De betekenis van IT-auditing voor risicobeheersing en IT-governance

Stan van Bommel, Lucien Peek en Joop Winterink

SAMENVATTING In dit artikel wordt beschreven op welke wijze een effectieve vertaalslag kan worden gemaakt om de impact van IT-controlebevindingen op de risicobeheersing in complexe IT-omgevingen te analyseren. Het melden en toelichten van IT-risico's krijgt onvoldoende aandacht in de externe risicoverantwoording. Wij menen dat een IT-auditor een belangrijke bijdrage kan leveren in risicobeheersing en IT-Governance. Het management, bestuur, accountant en toezichthouder krijgt inzicht in de kwaliteit van de risicobeheersing van IT-risico's en verantwoordingsinformatie over IT-governance. Dit inzicht biedt mogelijkheden voor een transparantere interne en externe verslaggeving.

RELEVANTIE VOOR DE PRAKTIJK Met het in dit artikel geboden kader voor informatie van en communicatie over de risicobeheersing van IT-risico's kunnen IT-auditors hun IT-controlebevindingen eenduidig communiceren en krijgen management, bestuur en accountant direct inzicht in de oorzaken en gevolgen van IT-risico's. Het kader biedt een handreiking voor de IT-auditor en de accountant en biedt de mogelijkheid management en audit committees te overtuigen van de weergave van een aantoonbare en transparante risicobeheersing van IT-risico's in het jaarverslag.

C.F. van Bommel RE en L.C. Peek RE RO zijn als IT-auditors werk–zaam bij de afdeling Internal Audit van de PGGM. J.A.W. Winterink RA RE was tot 1 september 2007 Hoofd Internal Audit bij PGGM. Vanaf 1 september 2007 is hij directeur interne accountantsdienst UVIT (Univé-V62-12A-Trias). Hij is als hoofd–docent verbonden aan de opleiding tot registeraccountant aan de universiteit van Tilburg en de TIAS postmaster opleiding IT-auditing.

1 Inleiding

In het kader van Corporate Governance worden in toenemende mate eisen gesteld aan de beheersing van bedrijfsprocessen. Hiermee wordt getracht de betrouwbaarheid van verantwoordingen te waarborgen. Het bestuur van organisaties moet aantoonbaar maken dat zij de bedrijfsprocessen beheerst. De inzet van informatietechnologie (IT) vormt een belangrijke schakel in de beheersing van de bedrijfsprocessen. IT dient daarom een integraal onderdeel van de risicobeheersing van de organisatie uit te maken. IT-governance is een direct onderdeel van Corporate Governance.

Voor de beoordeling van het IT-risico in het verantwoordingsproces is specialistische kennis van IT en IT-beheersing nodig. Daarom schakelen management, bestuur en accountant veelvuldig de IT-auditor in. De IT-auditor voert General IT-control onderzoeken uit en rapporteert aan management, bestuur en accountant die kennis nemen van de IT-controlebevindingen. Op basis hiervan kan:

- het management effectief de kwaliteit van risicobeheersing verbeteren;
- het bestuur het toezicht op IT-governance en het risicomanagementproces effectief vervullen;
- de accountant efficiënt zijn jaarrekeningcontrole met user en application controls inrichten.

In theorie lijkt dit eenvoudig, maar in de praktijk blijkt telkens weer dat de informatie en communicatie tussen IT-auditor, management, bestuur en accountant verre van optimaal is. Het ontbreekt structureel aan een concrete vertaalslag van de IT-controlebevindingen naar de betekenis voor risicobeheersing, IT-governance en jaarrekeningcontrole. Enerzijds wordt de betekenis van de IT-controlebevindingen onvoldoende geïnterpreteerd en anderzijds lukt het de

IT-auditor onvoldoende om het belang van zijn IT-controlebevindingen voor risicobeheersing en risicoverantwoording duidelijk te maken. Uit onderzoeken blijkt dat één op de tien IT-projecten volledig mislukt (Ernst & Young, 2007), maar in jaarverslagen van organisaties is vervolgens weinig terug te vinden over IT-governance en de risicobeheersing van IT-risico's (Ernst & Young, 2005).

Dit artikel probeert oplossingen aan te reiken voor de bovenstaande vraagstukken. Een eerder artikel (Van Bommel en Van Goor, 2004) beschrijft een methode voor de IT-auditor om met de accountant te komen tot een analyse van de te beoordelen General IT-controls in het kader van de controle van de jaarrekening. Een vervolg hierop beschrijft op basis van een concreet praktijkvoorbeeld de uitwerking van de methode waarmee accountant én IT-auditor het onderzoek naar General IT-controls onderbouwen (Van Bommel en Van Goor, 2005). In aansluiting hierop beschrijft een derde artikel op welke wijze een effectieve vertaalslag kan worden gemaakt om de impact van IT-controlebevindingen op de jaarrekeningcontrole voor de accountant te bepalen (Van Bommel, Van Goor, Peek en Winterink, 2006). Conclusie is dat de jaarrekeningcontrole efficiënter is uit te voeren, maar dat de gevolgen van IT-controlebevindingen voor de uitkomst van de jaarrekeningcontrole beperkt zijn. Bovendien worden de IT-controlebevindingen, intern terug te vinden in het accountantverslag en managementletter van de accountant, zelden gemeld en toegelicht in het externe jaarverslag. In het voorliggende artikel wordt beschreven hoe een effectieve vertaalslag kan worden gemaakt van IT-controlebevindingen in de interne risicoverantwoording, naar de externe risicoverantwoording van IT-risico's in jaarverslag.

