



ICT due diligence in de financiële sector



Ir. H.H. Koets RE

is als IT-audit manager werkzaam binnen KPMG IT Advisory. Belangrijke aandachtsgebieden in zijn werk zijn het verbeteren van de betrouwbaarheid van bedrijfsprocessen en informatiesystemen, corporate project risk management en due diligence. Hij heeft tevens ervaring opgedaan binnen de afdeling Transaction Services van KPMG op het gebied van financieel due diligence. koets.rene@kpmg.nl



Drs. ing. I. Benjaminse

werkt als IT-adviseur bij KPMG IT Advisory. Vanuit die positie heeft hij voor Transaction Services onderzoek gedaan naar ICT-aspecten binnen diverse due diligence-opdrachten. Daarnaast heeft hij ruime ervaring met data-analyses en voert hij IT-audits uit ter ondersteuning van jaarrekeningcontroles. benjaminse.lodewijk@kpmg.nl

Ir. René Koets RE en drs. ing. Lodewijk Benjaminse

De kranten staan al enkele jaren vol met nieuws omtrent fusies en overnames. Ook in de financiële sector beleeft men spannende tijden rondom overnames. Naast de juridische en financiële kant dient ook de ICT belicht te worden tijdens een fusie of overname. Ten tijde van het schrijven van dit artikel speelde onder meer de overname van ABN AMRO en waren er berichten in het nieuws over de overname van Binck Bank door Alex. Financiële instellingen¹ kennen over het algemeen een hoge graad van automatisering, waardoor het belang van ICT due diligence binnen deze sector groot is. Op basis van het due diligence-onderzoek wordt de waarde van de onderneming bepaald. Hierbij is het van belang om ook de waarde van de ICT-omgeving te bepalen. In dit artikel wordt ingegaan op de belangrijkste aandachtspunten voor een ICT due diligence binnen de financiële sector.

Inleiding

Financiële instellingen moeten zich steeds sneller kunnen aanpassen aan de veranderingen in de markt, veranderingen in wet- en regelgeving en veranderingen in technologie. Zo is bijvoorbeeld te zien dat binnen de financiële sector geïnvesteerd wordt in de vervanging en ondersteuning van mainframe-omgevingen voor bijvoorbeeld een .NET-omgeving. SEPA, MiFID, IFRS en Basel II zijn enkele voorbeelden van nieuwe wet- en regelgeving die direct invloed hebben op de ICT-omgeving van financiële instellingen. Meegaan in technologische ontwikkelingen zoals System Oriented Architectures en .NET zijn van belang om de concurrentie voor te kunnen blijven en klanten van nieuwe producten en diensten te kunnen voorzien. Maar meegaan in technologische ontwikkelingen bepaalt ook de waarde van ICT voor de onderneming, de flexibiliteit en robuustheid van de ICT-omgeving.

In dit artikel worden de ICT-aandachtspunten van het due diligence-onderzoek en de rol die de IT-auditor hierin kan spelen, toegelicht.

1) In de Wft wordt er gesproken over 'clearinginstelling, kredietinstelling, verzekeraar of bijkantoor'.

Belang ICT in due diligence

Financiële instellingen moeten zich er constant op blijven richten, dat (primaire en ondersteunende) processen zo efficiënt mogelijk ingericht zijn en blijven, om zo snel en efficiënt mogelijk transacties te kunnen afhandelen. Naast kosten en opbrengst per transactie is bijvoorbeeld ook het percentage 'straight through processing' een maatstaf voor de mate van efficiency in routinematige transactieverwerking. Goede ondersteuning door ICT is dan ook van groot belang voor de continuïteit en efficiency van de bedrijfsprocessen.

De algemene verwachting van de stakeholders bij een fusie of overname is dat synergievoordelen worden gerealiseerd. De verwachte voordelen worden vaak al meegenomen in het bepalen van de (ver)koop prijs, evenals de termijn waarop deze voordelen verzilverd kunnen worden. Op basis van de ICT-aspecten die in het due diligence-rapport naar voren zijn gekomen, kan aan aandeelhouders een realistisch beeld worden geschetst over de te maken kosten en de te behalen synergievoordelen. Derhalve dient al tijdens het due diligence-onderzoek te worden nagedacht over de situatie die na de overname gewenst is. Men kan bijvoorbeeld door het samenvoegen van product- of klantbestanden een completere dekking verkrijgen van de markt. Daar waar systemen komen te vervallen zal dit tot lagere beheerkosten kunnen leiden.

