Corporate Governance: de relatie naar ICT

Drs. J.C. de Boer RE en mw. ir. E.R. van Sommeren RE

Corporate Governance staat momenteel sterk in de belangstelling. In de tot nu toe verschenen publicaties speelt ICT en de beheersing daarvan geen grote rol in de Corporate Governance-discussie. Gelet echter op de functie van ICT bij de besturing en beheersing van een organisatie en de alsmaar toenemende ICT-afhankelijkheid van organisaties lijkt voor ICT op (korte?) termijn een aanzienlijke rol te zijn weggelegd in deze discussie.

Inleiding

Corporate Governance staat de afgelopen jaren sterk in de belangstelling. Dit komt onder andere door onverwachte faillissementen (zoals van Maxwell, BCCI en Barings) die mede zijn veroorzaakt door tekortschietend intern beheer. De discussies richten zich niet alleen op de taken en verantwoordelijkheden en de hoogte van vergoedingen van bestuurders, maar ook op de taken en verantwoordelijkheden van toezichthouders, zoals commissarissen, audit committees en benoemings- en beloningscommissies ([Cadb92]).

Ook in Nederland is de belangstelling voor Corporate Governance flink aangewakkerd. Reeds diverse organisaties hebben zich met dit onderwerp beziggehouden, zoals de door de Vereniging voor Effectenhandel/ Amsterdamse Effectenbeurs ingestelde 'Commissie Corporate Governance' ([Comm97]). Deze commissie heeft in juni 1997 een rapport uitgebracht waarin de 'aanbevelingen inzake Corporate Governance in Nederland' zijn opgenomen. Het betreft hier aanbevelingen voor goed bestuur, adequaat toezicht en het afleggen van verantwoording.

Gezien de functie van de Informatie- en Communicatietechnologie (ICT) bij de besturing en beheersing van een organisatie en de toenemende afhankelijkheid van organisaties van Informatietechnologie (IT), lijkt voor ICT een rol weggelegd te zijn. In dit artikel is getracht meer inzicht te verkrijgen in de rol van de besturing en beheersing van ICT binnen Corporate Governance. Daarnaast wordt in dit artikel ingegaan op de vraag welke rol de ICT-auditor in dit kader kan spelen. Hieraan voorafgaand wordt het begrip Corporate Governance toegelicht.

Corporate Governance

Corporate Governance wordt in Nederland steeds actueler maar is bij organisaties nog relatief onbekend. Om begripsverwarring te voorkomen, is een definitie gewenst. In dit artikel zal worden uitgegaan van de volgende definitie:

Corporate Governance omvat het besturen en beheersen van een onderneming, alsmede het toezicht dat op de organisatie wordt uitgeoefend en de verantwoording die daarover wordt afgelegd ([KPMG96]).

Randvoorwaarden bij dit proces zijn dat de besturings- en beheerssystemen op een juiste manier werken zodat de bedrijfsprocessen op een adequate wijze worden uitgevoerd. Hierdoor kan de waarde van de onderneming toenemen en de continuïteit worden gewaarborgd ([KPMG96]).

Ondanks het feit dat de elementen uit de definitie weinig vernieuwend lijken, heeft de praktijk laten zien dat onverwachte faillissementen toch kunnen plaatsvinden. Dit betekent dat in de uitvoering van het besturings- en beheersingsproces zich knelpunten kunnen voordoen die invloed hebben op het bereiken van de organisatiedoelstellingen. Om meer zekerheid te verkrijgen dat een organisatie op een juiste wijze wordt bestuurd en beheerst, is het van belang dat periodiek een beoordeling plaatsvindt, eventueel uitgevoerd door een onafhankelijke en onpartijdige organisatie. Ook deze beoordeling is niet echt als nieuw aan te duiden, tenzij een dergelijke beoordeling verplicht wordt en/of organisaties worden verplicht hierover iets op te nemen in de jaarstukken. De verslaggeving van het proces wordt hiermee meer geformaliseerd.

Corporate Governance en Internal Governance

Bij de definitie van Corporate Governance is aangegeven dat de belangrijkste randvoorwaarde voor de realisatie van een goede Corporate Governance is dat *besturings- en beheerssystemen* op een juiste manier werken en adequaat worden uitgevoerd. Volgens Strikwerda ([Stri97]) kan dit laatste worden aangeduid als *Internal Governance*. De kwaliteit van Internal Governance is onderwerp van Corporate Governance maar dient naar onder andere uitvoering en verantwoordelijkheid te worden gescheiden van Corporate Governance.