De opzet van dit artikel is als volgt:

- in paragraaf 2 analyseren we de vereiste aandacht voor het IT-risico en IT-governance in jaarverslagen;
- in paragraaf 3 beschrijven we de interpretatie van IT-controlebevindingen naar IT-risico's en IT-governance;
- in paragraaf 4 volgen twee voorbeelden van IT-risico's en hun impact op risicobeheersing en IT-governance. Per IT-risico wordt een voorstel tot melding en toelichting in het jaarverslag gegeven en uitgewerkt;
- paragraaf 5 sluit af met onze conclusies.

2 Corporate Governance, IT-governance, IT-risico's en jaarverslaggeving

Corporate Governance gaat over het aantoonbaar goed besturen en beheersen van organisaties. De toepassing van IT stelt organisaties in staat haar bedrijfsprocessen effectief te beheersen. IT vormt in toenemende mate een integraal onderdeel van de strategie van organisaties. De grote(re) afhankelijkheid van IT vereist een effectieve risicobeheersing van IT-risico's. IT-governance gaat over effectieve en aantoonbare risicobeheersing en -verantwoording van IT-risico's. Jaarverslagen van organisaties schrijven in toenemende mate over risico's en risicobeheersing. Krijgen IT-risico's, IT-risicobeheersing en IT-governance in de jaarverslaggeving voldoende aandacht?

Om tot een adequate interne en externe verslaggeving van IT-risico's te komen is inzicht nodig in de principes van Corporate Governance én IT-governance. Vervolgens is geïnventariseerd of jaarverslagen IT-risico's melden én of er toelichting wordt gegeven op de risicobeheersing van IT-risico's. Hiermee wordt vastgesteld of de verantwoording over IT-risico's voldoet aan de principes van Corporate Governance én IT-governance.

2.1 Corporate Governance

De essentie van Corporate Governance is het goed besturen en beheersen van organisaties en het aantoonbaar verantwoorden dat dit ook zo gebeurt (Commissie Corporate Governance, 2003). Er zijn in hoofdzaak twee manieren om Corporate Governance te organiseren. SOX, de aanpak van de VS, is rules-based, vooral gericht op financiële verantwoording en te omschrijven als 'comply or die', met harde sancties op het niet naleven van de regels en verantwoordelijkheden.

De code-Tabaksblat voor Corporate Governance volgt de lijn van 'apply or explain': pas je de principes van Corporate Governance niet toe, dan moet je uitleggen waarom. Het is een principles-based aanpak, gericht op het afleggen van verantwoording, het geven van inzicht in de relevante bedrijfsrisico's in brede zin en de beheersing van die risico's.

Naast regels en principes speelt bij Corporate Governance vertrouwen een belangrijke rol. Inzicht en transparantie, een kwalitatief goede en betrouwbare verslaggeving en een heldere bedrijfscultuur: dat zijn belangrijke normen en waarden waar het om draait. Juist de combinatie van diverse factoren zorgt voor hogere risico's op een debacle (Deloitte, 2005). Er zijn dus meer factoren in het spel dan accounting en compliance gerelateerde risico's alleen.

De monitoringcommissie Frijns (Monitoring Commissie Corporate Governance, 2006) heeft een compromis gezocht en voorgesteld om een robuust ICS (In Control Statement) af te leggen als het gaat om financiële verslaggevingsrisico's, en op het punt van

de overige risico's en beheersmaatregelen een meer kwalitatieve evaluatie te vragen. Ten aanzien van de overige risico's (strategische en operationele risico's, financieringsrisico's en compliance risico's) wordt aanbevolen:

- een beschrijving in het jaarverslag op te nemen van de risicobeheersings- en controlesystemen op basis van de geïdentificeerde belangrijkste risico's;
- indien van toepassing, belangrijke tekortkomingen die in het verslagjaar zijn geconstateerd te melden, waarbij tevens aangebrachte of geplande verbeteringen worden aangegeven.

Gaat het om de overige risico's, waaronder het IT-risico, dan heeft het bestuur tot taak aan te geven wat de materiële risico's zijn, hoe die beheerst worden, welke tekortkomingen zijn vastgesteld en welke verbeteringsmaatregelen zijn getroffen.