Bij fusie of overname is sprake van verticale of horizontale integratie. Bij een horizontale samenvoeging van bedrijfsprocessen behouden beide organisaties hun primaire processen en dient er naar de koppeling tussen de twee organisaties gekeken te worden. In dit geval kunnen met name ondersteunende activiteiten worden samengevoegd, zoals de helpdesk en het netwerkbeheer. Wanneer verticaal wordt geïntegreerd, kan voordeel worden behaald door delen van de procesketen op elkaar aan te laten sluiten en de onderliggende infrastructuur samen te voegen.

De risico's van het samenvoegen zijn echter niet altijd op voorhand duidelijk. Het is onduidelijk of beide organisaties de gewenste samenvoeging technisch kunnen realiseren en of ze tot integratie kunnen komen om zo de beoogde kostenvoordelen te behalen. Als het zover komt dat beide organisaties integreren, moet worden vastgesteld welke investeringen dan benodigd zijn.

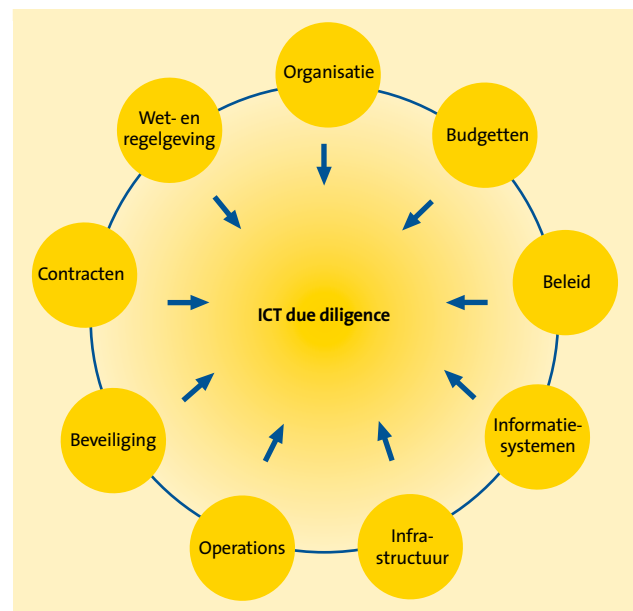
Het belang van ICT due diligence binnen de financiële sector is groot

ICT vormt bij fusies en overnames in de financiële sector dan ook een belangrijk aspect binnen het due diligence-onderzoek.

De IT-auditor kan hierbij een belangrijke onafhankelijke rol spelen omdat hij vanuit zijn achtergrond zicht heeft op en kennis heeft van de geautomatiseerde gegevensverwerking. Tevens kan de IT-auditor de aangetroffen systemen, medewerkers en geïmplementeerde (beheer)processen op waarde schatten.

Onderzoeksaanpak

Een due diligence-onderzoek gericht op ICT is binnen banken en verzekeringen belangrijk gezien de cruciale rol van ICT in deze hoog geautomatiseerde omgevingen. Om de rol die de IT-auditor kan spelen in het due diligence-onderzoek toe te lichten, beschrijven wij de onderwerpen die de IT-auditor onderzoekt in een dergelijk onderzoek. Afhankelijk van de omgeving waarin het onderzoek plaatsvindt zal de IT-auditor andere accenten leggen tijdens zijn onderzoek. Bij (pensioen)verzekeraars zal bijvoorbeeld veel aandacht worden besteed aan de robuustheid en actualiteit van de gehanteerde systemen, terwijl bij banken meer aandacht wordt besteed aan integreerbaarheid van systemen en omgevingen.



Figuur 1. ICT due diligence-aandachtspunten.

Aanpak en onderzoeksactiviteiten

Binnen een ICT due diligence-onderzoek verdient een veelheid aan onderwerpen de aandacht (zie figuur 1). Zo dient niet alleen naar de 'harde' kant van ICT (informatiesystemen, applicatieportfolio, infrastructuur en tools) gekeken te worden, maar juist ook naar de organisatie daaromheen (beheer, budgetten, beleid en contracten). Met deze onderwerpen tezamen is het mogelijk zich een goed beeld te vormen van de ICT binnen een bedrijf.

Om de kopende organisatie van een goed advies te kunnen dienen moet de IT-auditor niet alleen de huidige ICT beoordelen, maar ook een beoordeling van de toekomstvastheid en mogelijkheden van integratie- c.q. ontvlechtingsmogelijkheden in de rapportage meenemen.

Onderstaand beschrijven wij per onderwerp de belangrijkste aandachtspunten van de IT-auditor.

