Ontwikkelingen in de beheersing van ICT in de financiële sector

Drs. J.J. van Beek RE RA en drs. F.R. Schut RE RA

Ontwikkelingen in de beheersing van ICT van financiële instellingen verlopen stormachtig en meer en meer treden knelpunten en risico's aan het licht. Door de toegenomen complexiteit is het gevaar aanwezig dat niemand het overzicht meer heeft om de ontwikkelingen in de greep te kunnen houden. In dit artikel wordt een beschrijving van de ontwikkelingen en de knelpunten gegeven en een aantal nieuwe eisen aan moderne systemen afgeleid. Ook door toezichthouders worden voortdurend nieuwe eisen gesteld aan de beheersing van ICT. Door vervolgens een aantal oplossingsrichtingen te beschrijven worden handvatten gegeven voor het management, de ICT-organisatie en de IT-auditors om de noodzakelijke veranderingen te kunnen beheersen.

Inleiding

De laatste jaren is de markt voor financiële instellingen sterk in beweging geweest. Als gevolg van globalisering, veranderende regelgeving, technologische en demografische ontwikkelingen, de toegenomen welvaart en individualisering zijn de klantvragen en daarvan afgeleid de informatiebehoeften aanzienlijk veranderd. De financiële instellingen dienen zich steeds sneller aan te passen aan de veranderingen.

De concurrentie tussen financiële instellingen is sterk toegenomen op de markt en om de klanten te bereiken worden in toenemende mate verschillende distributiekanalen aangewend. In aanvulling daarop heeft een golf van fusies en overnames het landschap van de financiële marktpartijen opnieuw vormgegeven. In de concurrentiestrijd zijn productvernieuwing en het snel en efficiënt afhandelen van transacties belangrijke succesfactoren.

Informatie- en communicatietechnologie (ICT) vormt al jaren bij al deze ontwikkelingen een factor van belang in de diverse segmenten van de financiële sector. Dit geldt voor de individuele financiële instellingen, voor de koepelorganisaties en aanbieders van de gezamenlijke infrastructuren, en niet in de laatste plaats voor de partijen belast met het wettelijk toezicht op de markten. Het beheersen van het gebruik van ICT is binnen deze sector vroegtijdig opgepakt als object voor auditors. Met name het memorandum van De Nederlandsche Bank uit 1988 over dit onderwerp heeft een voortrekkersrol vervuld. Door het management van de instellingen, de interne en externe auditors én door de toezichthouders op de financiële markten is ICT-auditing ingepast in het geheel van maatregelen voor kwaliteitsbeheersing en -toetsing. In dit artikel wordt op hoofdlijnen inzicht gegeven in ontwikkelingen in het gebruik van ICT in deze sector en aangegeven welke belangrijke risico's en knelpunten daarbij optreden. Hieruit kunnen veranderde eisen worden afgeleid aan de informatievoorziening binnen de financiële sector. Ook wordt nadrukkelijk stilgestaan bij de ontwikkelingen in het beleid en optreden van de nationale en internationale toezichthouders. Mede op basis van de nieuwe eisen en recente nieuwe regelgeving wordt vooruitgekeken naar mogelijke oplossingsrichtingen en de verwachte invloed op het vak van de ICT-auditor in deze markt.

Belangrijke ontwikkelingen en knelpunten in de informatievoorziening

Financiële instellingen behoren van oudsher tot de intensieve gebruikers van informatietechnologie (IT) voor het automatiseren van processen voor gegevensverwerking, de informatievoorziening en het digitaliseren van de (transactie)communicatie. In eerste instantie is begonnen bij de operaties van de back-offices, waarbij de nadruk lag op het behalen van efficiëntievoordelen bij de omvangrijke en gestandaardiseerde gegevensverwerkende processen.

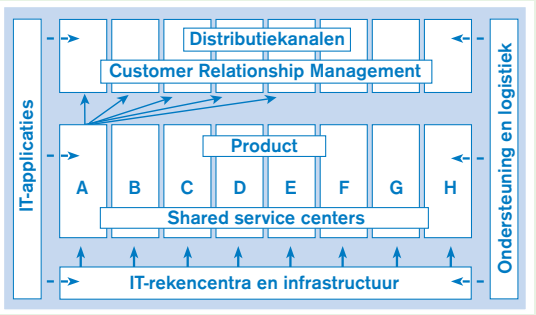
Zonder een volledig beeld van ontwikkelingen na te streven wordt hieronder ingegaan op enkele belangrijke ontwikkelingen en knelpunten in relatie tot het huidige gebruik van ICT.

Steeds verdergaande integratie

De afgelopen tijd heeft een verschuiving laten zien van investeringen in de back-office naar de IT-ondersteuning van de front-office en de ontwikkeling van nieuwe producten en diensten. Tevens vindt steeds verdergaande integratie plaats van de gehele transactieketen.

De integratie van de transactieketen vindt in eerste instantie binnenshuis plaats, maar daarnaast zijn ook meer en meer de belangrijkste externe koppelingen daarbij betrokken. Deze ontwikkelingen werden onder meer mogelijk gemaakt door de opkomst van de internettechnologie. De grootscheepse integratieslagen die doorgevoerd zijn of nog worden doorgevoerd, zijn veelal gekoppeld aan programma's voor procesoptimalisatie en -herontwerp. De behoefte om de belangrijkste transactieketens in een geheel geautomatiseerde procesgang te kunnen behandelen heeft geleid tot koppelingen tussen front-, middle- en back-offices, waarbij ook het (externe) contact met de markt en de achterliggende settlementprocessen betrokken worden. 'Straight through processing' is momenteel in een groot aantal markten eerder noodzaak dan luxe.