2.2 IT-governance

Informatievoorziening ondersteunt organisaties bij het realiseren van haar doelstellingen en IT vormt in toenemende mate een integraal onderdeel van de strategie van een organisatie. IT-governance is direct met Corporate Governance verbonden en gaat over het besturen, beheersen, uitvoeren, verantwoording afleggen over en het toezicht op de informatievoorziening binnen organisaties. Het gaat bij IT-governance om het effectief beheersen van de IT-risico's. In lijn met de uitgangspunten van Corporate Governance dienen organisaties via hun jaarverslagen, extern verantwoording af te leggen over IT-governance en IT-risico's aan alle belanghebbenden.

De beroepsorganisatie voor IT auditors, de NOREA, heeft in een verkenning over IT-governance een aantal praktijksituaties toegelicht en de betekenis en consequenties van IT-governance voor IT-auditing verkend (NOREA, 2004). NOREA heeft bewust geen nieuw model of een eigen visie op IT-governance geïntroduceerd, maar aansluiting gezocht met reeds bestaande modellen en begrippen, zoals CobiT (Control Objectives for Information and related Technology).

CobiT definieert IT-governance als volgt: *IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organisation's IT sustains and extends the oragnisation's strategies and objectives* (bron: Information Systems Audit and Control Association (ISACA) en het IT-governance Institute).

IT-governance en IT-management worden hierbij ten opzichte van elkaar gepositioneerd. IT-management is gericht op de besluitvorming, uitvoering en verantwoording van IT-activiteiten binnen de IT-organisatie. Hierbij wordt een nader onderscheid gemaakt tussen ontwikkelactiviteiten en activiteiten in het kader van beheer en exploitatie. IT-governance gaat over spelregels, kaders, beleid, aansturing, verantwoording en toezicht.

De uitgangspunten van Corporate Governance vertalend naar de betekenis voor IT-governance levert een drietal aandachtsgebieden voor IT-auditing op:

- de beheersing van IT-risico's binnen een organisatie. Het gaat hierbij om het besturen, beheersen en uitvoeren van de informatievoorziening (zoals informatiebeleid, informatiearchitectuur, informatiebeveiliging, IT-processen, IT-infrastructuur);
- het afleggen van verantwoording over de beheersing van IT-risico's (intern én extern);
- het aantoonbaar uitoefenen van toezicht op de beheersing van IT-risico's.

De rol van de IT-auditor beschrijven wij in hoofdstuk 3.

2.3 IT-risico's, IT-governance, Corporate Governance en jaarverslaggeving

DNB (2005) definieert het IT-risico als het risico dat bedrijfsprocessen en informatievoorziening onvoldoende integer, niet continu of onvoldoende beveiligd worden ondersteund door IT. Items van het IT-risico zijn: Strategie en Beleid, Beveiliging, Beheersbaarheid en Continuïteit. IT-governance gaat over het afleggen van verantwoording over de beheersing van IT-risico's.

Corporate Governance zorgt er voor dat in jaarverslagen van organisaties expliciet aandacht wordt besteed aan risico's en risicobeheersing. Specifiek voor het IT-risico is geïnventariseerd óf hier aandacht voor is én als dat het geval is in welke mate belangrijke tekortkomingen zijn onderkend waarbij aangebrachte of geplande verbeteringen worden aangegeven.

Over de jaarverslagen 2005/2006 kan worden vastgesteld dat:

- er steeds meer aandacht komt voor Corporate Governance, risico's en risicobeheersing (De Groot, 2006);
- er weinig tot geen specifieke aandacht is voor IT-risico's en IT-governance (BNG is één van de weinige organisaties die het IT-risico wel expliciet toelicht);
- belangrijke tekortkomingen voor IT-risico's in jaarverslagen niet worden verantwoord en ook geplande verbeteringen hierop niet worden aangegeven.

Dit lijkt in strijd met de volgende issues:

- meer dan de helft van alle IT-projecten mislukt (Ernst & Young, 2007):

- één van de tien mislukt volledig;
- vijf van de tien (mis)lukt gedeeltelijk (voldeed niet aan de verwachtingen, liep uit op de tijdsplanning, kostenoverschrijdingen);
- vier van de tien succesvol zijn afgerond én geïmplementeerd;
- we regelmatig in de krant lezen over de storingen bij de Postbank in internetbankieren (Trouw, 2007):
- klanten kunnen regelmatig niet inloggen op hun rekeningen;
- klanten kunnen zelfs inloggen op de rekening van anderen;
- er wordt € 40 miljoen opzij gezet om knelpunten en nieuwe storingen te voorkomen.