Organisatie

De opzet van de ICT-organisatie bestaat onder andere uit interne medewerkers, externe medewerkers, functies, handboeken en uitbestede onderdelen. Dit is voor de IT-auditor van belang binnen het due diligence-onderzoek om zich een beeld te vormen van de toegekende taken en toebedeelde verantwoordelijkheden (zowel intern als extern) binnen de ICT-organisatie.

Een overzicht van de aanwezige ICT-locaties (rekencentra, systeemontwikkeling, eventuele stafafdelingen) in alle landen geeft inzicht in de mogelijke complexiteit van het netwerk en communicatiemiddelen. Ook kan met deze informatie worden gekeken of bijvoorbeeld het uitwijkplan hierop juist is aangepast. In de financiële sector is het beschikken over een uitwijkplan en het periodiek uitvoeren van uitwijktests vereist door DNB.

Met behulp van organisatieschema's van de ICT-afdelingen kan de IT-auditor beoordelen of afdelingen behouden dienen te worden na de overname. Afdelingen die overbodig zijn, kunnen worden afgestoten of kunnen worden samengevoegd met vergelijkbare afdelingen binnen de kopende organisatie. Daarnaast wordt op basis van benchmarkonderzoeken gekeken naar een normale bezetting en verdeling van de personeelsleden in verhouding tot het aantal klanten, het aantal transacties dat de financiële instelling verwerkt en het aantal gebruikers binnen de financiële instelling.

In een bericht over de overname van Binck Bank wordt vermeld dat synergievoordelen al snel een besparing van € 19 miljoen per jaar kunnen opleveren. In dat bericht worden voordelen 'op het punt van kosten voor het beheer van de systemen en [...] van de zelf [...] te maken kosten per transactie' genoemd. Ook wordt de nettoprovisieopbrengst per transactie berekend: € 18,20 bij Alex en € 15,93 bij Binck Bank. Hierbij speelt informatie over het aantal klanten, transacties en winst dus een belangrijke rol.

De IT-auditor brengt in kaart wat het ervarings- en opleidingsniveau van de medewerkers automatisering is. Daarbij speelt de kennis van systemen een belangrijke rol, evenals de mate waarin de systemen worden ingezet. Wanneer de medewerkers slechts van één systeem/platform kennis hebben, zal het moeilijk zijn deze voor andere systemen in de nieuwe organisatie in te zetten. Dit is met name het geval bij banken waar veel legacy-automatisering wordt gebruikt. Bij een overgang naar bijvoor-

beeld een .NET-omgeving zal een deel van de medewerkers deze ontwikkeling niet kunnen of willen doormaken. De onderverdeling naar productie, onderhoud en ontwikkeling kan hierbij helpen. De ervaring en het opleidingsniveau van de medewerkers geven verder inzicht in de te verwachten salariskosten. Gecombineerd met organogrammen kan inzicht worden verkregen in overlap met of aanvulling op de medewerkers binnen de kopende organisatie.

Bij extern ingehuurde medewerkers bestaat de kans dat die met de overname niet meegaan, door bijvoorbeeld ontbindende voorwaarden in het contract. Ook is het mogelijk dat zij (gezien hun flexibele arbeidsrelatie) er zelf voor kiezen om niet naar de kopende organisatie te gaan. Deze informatie is van belang om te kunnen inschatten hoeveel medewerkers met welke kennis en ervaring in de organisatie aanwezig zijn na de overname.

De professionaliteit van documentatie en richtlijnen geeft een indruk van de volwassenheid van de IT-organisatie

De IT-auditor kan zich aan de hand van handboeken, richtlijnen, gebruikte standaarden en ontwikkelmethodieken een goed beeld vormen van de volwassenheid van de ICT-organisatie bij de over te nemen organisatie. (Zie ook 'Volwassenheid van de ICT-organisatie' verderop.) Gebrek aan standaarden en documentatie geeft niet alleen aan dat veel ad hoc bedacht wordt, maar heeft ook invloed op beheerprocessen en ontwikkelde applicaties. In de financiële sector is bijvoorbeeld het percentage straight through processing een belangrijk kengetal. Aan de hand van de professionaliteit van de documentatie en richtlijnen kan de IT-auditor zich hier een beeld bij vormen.

Budgetten

Om een beeld te krijgen van de financiële situatie op het moment van onderzoek en de komende jaren, moeten budgetten en werkelijk behaalde financiële resultaten worden bestudeerd. Het is voor de kopende organisatie van belang om te weten welke kosten met de ICT-organisatie gemoeid zijn.