Bij de tendens tot verdergaande integratie moet ook het aspect van de vele fusies en overnames in de financiële sector worden betrokken. Veel van de grote instellingen maken in dit verband momenteel (post-merger) integratieslagen door. Het bereiken van echte synergie vergt soms lastige keuzen en de nodige doorlooptijd. Hoewel in een aantal gevallen de integratieslagen na de fusie nog even konden worden uitgesteld, zitten we tegenwoordig in een tijd van consolidatie en rationalisatie, gevoed door onder meer de terugloop van de economische groei en de grote terugval op de beurzen. Na de veelheid aan vernieuwende projecten in de front-office komt er nu aandacht voor kostenbesparingen en het wegwerken van de opgelopen achterstand ten aanzien van integratie- en synergiedoelstellingen. Het in toenemende mate opzetten van zogenaamde shared service centers kan in dit licht worden beschouwd.



Figuur 1. Model van een shared service center voor een grote bank.

Feitelijk dient deze integratieslag te leiden tot aanpassingen op het niveau van processen, applicaties en gegevensmanagement en de onderliggende technische infrastructuur. Echter, tijdens de verbetertrajecten blijkt vaak dat de bestaande IT en de informatiesystemen de aanpassingen moeilijker maken: de meeste financiële instellingen hebben verouderde systemen die relatief star en productgericht (hypotheken, schadeverzekeringen, etc.) zijn opgezet.

Problemen in de productgeoriënteerde kernsysteemarchitectuur zijn:
* gebrek aan flexibiliteit van de mainframesystemen (geen toepassing van het drielagenmodel, d.w.z. scheiding tussen data, logica en presentatie) waardoor integratie wordt bemoeilijkt;
* op één product of distributiekanaal gerichte opzet van systemen die om de back-office mainframes worden opgezet, waardoor veel functionaliteit bij iedere aanpassing (bijvoorbeeld specifieke productlogica of fiatmechanismen) opnieuw moet worden ontwikkeld;
* bij oudere systemen mogelijk gebrek aan structuur vanwege de vele ad-hocoplossingen die in de loop der jaren worden gemaakt;
* een groot aantal koppelingen tussen allerlei systemen vanwege de toegenomen behoeften om combinaties van producten aan te bieden.

In combinatie met de ontwikkelingen genoemd in de volgende subparagraaf blijkt vaak dat de oorspronkelijke productarchitectuur niet meer geschikt is om te voorzien in de nieuwe informatiebehoeften van de financiële instellingen. De behoefte aan integratiemogelijkheden leidt tot een gewenste opzet van infrastructurele systemen die één procesfase zoveel mogelijk afdekken maar eenvoudig kunnen worden geassembleerd voor verschillende producten. Hierbij dienen wel duidelijke afspraken te worden gemaakt over de interfacing tussen de procesfasen en het eigenaarschap van gegevens, zoals voor het centraal opslaan van cliëntgegevens.

Multi-channel, multi-product en time-to-market

Tot ruim tien jaar geleden was het kantorennet decennialang het enige distributiekanaal voor banken. Dit geldt ook voor de verzekeraars met hun tussenpersonenorganisatie. De afgelopen tien jaar ontstonden echter in snel tempo nieuwe distributiekanalen: in de verzekeringsbranche bijvoorbeeld direct writers, bij banken electronic banking, geld- en betaalautomaten, bij alle financiële instellingen callcenters en het internet. Ook zijn voor de nabije toekomst meer nieuwe distributiekanalen te verwachten (short messages via GSM, I-mode, buzzer, pagers, set-top boxes voor interactieve televisie).

Het is niet verwonderlijk dat banken en verzekeraars gezien de opzet van de huidige systemen en de organisatie in eerste instantie niet ingesteld waren op deze nieuwe kanalen. De afgelopen jaren heeft dit ook tot veel knelpunten in de informatievoorziening geleid. Meer concreet zijn de volgende problemen zichtbaar geworden:
* De time-to-market van nieuwe applicaties is te lang, met name het testen van nieuwe aangepaste applicaties kost te veel tijd.
* Vergelijkbare functionaliteit wordt binnen financiële instellingen meermalen opnieuw ontworpen en geïmplementeerd.
* Het opzetten van nieuwe distributiekanalen gaat moeizaam.
* De invulling van kanalen met meerdere producten gaat zo mogelijk nog moeizamer.
* Er ontbreekt een consistent en compleet beeld van de (individuele) cliënt.
* Multiloketsituatie: de klant heeft te maken met een veelvoud aan interactiepunten.
* Ondersteuning van nieuwe producten in de IT-architectuur die bestaan uit combinaties van bestaande producten, zoals hypotheken, verzekeringen en beleggingen, verloopt moeizaam.

De problematiek speelt des te sterker binnen financiële instellingen waar gewerkt wordt volgens de all finance-gedachte waarbij met alle producten in alle distributiekanalen wordt gewerkt, maar waarbij er vaak ook behoefte is om tot een zekere synergie te komen en niet met allerlei verschillende systemen te werken.

Analyse van deze symptomen leidt tot de achterliggende oorzaak van het werkelijke probleem, namelijk: de oorzaak van deze symptomen ligt in de botsing tussen nieuwe bedrijfskundige eisen en een IT-architectuur die hier niet op ingericht is. Hieruit blijkt dat de IT-architectuur eigenlijk het probleem ís. De nieuwe bedrijfskundige eisen zijn immers leidend; de IT moet deze eisen ondersteunen en niet vice versa. Het ligt dan voor de hand om ook de oplossing te formuleren in termen van een nieuwe architectuur die wel aansluit bij de nieuwe bedrijfskundige fase, temeer daar nieuwe technologische ontwikkelingen dit ook binnen bereik brengen.