3 Vertaalslag van IT-controlebevindingen naar risicobeheersing en IT-governance

De IT-auditor rapporteert IT-controlebevindingen aan het management dat verantwoordelijk voor IT-risico's. De kwaliteit van de risicobeheersing van de IT-risico's wordt beoordeeld op een vierpuntschaal. IT-risico's met de beoordeling onvoldoende worden toegelicht in de interne risicoverantwoording. IT-risico's met de beoordeling onaanvaardbaar komen terecht in het externe jaarverslag (risico hoofdstuk).
De kwaliteit van de risicobeheersing van IT-risico's beoordeelt de IT-auditor op een vierpuntschaal: goed, voldoende, onvoldoende en onaanvaardbaar. Het eenduidig naar vier soorten conclusies interpreteren van IT-controlebevindingen maakt het voor de stakeholders direct duidelijk wat de impact van de bevindingen over de risicobeheersing van IT-risico's zal zijn: wel óf niet opnemen en toelichten in het risicohoofdstuk van het externe jaarverslag van de organisatie. De uitdaging van de IT-auditor als 'lakmoesproef voor risicobeheersing' (Winterink en de Bruin, 2006) is gebaseerd op ervaringen bij het Internal Audit PGGM.

3.1 Internal Audit afdeling: de IT-auditor beoordeelt de beheersing van IT-risico's

Een Internal Audit afdeling ondersteunt management en bestuur van een organisatie bij de besturing en de beheersing van de organisatie, inclusief de interne en de externe verantwoording daarover. Door aan te sluiten op het risicomanagementproces van de organisatie kan de Internal Audit afdeling zekerheid verschaffen over de risicobeheersing van bedrijfsprocessen, inclusief de IT-risico's. IT-audit vormt integraal onderdeel van een Internal Audit afdeling, met als specifiek aandachtsgebied de beoordeling van de beheersing van IT-risico's. De auditor heeft een onafhankelijke, controlerende en toetsende functie.

De IT-auditor beoordeelt de beheersing van het IT-risico van de IT-organisatie en IT-processen, de informatiesystemen in ontwikkeling en de technische IT-infrastructuur. Met audits worden de IT-risico's ten aanzien van de IT-organisatie, -beleid, -processen, -diensten en -middelen en de getroffen beheersmaatregelen getoetst. Per audit worden de IT-controlebevindingen gerapporteerd aan het verantwoordelijke management: elke audit sluit de IT-auditor af met een conclusie over de risicobeheersing van het IT-risico. Hij komt tot één van de volgende conclusies:

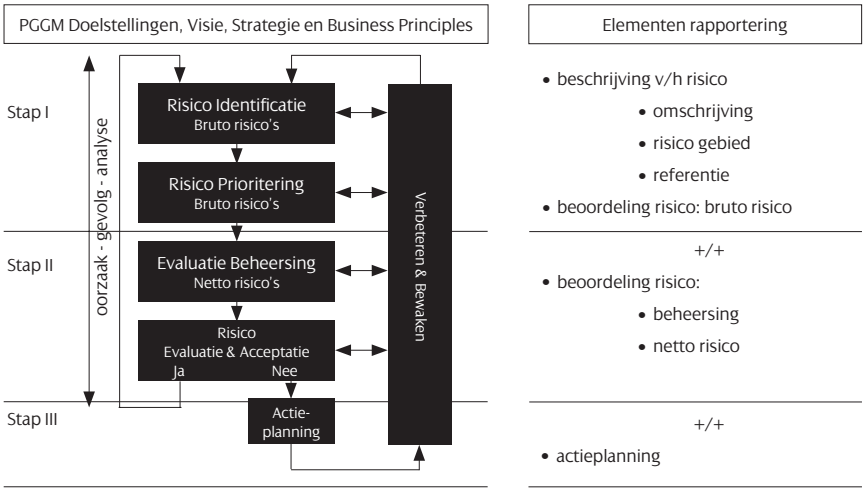
- **de risicobeheersing van het IT-risico is goed**
  Uit het onderzoek zijn alleen positieve IT-controlebevindingen naar voren gekomen. Kenmerken hiervan zijn een proactieve risicobeheersing en een continue bewaking;
- **de risicobeheersing van het IT-risico is voldoende**
  Hierbij zijn één of enkele IT-controlebevindingen geconstateerd die leiden tot wenselijke verbeteringen. Kenmerken hierbij zijn een actieve risicobeheersing en bewaking. Verbeteringen worden direct opgepakt en zijn snel te realiseren;
- **de risicobeheersing van het IT-risico is onvoldoende**
  Hierbij zijn één of enkele IT-controlebevindingen vastgesteld met noodzakelijke verbeteringen. Kenmerken hierbij zijn een re-actieve risicobeheersing en ad-hoc bewaking. Verbeteringen worden te laat opgepakt en zijn niet eenvoudig te realiseren;
- **de risicobeheersing van het IT-risico is onaanvaardbaar**
  De IT-auditor komt vooral tot negatieve IT-controlebevindingen met noodzakelijke verbeteringen. Van risicobeheersing is nauwelijks sprake, het IT-risico wordt niet beheerst. Het risico dat bedrijfsprocessen en informatievoorziening onvoldoende integer, niet continu of onvoldoende beveiligd worden ondersteund door IT is onaanvaardbaar.