'De reden dat ABN AMRO overgenomen wilde worden, moet gezocht worden in schaalvoordelen, 65% van de omzet bestaat uit kosten, bij andere banken is dat 55%. ABN AMRO hoopt dat door de overname kosten gereduceerd kunnen worden, de vraag is of de ICT makkelijk kan worden samengevoegd.'
(Bron: zie Literatuur, laatste item.)

Een overzicht met de feitelijke en gebudgetteerde kosten van de afgelopen jaren is hierbij van belang. Verder dient gekeken te worden naar de gebudgetteerde kosten voor de komende jaren en de planning van investeringen en projecten.

Over het algemeen komen kosten en budgetten in de financiële due diligence aan de orde. Echter, niet alleen zijn de geplande kosten van een investering of project van belang, de IT-auditor moet ook een inschatting maken van de achterliggende reden van de investering dan wel het project. Investerings- en projecten kunnen te maken hebben met niet (meer) goed functionerende of verouderde ICT-omgevingen.

Beleid

Informatie over projecten bij de over te nemen organisatie geeft inzicht in enerzijds de mate waarin zij volwassen met haar ICT-organisatie omgaat en anderzijds welke risico's er zijn en in welke mate deze worden beheerst. Door informatie op te vragen over het informatiebeleid, waarin de stand van zaken en de plannen voor de toekomst worden beschreven, krijgt de IT-auditor een goed beeld van de actuele ontwikkelingen binnen de ICT-organisatie. Een overzicht met een beschrijving van de projecten maakt deel uit van deze ontwikkelingen. Recent uitgevoerde projecten geven aan waar zwakke onderdelen in de ICT-organisatie zaten en welke onderdelen nu mogelijk vooroplopen ten opzichte van de marktontwikkelingen. Overzichten van de huidige en komende projecten geven inzicht in de huidige problemen die binnen de ICT-organisatie spelen. Hierbij hoort informatie over aanleiding, doel, omvang, budget, planning, tijdsplan, geïdentificeerde risico's, issue log, aangevane verplichtingen, huidige status, periodieke rapportages, et cetera.

Binnen de financiële sector is het van belang zicht te hebben op de ICT-gerelateerde plannen met betrekking tot grote wijzigingen in wet- en regelgeving die de organisatie treffen. Met name SEPA, Basel II en MiFID hebben de afgelopen jaren druk gelegd op de ICT-organisatie binnen financiële instellingen.

Essentieel in een due diligence-onderzoek bij een financiële instelling is de technische infrastructuur

Informatiesystemen en applicatieportfolio

Informatie over informatiesystemen en de applicatieportfolio geeft de IT-auditor inzicht in de wijze waarop primaire en secundaire bedrijfsprocessen worden ondersteund door systemen en medewerkers.

Het is voor de IT-auditor van belang te weten welke bedrijfsprocessen door welke systemen en mensen worden ondersteund. Hierdoor kan worden beoordeeld wat het effect is wanneer enkele bedrijfsprocessen weg zouden vallen in geval van overlap en welke efficiency (kostenbesparing) behaald kan worden. Aanvullend hierop moet de IT-auditor een overzicht ontvangen met de aanwezige systemen. Hierbij is onder meer van belang te beschikken over informatie omtrent de volgende onderwerpen:

- globale beschrijving van de opzet (functionaliteiten) van de systemen;
- relaties met andere systemen en eventuele interfaces;
- de omvang, bijvoorbeeld uitgedrukt in functiepunten of aantal te verwerken transacties;
- de ouderdom;
- plannen tot vervanging;
- het eigenaarschap (eventueel voorzien van een escrow-overeenkomst);
- standaardpakket of maatwerk;
- 'open source';
- aantal gebruikers;
- afhankelijkheid van andere systemen;
- onderliggende programmeertaal en databasemanagementsysteem;
- eigenaarschap en gerelateerde (onderhouds)contracten;
- overzicht beschikbare documentatie;
- koppelingen met externe systemen zoals dealingroom, SWIFT, Equens, clearing house en externe dataproviders (bijvoorbeeld Reuters en Bloomberg).

Bovengenoemde punten lijken in sommige gevallen wellicht overbodig. Echter, om een compleet beeld van de kwaliteit van de informatie- en transactieverwerkende systemen te krijgen, is het wel noodzakelijk om hiervan kennis te nemen. Diverse banken hebben bijvoorbeeld (technische) problemen met de applicaties die het bankieren door klanten door middel van het internet faciliteren. Een grote Nederlandse bank heeft onlangs € 40 miljoen uitgetrokken om verstoringen in deze techniek te verhelpen. Dit is een investering die bij een due diligence een belangrijke invloed op de prijs heeft.