Voor de financiële instelling manifesteert de nieuwe fase zich door een cliëntgerichte bedrijfsstrategie, de opkomst van nieuwe distributiekanalen (een duidelijke cliëntgerichte ontwikkeling) en hogere eisen aan de time-to-market van zowel producten als informatiesystemen (andere wensen van de cliënt ook sneller kunnen implementeren in de organisatie). Wensen van de cliënt dienen immers veel sneller geabsorbeerd te worden door de financiële instelling en tot uitdrukking te worden gebracht in verbeterde dienstverlening. De nadruk ligt op het verkopen van zoveel mogelijk producten *aan een bepaalde cliënt*. In tabel 1 worden de nieuwe bedrijfskundige eisen en de gevolgen voor de IT-afdeling weergegeven.

Vaak worden in dit verband ook Customer Relationship Management (CRM)-systemen geïmplementeerd. Daarbij zorgen middlewaresystemen voor de aansluiting tussen de back-offices en het CRM-systeem. CRM moet resulteren in de inrichting van een cliëntencockpit met alle relevante cliëntgegevens (cliëntendossier), die ter beschikking staat van de medewerkers in de verschillende distributiekanalen. In de praktijk blijken implementaties van CRM-systemen nogal eens weerbarstiger dan gedacht ([West02]).

Complexe problematiek maar wel oplosbaar

Centraal in de veranderingen staan steeds de begrippen cliënt, product, kanaal en proces: cliënten consumeren producten in processen, die zich afspelen binnen distributiekanalen. De samenhang tussen de begrippen cliënt, product, kanaal en proces maakt de zaak complex. Dit is gevisualiseerd in figuur 2. Hierdoor ontstaat de noodzaak van een nieuwe categorie functies: procesbesturingsfuncties, hier multi-channel multi-productmanager genoemd. Indien de IT-architectuur hiermee geen rekening houdt kan een onbeheersbare situatie ontstaan, niet alleen vanuit technisch oogpunt maar met name ook functioneel. Bij het inrichten van de zogenaamde shared service centers is het van belang dat een duidelijke knip wordt gelegd tussen de front- en de back-office functionaliteit. In een bestaande organisatie wordt vaak de complexiteit nog vergroot bij het inrichten van een shared service center doordat verschillende processen moeten worden gestroomlijnd en geïntegreerd in één uiteindelijke procesgang en IT-ondersteuning.

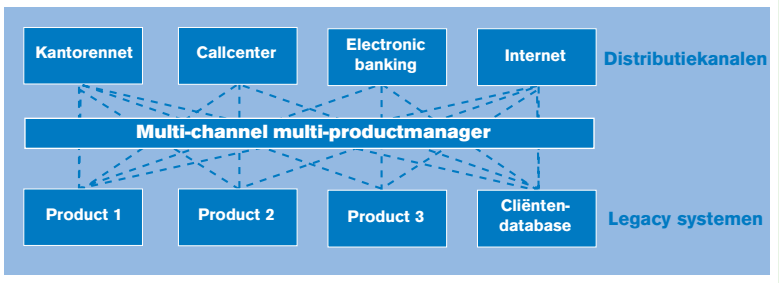
In [Beek99] wordt beschreven welke aanpak gevolgd kan worden om de problematiek op te lossen en een IT-architectuur te krijgen voor de nieuwe eisen. Gepleit wordt voor een architectuur die 'flexibiliteit binnen kaders' biedt. Met 'flexibiliteit binnen kaders' wordt bedoeld dat de kaders, gevormd door een goede infrastructurele basis en een raamwerk waarbinnen op flexibele (en dus snelle) wijze nieuwe applicaties gebouwd kunnen worden en ondersteund door architecturele hulpmiddelen, de randvoorwaarden bepalen waarbinnen applicaties gebouwd worden. Om flexibiliteit te behouden is het belangrijk dat de 'kaders' de architectuur niet overspecificeren. Het bepalen van het juiste evenwicht tussen voorschrijven (specificeren) en vrijlaten is een algemeen onderkend probleem.

Bedrijfskundige eisen	Nieuwe eisen aan IT als gevolg hiervan
Cliëntspecifieke bedrijfsprocessen	Betere applicatieve ondersteuning van het cliëntproces, betere toegankelijkheid / meer eenduidigheid van gegevens
Meer productvarianten	Flexibel uit te breiden / aan te passen applicatiearchitectuur
Betere service	* Grotere beschikbaarheid (7x24) * Nieuwe en meer distributiekanalen
Snellere implementatie van veranderende eisen/wensen van de cliënt	Kortere time-to-market van nieuwe en aan te passen applicaties
Compleet cliëntbeeld i.p.v. een beeld dat versnipperd is over meerdere distributiekanalen	Multi-channel procesbesturing
Meer mogelijkheden tot cross- en deepselling	* Meer/gedetailleerdere gegevens over de cliënt bijhouden * Snelle en eenduidige identificatie van de cliënt

Tabel 1. Nieuwe bedrijfskundige eisen en de gevolgen voor de IT-afdeling.

Voor het beoordelen van IT-architecturen geven de auteurs aan dat het vooral belangrijk is te kijken naar de flexibiliteit. Flexibiliteit wordt hier gedefinieerd als een bepaald aspect van de IT-architectuur en niet als een kwaliteitsaspect van individuele applicaties, en bestaat uit de volgende onderdelen:

* *portabiliteit:* de mate waarin een applicatie zonder ingrijpende wijzigingen naar een ander platform kan worden overgezet;
* *distribueerbaarheid:* de mate waarin applicatiefuncties zonder ingrijpende wijzigingen over verschillende knopen in de (netwerk)architectuur verspreid kunnen worden;
* *uitbreidbaarheid:* de mate waarin applicatiefunctionaliteit zonder wijzigingen uitgebreid kan worden;
* *onderhoudbaarheid:* de mate waarin applicatiefunctionaliteit zonder ingrijpende gevolgen voor andere systemen veranderd kan worden;
* *hergebruik:* de mate waarin applicatiefunctionaliteit zonder ingrijpende wijzigingen gebruikt kan worden door meerdere applicaties. Hierbij wordt onderscheid gemaakt tussen het kunnen kopiëren van applicatiefunctionaliteit en het door meerdere applicaties gebruikt kunnen worden van dezelfde applicatiefunctionaliteit.