Door de IT-controlebevindingen van de IT-auditor eenduidig te communiceren en te presenteren, stimuleert dit enerzijds de IT-auditor tot duidelijke afwegingen bij zijn conclusies over de kwaliteit van de risicobeheersing van IT-risico's. Anderzijds krijgt het management daarmee direct inzicht in de consequenties van de IT-controlebevindingen voor de interne en externe verantwoording van IT-risico's en IT-governance.

3.2 Management, risicobeheersing en risicoverantwoording (IT)-risico's

Veel organisaties sluiten met hun risicomanagementproces aan op de uitgangspunten van het COSO model (COSO-ERM, 2004 en Van Leeuwen en Wallage, 2007). Periodiek doorloopt het management het proces

Figuur 1 Risk Management Framework



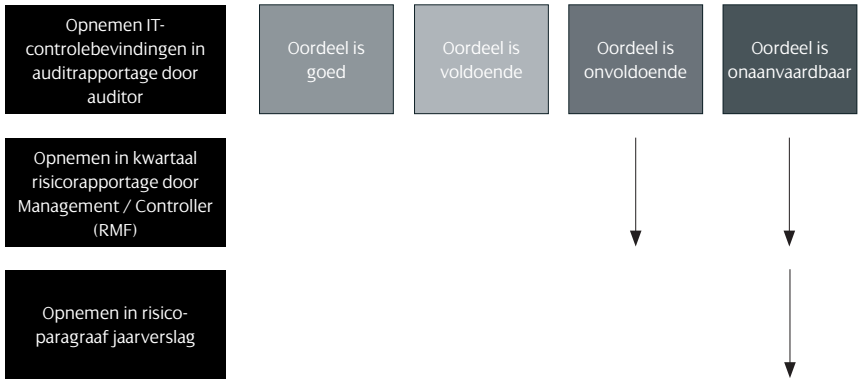
van risico-identificatie (bruto risico´s), beschrijving en beoordeling van de risicobeheersing, het vaststellen van de resulterende nettorisico's, met tenslotte risico-evaluatie en risicoacceptatie (inclusief IT-risico's). Figuur 1 geeft schematisch weer hoe PGGM invulling geeft aan haar risicomanagementproces.

Het management is verantwoordelijk voor de risicobeheersing binnen haar verantwoordelijkheidsgebied. Ter verantwoording stelt zij periodiek een risicorapportage op. De impact voor de interne en externe verantwoording van IT-risico's is duidelijk: bevindingen betreffende onaanvaardbare IT-risico's worden opgenomen en toegelicht in de interne risicorapportage én in de risicoverantwoording in het jaarverslag. IT-risico's die onvoldoende worden beheerst worden opgenomen én toegelicht in de interne risicorapportage, inclusief de maatregelen ter verbetering van de risicobeheersing. Dit kader is weergegeven is in figuur 2.

3.3 IT-audit, IT-risico's, IT-governance en risicoverantwoording in het externe jaarverslag

De IT-auditor beoordeelt periodiek de (IT-)risico's in de interne risicoverantwoording. De auditor inventariseert de belangrijkste bevindingen, de belangrijkste (IT-)controlebevindingen uit audits én de follow-up op aanbevelingen uit eerdere audits. Hierover rapporteert de auditor aan het management.
Hiermee zijn de (IT-)risico's geïdentificeerd en geanalyseerd die voor opname en toelichting in de risico-

Figuur 2 De betekenis van IT-controlebevindingen voor de interne en externe risicoverantwoording



verantwoording in het jaarverslag in aanmerking komen. Indien van toepassing kunnen de onaanvaardbare tekortkomingen die in het verslagjaar zijn geconstateerd worden gemeld én aangebrachte verbeteringen worden toegelicht.
Hierdoor wordt een degelijke basis gelegd voor een aantoonbaar goede risicobeheersing en -verantwoording van IT-risico's. Het bestuur kan effectief voldoen aan de principes van Corporate Governance én IT-governance.

4 Voorbeelden over de risicoverantwoording van IT-risico's in het jaarverslag

Onaanvaardbare tekortkomingen bij IT-risico's worden geïnterpreteerd naar twee voorbeelden. Een voorbeeld wordt gegeven bij onaanvaardbare tekortkomingen van belangrijke IT-projecten. Een ander voorbeeld gaat in op structurele tekortkomingen in de beschikbaarheid van IT. Per voorbeeld geven we de IT-controlebevindingen van de IT-auditor en beschrijven we de toelichting op het IT-risico die we hierop voorstellen in de risicoverantwoording in het jaarverslag. Hierna worden twee willekeurige voorbeelden beschreven, waarmee de verstaalslag van als onaanvaardbaar gerapporteerde IT-controlebevindingen naar een aantoonbare verantwoording van de beheersing van IT-risico's in het jaarverslag worden onderbouwd en uitgewerkt.