De kapitaalverschaffer moet geïnteresseerd zijn in de kwaliteit van Internal Governance. De realisatie daarvan is de verantwoordelijkheid van de Raad van Bestuur

([Stri97]). Deze 'dwangmatige' interesse voor Internal Governance, hier verder aangeduid als interne beheersing, wordt ondersteund door de resultaten van de National Commission on Fraudulent Financial Reporting (Treadway Commission) ([Waar97]). Deze commissie kwam in 1987 tot de conclusie dat het onvoldoende functioneren van internecontrole(beheersings-)systemen één van de belangrijkste oorzaken was van onbetrouwbare verslaggeving.

Interne beheersing wordt door het belang van de kwaliteit hiervan nader beschreven en als belangrijk element binnen Corporate Governance gezien. Onder interne beheersing wordt niet altijd door iedereen hetzelfde verstaan en het begrip is in de literatuur niet eenduidig gedefinieerd. In dit artikel wordt het omschreven als een proces, bestaande uit een serie van activiteiten, met als doel het geven van richting aan de verschillende organisatieprocessen en deze waar nodig bijsturen, om daarmee het gekozen beleid en de strategie van de organisatie te realiseren. Een effectief beheersingssysteem bestaat derhalve uit de processen: planning, uitvoering en evaluatie.

Het uitbesteden van ICT-activiteiten betekent niet dat ICT minder aansturing behoeft.

Corporate Governance en de relatie naar ICT

In de tot nu toe verschenen publicaties wordt de besturing en beheersing van ICT niet direct als onderdeel van Corporate Governance genoemd. De vraag is of op basis hiervan kan worden geconcludeerd dat de besturing en beheersing van ICT geen rol speelt in het besturen en beheersen van de organisatie. Voor het beantwoorden van deze vraag zijn de ontwikkelingen binnen organisaties en de aanbevelingen van de Commissie Corporate Governance nader geanalyseerd.

Ontwikkelingen

De ontwikkelingen binnen organisaties geven aan dat de behoefte een adequate besturing en beheersing van ICT nog nooit zo groot is geweest als op dit moment. Verwacht wordt dat deze behoefte in de toekomst verder zal toenemen. Voorbeelden van ontwikkelingen die hier een bijdrage aan leveren zijn ([KPMG99]):

* *het toenemende aantal omvangrijke fusies en acquisities van en door organisaties.* Elke afzonderlijke organisatie heeft in deze gevallen veelal een eigen ICT-infrastructuur, met eigen kenmerken en een eigen historie. Om de beoogde voordelen van de fusie of acquisitie te realiseren is één van de doelstellingen vaak het in korte tijd realiseren van een geïntegreerde ICT-infrastructuur, inclusief de aansturing en beheersing daarvan. De ervaring leert dat dergelijke trajecten complex zijn en niet eenvoudig te verwezenlijken;
* *de behoefte aan het realiseren van synergie- en integratievoordelen met behulp van de toepassing van ICT.* Het grote aantal ERP-implementaties van de afgelopen jaren is hiervan een sterk voorbeeld. Uit onze praktijk en uit diverse studies blijkt dat de beoogde voordelen van ERP-implementaties nog lang niet zijn gerealiseerd. Bij diverse organisaties zijn momenteel dan ook ERP-optimalisatieprojecten opgestart die elk afzonderlijk moeten worden gemanaged;
* *concentratie binnen organisaties op het uitvoeren van kernactiviteiten.* De exploitatie en het beheer van ICT is veelal geen kernactiviteit. Analisten voorspellen dan ook een gouden toekomst voor outsourcing. Volgens DataQuest zal de Application Service Providers-markt in 2003 zijn uitgegroeid tot $ 30 miljard (nu $ 900 miljoen in de Verenigde Staten). Geschat wordt dat dit voor Europa $ 7,1 miljard zal zijn. Het uitbesteden van ICT-activiteiten betekent niet dat ICT minder aansturing behoeft. Eén van de voorwaarden voor succesvol uitbesteden is dat het uitbestedingscontract goed wordt gemanaged;
* *de toepassing en het gebruik van moderne toepassingen van ICT.* Niemand zal in dit kader de ontwikkelingen op het gebied van e-business zijn ontgaan. De meer dan fantastische voordelen, de grote investeringen, maar ook de grote risico's die gepaard gaan met de toepassing van e-business maken het belang van een adequate beheersing en besturing groot. De Gartner Group heeft in 1999 voorspeld dat in 2002 75% van de e-businessprojecten niet succesvol zal zijn in het realiseren van de beoogde doelstellingen. Als belangrijke reden hiervoor wordt een falend projectmanagement aangegeven.