Figuur 2. Complexiteit van multi-channels.

In de praktijk wordt momenteel bij veel financiële instellingen aandacht besteed aan de IT-architectuur. In een aantal gevallen verloopt de implementatie van de systemen binnen de architectuur succesvol. De complexiteit lijkt dus inderdaad oplosbaar. Het is nog te vroeg om vast te stellen of volledig aan de nieuwe eisen wordt vol-

daan, maar de eerste stappen in de goede richting zijn gezet en in praktische oplossingen omgezet. Ook technisch blijken voldoende hulpmiddelen voorhanden.

Impact op risico's

De hiervoor genoemde voorbeelden van ontwikkelingen binnen de financiële sector in het gebruik van ICT hebben vanzelfsprekend gevolgen gehad voor de wijze waarop binnen de instellingen en door de auditors en toezichthouders is gekeken naar het algemene (risico)beheersingsvraagstuk inzake de inzet van ICT. De impact van de ontwikkelingen kan op hoofdlijnen als volgt worden weergegeven:

* Door de integratietendens blijft de verschuiving van de toepassingscontroles (procesbewakende controles) naar de geautomatiseerde omgevingen doorgaan. Er wordt steeds meer, al dan niet terecht, gesteund op de IT controls. Voor de IT-auditor blijft aandacht voor het onderzoeken van de general en de application controls dus onverminderd van belang. Het verkrijgen van systematisch inzicht in de risico's en beheersingsmaatregelen krijgt daarbij bij financiële instellingen in de praktijk niet altijd de noodzakelijke aandacht.

* De leeftijd van de bestaande kernsystemen en de veranderende eisen aan de kernsystemen hebben bij veel instellingen geleid tot de in de vorige paragraaf beschreven risico's en architectuurproblemen. Voor de IT-auditor is dit een nieuw aandachtsgebied waarbij andere kwaliteitsaspecten en meer strategische risico's belangrijk blijken. Uiteraard heeft de problematiek tot het vervangen van oude systemen geleid. Op dit moment zijn met name de middelgrote instellingen over de hele linie bezig met het selecteren en implementeren van standaardpakketten. Ook daaraan zijn beheersingsrisico's verbonden. Wij gaan hier in een volgende paragraaf verder op in.

* Door het combineren van projecten gericht op integratie en de noodzaak tegelijkertijd innovatief te blijven in de markt met behulp van de nieuwe technologieën is adequaat projectmanagement steeds meer als een beheersingsrisico naar voren gekomen. Te vaak bleken projecten niet op te leveren wat noodzakelijk was. Ook voor de IT-auditor een belangrijker geworden onderzoeksobject. Bij alle instellingen bestaat momenteel veel aandacht voor projectgovernance (strategisch belang van goed én snel).

* Door het steeds meer gebruiken van nieuwe netwerken mobiele technologie ontstaat het beheersingsvraagstuk voor de externe (gedeelde) infrastructuren. De intensivering van externe koppelingen bracht onder meer geheel nieuwe vraagstukken omtrent de beveiliging van de eigen netwerken/systemen met zich mee. Binnen de technical IT-audit heeft dit tot een apart specialisme geleid.

* De ontwikkeling (groei) van de ICT-functie, het inrichten van shared service centers voor gemeenschappelijke processen en de externe afhankelijkheden hebben invloed op het noodzakelijke ICT-governancemodel. Het belang van een goede integratie van ICT-beleid en operations met de primaire business (Business en IT alignment) is daarbij onverminderd groot gebleven.

* Onder druk van de economische ontwikkelingen is het outsourcingvraagstuk nadrukkelijker op de agenda van het hogere management gekomen. Recent is in dit kader een aantal grote transacties gedaan. Het uitbesteden van de geautomatiseerde gegevensverwerking aan externe dienstverleners, tot op heden met name door de middelgrote en kleine instellingen, vereist aandacht voor de keuze van de leverancier, service level agreement management en het managen van de kwaliteit van de diensten van de externe partij(en). Steeds meer organisaties vragen daarbij om zogenaamde third-partymededelingen van IT-auditors om zekerheid te krijgen over de kwaliteit van de gegevensverwerking.

Na de millenniumwisseling en de invoering van de euro staan de financiële markten ten minste twee grote organisatiebrede verandertrajecten te wachten door de invoering van de IAS (International Financial Reporting Standards)-regels voor de financiële verslaggeving en de invoering van Bazel II door de toezichthouder voor banken. Beide onderwerpen vergen een omvangrijk project, integrale aanpak (business en ICT) en conversie van de grote, soms oude, kernsystemen. Over Bazel II wordt in een volgende paragraaf kort iets gezegd. De nieuwe IAS-verslaggevingsregels kunnen grote impact hebben op de wijze waarop de financiële cijfers van instellingen worden gerapporteerd. Hoewel de invoering van IAS pas in 2005 is voorzien, dienen reeds nu voorbereidingen te worden getroffen. Het IAS-traject is veel meer dan alleen een accountingproject, en raakt net als bij de euro de business en alle systemen die de basisgegevens aanleveren voor de verslaggeving. Met name indien sprake is van legacy systemen zullen eventuele conversies een grote impact kunnen hebben, zodat een integrale programma-aanpak noodzakelijk is met sponsorship van het senior management.

Samenvattend kan worden gesteld dat de inzet van ICT binnen de financiële sector is uitgegroeid tot een uitermate belangrijke factor in het totale business- en beheersingsvraagstuk. Mede hierdoor is het onderwerp als zodanig vaker op de agenda's van het hogere management gekomen.