De IT-auditor heeft bij zijn werkzaamheden eveneens informatie nodig over de systemen van derden. Dit is van belang bij het splitsen van de over te nemen financiële instelling en het samenvoegen met de kopende organisatie. Indien diensten worden overgenomen, waarbij cliënten toegang tot systemen verschaft wordt, moet de IT-auditor weten welke systemen dat zijn en welke verplichtingen daaruit voortvloeien.

Infrastructuur en tools

Door de technische infrastructuur te beoordelen wordt inzicht verkregen in de mogelijke synergie, wanneer onderdelen van beide organisaties elkaar overlappen. Andersom zou het moge-

lijk kunnen zijn dat het nodig is extra kosten te maken voor investeringen, wanneer veel vervangingen noodzakelijk zijn.

Essentieel in een due diligence-onderzoek bij een financiële instelling is de technische infrastructuur. Er moet worden gekeken naar mogelijke zwakheden, onder andere met het oog op beveiliging en overlap met de aanwezige infrastructuur bij de kopende organisatie. In geval van oude componenten in de infrastructuur moet de kopende organisatie rekening houden met forse investeringen om deze weer actueel te krijgen. Overlap met de aanwezige infrastructuur kan op termijn financiële voordelen opleveren. Financiële instellingen zijn een belangrijke prooi voor hackers. Derhalve zijn de investeringen die gemoeid zijn met het up-to-date brengen en houden van de beveiliging van de technische infrastructuur aanzienlijk. Binnen dit overzicht moet ook rekening worden gehouden met datacommunicatie met andere vestigingen, die zich mogelijk in het buitenland bevinden. Over de componenten in de infrastructuur moet bijvoorbeeld de volgende informatie beschikbaar zijn:

- ouderdom;
- eigenaarschap (in eigendom of gehuurd);
- geplande vervangingen;
- schaalbaarheid bij toenemend gebruik.

Denkbare componenten zijn servers, werkstations, besturings-systemen, databasemanagementsystemen, firewalls, netwerksoftware, protocollen, switches, modems en bekabeling.

Om de IT-auditor een beeld te geven van de volwassenheid van de beheerorganisatie, wordt gekeken naar de tools die worden ingezet voor:

- projectmanagement;
- beheer van de ontwikkel-, test-, acceptatie- en productie-omgeving;
- versiebeheer en change management.

Operations

Incidenten en performanceproblemen geven inzicht in de kwaliteit van de systemen binnen de organisatie en in welke mate deze systemen voldoen aan de verwachtingen en eisen van gebruikers. Op het niveau van de operationele uitvoering dient de IT-auditor inzicht te krijgen in de bezetting en de maximale capaciteit van het rekencentrum per platform. De twee organisaties zullen worden samengevoegd, waardoor het volume van de transacties toe zal nemen. De nieuwe ICT-omgeving zal deze hogere volumes volledig en juist moeten kunnen verwerken. Hiervoor is het van belang inzicht te krijgen in het aantal van de transacties van beide organisaties, aangevuld met de planning van de beschikbare capaciteit van netwerk, rekenkracht en opslag. Zodoende kan worden beoordeeld in welke mate de kritische grenzen zijn bereikt. De wijze waarop incident en performance management wordt ingevuld binnen de orga-

nisatie, geeft informatie over de volwassenheid van de beheerorganisatie. De service level rapportages hierover geven inzage in de feitelijke incidenten, problemen en prestaties van de systemen en de organisatie.

Beveiliging

Beveiliging is van groot belang bij financiële instellingen. Dit onderdeel speelt dan ook een belangrijke rol in het due diligence-onderzoek. De IT-auditor moet het algemene beveiligingsbeleid van de organisatie en in het bijzonder dat van de ICT-afdeling opvragen.

Per systeem wordt beoordeeld of de systemen die de financiële processen ondersteunen voldoende beveiligd zijn. Ten aanzien van de gesignaleerde risico's moet een overzicht van de getroffen maatregelen aanwezig zijn, om in te schatten in welke mate de onderliggende bedrijfsprocessen risico lopen. Hierbij kan worden gedacht aan uitwijkprocedures, back-up en recovery.

Aanvullend hierop geven rapportages van (interne en externe) auditors of toezichhouders een goed beeld van mogelijke onvolkomenheden op het gebied van beveiliging.



