IT governance in relatie tot IT-toezicht bij bancaire instellingen

Samenhang SOX 404, Regeling Organisatie en Beheersing en de Nadere Regeling Gedragstoezicht Effectenverkeer 2002

Mw. B. Beugelaar RE RA

De diverse eisen vanuit wet- en regelgeving bij bancaire instellingen hebben in toenemende mate een impact op de IT-organisaties van deze instellingen en de omvang van de uit te voeren 'compliance'-activiteiten. Bancaire instellingen met een Amerikaanse beursnotering dienen behalve aan de Nederlandse wet- en regelgeving per 31 december 2006 ook te voldoen aan de eisen van de Sarbanes-Oxley Act 404 (SOX 404). Dit artikel geeft een overzicht van de samenhang en verschillen in de IT-toezichteisen van SOX 404, de Regeling Organisatie en Beheersing van De Nederlandsche Bank en de Nadere Regeling Gedragstoezicht Effectenverkeer 2002 van de Autoriteit Financiële Markten. Dit overzicht kan bancaire instellingen helpen bij het inzicht krijgen in de scope en omvang van de 'compliance'-activiteiten en het voorkomen van inefficiënties in de uitvoering van deze activiteiten. Tegelijkertijd wordt daarmee de aantoonbaarheid van het 'in control' zijn ten aanzien van de IT-toezichteisen ondersteund.

Inleiding

Financiële instellingen dienen aan verschillende toezichthouders verantwoording af te leggen omtrent het voldoen aan de diverse eisen die aan hen gesteld worden voor wat betreft de uitvoering van de bedrijfsactiviteiten. Uiteindelijk wordt door de instellingen ten aanzien van de bedrijfsvoering verantwoording afgelegd via onder meer het financiële jaarverslag. Nu geldt dat de bedrijfsvoering bij banken in belangrijke mate wordt ondersteund door geautomatiseerde systemen. Dit betekent derhalve dat ook vanuit de toezichthouders eisen worden gesteld ten aanzien van de betrouwbaarheid en continuïteit van de IT-omgeving bij banken. Aangezien de verschillende toezichthouders steeds meer eisen stellen en banken een omvangrijke en complexe IT-omgeving kennen, is het voorstelbaar dat inefficiënties ontstaan in de uitvoering van de compliance-activiteiten. Om inefficiënties bij het voldoen aan de toezichteisen te voorkomen is het van belang om vast te stellen of er een mogelijke redundantie aanwezig is in de verschillende wet- en regelgeving van de toezichthouders. Op basis van dit inzicht kan een overzicht dan wel handboek worden opgesteld dat als voordeel heeft, dat op elk gewenst moment kan worden nagegaan wat de toezichteisen zijn en de status ten aanzien van de mate van compliance met deze eisen. Tevens heeft dit handboek als voordeel dat de normen vanuit de verschillende toezichteisen herbruikbaar zijn. Het overzicht/handboek is mede een belangrijk hulpmiddel in de communicatie naar de medewerkers van de IT-organisatie ten behoeve van de

Mw. B. Beugelaar RE RA
is als senior manager werkzaam binnen de Line of Business Financial Services van KPMG Information Risk Management. In deze functie heeft zij een brede ervaring opgedaan in de dienstverlening aan met name bancaire instellingen. Momenteel vervult zij activiteiten ten aanzien van de advisering en controle op het gebied van SOX 404. Daarnaast is zij gespecialiseerd in de dienstverlening ten aanzien van implementatietrajecten van bankpakketten en het opzetten en beoordelen van internecontrolestructuren rondom bancaire processen.

beugelaar.brigitte@kpmg.nl

uitvoering en vastlegging van de uitgevoerde werkzaamheden in het kader van de wet- en regelgeving.

De toezichthouders die in dit artikel worden betrokken, zijn De Nederlandsche Bank (DNB), de Autoriteit Financiële Markten (AFM) en de Securities and Exchange Commission (SEC). De wet- en regelgeving van deze instanties wordt onderling vergeleken op overeenkomsten en verschillen. Opgemerkt wordt dat de wet- en regelgeving van de SEC, te weten SOX 404, alleen van toepassing is op instellingen met een Amerikaanse beursnotering. In Nederland geldt deze wet derhalve voor een beperkt aantal bancaire instellingen.

Dit artikel start met achtergrondinformatie omtrent wet- en regelgeving van de drie toezichthouders, vervolgens wordt een overzicht gegeven van de overeenkomsten en verschillen in de verschillende toezichteisen op het gebied van de geautomatiseerde gegevensverwerking, alsmede de impact hiervan voor de banken en de interne en externe accountants. Het artikel wordt afgesloten met een voorbeeldoverzicht van IT-toezichteisen op basis van onze praktijkervaringen.

Achtergrondinformatie (IT) toezicht bij banken

In Nederland dienen banken onder meer te voldoen aan de wet- en regelgeving van De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM). Ten aanzien van deze twee toezichthouders wordt stilgestaan bij de IT-aspecten in de Regeling Organisatie en Beheersing (ROB) en de Nadere Regeling Gedragstoezicht Effectenverkeer 2002 (NR2002). Voor banken met een Amerikaanse beursnotering geldt een verplichting om per 31 december 2006 te voldoen aan SOX 404. De werkzaamheden hiertoe dienen echter al gedurende 2006 te worden uitgevoerd. Als gevolg van SOX 404 worden ook eisen gesteld aan de IT-omgeving. Voor bespreking van de effecten van de Nederlandse code-Tabaksblat wordt verwezen naar andere artikelen in deze Compact. Dezelfde methode van analyse als beschreven in dit artikel kan uiteraard ook op deze regelgeving worden toegepast.

In onderstaande paragrafen wordt kort enige achtergrondinformatie gegeven ten aanzien van de doelstellingen van de ROB, NR2002 en SOX 404.

Regeling Organisatie en Beheersing

In de ROB is als doelstelling opgenomen: ‘Deze regeling heeft tot doel richtlijnen en aanbevelingen te geven voor de organisatie en beheersing van bedrijfsprocessen bij instellingen. Uitgangspunt hierbij is dat instellingen verantwoordelijk zijn voor een zodanige organisatie en beheersing van bedrijfsprocessen, dat daarmee wordt voorzien in een beheerste en integere bedrijfsvoering’ ([DNB02]).