Analyse van de aanbevelingen van de Commissie Corporate Governance

Voor aanknopingspunten voor de rol van ICT binnen Corporate Governance zijn tevens de veertig aanbevelingen van de Commissie Corporate Governance nader geanalyseerd. In deze aanbevelingen wordt geen directe link gelegd naar ICT. Indirect is wel een link te leggen naar het belang van ICT. Aanknopingspunten kunnen worden gevonden in onder andere de volgende aanbevelingen:

* *Aanbeveling 17.* De Raad van Commissarissen bespreekt ten minste eenmaal per jaar de strategie en de risico's verbonden aan de onderneming en de uitkomsten van de beoordeling door de Raad van Bestuur van de opzet van de interne beheersingssystemen. Van het houden van de bespreking wordt melding gemaakt in het verslag van de Raad van Commissarissen in het jaarverslag.
* *Aanbeveling 21.* De Raad van Bestuur rapporteert schriftelijk aan de Raad van Commissarissen over de ondernemingsdoelstellingen, de strategie, de daaraan verbonden risico's en de mechanismen tot beheersing van risico's van financiële aard. De hoofdzaken van de rapportage behoren een vaste plaats in het jaarverslag te hebben. Kwantificering kan als hulpmiddel dienen om de doelstellingen en strategie duidelijker naar voren te brengen. Indien er kwantificeringen zijn gegeven, dienen deze te worden benut bij vergelijkingen met realisaties.
* *Aanbeveling 36.* De accountantscontrole van de jaarrekening vormt één van de hoekstenen van een goed systeem van Corporate Governance.

In Aanbeveling 21 van de Commissie Corporate Governance is opgenomen dat dient te worden gerapporteerd over de ondernemingsdoelstellingen, de strategie, de daaraan verbonden risico's en de mechanismen tot beheersing van risico's van financiële aard (beheersingssystemen). Effectieve interne beheersingssystemen zijn vaak in belangrijke mate afhankelijk van de kwaliteit van de onderliggende ICT ([Rene96]).

De rol van ICT binnen Corporate Governance

De ontwikkelingen binnen organisaties en de analyse van de aanbevelingen geven aan dat voor het besturen en beheersen van een onderneming de kwaliteit van de onderliggende ICT een rol speelt. Automatiseringsprojecten bijvoorbeeld kunnen gezien hun grote impact op de bedrijfsvoering een bedrijfsrisico vormen, net als het niet op orde hebben of het niet up-to-date zijn van de automatisering in de organisatie. De kwaliteit van de geautomatiseerde informatieverwerking bepaalt immers direct de kwaliteit van de opgeleverde informatie; rapportering over de besturing en beheersing van ICT lijkt derhalve onderdeel van Corporate Governance te moeten uitmaken.

Rol voor de ICT-auditor

Net als voor de rol van de besturing en beheersing van ICT binnen Corporate Governance geldt voor de rol van de ICT-auditor dat deze niet expliciet is gedefinieerd. Indirect is ook deze rol aanwezig. In de veertig aanbevelingen wordt gesproken over het controleren van de jaarrekening. In het kader van de jaarrekeningcontrole beoordeelt de ICT-auditor de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. In geval van redelijk complexe ICT binnen organisaties zijn accountants veelal verplicht dan wel gedwongen om voor de beoordeling van ICT een specialist in te schakelen: een ICT-auditor. Hiermee is de rol van de ICT-auditor binnen Corporate Governance nader gedefinieerd. Deze rol is slechts indirect aanwezig ([Boer96]).

Opgemerkt wordt dat de accountantsrapportage slechts over een deel van het interne beheersingssysteem opmerkingen bevat. De resultaten van de controle van de jaarrekening zijn derhalve onvoldoende om enkel en alleen als basis te dienen voor het beoordelen van de kwaliteit van het besturen en beheersen van een organisatie. Op de invloed van Corporate Governance op de jaarrekeningcontrole wordt in dit artikel niet ingegaan.

Rapportering over besturing en beheersing van ICT

Rapportering over de besturing en beheersing van ICT lijkt een onderdeel te moeten uitmaken van Corporate Governance. Om hieraan nadere invulling te kunnen geven is het van belang om onder andere antwoord te verkrijgen op de volgende vragen:

* Welke doelstellingen worden gesteld ten aanzien van ICT?
* Welke informatie kan door het management worden verlangd om vast te stellen dat de doelstellingen zijn gerealiseerd?
* Op welke wijze kan meting van de besturing en beheersing van ICT plaatsvinden?

Voor het beantwoorden van deze vragen zijn in dit artikel voorstellen gedaan.

Doelstellingen ten aanzien van ICT

Volgens de omschrijving van interne controle in het COSO-rapport ([COSO94]) bieden effectieve interne beheersingssystemen redelijke zekerheid dat de bedrijfsdoelstellingen van organisaties worden bereikt inzake de volgende categorieën:

1. de effectiviteit en de efficiëntie van bedrijfsprocessen;
2. de betrouwbaarheid van de (financiële) informatieverzorging;
3. het naleven van relevante wet- en regelgeving.

Opgemerkt wordt dat de betrouwbaarheid van de informatieverzorging niet beperkt is tot de financiële informatie.