Contracten

Lopende contractuele verplichtingen verschaffen inzicht in de te verwachten kosten gedurende de komende jaren en op welke termijn deze mogelijk afgekocht zouden kunnen worden.

Contracten geven de IT-auditor inzage in alle diensten en producten die de organisatie afneemt bij derden en de financiële verplichtingen die daarbij horen. Gezien de kennis die een IT-auditor heeft van ICT is het beoordelen van ICT-gerelateerde contracten een waardevolle aanvulling op de juridische due diligence. Diensten die worden afgenomen, hebben veelal betrekking op de volgende onderwerpen:

- de inzet van externen;
- projecten;
- hardware (onder meer onderhoud);
- datacommunicatie;
- software (onder meer onderhoud en licenties);
- toegang/gebruik van systemen door derden;
- uitwijkfaciliteiten;
- escrow (ten behoeve van programmatuur);
- uitbesteding;
- mogelijkheden om contracten aan te passen aan de overnemende organisatie.

Het is van belang te kijken welke financiële verplichtingen uit deze contracten voortvloeien en hoelang een contract nog van toepassing is onder geldende voorwaarden (bijvoorbeeld ontvangen korting). De IT-auditor let hierbij op het eigenaarschap van de geleverde diensten, bijvoorbeeld servers, software en externen. Dit is onder andere van belang wanneer de kopende organisatie van plan is de contracten te beëindigen na het samenvoegen van de organisaties. Ook dient er aandacht besteed te worden aan de betrouwbaarheid en de levensvatbaarheid van de leverancier. Mogelijk wordt deze leverancier binnenkort overgenomen, stopt hij met enkele diensten of voldoet hij niet aan de hoge(re) eisen die de kopende organisatie stelt aan zijn diensten.

Wet- en regelgeving

Op diverse plaatsen in wet- en regelgeving wordt over data, gegevensverwerking, bewaren van data en privacy gesproken.

Onder andere de Wbp², Wft³ en MiFID⁴ stellen eisen op deze terreinen. Voor de overname is het al van groot belang hier rekening mee te houden.

- Op het gebied van privacy dient bij het samenvoegen van klantgegevens rekening te worden gehouden met de Wbp. 'Deze wet is van toepassing op de geheel of gedeeltelijk geautomati-

seerde verwerking van persoonsgegevens'. Wanneer klantgegevens van eigenaar wisselen (zoals bij een overname het geval is), moet de klant hierover worden geïnformeerd. Vanuit technisch oogpunt is het mogelijk en vaak ook wenselijk gegevens binnen de gehele organisatie samen te voegen en aan elkaar te koppelen. Soms moeten klantgegevens echter gescheiden worden bewaard van andere organisatieonderdelen. Ook dient de overnemende organisatie rekening te houden met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld door de overgenomen organisatie. De Wbp schrijft voor dat de verwerking van de gegevens 'niet onverenigbaar' mag zijn met het doel waarvoor de persoonsgegevens zijn verzameld. Cliënten moeten tevens worden geïnformeerd over de nieuwe ontwikkelingen bij de kopende organisatie betreffende de gegevensverwerking en hebben het recht bezwaar ('recht van verzet') hiertegen te maken. Daarnaast worden er een bewaarplicht en -termijn van de gegevens voorgeschreven in de Wbp.

- De Wft stelt met name eisen aan de maatregelen die de organisatie dient te nemen om informatiesystemen goed te kunnen beheren. Zo dient de organisatie te beschikken over een 'informatiesysteem dat een effectieve beheersing van de bedrijfsprocessen en de risico's mogelijk maakt'. Daarnaast moet de organisatie maatregelen treffen ten aanzien van de integriteit, beschikbaarheid, functiescheiding en beveiliging van geautomatiseerde gegevensverwerking. Een financiële instelling is verplicht te beschikken over 'een onafhankelijke compliancefunctie voor het toezicht op de naleving van wettelijke regels en van interne regels' die door de organisatie zelf zijn opgesteld.

- In de MiFID is vastgelegd hoe organisaties dienen om te gaan met de afhandeling van aandelenorders door beleggingsorganisaties, waarbij de transparantie een belangrijk aandachtspunt is. De MiFID heeft als doel 'de bevordering van een eerlijke, transparante, efficiënte en geïntegreerde financiële markt met behoud van optimale beleggersbescherming'. Er worden expliciete regels gesteld aan bijvoorbeeld de organisatiestructuur, informatiesystemen, rapportages, persoonlijke transacties en uitbesteding.