De regeling is op 1 april 2001 in werking getreden met een overgangsregeling van een jaar. Sinds de inwerkingtreding van genoemde wet hebben de snelle veranderingen in de financiële sector een significante invloed gehad op de structuur en het risicoprofiel van banken. De toenemende aandacht voor thema’s als corporate governance, compliance en integriteit, alsmede de ontwikkelingen in het internationale bankentoezicht zijn voor DNB aanleiding geweest om deze regeling uit te brengen.

De kans op het ontstaan van inefficiënties in de uitvoering van de compliance-activiteiten is zeker aanwezig

De inhoud van de regeling is in de ROB als volgt gedefinieerd: ‘De regeling betreft de beheersing van risico’s die instellingen lopen, daarbij inbegrepen de risico’s voortvloeiende uit het niet of onvoldoende naleven van regelgeving en inbreuken op de integriteit van de bedrijfsvoering. Het gaat hierbij om de materiële risico’s, dat wil zeggen risico’s die de financiële prestaties, financiële positie, continuïteit of reputatie van de instelling in belangrijke mate kunnen aantasten. Bij dit alles is het uitgangspunt dat de verantwoordelijkheid voor het opstellen van procedures, regels en normen, de inbedding hiervan in de bedrijfsprocessen en het toezicht op de werking en de naleving bij de instelling zelf ligt. Het bestuur van de instelling ziet er op toe dat dit in de praktijk gerealiseerd wordt.

De regeling spitst zich toe op de elementen (1) risicobeheersing, (2) organisatorische maatregelen, (3) informatie en communicatie en (4) toetsing, beoordeling en bijstelling. De juiste aandacht voor deze elementen moet resulteren in de goede sturing en beheersing van bedrijfsprocessen.

De regeling beoogt, in samenhang met de hierna te noemen beleidsregels, een kader te scheppen waaraan instellingen zelf een nadere invulling dienen te geven. Deze aanpak laat ruimte voor een invulling die recht doet aan de specifieke situatie van een instelling en aan nieuwe ontwikkelingen’ ([DNB02]).

In de ROB wordt in paragraaf 2.5 expliciet aandacht gegeven aan de beheersing van de IT-risico’s van de bedrijfsvoering. DNB kent aan de IT een zodanig gewicht toe voor een betrouwbare en ongestoorde bedrijfsvoering dat een specifieke focus op de IT-aspecten gerechtvaardigd wordt geacht.

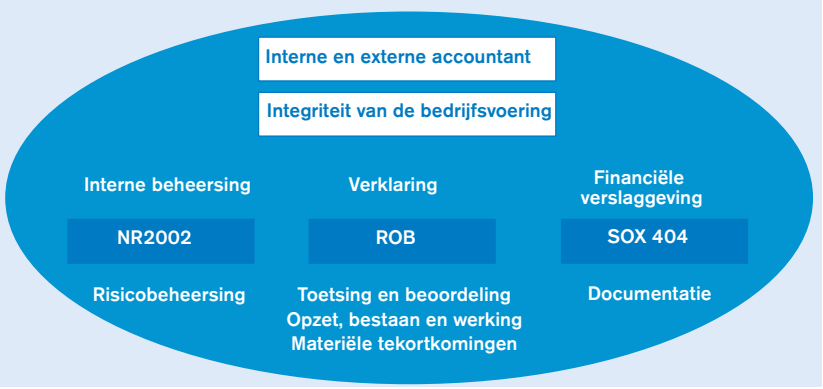
Nadere Regeling 2002

De AFM is de gedragstoezichthouder voor de gehele financiële marktsector. Alle financiële instellingen staan op basis van verschillende wetten onder het gedragstoezicht van de AFM. Voor banken met effectenactiviteiten geldt onder meer de Wet toezicht effectenverkeer (Wte) 1995. De algemene normen van de Wte 1995 zijn verder uitgewerkt in het Besluit toezicht effectenverkeer (Bte) 1995 en veel bepalingen van de Bte 1995 zijn weer uitgewerkt in de NR2002.

In de Bte zijn als eisen opgenomen dat een effecteninstelling beschikt over een goede administratieve organisatie, adequate internecontroleprocedures en een deugdelijke registratie van de verrichte diensten, alsmede over systemen voor een adequate bewaking en beheersing van het risico met betrekking tot haar gehele bedrijf en over systemen om te allen tijde nauwkeurig haar financiële positie te berekenen ([BTE95]). Deze organisatie, procedures, registratie en systemen moeten de AFM in staat stellen na te gaan of de regels inzake de bedrijfsvoering en de financiële waarborgen worden nageleefd. Derhalve behoudt de AFM zich het recht voor om regels te stellen met betrekking tot de administratieve organisatie, internecontroleprocedures, registratie en systemen.

De banken met effectenactiviteiten dienen naast de ROB derhalve ook te voldoen aan de eisen vanuit de NR2002. Ook in de NR2002 worden expliciete eisen gesteld ten aanzien van de geautomatiseerde gegevensverwerking. Omtrent de geautomatiseerde gegevensverwerking wordt het volgende gesteld: 'De effecteninstelling die gebruikmaakt van geautomatiseerde gegevensverwerking dient zodanige maatregelen en procedures door te voeren dat de beveiliging (vertrouwelijkheid, integriteit en continue beschikbaarheid) van de geautomatiseerde gegevensverwerking is gewaarborgd' ([AFM02]).

Figuur 1.