Een in februari 2002 uitgevoerd wereldwijd KPMG-onderzoek ('KPMG Global security Survey') toont aan dat organisaties in de financiële sector over het algemeen de zaken beter hebben georganiseerd ten aanzien van de beveiliging van systemen en informatie. 'Goed, maar niet goed genoeg' is echter het devies. Onder meer de gebeurtenissen rond 11 september hebben bij veel instellingen geleid tot een extra check op maatregelen getroffen ten behoeve van de continuïteit van de business. Tabel 2 geeft enig cijfermatig inzicht in de uitkomsten van het onderzoek ([Cole02]).

Type beveiligingsleemte	Gemiddeld aantal dagen verloren (jaar)	Gemiddeld US $ (x 1000) verloren (jaar)	Hoogste in US $ (x 1 miljoen) gerapporteerde verlies (jaar)
Diefstal IT-middelen	47	180	2,2
Verlies van bedrijfsdocumenten (hardcopy)	23	30	0,1
Verlies van software	19	310	2,9
Virusincident	52	270	4,5
'Denial of service'-aanval	30	60	0,2
E-mail 'spamming'	19	40	0,2
Fraude met input of output	7	10	0,01
Website 'hacking'	9	30	0,2
Uitval kritieke systemen	83	60	0,2
Verlies van confidentiële gegevens	29	200	0,5

Tabel 2. Enkele cijfers uit de 'KPMG Global security Survey', februari 2002.

De resultaten geven aan dat bij veel financiële instellingen IT controls en -beveiliging nog steeds een belangrijk beheersingsrisico vormen, met name ook de beveiliging van interne en externe netwerken. Begrippen als firewalls, Trusted Third Party en Public Key Infrastructure (om encryptie mogelijk te maken) staan de laatste tijd sterk in de aandacht omdat de beveiliging van de transacties met behulp van de nieuwe technologieën in de praktijk nog niet afdoende is geregeld. Juist voor succesvolle acceptatie van de nieuwe technologie dient er voldoende vertrouwen in de beveiliging te zijn. Instellingen en organisaties hebben dat zelf ook onderkend en zijn verbeterprojecten gestart, vaak op basis van de Code voor Informatiebeveiliging, waarin een aantal best practice-beveiligingsmaatregelen van een groot aantal organisaties wordt beschreven. Een belangrijk aandachtspunt hierbij is nog dat indien de IT-architectuur opnieuw wordt ontworpen, er ook voldoende aandacht voor security dient te zijn (het begrip security-architectuur wordt daarbij vaak genoemd). Achteraf inbouwen is kostbaar en in de nieuwe systemen eigenlijk onmogelijk.

Betekenis voor de ICT-organisatie: outsourcen of standaardpakketten?

Om een adequaat antwoord te geven op de veranderende informatiebehoeften zal ook de ICT-organisatie zich aan moeten passen. Aangezien de groeibehoeften van de gebruikersorganisatie veelal groot zijn, dient de ICT-organisatie zodanig te worden ingericht dat deze kan blijven voorzien in de behoeften van de gebruikers. Om succesvol te zijn moet de ICT-organisatie leren van veranderende omstandigheden en zich hieraan kunnen aanpassen. De ICT-organisatie dient net als haar afnemers producten en diensten aan te bieden die aan de verwachtingen van de gebruikers ten aanzien van functionaliteit en kwaliteit voldoen. Ook als de eisen en wensen ten aanzien van ICT sterk veranderen. Veel ICT-organisaties bevinden zich midden in deze transformatiefase. Veelgebruikte begrippen bij het doorvoeren van verbeteringen in de processen van de ICT-organisatie in deze fase zijn Information Technology Infrastructure Library (ITIL), dat zich meer op de rekencentrumfunctie van de ICT-organisatie richt, en voor de systeemontwikkelorganisatie bijvoorbeeld het Capability Maturity Model (CMM).

Om te weten in welk stadium de ICT-organisatie zich bevindt, wordt vaak gewerkt met het groeifasenmodel ([Boer98]). In het groeifasenmodel worden vijf generieke fasen van volwassenheid van processen onderscheiden gericht op producten en diensten. De groeifasen kunnen achtereenvolgens globaal worden aangeduid met:

* *technologiegericht*. In deze fase is de gebruiker niet leidend maar volgend voor wat betreft de eisen en wensen. De meeste IT-processen worden ad hoc uitgevoerd.
* *taakgericht*. De gebruikersrol verandert van lijdzaam volgen naar het maken van keuzen. De ICT-organisatie beheerst haar processen redelijk maar haar processen zijn niet gericht op de klant.
* *servicegericht*. De gebruiker mag niet alleen kiezen maar bepaalt ook hoe en welke ICT-producten en diensten geleverd moeten worden.
* *klantgericht*. De gebruiker wordt eigenaar van de ICT-producten en diensten en klantgerichte processen zijn ingericht maar hebben nog een reactief karakter.
* *businessgericht*. In deze fase is de gebruiker niet alleen eigenaar maar stuurt deze ook de ontwikkeling van de ICT-organisatie zelf.

Het moge duidelijk zijn dat een architecturele aanpak zoals geschetst in de paragraaf over ontwikkelingen en knelpunten ook van de ICT-organisatie vergt dat zij vergevorderd is in haar transformatieproces. Uit waarnemingen in de praktijk blijkt dat de meeste ICT-organisaties nog niet verder komen dan servicegericht. Er zal door de ICT-organisaties derhalve nog veel werk moeten worden verzet omdat de complexiteit van de problematiek van de informatievoorziening bij financiële instellingen eigenlijk nu al vraagt om klant-/businessgerichte organisaties. Een belangrijke belemmering in dit proces vormt de beperkt beschikbare capaciteit in de ICT-organisaties omdat tegelijkertijd ook de bestaande legacy systemen moeten worden onderhouden en beheerd. Veel externe inhuur is het gevolg. Outsourcing van IT wordt hierbij ook vaak als de oplossing beschreven. Een positief effect van outsourcing is dat toegang kan worden verkregen tot 'state of the art'-informatietechnologie en vitale kennis en capaciteit vrij kan worden gemaakt voor nieuwe ontwikkelingen die businesskansen opleveren. In de volgende paragraaf wordt verder over outsourcing gesproken.