Volwassenheid van de ICT-organisatie

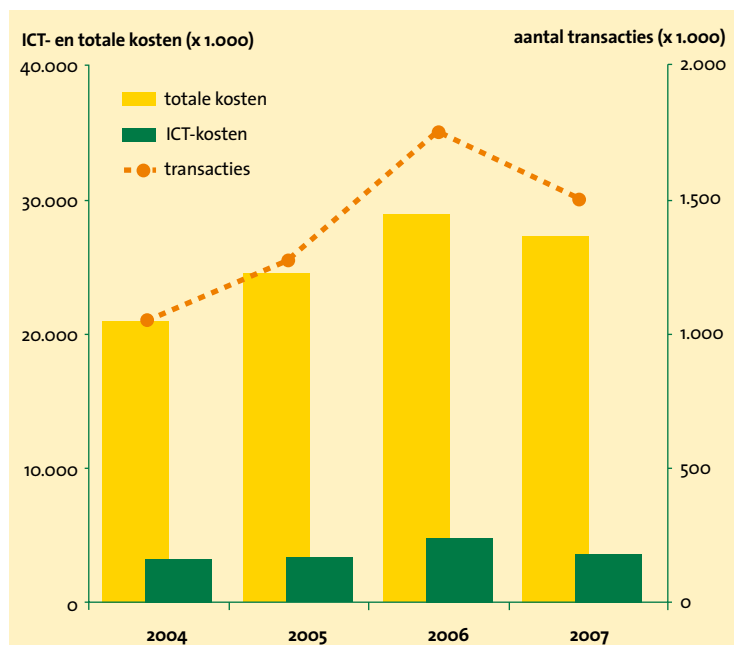
Een volledig uitgevoerde ICT due diligence biedt voldoende inzicht in de ICT-organisatie om zich een oordeel over de volwassenheid van (delen van) de ICT-organisatie te kunnen vor-

Met de invloed van wet- en regelgeving omtrent privacy moet bij overname rekening worden gehouden

2) Wet bescherming persoonsgegevens.

3) Besluit van 12 oktober 2006, houdende prudentiële regels voor financiële ondernemingen die werkzaam zijn op de financiële markten (Besluit prudentiële regels Wft).

4) Markets in Financial Instruments Directive.



Figuur 2. ICT-kosten versus de totale kosten en het aantal transacties.

men. Een veelgebruikt model hiervoor is het *Stages of growth*-model van Richard L. Nolan. Dit model onderkent de volgende fasen in volwassenheid van een ICT-organisatie:

1. Het stadium 'initiation' wordt gekenmerkt door lage uitgaven aan dataprocessing en beperkte betrokkenheid van gebruikers en management.
2. Voor het stadium 'contagion' is het kenmerkend dat budgetten hoger worden en tegelijkertijd het gebruik van systemen erg snel toeneemt, wat voor een ongecontroleerde omgeving met incidenten zorgt.
3. Vervolgens wordt bij 'control' dataprocessing serieus genomen door het management en er worden controls geformuleerd om systemen te beheersen. Desondanks is communicatie tussen systemen nog foutgevoelig.
4. In het stadium 'integration' krijgt dataprocessing een groter budget toegekend en worden online diensten verlangd door gebruikers. Het management past meer formele werkwijzen toe, zoals projectmanagement, standaardprocedures en controls.
5. De applicatieportfolio is bij 'data administration' geïntegreerd in de organisatie. Dataprocessing wordt nu als dienst aangeboden.
6. Als laatste kenmerkt het stadium 'maturity' zich door de strategische plek die dataprocessing in de organisatie krijgt. De CIO en de CFO hebben een even belangrijke rol toebedeeld gekregen.

Op te vragen informatie

In het voorgaande zijn documenten en informatie genoemd die de IT-auditor nodig heeft bij het opstellen van zijn rapportage. Deze documenten worden tegenwoordig steeds vaker digitaal

aangeleverd in een *virtual dataroom*. De over te nemen organisatie levert eenmalig alle data op die op een centrale, virtuele plek benaderd kunnen worden door financiële, ICT- en juridische experts. Mede omdat de documenten vaak voor diverse experts interessant zijn (bijvoorbeeld ICT-contracten) werkt dit efficiënter. Deze datarooms en de opgeslagen documenten zijn uitgebreid beveiligd. Uitgifte van gebruikersrechten is over het algemeen in handen van het begeleidend advocatenkantoor.