SOX 404

In 2002 is, na de schandalen met onder meer Enron en Worldcom, door de Securities and Exchange Commission (SEC) SOX 404 uitgevaardigd. Als gevolg van de inwerkingtreding van SOX 404 dienen Nederlandse instellingen met een Amerikaanse beursnotering per 31 december 2006 te voldoen aan de eisen gesteld vanuit SOX 404. SOX 404 vereist van de ondernemingsleiding van iedere in Amerika aan de beurs genoteerde onderneming dat de betrouwbaarheid van de financiële verslaggeving gewaarborgd is. SOX 404 schrijft voor dat het management (CEO en CFO) verantwoordelijk is voor het opzetten en onderhouden van adequate 'internal controls' (beheersingsmaatregelen) en procedures voor de financiële verslaggeving. Het management dient jaarlijks verantwoording af te leggen over de effectiviteit van de internal controls ten aanzien van de financiële verslaggeving. Door de Public Company Accounting Oversight Board (PCAOB) zijn, afgeleid van SOX 404, specifieke richtlijnen en procedures geformuleerd voor de werkzaamheden van de externe accountant. De externe accountant dient de verantwoording van het management te beoordelen en een eigen verklaring af te geven betreffende de effectiviteit van de 'internal controls' ten aanzien van de financiële verslaggeving. De standaarden in de PCAOB Standard 2 (An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements) zijn bepalend voor het stellen van eisen aan de 'SOX 404-processen' van organisaties. Bij SOX 404 wordt vanuit de selectie van 'significant accounts' een selectie gemaakt van de SOX 404-relevante processen en zogenoemde 'key controls' binnen de SOX 404-processen. De 'key controls' kunnen zowel handmatige als geprogrammeerde controles zijn. In geval in de SOX 404-relevante processen wordt gesteund op geprogrammeerde controles in applicaties ('key controls') dienen deze geprogrammeerde controles ('application controls') op effectiviteit te worden beoordeeld. Deze beoordeling omvat een 'Test of Design Effectiveness' (TOD) alsmede een 'Test of Operating Effectiveness' (TOE). De TOD en TOE dienen primair door het management te worden uitgevoerd en vervolgens door de externe accountant. In geval van geselecteerde application controls dient ook een beoordeling plaats te vinden van de TOD en TOE ten aanzien van de IT general controls. Het stelsel van beheersingsmaatregelen ten aanzien van de IT heeft derhalve zowel betrekking op application controls als op de IT general controls. In dit artikel wordt nader ingegaan op de IT general controls, die in het kader van SOX 404 als relevant worden aangemerkt.

In bovenstaande paragrafen zijn diverse begrippen genoemd (zie figuur 1). In de volgende paragraaf zal worden aangegeven wat de overeenkomsten en verschillen zijn tussen de verschillende toezichteisen, alsmede de impact hiervan voor de banken en de interne en externe accountants.

Overeenkomsten en verschillen tussen de diverse toezichteisen

In deze paragraaf zal meer inzicht worden gegeven in enkele algemene overeenkomsten en verschillen in de toezichteisen. Primair is het van belang om op hoofdlijnen vast te stellen wat de scope, reikwijdte en omvang van de uit te voeren compliance-activiteiten per toezichthouder zijn. De inhoudelijke eisen, inclusief overeenkomsten en verschillen, ten aanzien van de IT-aspecten worden in de volgende paragraaf uiteengezet. In tabel 1 worden de begrippen van de relevante toezichteisen uit figuur 1 als uitgangspunt genomen en onderling vergeleken. Overigens geldt dat deze begrippen niet een limitatieve opsomming betreffen, echter de belangrijkste aspecten zijn hierbij wel meegenomen.

Op basis van tabel 1 kan geconcludeerd worden dat er grotendeels overeenkomsten aanwezig zijn tussen de genoemde specifieke Nederlandse wet- en regelgeving en dat de verschillen met name gelden ten opzichte van de Amerikaanse SOX 404-wetgeving.

Overeenkomsten in alle toezichteisen zijn onder meer de aandacht voor de integriteit van de bedrijfsvoering, de aandacht voor de rol van de interne en externe accountant en de eisen die gesteld worden aan de betrouwbaarheid van de financiële verslaggeving.

De verschillen tussen de Nederlandse wet- en regelgeving en SOX 404 worden mede ingegeven door het feit dat SOX 404 is gebaseerd op Amerikaanse wetgeving die veelal als 'rule-based' wordt ervaren. De wetgeving van DNB en AFM geeft meer vrijheid aan de instellingen voor wat betreft de wijze van invulling van de compliance-activiteiten ('principle-based'). Een belangrijk verschil betreft het aspect continuïteit van de bedrijfsvoering. Voor zowel DNB als de AFM wordt dit van belang geacht, maar voor SOX 404 worden op dit punt geen eisen gesteld (met één uitzondering, te weten de eisen ten aanzien van de back-up en recovery van gegevens). Een ander belangrijk verschil is dat SOX 404 zich alleen richt op het identificeren van beheersingsmaatregelen voor die bedrijfsprocessen en systemen die een significante bijdrage leveren aan de financiële verantwoording.

Verder bestaan er verschillen ten aanzien van de focus in de risicoanalyse en risicobeheersing. SOX 404 heeft met name een focus ten aanzien van de beheersing van de financiële risico's (identificeren van eventuele materiële tekortkomingen), terwijl de ROB en de NR2002 ook aandacht besteden aan de beheersing van de operationele bedrijfsrisico's. In de ROB wordt onder meer expliciete aandacht besteed aan het marktrisico en operationele risico's, waaronder het continuïteitsrisico.

Een ander belangrijk verschil betreft de mate van aantoonbaarheid (documentatie) van het 'in control' zijn. In SOX 404 worden expliciete eisen gesteld ten aanzien van het documenteren van de door het management uitgevoerde beheersingsmaatregelen. Met name deze eis, alsmede de eis ten aanzien van het jaarlijks uitvoeren van TOD- en TOE-tests door het management, hebben een grote impact op de werkzaamheden die door de instellingen moeten worden uitgevoerd. Instellingen dienen meer tijd te besteden aan het documenteren en testen van de beheersingsmaatregelen voor SOX 404 dan in de Nederlandse toezichteisen wordt gevraagd. In het kader van de ROB wordt bij instellingen voor de beoordeling van de IT-omgeving veelal een driejaarscyclus gehanteerd op basis van een risicoanalyse. Bij SOX 404 geldt het principe 'Each year's audit has to stand on its own'. Daarenboven dient het management jaarlijks een verklaring af te geven (SOX 404-statement) dat het 'in control' is ten aanzien van het proces van de financiële verslaggeving en verantwoording. Materiële tekortkomingen voor SOX 404 dienen door het management expliciet te worden gerapporteerd.