De te bereiken doelstellingen voor effectieve interne beheersingssystemen zijn aangevuld met de mogelijke rol van ICT, voorbeelden van risico's bij onvoldoende beheersing en de mogelijke rol van de ICT-auditor (zie tabel 1).

Doelstellingen	Rol/belang ICT	Risico's	Rol ICT-auditor
De effectiviteit en de efficiëntie van bedrijfsprocessen.	ICT-hulpmiddelen spelen een belangrijke rol in ondersteunen van bedrijfsprocessen en het realiseren van strategische voorsprongen.	* Onvoldoende bewaking grote ICT-projecten en daarmee sterke operationele organisatieproblemen. * Onbeheersbare (hoge) kosten. * Te lange doorlooptijden. * Onvoldoende leverbetrouwbaarheid.	Beoordelen van/ adviseren over de inzet van ICT en de ICT-hulpmiddelen.
De betrouwbaarheid van de (financiële) informatieverzorging.	De betrouwbaarheid van informatie is mede afhankelijk van de betrouwbaarheid en continuïteit van de ICT.	* Hoge klachtenpercentages en hoge omzetcorrecties. * Onbetrouwbare management-informatie. * Verlies van bedrijfsinformatie. * Fraude. * Ongeautoriseerde transacties.	Beoordelen van/ adviseren over de general ICT controls en de application controls.
Het naleven van relevante wet- en regelgeving.	Informatie is opgeslagen met behulp van ICT-hulpmiddelen. Voorbeelden: Wet persoons-registraties (WPR) en Wet computercriminaliteit (WCC).	* Handelen in strijd met wet- en regelgeving en daarmee in overtreding.	Beoordelen van/ adviseren over implementatie van de wetgeving.

Tabel 1. Mogelijke weergave van de rol van ICT en de ICT-auditor.

Bij tabel 1 moet worden opgemerkt dat een dergelijke 'zwart-witte' scheiding in de praktijk moeilijk is te maken. Indien bijvoorbeeld de informatievoorziening niet betrouwbaar is, heeft dit invloed op de effectiviteit en efficiëntie van de bedrijfsprocessen. Om zekerheid te verkrijgen over de realisatie van de genoemde doelstellingen is het voor een organisatie van belang grip te krijgen op de besturing en beheersing van ICT. De risico's bij onvoldoende beheersing laten zien dat de gevolgen voor een organisatie groot kunnen zijn.

Om hier een meer concrete invulling aan te geven zijn de in de tabel genoemde doelstellingen en de daarbij genoemde rol van ICT vertaald naar ICT-doelstellingen:
* de effectiviteit en de efficiëntie van de inzet van ICT;
* de betrouwbaarheid en continuïteit van ICT (en van de algehele informatievoorziening);
* het naleven van relevante wet- en regelgeving inzake ICT.

Om de beheersing van ICT te kunnen uitvoeren, is het voor het management van bedrijven van belang dat het hierover juist wordt geïnformeerd.

Informatie over ICT

Het juist informeren van het management van bedrijven is in de praktijk niet altijd eenvoudig. De informatiebehoeften van managers lopen veelal uiteen of zijn onvoldoende gedefinieerd. Daarnaast blijkt uit de praktijk dat informatie vaak moeilijk beschikbaar is. Vanuit diverse bronnen blijkt dat het management wel degelijk behoefte heeft om juist te worden geïnformeerd over de besturing en beheersing van ICT. In dit artikel is derhalve vanuit ICT-auditoogpunt gedefinieerd welke informatie mogelijk door het management zou kunnen worden verlangd om vast te stellen dat de doelstellingen ten aanzien van ICT zijn gerealiseerd.

De effectiviteit en de efficiëntie van de inzet van ICT
Het is niet eenvoudig om de effectiviteit en de efficiëntie van de inzet van ICT aan te duiden. Het is in ieder geval van belang een balans te vinden tussen onder andere:
* het belang van het informatiesysteem:
  – Hoe afhankelijk is de organisatie van het betreffende informatiesysteem?
  – Wat zijn de kosten indien het systeem niet operationeel is?
* de waarde van de informatie (classificaties van data, vertrouwelijkheid);
* de waarde van de apparatuur/componenten (de vervangingskosten);
* de kosten voor het waarborgen van de betrouwbaarheid en continuïteit.

Daarnaast is het van belang om inzicht te krijgen in antwoorden op onder andere de volgende vragen:
* In welke mate draagt ICT bij aan het behalen van de bedrijfsdoelstellingen en/of strategisch voordeel op de concurrent?
* Wat is de volwassenheid van de ICT-organisatie?
* Zijn de kosten van ICT niet te hoog (of te laag)?
* In welke mate is er sprake van een flexibel systeem (denk hierbij tevens aan de implementatie van de euro) voor wat betreft:
  – onderhoudbaarheid;
  – toekomstvastheid?
* In welke mate zijn gebruikers tevreden over (en maken ze juist gebruik van) de geautomatiseerde systemen?