Outsourcing: de oplossing voor alle problemen?

De financiële sector is van oudsher een sector waar qua automatisering sterk het credo geldt: intern oppakken en intern onderhouden. Dit heeft geleid tot uitermate professionele interne ICT-dienstverleners. Steeds vaker blijkt nu toch ook in deze sector het vraagstuk op te komen rondom het al dan niet op onderdelen uitbesteden van ICT-diensten.

De praktijk heeft al een aantal voorbeelden opgeleverd van soms zeer grootschalige trajecten, met wisselend succes. [Schu02] beschrijft dat de meeste outsourcing deals in de financiële sector moeizaam lijken te verlopen. Er is sprake van een worsteling om een balans te vinden tussen beheersing van de kwaliteit van de dienstverlening en de service levels, het creëren van een win-winsituatie voor leverancier en opdrachtgever, en de transparantie van de kostenniveaus. De bijzonder sterke verbondenheid met het directe businesssucces vormt een uitermate belangrijk aandachtspunt in het nadenken over uitbesteding en bij het inrichten van het toezicht op de diensten van de geselecteerde aanbieder. Er dient gestreefd te worden naar long term strategic partnership en niet naar een kortetermijnoplossing voor (kosten)problemen. Vaak blijkt in het laatste geval de opdrachtgever overgeleverd aan de outsourcingpartij en wordt uiteindelijk een veel hogere rekening betaald. Zeker op het onderdeel van de kernsystemen zal menige financiële instelling de touwtjes intern stevig in handen willen houden.

Figuur 3 laat zien dat het uitbestedingsproces uit een aantal processtappen bestaat, die achtereenvolgens worden doorlopen.

Figuur 3. Proces van uitbesteding.

Zoals hiervoor al gezegd dient ook het outsourcen van IT-activiteiten een zorgvuldig afwegingsproces te zijn. Aandachtspunten in de afweging zijn:

* Is er een helder inzicht in de scope van hetgeen wordt uitbesteed inclusief de processen, de geleverde diensten en kosten? Zijn de gegevens voldoende betrouwbaar?
* Zijn zowel de voor- als de nadelen van outsourcing in kaart gebracht? Is de doelstelling niet uitsluitend kostenbesparingen op korte termijn?
* Is bij het besluiten tot outsourcing ook nagedacht over de gewenste dienstverlening op een termijn van drie tot vijf jaar?
* Hebben de financiële afspraken niet te veel een openeindkarakter?

Diensten die veel bijdragen aan de concurrentiepositie kunnen beter in eigen beheer worden gehouden. Hierbij kan bijvoorbeeld worden gedacht aan het beheren van de architectuur en het leveranciers- en servicemanagement.

Standaardpakketten als oplossing?

Op specifieke onderdelen/processen en bij kleinere instellingen was het gebruik van standaardpakketten al bekend. Voor de kernsystemen bij de grotere financiële instellingen is dit echter nog veelvuldig een uitzondering. Ook als de basis wellicht een standaardtoepassing is, heeft de hoeveelheid aanvullend maatwerk vaak in het verleden geleid tot de situatie dat de ontwikkel- en onderhoudsactiviteiten door de instelling zelf verzorgd moesten worden. Juist in de maatwerkdelen zit heel veel kennis over de organisatie opgeslagen. Uit onderzoek blijkt dat een toenemend aantal financiële instellingen (inclusief de grote) zich sterk oriënteert op de invoering van standaardpakketten. Hiervoor is wereldwijd een redelijk tot goed aanbod van systemen en leveranciers voorhanden.

Veel financiële instellingen hebben inmiddels ervaring opgedaan met het traject van besluitvorming rondom pakketimplementatie, via selectie tot en met het implementeren en operationaliseren van een dergelijke standaardoplossing. In de praktijk lopen implementaties met wisselend succes. In [Beug02] wordt een goed overzicht gegeven van de valkuilen in de verschillende stappen bij een pakketselectie en -implementatie en wordt ook de rol van de IT-auditor belicht. Vaak blijkt een proactieve rol tijdens de implementatie aan te bevelen om te waarborgen dat voldoende aandacht wordt besteed aan de benodigde beheersingsmaatregelen.

Standaardpakketten kunnen dus wel degelijk een uitstekende oplossing bieden, maar dit is niet altijd het geval. In aanvulling op de slag van parametrisering (systeeminrichting naar de eigen wensen) blijkt er vrijwel altijd sprake van de noodzaak de bestaande processen en organisatie aan te passen aan de eigenschappen van het betreffende pakket. Belangrijk is om in te zien dat de architectuur als scharnierpunt tussen business en IT de lastige taak heeft om beide groepen te verbinden en tevreden te stellen. Voor de business moet duidelijk zijn wat de architectuur voor hem concreet aan toegevoegde waarde levert. Voor de IT moet duidelijk zijn hoe men concreet met de architectuur aan de slag kan wat betreft applicatieontwikkeling, waarbij de architectuur moet garanderen dat die applicaties ook leveren wat de business ervan verwacht.