Inzicht in de overeenkomsten in de toezichteisen ten aanzien van IT kan redundantie in compliance-activiteiten voorkomen

In de volgende paragraaf wordt op basis van enkele praktijkervaringen inzicht gegeven in de samenhang in toezichteisen ten aanzien van de IT-omgeving.

Overzicht van toezichteisen ten aanzien van de IT-omgeving

Om redundantie in de uit te voeren compliance-activiteiten te voorkomen is het van belang inzicht te hebben in wat de overeenkomsten zijn in de diverse toezichteisen ten aanzien van de IT-aspecten. Zowel in de ROB als in de NR2002 worden eisen gesteld ten aanzien van de beheersing van de IT-omgeving. Voor wat betreft de IT general controls in het kader van SOX 404 zijn in de SOX 404-wet en de PCAOB Audit Standard 2 geen expliciete detaileisen opgenomen. In de praktijk heeft een uitwerking plaatsgevonden door het 'IT Governance Institute'. In het document 'IT Control Objectives for Sarbanes-Oxley' ([ITGo04]) is een uitwerking opgenomen van de IT general controls. Dit document is gebaseerd op CobIT, waarbij ook onderdelen van ISO 17799 en ITIL (Information Technology Infrastructure Library) zijn meegenomen in de uitwerking.

Relevante toezichteisen	NR2002	ROB	SOX 404
Rol van de interne en externe accountant In de toezichteisen wordt expliciet een rol toegewezen aan de interne en/of externe accountant.	In de NR2002 is expliciet voor een aantal activiteiten een rol toegewezen aan de externe accountant. Verder blijkt uit de NR2002 dat een groot belang wordt toegekend aan controle en de uitvoering hiervan. Hierbij kan derhalve een belangrijke rol worden toegekend aan de interne accountant van een instelling.	In de ROB worden expliciete eisen gesteld aan het functioneren, alsmede de rol en taken van zowel de interne als de externe accountant.	In SOX 404 wordt expliciet een rol toegewezen aan de externe en interne accountant. De rol van de externe accountant is zeer expliciet belegd en vastgelegd in PCAOB Standard 2.
Integriteit van de bedrijfsvoering In de toezichteisen worden eisen gesteld ten aanzien van de integriteit van de bedrijfsvoering.	Aan de integriteit van de bedrijfsvoering worden expliciete eisen gesteld.	De integriteit van de bedrijfsvoering wordt in de ROB als een belangrijk element gekenmerkt. 'De regeling betreft de beheersing van risico's die instellingen lopen, daarbij inbegrepen de risico's voortvloeiende uit het niet of onvoldoende naleven van regelgeving en inbreuken op de integriteit van de bedrijfsvoering' ([DNB02]).	De achtergrond van SOX 404 geldt met name de integriteit van de bedrijfsvoering gericht op de betrouwbaarheid van de financiële verslaggeving. Ten aanzien van de integriteit van de bedrijfsvoering ('control environment') wordt als uitgangspunt onder meer het COSO-framework gehanteerd.
Financiële verslaggeving In de toezichteisen worden expliciet eisen gesteld aan de betrouwbaarheid van de financiële verslaggeving.	In de NR2002 worden niet zeer expliciete eisen gesteld aan de betrouwbaarheid van de financiële verslaggeving, zoals bij de ROB en SOX 404 het geval is. Wel kan bij de NR2002 indirect afgeleid worden dat hieraan eisen worden gesteld ten aanzien van de vastlegging van rechten en verplichtingen en de verantwoording van de orderafhandeling en de orderadministratie. In de Wte 1995 en de Bte 1995 worden wel eisen gesteld ten aanzien van de jaarrekening.	In de ROB worden expliciet eisen gesteld aan de betrouwbaarheid van de financiële verslaggeving. Het gaat hierbij om de beoordeling van de beheersing van materiële risico's, dat wil zeggen risico's die een materiële invloed kunnen hebben op de financiële prestaties, financiële positie, continuïteit of reputatie van de instelling. In de toetsing en beoordeling door de externe accountant worden de risico's en de beheersing daarvan in de beoordeling meegenomen. In aanvulling op de betrouwbaarheid van de financiële verslaggeving is ook de continuïteit van de bedrijfsvoering van belang en worden hiertoe aanvullende eisen gesteld.	SOX 404 heeft als uitgangspunt het detecteren van materiële tekortkomingen ten aanzien van de financiële verslaggeving. Derhalve zijn de eisen met name gericht op het beoordelen van 'key controls' die waarborgen dat de financiële verslaggeving betrouwbaar is.
Documentatie In de toezichteisen worden expliciet eisen gesteld aan het documenteren van procesbeschrijvingen, AO/IC-procedures en de uitvoering van de compliance-activiteiten.	Expliciete eisen ten aanzien van de documentatie door de instelling van het stelsel van AO/IC zijn opgenomen in de NR2002.	Expliciete eisen ten aanzien van de vastlegging van de documentatie zoals bij SOX 404 geldt, is bij de ROB niet van toepassing. Impliciet wordt wel verwacht dat procedures, regels en normen gedocumenteerd zijn. De ROB is geschreven met als insteek risicoanalyse en risicobeheersing. Ten aanzien van de onderkende risico's is aangegeven dat een informatiesysteem aanwezig dient te zijn voor de systematische meting, bewaking en documentatie van de krediet-, markt-, liquiditeits- en operationele risico's.	In de van SOX 404 afgeleide PCAOB Standard 2 zijn expliciete eisen opgenomen ten aanzien van de documentatie van het stelsel van beheersingsmaatregelen en de uitvoering van de compliance-activiteiten. Hoewel PCAOB Standard 2 primair van belang is voor de externe accountant zijn de daarin opgenomen richtlijnen in de praktijk tevens ook door het management grotendeels overgenomen bij de invulling van de SOX 404 compliance-activiteiten.
Opzet, bestaan (TOD) en werking (TOE) In de toezichteisen worden eisen gesteld ten aanzien van de uitvoering van activiteiten ter toetsing van opzet, bestaan en werking van AO/IC-procedures.	In de NR2002 zijn geen expliciete eisen gesteld ten aanzien van de uitvoering van TOD en TOE, zoals bij de ROB en SOX 404 het geval is.	De ROB voorziet in een opdracht aan de externe accountant waarbij de te verrichten werkzaamheden zijn gericht op de toetsing en beoordeling van de toereikendheid van de opzet, alsmede van de feitelijke implementatie in de bedrijfsprocessen (het bestaan) van de betreffende organisatieinrichting en het beheersingsmechanisme, en derhalve niet op de (doorlopend goede) werking.	In SOX 404 worden expliciete eisen gesteld ten aanzien van de door het management uit te voeren tests ten aanzien van de 'internal controls over financial reporting'. Deze omvatten zowel TOD als TOE. Ook door de extern accountant dienen TOD- en TOE-werkzaamheden uitgevoerd te worden, echter deze mogen pas starten op het moment dat het management zijn testwerkzaamheden heeft uitgevoerd en afgerond. 'Management goes first'. De TOD en TOE dienen jaarlijks te worden uitgevoerd.