De rapportering over alleen de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking (ICT) geeft onvoldoende inzicht in de effectiviteit en efficiëntie van de inzet van ICT. Het risico bestaat dat te veel middelen worden ingezet om de betrouwbaarheid en de continuïteit te waarborgen. Daarnaast bestaat het risico dat mogelijk een andere inrichting van ICT beter bijdraagt aan het realiseren van de organisatiedoelstellingen of het behalen van strategisch voordeel ten opzichte van directe concurrenten.

Te ontvangen informatie
Om inzicht te krijgen in de effectiviteit en de efficiëntie van ICT is het van belang informatie te ontvangen waaruit blijkt dat de inzet van ICT en de ICT-hulpmiddelen effectief en efficiënt plaatsvindt. Om zekerheid te verkrijgen over het feit dat de doelstelling 'de effectiviteit en efficiëntie van ICT' wordt gerealiseerd, kan informatie op hoofdlijnen vereist dan wel gewenst zijn over:
* het informatiebeleid en de informatieplanning (strategic alignment);
* de functionele en technische kwaliteit van de programmatuur/applicaties;
* de geplande en lopende automatiseringsprojecten;
* de kwaliteit en productiviteit van de automatiseringsmedewerkers;
* de kosten en baten van ICT.

Het verkrijgen van inzicht in de effectiviteit en efficiëntie is niet eenvoudig. Er zijn geen algemene normen of richtlijnen beschikbaar die aangeven of ICT effectief en efficiënt wordt ingezet in de organisatie. Beoordeling kan derhalve plaatsvinden op het feit of de door de organisatie gestelde doelen en/of normen zijn gerealiseerd. De kans bestaat dat de doelen weinig ambitieus of niet voldoende concreet zijn gedefinieerd. Soms ontbreken de doelen zelfs geheel. Om in dergelijke gevallen toch inzicht te krijgen in de effectiviteit en efficiëntie kan bijvoorbeeld gebruik worden gemaakt van benchmarking. Door het toepassen van deze techniek kunnen aspecten, zoals de volwassenheid van de ICT-organisatie en de kosten van ICT, met andere organisaties worden vergeleken.

De betrouwbaarheid en continuïteit van ICT
Gezien de toenemende afhankelijkheid van organisaties van automatisering wordt de beheersing ervan steeds belangrijker. Al jaren worden door ICT-auditors de sterkte(n) en zwakte(n) van de general ICT controls in kaart gebracht met als doel inzicht te krijgen in de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Op basis van de beoordeling wordt aan de opdrachtgever een aantal aanbevelingen gedaan hoe verbeteringen kunnen worden aangebracht. In dit proces spelen een gedegen risicoanalyse en professional judgement van de auditor een belangrijke rol.

Naast de general ICT controls wordt de betrouwbaarheid van een ICT-systeem beheerst door computercontroles die zich richten op de betrouwbare werking van een specifieke applicatie (de application controls of toepassingscontroles ([Munc95])). Bij voortschrijdende automatisering worden onder meer uit efficiëntieoogpunt in toenemende mate controles in de applicatie geïmplementeerd. Om ervoor te zorgen dat deze application controls bij voortduring effectief zijn, worden hogere eisen gesteld aan de general ICT controls. De general ICT controls dienen te voldoen aan de steeds hogere eisen die vanuit de administratieve organisatie en de applicaties worden gesteld.

Te ontvangen informatie
Ten eerste is het van belang inzicht te krijgen in de risico's die door de organisatie worden gelopen ten aanzien van de betrouwbaarheid en continuïteit van ICT. Vervolgens is het van belang informatie te ontvangen waaruit blijkt dat potentiële risico's voldoende met de huidige getroffen maatregelenset zijn afgedekt. Om zekerheid te verkrijgen over het feit dat de doelstelling 'de betrouwbaarheid en continuïteit van ICT (en van de algehele informatievoorziening)' wordt gerealiseerd, kan informatie op hoofdlijnen vereist dan wel gewenst zijn over:
* de risico's ten aanzien van de betrouwbaarheid van ICT (gegevensverwerking);
* de risico's ten aanzien van de continuïteit van ICT (gegevensverwerking);
* de mate waarin de getroffen maatregelen de bestaande risico's afdekken;
* de risico's die met de huidige maatregelenset niet worden afgedekt.

Bij het bepalen van de omvang/zwaarte van de risico's kunnen de volgende aandachtsgebieden een rol spelen:
* de afhankelijkheid van de organisatie van ICT;
* de beschikbare kennis van en ervaring met ICT en de beschikbaarheid van ICT-middelen;
* het bewustzijn van het management ten aanzien van de inzet van ICT[1].