Veel consultancy- en softwarebedrijven hebben kant-en-klare architecturen op de plank liggen. Vaak zijn deze echter gebaseerd op een eigen systeem/pakket/tool, dat zij toevallig gebruiken, of zijn ze erg algemeen. In beide gevallen sluit de architectuur niet goed aan op de eigen bedrijfssituatie. De onderhandelingspositie met dergelijke bedrijven wordt aanzienlijk verstevigd indien men zelf met een goed onderbouwd architectuurplan komt. Daarnaast sluit dit goed aan op de trend om meer kant-en-klare oplossingen te kopen in de vorm van pakketten en

op de trend om meer te gaan uitbesteden op het gebied van systeembouw. Pakketten veroorzaken echter vaak een *architecturele mismatch* waardoor de voordelen van pakketaanschaf grotendeels teniet worden gedaan. De oorzaak hiervan is dat architecturen vaak nog uitgaan van impliciete veronderstellingen, waarmee bij pakketselectie geen rekening wordt gehouden. Wat betreft de uitbesteding van systeembouw is het essentieel om geen fundamentele kennis omtrent de opzet van systemen kwijt te raken en daardoor afhankelijk te worden van externe partijen. Zolang men zelf de regie blijft voeren met betrekking tot de architectuur van uitbestede systeembouw kan men zich concentreren op de essentiële aspecten van systeemontwikkeling, en de relatief laagwaardige codering en eventueel ontwerp van individuele applicaties aan gespecialiseerde bedrijven overlaten. Dit lijkt de beste eerste stap op weg naar een compactere en beter beheersbare IT-afdeling. Want hoewel IT van levensbelang is voor de moderne financiële instelling, behoort automatisering op uitvoeringsniveau tot in details niet tot de corebusiness.

Bij het selecteren van een pakket en leverancier voor een belangrijk kernsysteem leert de praktijk dat het verstandig is dit proces ook vanuit het perspectief van langdurig partnership of zelfs uitbesteding te beschouwen. Ten slotte bepaalt het contract met en het feitelijk optreden van de gekozen leverancier een belangrijk deel van de flexibiliteit, slagvaardigheid en operationele kwaliteit van de instelling. Een belangrijke succesfactor is daarnaast nog gelegen in het managen van de relatie met de leverancier. Deze partij wordt immers door de keuze voor haar systeem een belangrijke businesspartner.

Toezicht op de financiële markten

Partijen en richtlijnen

In Nederland is het toezicht op de financiële markten verdeeld over de volgende partijen: De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (Autoriteit-FM) en de Pensioen- en Verzekeringskamer (PVK). Recent heeft enige herverdeling en aanscherping van de taken van de individuele toezichthouders plaatsgevonden. Bovengenoemde toezichthouders werken samen in de Raad voor Financiële Toezichthouders (RFT) met als doel de niet-sectorspecifieke regelgeving en het dito beleid te intensiveren.

De drie toezichthoudende instellingen hebben hun basisrichtlijnen voor toezicht vastgelegd in de volgende richtlijnen:
* DNB: Regeling Organisatie en Beheersing (ROB);
* Autoriteit-FM: Nadere Regeling;
* PVK: Principes Interne Beheersing (PIB).

Elk van de toezichthouders kent in aanvulling hierop een eigen set van nadere of bijzondere richtlijnen.

Het toezicht wordt onder meer ingevuld via:
* maandelijks verplicht op te leveren rapportages (onder meer de maandstaten);
* periodiek eigen onderzoek bij instellingen, waarbij ofwel op het niveau van een individuele instelling (op basis van een planning) een object voor onderzoek wordt vastgesteld dan wel onderzoek bij meerdere instellingen of van de gehele markt op een thema plaatsvindt;
* reactie op (vermoede) incidenten.

Ook in internationaal verband is sprake van coördineren en initiëren van regelgeving. De Bank for International Settlements (BIS) is actief op het gebied van het toezicht op de financiële markten. Momenteel verdienen in het bijzonder de nieuwe kapitaalsrichtlijnen (bekend als Bazel II) de aandacht. Bazel II heeft als doel de interne risicobeheersing binnen het bankwezen te verbeteren.

Uitvoering

De toezichthouders maken daarnaast in de uitvoering van hun taken gebruik van de uitkomsten van de werkzaamheden van de interne en externe auditors. Enerzijds betreft dit werkzaamheden van de auditors welke op specifieke instructie van de toezichthouders worden uitgevoerd (in opvolging van de richtlijnen), anderzijds behouden de toezichthouders zich het recht voor de door interne en externe auditors aan het bestuur van de instelling gerichte onderzoeksrapportages op te vragen via de instelling. Voor de bancaire sector is sprake van een geformaliseerd jaarlijks overleg tussen toezichthouder, extern accountant en vertegenwoordigers van de instelling.

Een korte inventarisatie van de bestaande regelgeving van toezichthouders leert dat in de afgelopen jaren sprake is van duidelijke tendensen. Belangrijkste ontwikkeling is geweest het uitvaardigen van nieuwe geïntegreerde sets van richtlijnen waarbij vooral de integrale risicomanagementbenadering opvalt. Het goed kennen en inschatten van de risico's verbonden aan de markt en de aard van de eigen instelling, alsmede het vervolgens goed beheersen van deze risico's wordt door de toezichthouders meer en meer centraal gesteld. Bijvoorbeeld op het gebied van ICT-risico's in de ROB wordt ook gevraagd naar de meer strategische risico's op het gebied van IT-architectuur en de onderhoudbaarheid van systemen waarover eerder in dit artikel is gesproken. Met de invoering van de Bazel II-richtlijnen wordt ook het daadwerkelijk meten van de risico's (risk measurement) ingevoerd. Belangrijk aandachtspunt in de nieuwe regelgeving is verder nog het transparant maken voor (onder meer) de toezichthouder van het systeem voor risicomanagement en de kwaliteit van de huidige implementatie.

Naast de algemene richtlijnen voor toezicht zijn toezichthouders meer en meer specifieke richtlijnen gaan uitvaardigen gericht op een bepaald issue of onderwerp. Voorbeeld is de Internet-richtlijn van de Autoriteit-FM. Toezichthouders komen hiermee onder andere tegemoet aan de vraag van de markt om meer concrete invulling van de eisen van de toezichthouder ten aanzien van bepaalde aspecten/onderwerpen.