Tabel 1. Overeenkomsten en verschillen in toezichteisen.

In de PCAOB Audit Standard 2 worden vier aandachtsgebieden voor de IT general controls geïdentificeerd, te weten:

- Access to programs and data;
- Program changes;
- Computer operations;
- Program development.

Per SOX 404 aandachtsgebied zal op basis van best practice-ervaring een relatie worden gelegd naar de raakvlakken met de Nederlandse toezichteisen (voorzover mogelijk). De opgenomen lijst van toezichteisen is niet limitatief. Afhankelijk van de specifieke situatie bij een instelling behoeft de lijst aanpassing. In dit artikel wordt bijvoorbeeld geen aandacht besteed aan de eisen die

Relevante toezichteisen	NR2002	ROB	SOX 404
Risicobeheersing In de toezichteisen worden eisen gesteld aan de invulling en uitvoering van risicoanalyse- en risicobeheersings-activiteiten.	De NR2002 geeft geen invulling aan het expliciet uitvoeren van risicoanalyse- en risicobeheersingsactiviteiten. Alleen op het gebied van procedures voor beheersing en beveiliging wordt bij de periodieke evaluatie van het beveiligingsbeleid geëist dat deze gebaseerd zijn op actuele risicoanalyses.	De ROB is opgesteld vanuit het oogpunt van risicobeheersing.	Ook in SOX 404 vormen de activiteiten ten aanzien van risicoanalyse een belangrijk onderdeel van de compliance-activiteiten. De focus ligt hier primair op de 'financial reporting risks'. In de ROB en de NR2002 wordt ook aandacht gegeven aan meer operationele en bedrijfsrisico's.
Interne beheersing In de toezichteisen worden eisen gesteld aan het hebben van een 'framework' van interne beheersing, inclusief aandacht voor de IT en/of COSO.	In de NR2002 zijn expliciete eisen opgenomen in bijlage 4 ten aanzien van de administratieve organisatie en het systeem van interne controle, inclusief de IT. Een expliciete referentie naar het COSO-framework is niet aanwezig. Echter, gelet op de aandacht voor de 'control environment' en AO/IC in de NR2002 kan indirect gesteld worden dat aan elementen vanuit het COSO-framework in belangrijke mate aandacht wordt besteed in de NR2002.	In de ROB wordt expliciet aandacht gegeven aan interne beheersing, waarbij in belangrijke mate de nadruk wordt gelegd op de beheersing van IT. Een expliciete referentie naar het COSO-framework is niet aanwezig. Echter, gelet op de aandacht voor de 'control environment' en interne beheersing kan indirect gesteld worden dat aan elementen vanuit het COSO-framework in belangrijke mate aandacht wordt besteed in de ROB.	In SOX 404 wordt expliciet verwezen naar het COSO-framework en ook de IT-controls worden als 'pervasive' controls aangeduid.
Toetsing en beoordeling In de toezichteisen worden expliciet eisen gesteld aan het (periodiek) toetsen en beoordelen van de eisen door het management.	In de NR2002 wordt niet expliciet een algemene eis gesteld ten aanzien van de uitvoering van een (periodieke) toetsing en beoordeling van de NR2002 door het management. Wel wordt hier op onderdelen van de eisen invulling aan gegeven.	In de ROB is het uitgangspunt dat de verantwoordelijkheid voor het opstellen van procedures, regels en normen, de inbedding hiervan in de bedrijfsprocessen en het toezicht op de werking en de naleving bij de instelling zelf ligt. Het bestuur van de instelling ziet erop toe dat dit in de praktijk gerealiseerd wordt. Bij de ROB wordt in de praktijk veelal op basis van een risicoanalyse de beoordeling van de IT-omgeving door middel van een driejarencyclus uitgevoerd.	In SOX 404 worden expliciete eisen gesteld ten aanzien van het periodiek (gedurende het jaar) toetsen en beoordelen van het bestaan en de werking van de 'internal control over financial reporting' (ICOFR). Hier geldt het principe 'Each year's audit has to stand on its own'.
Materiële tekortkomingen In de toezichteisen wordt expliciet aandacht besteed aan de wijze hoe om te gaan met materiële tekortkomingen in het stelsel van interne beheersing van de onderneming.	In de NR2002 wordt hieraan niet expliciet aandacht besteed.	In de ROB gaat het om de beheersing van materiële risico's. Er zijn verder expliciete eisen/richtlijnen opgenomen over de wijze van rapportering van majeure afwijkingen door de extern accountant. Deze rapportage van majeure afwijkingen betreft echter niet alleen financieel gerelateerde tekortkomingen maar bijvoorbeeld ook tekortkomingen op het punt van adequate waarborgen ten aanzien van een continue gegevensverwerking.	De SOX 404 compliance-activiteiten zijn gericht op het identificeren van materiële tekortkomingen ten aanzien van de ICOFR.
Verklaring In de toezichteisen worden expliciete eisen gesteld aan het verstrekken van een verklaring ten aanzien van de betrouwbaarheid van het stelsel van interne-beheersingsmaatregelen.	In de NR2002 wordt hieraan niet expliciet aandacht besteed. Management behoeft geen expliciete verklaring te verstrekken zoals bij SOX 404.	In de ROB wordt aan de externe accountant een separate opdracht gegeven ten aanzien van de toetsing van de compliance met de ROB en het verstrekken van een verklaring hierover. Management behoeft geen expliciete verklaring te verstrekken zoals bij SOX 404.	In SOX 404 worden expliciete eisen gesteld betreffende het afgeven van een verklaring zowel door het management als door de externe accountant ten aanzien van de 'effectiveness of internal control over financial reporting'.