4.1 IT-project: complexe integrale vervanging IT-infrastructuur en IT-applicaties

Aanleiding en doelstelling van het IT-project

Een organisatie heeft de afgelopen jaren diverse bedrijven overgenomen, waardoor de beheersbaarheid van informatiesystemen én IT-infrastructuur er niet gemakkelijker op is geworden. Om aan deze eilandautomatisering een einde te maken is besloten over te gaan op één standaard ERP-systeem, te beheren op één eenduidige IT-infrastructuur. Uitgangspunt is een gefaseerde bedrijfsbrede implementatie van het ERP-systeem en geen aanvullende functionaliteiten (maatwerk) te ontwikkelen. Budget is € 30 miljoen.

IT-risico

Het IT-risico voor het project is tweeërlei:

- enerzijds het niet op tijd, met onvoldoende kwaliteit en met forse budgetoverschrijding ontwikkelen en realiseren van het project;
- anderzijds het risico dat het ERP-systeem de bedrijfsprocessen onvoldoende ondersteunt en de IT-infrastructuur de continuïteit en integriteit van de informatievoorziening onvoldoende kan waarborgen.

IT-controlebevindingen

De IT-auditor is pro-actief bij het project betrokken. Diverse audits zijn uitgevoerd naar de projectbeheersing, projectverantwoording en risicobeheersing van het IT-project. De belangrijkste als onaanvaardbaar gerapporteerde IT-controlebevindingen zijn:

- er is veel aanvullende functionaliteit ontwikkeld, met als risico dat er een log, onwerkbaar en complex te beheren informatiesysteem wordt geïmplementeerd;
- 80% van het budget is op, terwijl 50% van de geplande werkzaamheden gereed is. De IT-auditor ziet als risico dat het project minstens het dubbele zal kosten en dat de doorlooptijd van het project minimaal met een jaar uitloopt;
- het testen van opgeleverde onderdelen van het ERP-systeem verloopt bijzonder moeizaam: gebruikers verwachten een informatiesysteem dat precies op hen is toegesneden. Het risico dat ze het ERP-systeem niet accepteren is groot;
- bij het project zijn meerdere externe én interne partijen betrokken. Samenwerking verloopt bijzonder moeizaam. Verantwoordelijkheden zijn niet goed afgesproken en de coördinatie en communicatie tussen partijen geeft dagelijks diverse conflicten.

De Monitoring Commissie Corporate Governance Code (commissie Frijns) beveelt aan belangrijke tekortkomingen die in het verslagjaar zijn geconstateerd te melden én aangebrachte verbeteringen toe te lichten. Onderstaand een uitgewerkt voorstel.

Toelichting IT-risico in het jaarverslag 2007

Om de beheersbaarheid van informatiesystemen én IT-infrastructuur te vereenvoudigen is in 2005 besloten over te gaan op één standaard ERP-systeem, te beheren op één eenduidige IT-infrastructuur. Doel is een gefaseerde bedrijfsbrede implementatie van een standaard ERP-systeem (SAP) op een Microsoft IT-infrastructuur, zonder maatwerkfunctionaliteit, waarmee de IT-exploitatie vanaf 2008 € 10 miljoen bespaart.
In 2007 zijn de IT-risico's van het project beoordeeld. Vastgesteld is dat niet op tijd (1 januari 2008 wordt 1 januari 2009), met onvoldoende kwaliteit (er is veel aanvullende functionaliteit ontwikkeld, dus geen maatwerk) en met forse budgetoverschrijding (budget is € 30 miljoen, overschrijding van tenminste 50% wordt verwacht) het project wordt gerealiseerd. De samenwerking tussen betrokken partijen verloopt moeizaam. Hiermee bestaat het risico dat het ERP-systeem vanaf 2008 de bedrijfsprocessen onvoldoende ondersteunt en de IT-infrastructuur de continuïteit en integriteit van de informatievoorziening

onvoldoende kan waarborgen. De besparing in de IT-exploitatie vanaf 2008 met € 10 miljoen wordt niet gerealiseerd. In 2008 neemt de IT-exploitatie eenmalig toe met € 4 miljoen, terwijl vanaf 2009 de IT-exploitatie € 8 miljoen bespaart.
In 2007 zijn de volgende verbeteringen op het project toegepast:

- de projectorganisatie is opnieuw ingericht: de eindverantwoordelijkheid voor sturing en beheersing van het project ligt nu bij de directie van de gebruikersorganisatie (dit was de directie van de IT-organisatie). Maandelijks rapporteert de directie aan de Raad van Bestuur over de beheersing van de IT-risico's;
- het project heeft een herstart gemaakt: er wordt geen aanvullende functionaliteit ontwikkeld, doel is één standaard SAP-systeem op één Microsoft IT-infrastructuur, te gebruiken vanaf 1 januari 2009;
- per 1 juli 2008 zullen de ontwikkelingen zijn afgerond en start de bedrijfsbrede implementatie. Per maand wordt het systeem bij drie bedrijven geïmplementeerd, zodat vanaf 1 januari 2009 alle bedrijven over zijn op het standaard SAP-systeem;
- het budget voor het project is van € 30 miljoen verhoogd naar € 45 miljoen;
- het budget voor IT-exploitatie voor 2008 is eenmalig met € 4 miljoen verhoogd.

