen, vaak tot op parameter niveau.
Maatregelen zijn onder te verdelen in preventieve, detectieve, correctieve en repressieve maatregelen.

Do/Implementeren
In het kader van SeM betekent dit het doen implementeren van de gestelde kaders. Ofwel ervoor zorgdragen dat de richtlijnen in de praktijk worden ingevoerd. Dat betekent dat de productbeheerders ertoe aangezet moeten worden om de beheerde componenten zodanig in te richten dat het vereiste beveiligingsniveau wordt bereikt. Het mag duidelijk zijn dat het verhogen van het niveau van beveiliging in een going concern niet eenvoudig is. De gevolgen zijn niet altijd evident en de kosten die ermee gemoeid zijn kunnen niet altijd op de klant verhaald worden.
Om die reden trachten de Beveiligingsbeheerders al aan het begin van het ICT voortbrengingsproces de richtlijnen als eisenpakket vanuit de beheerorganisatie mee te laten nemen, zodat het in het offertetraject meegenomen kan worden en implementatie niet leidt tot negatieve bijeffecten.

Check/Evalueren
In de BAC/BE situatie omvat deze fase het reageren op beveiligingsincidenten, beoordelen van de rapportages zoals uitgebracht door de interne accountantsdienst en de interne controlefunctie, alsmede het reageren op de resultaten van de uitgevoerde security scans.

Deze werkwijze wijkt in dezelfde mate af van het in ITIL beschreven proces, dat ook een meer tactische benadering wordt gekozen. SeM is zelf niet verantwoordelijk voor de daadwerkelijke uitvoering van de audits, noch voor het oplossen van bijvoorbeeld beveiligingsincidenten. Deze verantwoordelijkheid is wederom belegd bij de operationele (lees lijn-) afdelingen en processen. Het behoort tot de verantwoordelijkheden van de beveiligingsbeheerders om daarover afspraken te maken met deze uitvoerende organen.

Dit subproces levert de input voor de beoordeling van het effect van het proces. Kern is dat in dit proces aangetoond wordt dat het afgesproken niveau van beveiliging daadwerkelijk wordt gerealiseerd. Daarbij kan onder meer gedacht worden aan het opleveren van de noodzakelijke managementinformatie betreffende van het aantal beveiligingsincidenten.

Correct/Onderhouden
Dit subproces is op dit moment wellicht onvoldoende ingericht. De reden hiervoor is dat in de ITIL documentatie (vertaling zie IOC) het proces als *onderhoud* is benoemd. Onderhoud tendeert naar een proces waarin een bestaande situatie wordt aangepast om aan de tand des tijds weerstand te kunnen bieden. Dat betekent bijvoorbeeld dat richtlijnen worden aangepast om gebleken lacunes op te kunnen vullen. Op die manier is in ieder geval wel een invulling te geven aan het going concern, maar de relatie met de Deming Circle is hiermee wel verdwenen, immers er bestaat na onderhoud geen relatie met kaderstellen. Feitelijk is onderhoud op deze manier ook een vorm van kaderstellen. De cirkel is daardoor onderbroken. Momenteel wordt het subproces dan ook ingevuld op een manier die recht doet aan de procesgedachte: in deze fase wordt beoordeeld wie verantwoordelijk is voor onvolkomenheden in het beveiligingsniveau: het tactische proces (in welk geval het subproces kaderstellen wordt getriggerd) of het operationele proces (in welk geval getracht wordt de implementatie te laten wijzigen (trigger voor het Do-subproces). Doordat het proces als zodanig betrekkelijk recent is ingericht, is echter nog weinig ervaring met het onderhoudsproces, omdat er feitelijk nog geen producten zo ver in de levenscyclus zijn dat al onderhoud nodig is.