Vervolg tabel 1. Overeenkomsten en verschillen in toezicht-eisen.

worden gesteld vanuit SOX 404 ten aanzien van een 'end user computing'-omgeving. Dit betreft een omgeving waarbij voor de financiële verantwoording onder meer gebruik wordt gemaakt van Excel-applicaties.

In de ROB zijn de eisen ten aanzien van bovenstaande aandachtsgebieden niet expliciet benoemd. Het identificeren van een eenduidige relatie met een specifiek ROB-artikel is hierdoor lastig uit te voeren. In de ROB is in artikel 56 een algemene norm opgenomen die meerdere aandachtsgebieden van SOX 404 betreffende de IT-beheersing raakt. Het artikel omvat: 'De instelling draagt zorg voor de uitwerking en implementatie van beleids-uitgangspunten ter beheersing van IT-risico's in zichtbare organisatorische en administratieve procedures en maatregelen, welke geïntegreerd zijn in de IT-processen en de dagelijkse werkzaamheden van alle relevante geledingen. Tevens wordt voorzien in een systematisch toezicht op de naleving daarvan.' De praktische invulling van dit artikel heeft DNB overgelaten aan de instellingen. In enkele artikelen, zoals artikel 55 en 57, wordt een nadere uitwerking gegeven, die echter zeer beperkt is.

Voor de NR2002 geldt dat meer in detail een uitwerking heeft plaatsgevonden van de eisen van de geautomatiseerde gegevensverwerking. In de NR2002 wordt een

algemene eis (4.27 1) gesteld, te weten: 'De effecteninstelling die gebruikmaakt van geautomatiseerde gegevensverwerking dient zodanige maatregelen en procedures door te voeren dat de beveiliging (vertrouwelijkheid, integriteit en continue beschikbaarheid) van de geautomatiseerde gegevensverwerking is gewaarborgd. Daarbij dient aandacht te zijn besteed aan maatregelen op de volgende gebieden:
a. algemene beheersingsmaatregelen in de geautomatiseerde omgeving;
b. de gehanteerde functiescheidingen;
c. geprogrammeerde controles die zich richten op de betrouwbare werking van de gebruikte applicaties ('application controls'); en
d. de maatregelen in de gebruikersomgeving.'

Toegang tot programma's en gegevens (access to programs and data)

Binnen dit aandachtsgebied worden eisen gesteld ten aanzien van de logische en fysieke toegangsbeveiliging voor wat betreft programma's en gegevens voor elk platform dat gebruikt wordt voor de financiële verslaggeving, zoals applicaties, besturingssystemen en databases.

Normen die in het kader van SOX 404 onder meer van belang zijn:
1. Het treffen van maatregelen ten aanzien van de implementatie, het onderhoud en de naleving van een informatiebeveiligingsbeleid.
2. Communicatie van het informatiebeveiligingsbeleid aan betrokkenen binnen de organisatie.
3. Het inrichten van een informatiebeveiligingsfunctie binnen de organisatie.
4. Het opstellen van security baselines voor de diverse systemen en het periodiek evalueren van de feitelijke systeeminstellingen met de security baselines.
5. Het treffen van maatregelen betreffende de logische en fysieke toegangsbeveiliging tot applicaties en systemen die de financiële rapportage ondersteunen (zoals netwerk, infrastructuur, applicaties, databases, etc.) om ongeautoriseerde toegang te voorkomen. Het betreft hier onder meer eisen ten aanzien van de samenstelling van passwords, de beheersing van ('kritische') toegangsrechten, het hebben van een authenticatiemechanisme, 'role-based' toegang en de periodieke beoordeling van de logging.
6. Het treffen van maatregelen ten aanzien van een periodieke evaluatie van de toegekende toegangsrechten, alsmede het aanpassen van de toegangsrechten indien nodig.
7. Het treffen van maatregelen ten aanzien van de logische toegangsbeveiliging die functiescheiding binnen de belangrijke bedrijfsprocessen waarborgen.
8. Het treffen van maatregelen die waarborgen dat de fysieke toegang tot systemen en ruimten die belangrijk zijn voor de financiële rapportage, beperkt is tot alleen daartoe geautoriseerde personen. Het betreft hier onder meer eisen ten aanzien van het beperken van de toegang, het periodiek beoordelen van de toegang tot bijvoorbeeld de computerruimten, en het plaatsen van bedrijfskritische applicaties in afgesloten computerruimten.

Dit aandachtsgebied komt bij de NR2002 terug in onderstaande specifieke eisen:
1. De fysieke functiescheidingen van de effecteninstelling dienen te zijn doorgevoerd in de functiescheidingen binnen de geautomatiseerde gegevensverwerking. Deze functiescheidingen in het geautomatiseerde systeem dienen te zijn vastgelegd in competentietabellen. De effecteninstelling dient (4.27 3):
   a. op basis van de competentietabellen een logische toegangsbeveiliging door middel van wachtwoorden te implementeren;
   b. te beschikken over procedures die voorzien in het regelmatig wijzigen van wachtwoorden evenals in een adequate beheersing van de competentietabellen;
   c. te beschikken over maatregelen die voorkomen dat ongeautoriseerde wijzigingen in de competentietabellen kunnen worden doorgevoerd;
   d. het geautomatiseerde systeem te voorzien van geprogrammeerde controles die de juistheid van de ingevoerde gegevens toetsen op betrouwbaarheid; en
   e. te beschikken over een herstelprocedure die voorziet in handleidingen en gegevens op basis waarvan gegevens die foutief of ongeautoriseerd zijn gewijzigd of ingevoerd, kunnen worden hersteld.
2. De effecteninstelling dient zorg te dragen voor maatregelen en procedures die voorkomen dat storingen en calamiteiten optreden binnen de geautomatiseerde gegevensverwerking. Hiertoe dient de effecteninstelling:
   e. te voorzien in procedures die voorzien in een fysieke en logische beveiliging van de gegevensdragers en andere computerfaciliteiten. (4.27 4)
3. De effecteninstelling dient te beschikken over procedures waarin de uitgangspunten voor beheersing en beveiliging zijn vastgelegd. Er dient een planning- en evaluatiecyclus aanwezig te zijn, die voortdurend bewaakt of de juiste maatregelen zijn getroffen en waaruit de werking van het beleid blijkt. De periodieke evaluatie van het beveiligingsbeleid dient te zijn gebaseerd op actuele risicoanalyses. (4.27 5)