Om het bewustzijn van het management verder te kunnen vergroten kan bijvoorbeeld gebruik worden gemaakt van benchmarking van de ICT-beheersingsmaatregelen. Achterstand dan wel voorsprong op andere organisaties heeft veelal een grotere impact op het denken en handelen en leidt derhalve tot daadwerkelijke verbeteringen.

Het naleven van relevante wet- en regelgeving inzake ICT
Onafhankelijk van de twee vorige doelstellingen is het van belang om als organisatie te voldoen aan de wet- en regelgeving. Wet- en regelgeving kan op verschillende manieren invloed hebben op de inrichting van de informatiesystemen. Die invloed hoeft niet beperkt te blijven tot de verplichting om gegevens een bepaalde tijd te bewaren. Eveneens kan worden gedacht aan een verbod op het openbaar maken van gegevens en de manier van informatieverzameling ten behoeve van rapportering aan regelgevende organen. Het is derhalve van belang vast te stellen in hoeverre binnen de organisatie maatregelen zijn getroffen die waarborgen dat (tijdig) wordt voldaan aan de relevante wettelijke en contractuele voorschriften.

Te ontvangen informatie
Om inzicht te krijgen in de risico's ten aanzien van het (niet) naleven van relevante wet- en regelgeving inzake ICT, is het van belang informatie te ontvangen waaruit blijkt dat (potentiële) risico's voldoende met de huidige maatregelenset zijn afgedekt. Om zekerheid te verkrijgen over het feit dat de doelstelling 'naleven van relevante wet- en regelgeving inzake ICT' wordt gerealiseerd, kan informatie op hoofdlijnen vereist dan wel gewenst zijn over:
* de mate waarin wet- en regelgeving zoals de Wet computercriminaliteit, Wet persoonsregistraties etc. binnen de organisatie van toepassing zijn en welke gevolgen dit heeft voor automatisering;
* de mate waarin wordt voldaan aan relevante wet- en regelgeving en deze zijn geïmplementeerd in de informatievoorziening;
* de mate waarin niet wordt voldaan aan relevante wetgeving.

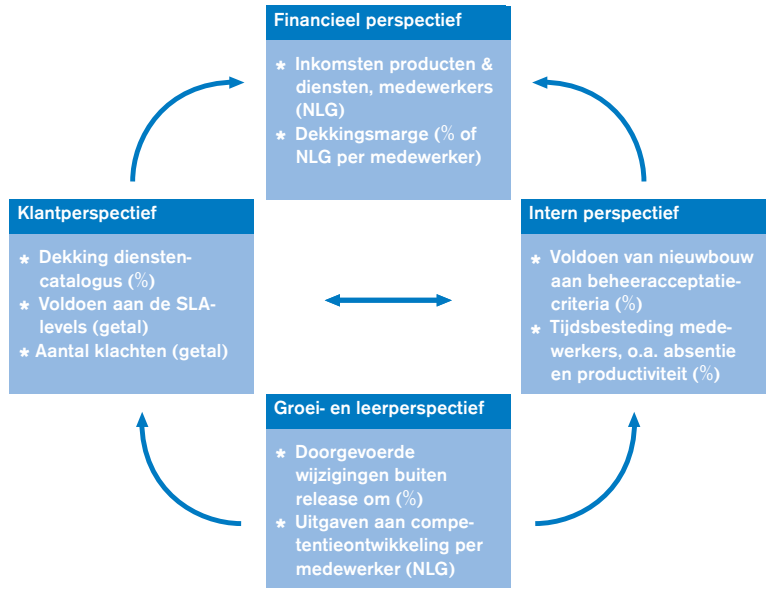
Het voldoen aan de relevante wet- en regelgeving en de implementatie hiervan in de (IT-)informatievoorziening kan als een ICT-beheersingsmaatregel op zich worden beschouwd. Om te voorkomen dat de organisatie niet of onvoldoende aandacht heeft besteed aan relevante wet- en regelgeving binnen de organisatie, is het van belang om te anticiperen op wijzigingen. Dit houdt in dat wijzigingen tijdig worden gesignaleerd en worden geïmplementeerd in de organisatie. Voor een tijdige implementatie is met name van belang in welke mate de geautomatiseerde systemen eenvoudig kunnen worden gewijzigd.

Meten van de besturing en beheersing van ICT: the Balanced Scorecard

Organisaties hebben verschillende hulpmiddelen en methodieken ter beschikking om informatie over de hiervoor genoemde ICT-doelstellingen te verkrijgen. In diverse eerdere nummers van Compact zijn hiervan verschillende voorbeelden gegeven: ITIL, CobIT en Code voor Informatiebeveiliging. Vanzelfsprekend kan de ICT-auditor met het uitvoeren van audits het management veel informatie verschaffen over de mate waarin de ICT-doelstellingen worden bereikt en gemanaged.