Control/Procesbeheersing
Dit subproces is betrekkelijk goed in kaart gebracht. Het subproces beoogt aan te geven of de procesmanager In Control is. Hoe dit waar te maken is feitelijk niet aangegeven. De vakliteratuur geeft hoe dan ook geen inzicht in het meten van de effectiviteit van het proces. Op dit moment wordt gestudeerd op het in kaart brengen van de Key Proces Indicators.
Een van de eerste resultaten van dit project is geweest dat een effectief proces niet noodzakelijkerwijs een hoog niveau van beveiliging oplevert. Het feit dat een procesmanager weet dat er knelpunten bestaan en dat er bijvoorbeeld een plan van aanpak voor verbetering van de situatie bestaat, kan wel binnen de evaluatie tot een positief oordeel omtrent het tactische proces leiden: de proces eigenaar is “in control”, maar dat wil dus in het geheel niet zeggen dat het niveau van beveiliging zelf afdoende is.
Binnen het B/AC is het proces in zoverre effectief, dat de proceseigenaar in een managementcontract zich aan meetbare grootheden heeft gecommitteerd (aantal richtlijnen, aantal afspraken, rapportagevorm) en dat er met andere proces en lijnmanagers afspraken omtrent onderlinge communicatie en coördinatie zijn gemaakt.

Resultaten

Binnen een jaar bleek dat het tactische deel van het proces Security Management daadwerkelijk beheerst werd. Uit de uitgevoerd interne controleprogramma's bleek dat de beheerdoelstellingen op tactisch niveau gerealiseerd waren. Ook zijn er stappen gezet om verschillende (onderdelen van) operationele processen effectiever in te richten[6].
Het op een effectieve manier inrichten van het gehele operationele deel van het proces (de daadwerkelijke uitvoering van de technische en organisatorische beveiligingsmaatregelen) bleek echter weerbarstiger dan de theorie en de ontwikkelde visie en modellen deed vermoeden, de goede Werking van het proces kon nog niet op alle operationele deelgebieden worden aangetoond.

Wie uiteindelijk, naast de proces eigenaar, met zo'n positief oordeel voor het tactische proces iets opschiet, is niet geheel duidelijk, als ook het daadwerkelijke beveiligingsniveau niet beheerst wordt. Vandaar dat het belangrijk is om vast te stellen dat het operationele security management proces ook een beheerst proces is.
Bovendien zijn nog enkele ander knelpunten niet opgelost. Zo bleek de afstemming van klant (de strategische vragensteller) naar de techniek onvoldoende ingericht. Dat was niet alleen te wijten aan de ICT organisatie, ook de klant is zich bewust van de lacunes. Ook de afbakening van taken, bevoegdheden en verantwoordelijkheden tussen de diverse spelers op het beveiligingsveld was onvoldoende doorgevoerd. Met name de vraag wie de *baas van beveiliging* was, de architecten (die producten en diensten ontwierpen) of de proceseigenaar en de beveiligingsbeheerders, bleek niet eenduidig te beantwoorden, al werd er in de informele relaties wel een werkbare situatie gecreëerd.

5.3. CENTRUM VOOR ICT

5.3.1. Organisatie

Voor de inrichting van het B/CICT is gekozen voor een andere structuur dan welke gangbaar was binnen het B/AC. De basisvorm is die van een matrixorganisatie. In eerste instantie is daarbij leidend de keten van processen die leidt tot dienstverlening aan de (interne) klant. Daarbij zijn de direct klantgerelateerde processen in de matrix als functionele sector benoemd en zijn de als ondersteunend aangemerkte processen als aspect aangemerkt. De matrix is als volgt vorm gegeven (de aspecten staan in de linkerkolom als rijen aangegeven):

Operatie / Aspect	Innovatie	Ontwikkeling	Continuïteit	Exploitatie	Dienstverlening
Inkoop.Mgt					
Architectuur					
Account.Mgt					
Resource.Mgt					
PFC					

Figuur 5-1 Besturingsmodel B/CICT

[6] Als voorbeeld geldt het change proces, waarin onderscheid wordt gemaakt tussen 'Soort'-changes en 'Exemplaar' changes. Elke Soort change wordt eenmalig getoetst aan de richtlijnen en expliciet geaccoordeerd. De exemplaren (ofwel, soortgelijke changes) worden binnen het operationele proces zelf beoordeeld (er wordt vastgesteld dat een exemplaar conform een goedgekeurde Soort change wordt uitgevoerd) en geaccoordeerd. Bezien vanuit de optiek van TQM is dan sprake van PDCA (de soort change) en SDCA (het standaard exemplaar).