4.2 Continuïteit van de informatieverzorging

Met betrekking tot de werking van de interne risicobeheersings- en controlesystemen geeft de Code Tabaksblat een directe relatie naar betrouwbaarheid en continuïteit van geautomatiseerde informatievoorziening, Hieronder is een voorbeeld uitgewerkt van IT-continuïteitsplanning om de continuïteit van de informatievoorziening te garanderen.

Aanleiding en doelstelling van IT-continuïteitsplanning

Een reisorganisatie is de afgelopen jaren voor de uitvoering en beheersing van de bedrijfsprocessen sterk afhankelijk geworden van informatietechnologie (IT). Informatiesystemen zijn kwetsbaar voor verschillende soorten calamiteiten: de continuïteit van de bedrijfsprocessen is een belangrijke voorwaarde voor het succesvol opereren van de organisatie in een sterk competitieve markt: als het verkoopkanaal op internet niet beschikbaar is, kopen klanten hun reis bij andere aanbieders.
Om op deze bedreigingen te anticiperen is door de organisatie een IT-continuïteitsplan opgesteld en ingevoerd. Door middel van een IT-continuïteitsplan is van te voren vastgelegd hoe de continuïteit van de informatievoorziening is geregeld bij calamiteiten.

IT-risico

Het IT-risico voor IT-continuïteitsplanning is dat herstel van de informatievoorziening langer duurt dan het break even-punt waarop de kosten door de uitgevallen informatiesystemen gelijk zijn aan de kosten die gemaakt moeten worden om de informatievoorziening te herstellen. De geoorloofde hersteltijd bij de organisatie is bepaald op 4 uur.

IT-controlebevindingen

De IT-auditor verricht regelmatig audits naar opzet, bestaan en werking van de IT-continuïteitsplanning. De belangrijkste onaanvaardbare IT-controlebevindingen zijn:

- in 2007 is er één calamiteit geweest: een externe stroomstoring van 2 uur. Tijdens de calamiteit is het niet gelukt de noodstroomvoorziening direct te gebruiken. Nadat de externe stroomvoorziening na 2 uur was hersteld, duurde het 4 uur voordat de informatievoorziening van de reisorganisatie weer online was: totale uitvalduur 6 uur;
- vier keer per jaar wordt de IT-continuïteitsplanning integraal getest. Tijdens de testen in 2007 is het één keer gelukt de normhersteltijd van 4 uur te realiseren;
- analyse van testen en calamiteiten leert dat bedreigingen en kwetsbaarheden onvoldoende zijn geïdentificeerd én dat communicatie en samenwerking bij betrokken partijen onvoldoende is georganiseerd.

Onderstaand een uitgewerkt voorstel voor de risicoverantwoording in het jaarverslag.

Toelichting IT-risico in het jaarverslag 2007

Onze reisorganisatie is de afgelopen jaren voor de uitvoering en beheersing van de bedrijfsprocessen sterk afhankelijk geworden van informatietechnologie. Om te anticiperen op dit IT-risico is in 2006 door de organisatie een IT-continuïteitsplanning opgesteld en ingevoerd. De geoorloofde hersteltijd bij de organisatie is bepaald op 4 uur.
In 2007 is er één calamiteit geweest met een hersteltijd van 6 uur (norm staat op 4 uur). In 2007 zijn er vier integrale continuïteitstesten geweest: bij één test werd de norm van 4 uur gehaald, bij de andere drie testen lukte het herstel binnen 6 uur.
In 2007 is door de raad van bestuur als volgt besloten:

- de geoorloofde hersteltijd bij calamiteiten vanaf 2008 vast te stellen op 8 uur.

5 Conclusies

Corporate Governance vereist een aantoonbare risicobeheersing van bedrijfsprocessen, met een transpa-

rante verantwoording en toelichting. Dit geldt voor alle belangrijke tekortkomingen.

Over de risicobeheersing van IT-risico's is in jaarverslagen weinig informatie terug te vinden. Dit is vreemd als we anderzijds in de krant lezen over het vaak mislukken van IT-projecten én we regelmatig met storingen in informatiesystemen worden geconfronteerd.

IT-governance gaat over de beheersing en verantwoording van IT-risico's in een organisatie. In interne risicorapportages komt de risicobeheersing van het IT-risico nadrukkelijk aan de orde. Waarom wordt de vertaalslag naar aantoonbare en transparante risicobeheersing van het IT-risico in het jaarverslag onvoldoende gemaakt? Communiceren IT-auditors de bevindingen onvoldoende eenduidig met het management, bestuur en accountant, óf zijn management, bestuur én accountant zich onvoldoende bewust van oorzaken en gevolgen van IT-risico's?