In aanvulling op de formeel in richtlijnen vastgelegde eisen en wensen van de toezichthouder is er nog het rechtstreekse contact van toezichthouders met individuele instellingen. Ook via deze weg geven toezichthouders (al dan niet formeel vastgelegd in rapportages) nadere invulling aan de gestelde eisen.

Drs. J.J. van Beek RE RA is als partner werkzaam bij KPMG Information Risk Management. Hij heeft een jarenlange ervaring in alle aspecten van het IT-auditvakgebied, met een zwaartepunt in het beoordelen van en adviseren over de geautomatiseerde informatievoorziening bij financiële instellingen.

Drs. F.R. Schut RE RA is als partner werkzaam bij KPMG Information Risk Management. Hij is de nationale leider van de line of business Financial Services voor de IT-auditors en heeft een brede ervaring op IT-auditgebied.

Afsluiting: Invloed op het werk van de ICT-auditor

Wat betekent het geheel van de hiervoor geschetste ontwikkelingen in de markten van de financiële sector, alsmede de ontwikkelingen in het optreden van de toezichthouders nu voor het vakgebied ICT-auditing en het optreden van de ICT-auditor?

Het algemene karakter van de markt en de ontwikkelingen daarbinnen maken de financiële sector in de breedte tot een omgeving waarin voor ICT-auditing een duidelijke rol zou moeten zijn weggelegd. De uitdagingen voor de toekomst lijken onder meer te liggen in het verder integreren van het ICT-element en de daarmee verbonden risico's in het gehele risicomodel van instellingen en markten en het concretiseren van de daadwerkelijk relevante risico's.

Voor de ICT-auditors geldt dat er in de nieuwe regelgeving over het algemeen minder gedetailleerde voorschriften inzake ICT zijn opgenomen. Bij het uitvoeren van onderzoeken zal meer gebruik worden gemaakt van de beleidsuitgangspunten en risico-inschattingen van de instellingen zelf. Wel hebben de toezichthouders in hun nieuwe richtlijnen verwijzingen naar de *sound practices*, zoals de Code voor Informatiebeveiliging en CoBIT, opgenomen als standaarden voor de instellingen en daarmee voor de controlerende auditors.

De nieuwe regelgeving bevat over het algemeen minder gedetailleerde voorschriften inzake ICT.

Eerder in dit artikel is opgemerkt dat de aandacht van de auditors de laatste jaren in belangrijke mate gericht is geweest op de general IT en application controls en in enige mate op de bijzondere projecten, waaronder internettoepassingen. Dat is op zich een goede zaak, maar het kan ook betekenen dat er voor de onderliggende problemen in de informatievoorziening te weinig aandacht is geweest. Het lijkt erop dat juist door de nieuwe richtlijnen voor toezicht zowel de instellingen als de auditors worden gedwongen het geheel aan risico-inschatting en -management voor de instelling als totaliteit opnieuw te analyseren, inzichtelijk te maken en te toetsen. Geactualiseerde beleidsregels en heldere inschattingen van de geldende risico's geven vervolgens een geschikt uitgangspunt voor afgewogen auditprogramma's. Auditprogramma's die de auditors van de financiële instellingen in staat moeten stellen uitspraken te doen over de belangrijke kwaliteitsvragen inzake de geautomatiseerde gegevensverwerking. Op dit terrein dient het vakgebied IT-auditing zich nog verder te ontwikkelen, want niet voor alle kwaliteitsvragen zijn die programma's reeds aanwezig.

Uit de voorgaande paragrafen mag duidelijk zijn dat het beoordelen van de betrouwbaarheid en continuïteit nog maar een deel van het werkterrein vormt voor de IT-auditor. De geschetste vraagstukken op het gebied van de informatievoorziening bij financiële instellingen vragen juist om een toekomstgerichte IT-auditor die meer aandacht besteedt aan kwaliteitaspecten als efficiency en effectiviteit van de IT-ondersteuning.

De IT-auditor is gezien zijn opleiding en zijn ervaring bij uitstek de deskundige die de ontwikkelingen op informatievoorzieningsgebied bij financiële instellingen kan beoordelen en daarover kan adviseren. Er is sprake van een complexe problematiek en oplossingen zijn de komende jaren zeker niet vanzelfsprekend. Gezien de overkoepelende rol die de architectuur speelt bij het beter beheersen van de IT-investeringen is het noodzakelijk om de input van de IT-auditor niet te beperken tot alleen de securityaspecten van de informatiearchitecturen. Indien wordt gekozen voor het implementeren van standaardpakketten of wordt gedacht aan outsourcing, dan heeft de IT-auditor een natuurlijke adviesfunctie te vervullen.

Literatuur

[Beek99]
J.J. van Beek en J.W. de Klerk, *Ontwikkelingen in beheersing van de informatievoorziening bij financiële instellingen en de rol van de IT-auditor*, in: Compact & ICT-auditing, 25 jaar Compact, jubileumuitgave, 1999.

[Beug02]
B. Beugelaar e.a., *Standaardpakketten in de financiële sector*, Compact 2002/1.

[Boer98]
J.C. de Boer en J.R.M VandeCasteele, *De EDP-auditor en de veranderende ICT-organisatie*, Compact 1998/2.

[Cole02]
R. Coles and N. Bryden, *Good ... but not good enough*, Frontiers in finance, juni 2002.

[Dral02]
E. Dralans, *Technology challenges after a period of acquisition, Future of financial services, winning in the age of technology*, 2001.

[Schu02]
E. Schut en M. Reijnders, *Dissolving the Kingdom*, Frontiers in finance, juni 2002.

[West02]
S.J. Westra, *Customer Relationship Management: het belang voor financiële organisaties en de rol van de IT-auditor*, Compact 2002/1.