De voorzitters van de 10 sectoren en aspecten vormen samen met de directie het management team van B/CICT.

Opvallend in dit model is dat wordt uitgegaan van functionele sturing door de aspecten (voor de medewerkers binnen de sectoren Innovatie en Ontwikkeling worden vanuit de sector (aspect) Resource Management ook de leidinggevende (dus hiërarchische) verantwoordelijkheden belegd). Er is (buiten een besturingsorgaan) niet voorzien in andere staforganen dat functionele sturing realiseert.
Een duidelijk voorbeeld van functionele sturing is te vinden in de sector Planning, Finance & Control (PFC). Deze sector voert aspectsturing uit zowel in de vorm van voorschriftgeving op het gebied van bijvoorbeeld de financiële verantwoording, als in de vorm van toezicht op naleving van deze voorschriften.

5.3.2. Security Management

Security Management is binnen B/CICT pas nadat het ontwerp van alle sectoren was afgerond, toegevoegd aan de sector PFC. De reden hiervoor was tweeledig: enerzijds was het niet gewenst de Beveiligingsdiscipline over te laten aan elk van de sectoren (ter voorkoming van kennisderving en eilandvorming) en anderzijds omdat ingezien werd dat Security Management zich hoofdzakelijk bezighoudt met het Planningsproces en het Controle proces (P&C) van beveiliging. Bezien vanuit die optiek is het dus logisch beveiliging als aspect binnen de organisatie neer te leggen: Beveiliging raakt alles, is een aspect van alle processen en producten.
Gezien de formele inrichting van de organisatie bleek het niet mogelijk om het aspect Beveiliging zelfstandig in de matrix op te nemen. Aangezien op tactisch niveau met name de deelprocessen Planning en Control worden uitgevoerd, is besloten om *beveiliging* in de Sector PFC op te nemen.
Een alternatief zou kunnen zijn om het aspect Security Management onder te brengen binnen de sector Architectuur, maar daarmee verliest Security Management wel de min of meer de gewenste onafhankelijke positie.

Grootste knelpunt lijkt nu te worden wat het mandaat van Security Management zal zijn. De functionele aspectsturing binnen de matrix is geregeld voor de 5 functionele sectoren (Innovatie tot Dienstverlening). Door de gekozen matrixvorm is echter geen rechtstreekse functionele relatie met de andere aspecten voorzien. Dat houdt in dat het niet eenvoudig is om aan te geven welk aspect verantwoording verschuldigd is aan welk ander aspect. Dit lijkt een belangrijke test case te worden bij de vaststelling van de (tactische) verantwoordelijkheid op het gebied van informatiebeveiliging.

5.4. UITKOMST CASE STUDY

Procesmatig werken is niet per definitie eenvoudig werken. Er bestaat een belangrijk aandachtspunt dat opgelost moet worden:
In de oude organisatie is veel ervaring opgedaan met procesmatig werken. Het op een procesmatige wijze realiseren van Security Management is haalbaar gebleken. De gestructureerde werkwijze maakt het daadwerkelijk mogelijk om een kwaliteitsaspect als Informatiebeveiliging te managen en om in control te geraken. Een effectieve werking levert ook een kwaliteitsverbetering op, met name door de structurele inbedding in het totale beheersysteem.