Uiteraard is het van belang met enkele belangrijke functionarissen, zoals de CIO en de CTO, een gesprek te hebben om zo meer inzicht te krijgen over de ontvangen informatie. Verder kan de IT-auditor tijdens het interview ingaan op nog openstaande vragen.

Op te leveren eindproduct (rapport)

In het rapport worden de feitelijke observaties gescheiden van de bevindingen. Zodoende wordt duidelijk wat enerzijds is geconstateerd en anderzijds welk (mogelijk) effect dat in de ogen van de IT-auditor op de ICT-organisatie heeft.

In figuur 2 is een voorbeeld gegeven van een uitgevoerde analyse van de ontwikkeling van de ICT-kosten ten opzichte van het aantal te verwerken transacties binnen een financiële instelling. Aanvullend hierop kunnen berekeningen worden gemaakt om de kosten per transactie of het percentage ICT-kosten als deel van de totale kosten te verkrijgen.

Onderstaand zijn ter illustratie enkele bevindingen uit IT due diligence-rapportages opgenomen:

- Het ICT-personeel op de sleutelposities heeft veel kennis van de ICT-omgeving en werkt gemiddeld 20 à 25 jaar bij bedrijf X. Hierdoor is bedrijf X erg afhankelijk van deze medewerkers, wat mede wordt veroorzaakt door de complexiteit van de ICT-infrastructuur en het gebrek aan documentatie.
- Het project voor het vervangen van de infrastructuur kost € 4,8 miljoen. Dit is de komende vier jaar het belangrijkste project. Een groot deel van deze investering, à € 1,26 miljoen, is nodig omdat netwerkcomponenten de komende jaren aan het einde van hun life cycle zijn.
- Systeem A is een erg complexe applicatie, die niet volledig gedocumenteerd is. In de nabije toekomst zal een migratie naar een .NET-omgeving overwogen moeten worden.

Aanpak tijdens en belang van de fase na afronding van de fusie

Om tijdig inzicht te krijgen in de mogelijke knelpunten bij integratie dient gedurende het due diligence-onderzoek aandacht

te worden besteed aan de mate van integratie die wordt nagestreefd. Indien de organisatie een hoge mate van integratie nastreeft, is een onderzoek naar de mogelijkheden om de ICT-organisatie, -systemen en -projecten te integreren, relevanter dan bij een lagere mate van integratie. Derhalve dient het management van de overnemende organisatie in een vroeg stadium te beslissen over de gewenste en verwachte mate van integratie na de fusie, onder andere in verband met de te behalen mate van efficiency.

Zelfs bij overname van een financiële instelling met vergelijkbare processen kan de integratie een uitdaging worden. Indien verschillende applicaties en infrastructuur worden gebruikt, kan integratie een ingewikkeld traject worden. Op basis van zijn kennis en ervaring kan de IT-auditor ook na de fusie een belangrijke rol in de integratie spelen. Dit kan een beoordelende (quality assurance) rol tijdens het project zijn, maar ook een actieve rol in het projectmanagement of bij uitvoerende werkzaamheden tijdens de integratie. Verder kan met data-analyse de conversie gecontroleerd worden op juistheid en volledigheid.

Samenvatting

In dit artikel hebben wij het belang van een ICT-onderzoek toegelicht en de rol die de IT-auditor binnen een due diligence-onderzoek kan spelen. Tevens is aangegeven welke aandachtspunten de IT-auditor daarbij hanteert.

De ICT due diligence heeft inzicht gegeven in de status (volwassenheid) van de ICT en de ICT-organisatie en in mogelijke knelpunten. Afhankelijk van de integratiedoelstellingen van de organisatie is het van belang al voor de fusie een integratieplan op te stellen zodat na de fusie voortvarend kan worden begonnen met de integratie. In deze fase kan de IT-auditor vanuit zijn ervaring met ICT-organisaties en complexe veranderingstrajecten een belangrijke adviserende of controlerende rol spelen tijdens het integratieproces.

Literatuur

- wetten.overheid.nl/cgi-bin/sessioned/browsercheck/continuation=19860-002/session=051182725609744/action=javascript-result/javascript=yes
- www.dft.nl/goeroes/joopnederstigt/2821313/Slimme_fusie_Binck_Bank_en_Alex.html
- www.dnb.nl/dnb/home/file/fmo6-1260c_tcm46-145514.pdf
- www.minfin.nl/nl/onderwerpen,financiele_markten/consultaties/mifid#top
- Specialist in maart 2007: www.google.com/notebook/public/13528031618643256697/BDQs4SwoQtJ74xNgh