De laatste jaren nemen wij een trend waar dat organisaties de performance van ICT en de ICT-organisatie steeds meer gaan meten. Hiertoe worden steeds vaker methoden geadopteerd die ook voor de reguliere business worden toegepast. Een voorbeeld daarvan is het gebruik van de Balanced Scorecard ([Grem97]). De Balanced Scorecard is door Kaplan en Norton ontwikkeld om een performance-managementsysteem te bieden aan managers dat ernaar streeft een ideaal evenwicht te creëren tussen doelstellingen op korte en op lange termijn, tussen financiële en niet-financiële metingen en tussen interne en externe prestatieperspectieven. In dit systeem wordt erkend dat financiële prestaties weliswaar belangrijk zijn, maar wordt de nadruk gelegd op het feit dat de basis van goede financiële prestaties ligt bij tevreden afnemers, een hoge mate van innovatie en uitstekende interne bedrijfsprocessen.

1) Een zeer belangrijk informatiesysteem zal extra aandacht vergen van het management gezien de mogelijke invloed op de bedrijfsprocessen.



Figuur 1. Voorbeeld Balanced Scorecard van een ICT-organisatie.

De Balanced Scorecard vertaalt de visie en de strategie van de onderneming in concrete doelstellingen, georganiseerd volgens de vier verschillende perspectieven: het financieel perspectief, het klantperspectief, het perspectief van interne bedrijfsprocessen en het groei- en leerperspectief. Samen vormen deze perspectieven het raamwerk van de Balanced Scorecard.

In de praktijk hebben verschillende organisaties de traditionele Balanced Scorecard toegepast voor de besturing van ICT en ICT-organisaties ([KPMG99]). In figuur 1 is een voorbeeld gegeven van een uitgewerkte Balanced Scorecard voor een ICT-organisatie. Bij elk van de perspectieven is er een aantal kernprestatie-indicatoren (KPI) benoemd, in de praktijk veelal tussen de zestien en twintig in totaal. Deze KPI's geven aan wat het resultaat is bij het behalen van de kritieke succesfactoren (KSF).

Het spreekt voor zich dat het opstellen, implementeren en naleven van een dergelijke uitgewerkte scorecard inclusief alle onderliggende processen, de detailrapportages, de handmatige en geautomatiseerde systemen, etc. geen eenvoudige opgave is. Voor het bepalen van deze set speelt de volwassenheid van de gebruikers- en ICT-organisatie een belangrijke rol. Naarmate de gebruikers- en ICT-organisatie meer volwassen wordt neemt het aantal gebieden waarop kan worden gemeten verder toe, ontstaat er een balans tussen de scorecardperspectieven, en wordt de relatie met de businessprestaties transparanter. Performancemanagement door middel van de Balanced Scorecard biedt ICT-managers een goede ondersteuning om op basis van prestaties betere en meer overwogen beslissingen te nemen om de doelen van hun ICT-organisatie en daarmee de gehele organisatie te realiseren.

Conclusies

Het besturen en beheersen van een organisatie kan niet los worden gezien van de besturing en beheersing van ICT. Het management van organisaties onderkent deze situatie en is zich er veelal van bewust dat een niet-adequate besturing en beheersing van ICT de continuïteit van de organisatie in gevaar kan brengen. Hiermee lijkt een rol voor ICT en voor de ICT-auditor te zijn weggelegd binnen een onderzoek naar Corporate Governance. Wellicht is het noodzakelijk om bij organisaties met een sterke afhankelijkheid van ICT toe te werken naar een verplichting of dient een verwijzing naar uitspraken te zijn opgenomen in de jaarstukken.

Om een juiste beoordeling te kunnen uitvoeren moet(en) de betreffende functionaris(sen) over bepaalde kwaliteiten en kennis beschikken om uitspraken te kunnen doen over de betrouwbaarheid, continuïteit, effectiviteit en efficiëntie van ICT. Dit hoeft niet per definitie een ICT-auditor te zijn. Aspecten die spreken voor het inzetten van een ICT-auditor zijn onder andere kennis en ervaring met te beoordelen objecten en het kunnen beschikken over geschikte tools/methodieken om te kunnen adviseren dan wel beoordelen. Tevens is de ICT-auditor gebonden aan gedrags- en beroepsregels die voor organisaties aanvullende waarborgen bieden.

Indien in Nederland wordt toegewerkt naar een verdere integratie van Corporate Governance en de rol van de besturing en beheersing van ICT, direct dan wel indirect gedefinieerd, is het van belang dat in deze ontwikkeling de volgende punten een rol spelen:

* verplichting inzake rapportering over de effectiviteit en efficiëntie van de bedrijfsprocessen en direct of indirect over de besturing en beheersing van ICT;
* richtlijnen/normen voor de rapportering over en de wijze van rapportering.