Regeling Organisatie en Beheersing:
1. In de ROB worden geen expliciete eisen gesteld aan de toegang tot programma's en gegevens. In artikel 54 van de ROB wordt door DNB aangegeven, dat zij verwacht dat instellingen gebruikmaken van 'sound practices' met betrekking tot risicobeheersing op IT-gebied. In dit artikel wordt aangegeven dat de informatie- en beveiligingsbeleidsplannen op geïntegreerde wijze deel dienen uit te maken van het beheersingsmechanisme van de instelling als geheel.

Programmawijzigingen (program changes)

Binnen dit aandachtsgebied worden eisen gesteld ten aanzien van het doorvoeren van wijzigingen in programma's. Het risico van het ongeautoriseerd aanbrengen van wijzigingen dient gemitigeerd te worden.

Normen die in het kader van SOX 404 onder meer van belang zijn:

1. Het change-managementproces is beschreven en geborgd binnen de organisatie. Er dient een heldere, eenduidige procedure aanwezig te zijn die formeel door het management is goedgekeurd en voorziet in een vaste werkwijze en communicatie.
2. Alle wijzigingen ten aanzien van de systemen en applicaties dienen gedocumenteerd te worden. In de documentatie dient de processtroom van transacties en gerelateerde controles te zijn beschreven, alsmede dient deze actueel te worden gehouden naar aanleiding van wijzigingen.
3. Wijzigingen in de ICT-voorzieningen vinden alleen plaats na goedkeuring door daartoe bevoegde medewerkers zoals eigenaren van de bedrijfsprocessen, die gebruikmaken van de te wijzigen ICT-voorzieningen.
4. Beheersingsmaatregelen dienen aanwezig te zijn die waarborgen dat wijzigingen in applicaties en systemen getest, gevalideerd en geaccepteerd worden voordat de applicaties en systemen in de productieomgeving in gebruik worden genomen. Hiertoe is een formeel test- en acceptatieproces ingericht waarbij zowel het IT-beheer als de gebruikersorganisatie een rol speelt.
5. Scheiding is aanwezig tussen de test- en de productieomgeving.
6. De organisatie archiveert de testdocumentatie van alle wijzigingen.
7. Beheersingsmaatregelen dienen aanwezig te zijn die waarborgen dat de toegang tot het implementeren van wijzigingen in de productieomgeving voorbehouden is aan een beperkt aantal medewerkers (change-managementmedewerkers).
8. Alle wijzigingen in de productieomgeving dienen te worden gelogd door securitysoftware (bijvoorbeeld change monitoring tools) en de toegang tot het direct kunnen doorvoeren van wijzigingen in de productieomgeving dient beperkt te worden.
9. Wijzigingen in de productieomgeving die plaatsvinden buiten het reguliere change-managementproces om worden beoordeeld en indien nodig worden correcties uitgevoerd.
10. Een procedure dient aanwezig te zijn ten aanzien van spoedwijzigingen in de configuratie van systemen, applicaties en infrastructuur. Deze procedure voorziet onder meer in het loggen, het documenteren en het beoordelen van de wijziging de volgende dag. Urgente change requests zijn onderdeel van de formele change-managementprocedure.

Dit aandachtsgebied komt bij de NR2002 terug in onderstaande specifieke eisen:

1. De effecteninstelling dient maatregelen te nemen (4.27 2.1):
   a. die voorkomen dat ongeautoriseerde implementatie van nieuwe programmatuur en automatiseringssystemen plaatsvindt alsmede dat ongeautoriseerde wijzigingen in bestaande programmatuur en systemen worden doorgevoerd;
   b. die voorzien in een functiescheiding tussen de ontwikkelings- en testomgeving en de operationele omgeving, indien de effecteninstelling zelf specifieke programmatuur ontwikkelt of laat ontwikkelen;
   c. die voorzien in het testen van de diverse modules door de operationele omgeving alvorens de modules worden geïmplementeerd, indien de effecteninstelling gebruikmaakt van standaardprogrammatuur.
2. De effecteninstelling dient maatregelen en procedures te implementeren die bewaken dat de operationele omgeving gebruikmaakt van de juiste programmatuur, stamgegevens en geprogrammeerde controles. (4.27 3)
3. De effecteninstelling dient ervoor zorg te dragen dat veranderingen in informatiebehoeften en de daartoe benodigde aanpassingen in de automatiseringssystemen worden vastgesteld en doorgevoerd op basis van veranderingen in de doelstellingen en in het risicoprofiel van de effecteninstelling. (4.27 6)

Regeling Organisatie en Beheersing:

1. In de ROB worden geen expliciete eisen gesteld aan programmawijzigingen. In het kader van artikel 56 en ter beheersing van de IT-risico's dient een adequate procedure voor change management te zijn ingericht en kan hierbij gebruik worden gemaakt van de in SOX 404 en de NR2002 opgenomen aspecten.