Op grond van de opgedane praktijkervaringen (zowel de positieve ervaringen als de zaken die nog

niet voldoende effectief werden ingericht) kunnen de volgende adviezen verstrekt worden:

- Draag zorg voor een permanente escalatie en terugkoppeling vanuit de operationele organisatie naar het tactische proces door het maken van onder meer onderlinge werkafspraken (realiseer een adequaat CAPD-proces binnen de verantwoordelijkheid van het Security Management proces);
- Zorg ervoor dat ook de terugkoppeling vanuit het tactische naar het strategische niveau zodanig wordt ingericht dat het strategische niveau zelf in staat is het tactische proces van kaderstelling, alsmede het resultaat daarvan te toetsen;
- Ondersteun de klant in het differentiëren van de gewenste beveiligingsniveau's. Dat is enerzijds nodig om efficiency te kunnen realiserente (het is niet oodzakelijk om altijd het hoogste niveau van beveiliging te realiseren) en om te voorkomen dat de te treffen beveiligingsmaatregelen nog steeds technology driven zijn (PKI is wellicht heel fraai, maar misschien de organisatie er nog niet klaar voor);
- Zorg voor een duidelijke afbakening van taken, bevoegdheden en verantwoordelijkheden. In het algemeen kan gesteld worden dat er een overlap bestaat in die zin dat strategen/architecten zich met operationele normen bezighouden en dat operationele medewerkers (bij gebrek aan inzicht) zelf normen definiëren. Deze overlapping komt de duidelijkheid niet ten goede. Gebruik het inrichten van het tactische proces Security management als instrument om de overlap uit te bannen.

Toetsing van het model aan het B/AC leidt tot de conclusie dat het model valide is, maar dat de organisatie nog niet zo ver is dat het model in de praktijk werkt.
Toetsing van het model aan B/CICT ontwerp is nauwelijks mogelijk, omdat op dit moment praktijkervaring ontbreekt. De toetsing geeft veeleer aanleiding te veronderstellen dat, uitgaande van de validiteit van het model, het beleggen van de taken en bevoegdheden voor het vakgebied in deze nieuwe situatie vermoedelijk tot competentiestrijd zal gaan leiden, aangezien in het ontwerp van B/CICT niet is voorzien in tactische, functionele, sturing.

5.5. EXTRAPOLATIE…?

De onderzoeksvraag richt zich op het tactische ITIL proces Security Management. Maar, wat weerhoudt ons ervan om daar waar Security staat dit te vervangen door de naam van een ander tactisch ITIL proces. Ofwel kan het Ankermodel toegevoegde waarde bieden voor bijvoorbeeld het tactische proces Capacity Management?

Het lijkt erop dat die vraag, in ieder geval voor B/CICT, positief te beantwoorden is. Met name wanneer de verbeterpunten, zoals ze zijn verwoord in paragraaf 5.4, in beschouwing worden genomen, kan geconstateerd worden dat de afstemmingen tussen de verschillende strategische, tactische en operationele processen procesmatig ingericht kunnen worden. Daarmee wordt het los van de overkoepelende organisatie en andere (gerelateerde) processen opereren van een proces (hetgeen ineffectief en inefficiënt kan heten) op een effectieve wijze voorkomen.

Dus misschien is het inrichten van het tactische proces Security management de opmaat voor het inrichten van andere tactische processen (wat op dit moment namelijk nog niet in gang is gezet). Of dit haalbaar is, zal wellicht in een latere studie onderzocht kunnen worden.

6. CONCLUSIES EN AANBEVELINGEN

We hebben kunnen constateren dat er een kloof bestaat tussen de strategische besluitvorming in een organisatie en de daadwerkelijke realisatie. In verschillende onderzoeken is getracht een verklaring te geven voor dit verschijnsel en om aan te geven of er een relatie bestaat tussen effectiviteit en efficiency van een organisatie enerzijds en structurering anderzijds.

In deze analyse is naar voren gekomen dat deze kloof tussen *strategie* en *techniek* misschien niet alleen onvermijdelijk is, maar dat deze kloof zelfs noodzakelijk is. Uit het ankermodel valt af te leiden dat tussen de Strategie en de Techniek een vorm van buffer moet bestaan om de frictie op te vangen die ontstaat doordat de tijdshorizon zo verschillend is.
De kloof is ook zeer wenselijk. Wanneer een 1 op 1 relatie zou bestaan, betekent dat tevens dat een starre structuur bestaat, waarbij enige flexibiliteit niet meer kan bestaan.