Een verplichting inzake rapportering over ICT in de jaarstukken anders dan ingevolge BW II artikel 393 lid 4, is in Nederland niet aanwezig. Tevens wordt een dergelijke verplichting door een groot aantal organisaties niet onderschreven maar wordt zij wel als wenselijk beschouwd. Uit een door KPMG Engeland uitgevoerd onderzoek bleek onder andere dat de 'Code of Best Practice' pas goed werd nageleefd nadat het rapporteren over interne (financiële) controls verplicht was gesteld (vanaf 1 januari 1995). Hiermee doemt direct een volgend probleem op: hoe zien richtlijnen/normen voor de rapportering er dan uit? Uit het eerdergenoemde onderzoek kwam naar voren dat de beoordeling van interne beheersing in de praktijk tot de nodige problemen leidt. Een groot probleem vormt het opstellen van richtlijnen/normen waaraan een effectief en efficiënt systeem dient te voldoen. Uit de analyse van de mogelijke ICT-informatiebehoeften van het management blijkt dat het beoordelen van ICT per organisatie maatwerk is, gebaseerd op onder andere risicoanalyses en professional judgement van de auditor.

Literatuur

[Boer96]
J.C. Boer RE RA, ir. J.A.M. Donkers RE, drs. R.M. Renes en prof. dr. P. Wallage RA, *Corporate Governance; de betekenis voor de ICT-auditor*, Compact 1996/5.

[Cadb92]
A. Cadbury e.a., *Report of the Committee on the Financial Aspects of Corporate Governance: Report with Code of Best Practice*, Gee, London 1992.

[Comm97]
Commissie Corporate Governance, *Aanbevelingen inzake Corporate Governance in Nederland*, 25 juni 1997.

[COSO94]
COSO, Committee of Sponsoring Organizations of the Treadway Commission, (two volume edition 1994), *Internal Control – Integrated Framework*, American Institute of Certified Public Accountants, Jersey City.

[Grem97]
W. van Grembergen en R. van Bruggen, *Measuring and improving corporate information technology through Balanced Scorecard*, Universiteit van Antwerpen, 1997.

[KPMG96]
Diverse publicaties met betrekking tot het onderwerp Corporate Governance en internal control.

[KPMG99]
L. Acda, M. Burger, D. Grund en J. Vandecasteele, *Visie op Performance Management in ICT-organisatie*.

[Munc95]
W.A. de Munck, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering*, Compact 1995/3.

[Rene96]
Drs. R.M. Renes RA, *De commissie Peters over Corporate Governance en interne beheersing*, Nieuwsbrief accountancy, december 1996.

[Stri97]
Dr. J. Strikwerda, *Geen Corporate Governance zonder Internal Governance*, Nijenrode Management Review, nummer 3, maart/april 1997.

[Waar97]
Prof. J. Waardenburg, drs. E.C. Pijst en drs. K.J. Vogel, *Publieke managementrapportages over internal control*, MAB, juni 1997.

Overige literatuur:
* Prof. mr. M.J.G.C. Raaijmakers en dr. W.J. de Ridder, *Corporate Governance in Nederland, Besluitvorming en verantwoording in beursondernemingen*.
* Corporate Governance, interview met mr. R. van der Vlist, Algemeen procuratiehouder Koninklijke Olie, Magazine van de Commissie Voortgezette Educatie Registeraccountants (VERA), 8e jaargang, 10 juni 1997.
* Prof. dr. P. Wallage RA, *Corporate Governance en de rol en functie van de accountant*, inaugurele rede Universiteit van Amsterdam, 27 oktober 1997.
* Ir. J.A.M. Donkers RE en mw. ir. E.R. van Sommeren, *Benchmarking, een hulpmiddel voor de ICT-auditor?*, Compact 1996/2.
* Drs. R.M. Renes RA, *De invloed van management control op accountantscontrole in Nederland*, afstudeerscriptie Erasmus Universiteit Rotterdam aan de faculteit der Economische Wetenschappen, Vakgroep ACAB, 14 november 1994.
* Drs. R.M. Renes RA, *Management control en accountantscontrole – Veranderende inzichten?*, Compact 1996/5.

Drs. J.C. de Boer RE
is als manager werkzaam bij KPMG Information Risk Management. Belangrijke aandachtsgebieden in zijn werk zijn de inrichting, de beheersing en het doorlichten van de informatievoorziening binnen organisaties.

Mw. ir. E.R. van Sommeren RE
is als manager werkzaam bij KPMG Information Risk Management. Belangrijke aandachtsgebieden in haar werk zijn de inrichting en beheersing van de informatievoorziening binnen organisaties en het begeleiden van organisaties bij het verbeteren van de processen. Onderwerp van haar afstudeerreferaat ten behoeve van de postdoctorale studie ICT-auditing was Corporate Governance en de vertaling naar ICT.