IT-auditing beoordeelt de kwaliteit van de risicobeheersing van IT-risico's. De vertaalslag van IT-controlebevindingen naar interne én externe risicoverantwoording is eenduidig te interpreteren en te organiseren. In dit artikel is een effectief kader voor informatie en communicatie over de risicobeheersing van IT-risico's beschreven. Als IT-auditors hun IT-controlebevindingen hiermee eenduidig gaan communiceren, dan krijgen management, bestuur en accountant direct inzicht in de oorzaken en gevolgen van IT-risico's.

De IT-auditor verdient anno 2007 zijn plaats in IT-governance proces (Van der Pijl, 2004). Met de toepassing van het beschreven kader voor informatie en communicatie over de risicobeheersing van IT-risico's geven we een handreiking om die verantwoordelijkheid te nemen, én daarmee directies en auditcommittees te overtuigen van de mogelijkheden tot een aantoonbare en transparante risicobeheersing van IT-risico's in het jaarverslag. ■

Literatuur

Boer, J.C. (1999), ICT-aspecten bij de accountantscontrole van de routinematige transactieverwerking, *Compact*, jg. 26, pp. 25-29.

Bommel, C.F. van en H.M. van Goor, (2004), IT-auditing in het kader van de jaarrekeningcontrole?, *Compact*, jg.31, nr. 2, pp. 10-16.

Bommel, C.F. van en H.M. van Goor (2005), IT-auditing afbakenen in het kader van de jaarrekeningcontrole, in *Maandblad voor Accountancy en Bedrijfseconomie*, jg.79, nr. 6, pp. 284-292.

Bommel, C.F. van en H.M. van Goor, L.C. Peek, en J.A.W. Winterink (2006), de betekenis van IT-auditing in het kader van de jaarrekeningcontrole ontrafeld, *Maandblad voor Accountancy en Bedrijfseconomie*, jg.80, nr. 10, pp. 487-493.

Commissie Corporate Governance (Tabaksblat, 2003), *De Nederlandse Corporate Governance Code: beginselen van goed ondernemingsbestuur en best practice bepalingen*; zie: www.commissiecorporategovernance.nl.

COSO-ERM (2004) - Enterprise Risk Management; zie: www.coso.org/publications.htm.

Deloitte (2005), Disarming the value killers, 2005; zie: www.deloitte.com/dtt/cda/doc/content/us_assur_Value%20Killers%20Report%20.pdf.

DNB, (2005), FIRM Financiële Instellingen Risicoanalyse Methode; zie: www.dnb.nl/dnb/home/toezicht/handboek_firm/nl/46-150689-64.html

Ernst & Young, (2007), Trends in ICT 2007, jg.11; zie: www.ict-barometer.nl/_files-cms/File/Trends_in_ICT.pdf.

Ernst & Young, (2005), Rapportages over interne beheersing en risicomanagement onder de maat, persbericht E&Y; zie: www.ey.nl/?pag=788&nieuws_id=2302.

Fijneman, R.G.A., (1999), *De betekenis en inhoud van 'jaarrekening ICT-Auditing' als onderdeel van de jaarrekeningcontrole; 'Common body of knowledge'- Consequenties voor de accountantscontrole*, proefschrift, Tilburg University Press, Tilburg.

Groot, de J. (2006), De 'in-control' good practice van de Commissie Frijns lost slechts een deel van de puzzel op, in *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 80, nr. 7/8, pp. 392-400.

IT Governance Institute, (2007), *COBIT, 4.1*; zie: www.itgi.org.

Leeuwen, van O en P. Wallage (2007), De zoektocht naar meer transparantie, in *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 81, nr. 10, pp. 469-479.

Monitoring Commissie Corporate Governance (Commissie Frijns) (2006), *Jaarrapport 2005 (2006) inzake de naleving van de corporate governance code*; zie: www.commissiecorporategoverance.nl.

Neisingh, A.W. (2002), Accountantscontrole en informatietechnologie: 'bij elkaar deugen ze niet en van elkaar meugen ze niet', *Compact,* jg. 29, nr. 4, pp. 4-11.

NIVRA (2002), Richtlijnen voor de Accountantscontrole.

NIVRA (2007), Controle- en Overige Standaarden; zie: www.nivra.nl/.

NOREA (2005), Samenwerking RA-RE inzake de jaarrekeningcontrole, concept versie.

NOREA (2004), IT-Governance - een verkenning; zie: www.norea.nl/Publicaties/publicaties.asp

Pijl, G.J. van der, (2004), IT-auditor, lid van de governance familie?, *De EDP-Auditor*, jg. 13, nr. 2, pp. 6-7.

Trouw (2007), Postbank wordt niet moe van zoveelste storing, 3 augustus 2007.

Winterink, J.A.W. en F. de Bruin (2006), Lakmoesproef voor risicobeheersing, in *AUDIT magazine*, 2006, nr. 3, pp. 6-10.