Uit de case study kunnen verschillende conclusies getrokken worden. De belangrijkste (waarbij aangehaakt kan worden bij het ankermodel) conclusies zijn deze:

- Het tactische proces lijkt het spilproces te zijn. Wanneer dit proces voldoende gemandateerd wordt, kan sprake zijn van een beheerst beveiligingsproces.
- Bij een aanpassing van de inrichting van het ITIL proces in die zin dat de relaties tussen het strategische en het tactische niveau en de relatie tussen het tactische en het operationele niveau procesmatig worden ingericht, wordt zowel aan de top-down benadering als aan de bottom-up benadering recht gedaan.
- Toepassing van het ESM model impliceert een onafhankelijk rol van het proces, dat in een stafachtige omgeving wel gepositioneerd dient te worden om functionele aansturing van de lijnorganisatie te kunnen garanderen.

Hieruit valt te constateren dat het Ankermodel een bruikbaar model is om het tactische proces Security Management in te richten.

Het slechts inrichten van een proces op tactisch niveau kan natuurlijk niet voldoende zijn, als daarbij de randvoorwaarden niet ingevuld worden:

- Het proces moet structureel ingebed worden in een organisatie. Daarbij dient de administratieve organisatie (met name de procesbeschrijving) goed gestructureerd worden met een adequaat ingeregeld proces van interne controle.
- Voor alles dient er committent te bestaan. Het management van een organisatie dient de verantwoordelijkheid voor het normeren van beveiliging over te dragen aan een betrekkelijk autonoom opererend proces.

Wanneer het tactische proces het mandaat krijgt om niet alleen beveiligingkaders te stellen, maar ook toe te zien op naleving, zal beveiliging niet alleen procesmatig binnen de techniek goed werken, maar lijkt het totale niveau van beveiliging organisatiebreed ook een positieve impuls te kunnen krijgen.

Als na toepassing van de ontwerpregels van het Ankermodel ook deze beide voorwaarden zijn vervuld, dan moet de conclusie luiden dat informatiebeveiliging binnen de organisatie wel degelijk kan zijn verankerd.

André Koot

APPENDIX 1: LITERATUUROVERZICHT

- [bang2001] Host Security, bangalorelabs, 2001, www.bangalorelabs.com/advisesec/knowledge_management/Host_Security_Microsoft.pdf
- [bere2001] Informatiebeveiligingsmodel met praktische inslag Paul Barends, 2001, IT Beheer 7, september 2001
- [cibo2000] From control to drift Ciborra and associates, 2000, ISBN 0 19 924663 7
- [code2000] Code voor informatiebeveiliging (NEN, BS7799, ISO 17799)
- [edp] Handboek EDP Auditing (Nivra, Kluwer)
- [erns2002] Global Information Security Survey, Ernst&Young, 2002, http://www.ey.com/GLOBAL/gcr.nsf/UK/Information_Systems_Assurance_&_Advisory_Services_-_Overview
- [fbi2002] 2002 CSI/FBI Computer Crime and Security Survey FBI, 2002
- [grin1995] Managing I.T. at Board level. Kit Grindley, 1995, ISBN 0 273 61305 7
- [ink1993] De Nederlandse Kwaliteitsprijs en Onderscheiding. T.W.Hardjono/F.W.Hes, 1993, ISBN 90 267 2074 2
- [iqd1998] TQM, Definition of Total Quality management, IQD Inc http://www.iqd.com/hoshin_def.htm
- [isma2002] International Security Management Association (ISMA) Survey ISMA 2001, www.securitymanagement.com/library/isma_executive0202.pdf
- [Itil1999] Security Management ITIL 1999, ISBN 011 330014 X
- [keen1991] Shaping the future. Peter Keen, 1991, ISBN 0 87584-237-2
- [kpmg2001] Global E-Fr@ud.Survey KPMG, 1991, http://www.kpmg.nl/site.dws?id=1677&process_mode=mode_doc&doc_id=13346
- [looi2000] Beheer van de informatiesystemen Maarten Looijen, 2000, Kluwer
- [maes1999] Reconsidering Information management Through a Generic Framework Rik Maes, 1999, Primavera.fee.uva.nl

- [mint1983] Organisatie structuren (Structures in fives: designing effective organizations)
  Henry Mintzberg, 1983, ISBN 90 5261-050-9

- [pols2000] Informatiebeveiliging onder controle: grondslagen, management, organisatie en techniek
  Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit, 2000, ISBN 90 430 0289 5

- [pols2000a]Informatiebeveiliging als beheersd proces
  Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit, 2000, Primavera.fee.uva.nl

- [pvhd2000] Het ontwerpen van een onderzoek
  Piet Verschuren, Hans Doorewaard, 2000, ISBN 90-5189-886-X

- [smbg1996] A formal model for Total Quality management
  S.C. van der Made-Potuijt, H. Boudewijn Bertsch, L.P.J. Groenewegen, 1996,
  www.few.eur.nl/few/research/pubs/cs/EUR-FEW-CS-96-05

- [trui2000] Het Strategic Alignment model als hulpmiddel bij IT-strategie advies
  O. Truijens, 2000, Primavera.fee.uva.nl

- [vir1994] Voorschrift informatiebeveiliging Rijksdienst (Min.v.Binnenlandse zaken)

APPENDIX 2: INK-MODEL

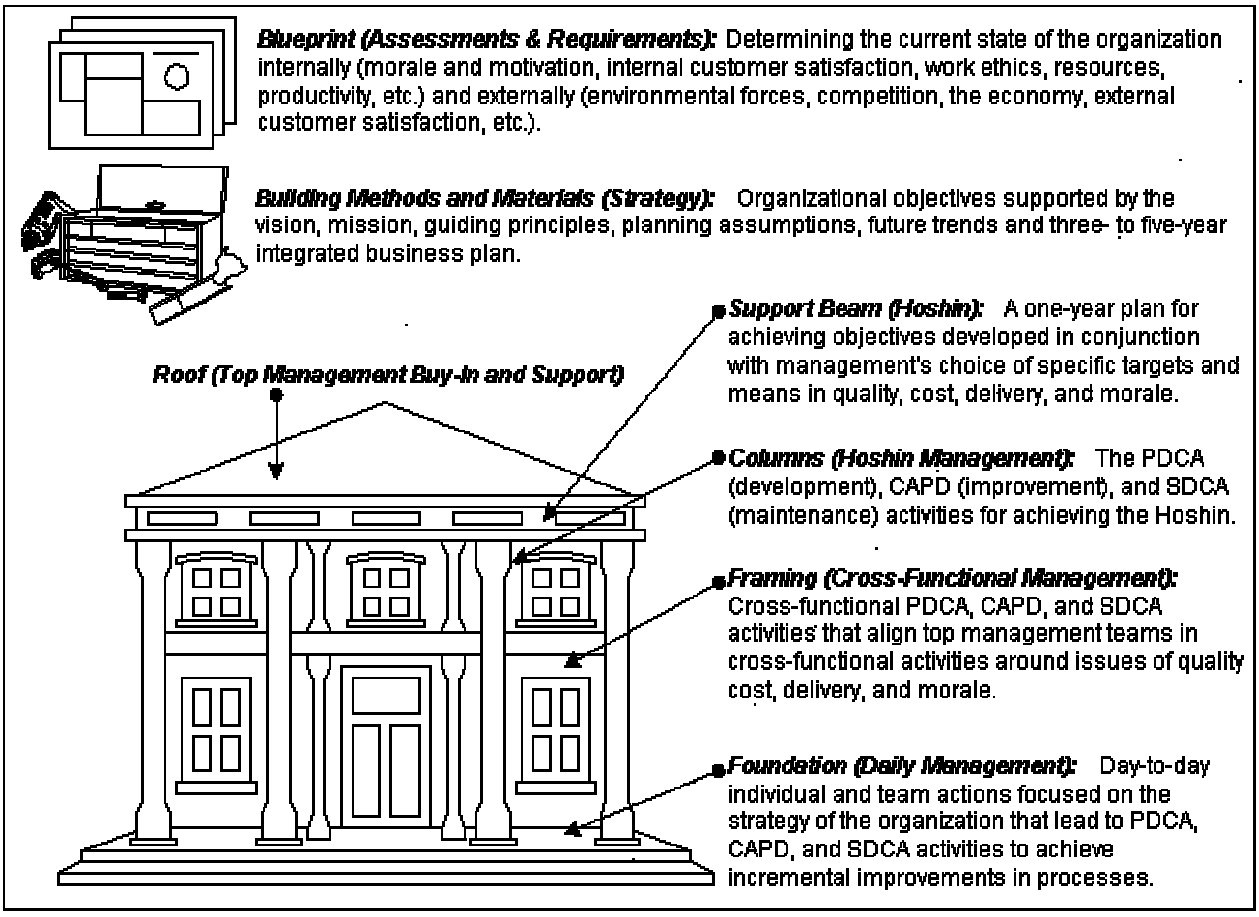
Het INK model van de Nederlandse Kwaliteitsprijs onderkent verschillende fasen waarin een organisatie groeit van een beperkt beheerst systeem naar een systeem dat volledig beheerst wordt in de zin van het gecontroleerd, conform afspraak bereiken van het beoogde kwaliteitsniveau.

De fasen en hun kenmerkend zijn

Fase	Enkele kenmerken
Product georiënteerd	Het proces richt zich op 'output controle', waarbij een gegeven normenkader als toetsingskader wordt gehanteerd. Belangrijke activiteit is meten.
Proces georiënteerd	Het wordt als onvoldoende efficiënt geacht om alleen de output te toetsen: alle kosten zijn reeds gemaakt, zodat afkeur duur is. Vandaar dat op alle tussenliggende meetpunten toetsing plaatsvindt en vastgesteld wordt of de leverancier voldoet aan de eisen en of de afnemer tevreden is..
Systeem georiënteerd	Geconstateerd wordt dat niet alleen het primaire proces een bijdrage aan de kwaliteit levert, maar dat de gehele organisatie, dus inclusief de ondersteunende diensten een bijdrage leveren.
Keten georiënteerd	Er is sprake van integratie met processen van de leverancier en die van de afnemer, zodat veel energie gestoken moet worden in de onderlinge afstemming.
Totale Kwaliteit	Het begrip kwaliteit is geïnternaliseerd in de gehele onderneming, sterker, er is een centrale visie die als basis wordt gehanteerd. Er wordt dan ook integraal afgerekend op het bereiken van de doelstellingen. Bestrijding van verspilling staat centraal.

APPENDIX 3: TQM-MODELLEN

"Total Quality Management is a structured system for satisfying internal and external customers and suppliers by integrating the business environment, continuous improvement, and breakthroughs with development, improvement, and maintenance cycles while changing organizational culture" [iqd1998].



Opgemerkt moet worden dat het TQM systeem gericht is op verbetering in een betrekkelijk kort tijdsbestek (in principe 1 jaar).

In [smbg1996] wordt ook een variant beschreven waarin een ander proces bestaat, namelijk het Manager proces. Dit proces stuurt beide andere (PDCA en SDCA) processen aan en zorgt (als enige) voor de procesoverdrachten. Er is geen rechtstreekse communicatie tussen beide DCA processen. Dat betekent in concreto dat de manager de operatie start en afhankelijk van de operatie kan besluiten om (reactief) een verbeterproces in de vorm van PDCA te starten.