Operationeel beheer (computer operations)

De IT-infrastructuur van een bank bestaat veelal uit diverse platformen en informatiesystemen. Hierbij worden allerlei activiteiten uitgevoerd, zoals het monitoren van de systemen, het opstarten van de batches, het afsluiten van applicaties, het distribueren van output, het bijhouden van de voorraad print- en mediabenodigdheden en het schoonhouden van de vitale apparatuur. Er zijn dus talloze activiteiten die ervoor zorgen dat de applicaties dagelijks actief zijn en dat de verwerking niet alleen overdag maar ook 's nachts plaatsvindt. Duidelijk is dat ook aan deze werkzaamheden normen moeten worden gesteld, zeker gezien het feit dat sommige van deze activiteiten kunnen worden betiteld als 'kritiek'. Computer operations is de beheersingsdiscipline die alle activiteiten omvat met betrekking tot het plannen en uitvoeren van dagelijkse, operationele activiteiten ten behoeve van het waarborgen van de adequate werking van de IT-infrastructuur.

Normen die in het kader van SOX 404 onder meer van belang zijn:
1. De organisatie heeft een back-up- en recoveryprocedure ingericht en geïmplementeerd ter waarborging dat kritieke data, transacties en programma's hersteld kunnen worden indien nodig. De procedure bestaat onder meer uit het op vastgestelde tijdstippen maken van back-ups, het bewaren van de back-ups offsite en het toewijzen van de back-up- en recoverywerkzaamheden aan daartoe bevoegde medewerkers.
2. Het periodiek testen van de effectiviteit van het 'restore'-proces en de back-ups (onsite en offsite).
3. Maatregelen dienen getroffen te zijn dat alleen geautoriseerde medewerkers toegang hebben tot de back-uptapes en de back-uptapelocatie (onsite en offsite).
4. De organisatie heeft een problem-managementprocedure ingericht en geïmplementeerd om problemen en incidenten te registreren, te analyseren en op te lossen.
5. Het management van de instelling heeft procedures geïmplementeerd ter waarborging van een juiste, volledige en tijdige verwerking van systeem jobs, inclusief batch jobs en interfaces. Hierbij dient gedacht te worden aan 'job processing'- en 'monitoring'-controles ten aanzien van de vastlegging en uitvoering van systeem jobs (job schedules), inclusief de bevestiging dat de jobs adequaat zijn uitgevoerd.

Dit aandachtsgebied komt bij de NR2002 terug in onderstaande specifieke eisen:
1. De effecteninstelling dient procedures te hebben die voorzien in het registreren, analyseren en oplossen van problemen die zich in het geautomatiseerde proces voordoen. (4.27 2.2)
2. De fysieke functiescheidingen van de effecteninstelling dienen te zijn doorgevoerd in de functiescheidingen binnen de geautomatiseerde gegevensverwerking. Deze functiescheidingen in het geautomatiseerde systeem dienen te zijn vastgelegd in competentietabellen. De effecteninstelling dient:
   e. te beschikken over een herstelprocedure die voorziet in handleidingen en gegevens op basis waarvan gegevens die foutief of ongeautoriseerd zijn gewijzigd of ingevoerd, kunnen worden hersteld. (4.27 3.e)
3. De effecteninstelling dient zorg te dragen voor maatregelen en procedures die voorkomen dat storingen en calamiteiten optreden binnen de geautomatiseerde gegevensverwerking. Hiertoe dient de effecteninstelling (4.27 4):
   a. te beschikken over een herstelprocedure die voorziet in handleidingen en instructies op basis waarvan de geautomatiseerde gegevensverwerking hersteld kan worden indien deze door calamiteiten of storingen is uitgevallen;
   b. te beschikken over adequate documentatie en gebruikershandleidingen voor de applicatieprogrammatuur;
   c. te voorzien in procedures voor het maken van veiligheidskopieën;
   d. te voorzien in procedures die het mogelijk maken om uit te wijken;
   e. te voorzien in procedures die voorzien in een fysieke en logische beveiliging van de gegevensdragers en andere computerfaciliteiten.

Regeling Organisatie en Beheersing:
1. In de ROB worden expliciete eisen gesteld aan computer operations. In artikel 57 worden nadere eisen gesteld aan onder meer het toepassen van back-up- en recoverymaatregelen. In het kader van artikel 56 en ter beheersing van de IT-risico's dient een adequate procedure voor computer operations te zijn ingericht en kan hierbij gebruik worden gemaakt van de in SOX 404 en de NR2002 opgenomen aspecten.

Systeemontwikkeling (program development)

Het in gebruik nemen van nieuwe systemen of het uitbreiden van bestaande systemen dient te worden ondersteund door richtlijnen en maatregelen die de betrouwbaarheid en de beveiliging van de systemen en bestanden waarborgen. Het is van groot belang om bij het ontwikkelen en aanpassen van systemen te voorkomen dat verlies, wijziging of misbruik van gegevens in toepassingssystemen mogelijk is. Beveiligingseisen dienen te worden onderkend en goedgekeurd voordat informatiesystemen worden ontwikkeld. Hiertoe moet erop worden toegezien dat beproefde methoden en technieken worden gebruikt voor voorbereiding, bouw, test en implementatie van de nieuwe of gewijzigde componenten. Nieuwe en aangepaste programmatuur dient slechts na autorisatie door de eigenaar, conform change management, in de operationele omgeving actief te worden.

Normen die in het kader van SOX 404 onder meer van belang zijn:
1. Beheersingsmaatregelen dienen te zijn getroffen die waarborgen dat nieuwe programma's en infrastructurele ontwikkelingen en investeringen goedgekeurd zijn door een daartoe bevoegd managementniveau (IT- en business management). Hierbij dient onder meer gedacht te worden aan inkoopprocedures, de implementatie van een ontwikkelmethodiek en een goedkeuringsprocedure voor projecten.
2. Het inrichten van een adequate ontwikkelmethodiek en projectmanagementstructuur ten behoeve van de ontwikkeling of aanschaf/inrichting van systemen en applicaties.
3. Het inrichten, toevoegen en aanpassen van controles die waarborgen dat de vastgestelde controledoelstellingen gehaald blijven worden in geval van implementatie of aanpassing van nieuwe systemen en applicaties. Hierbij dient onder meer gedacht te worden aan het documenteren van controles in functionele beschrijvingen en procedures voor het testen van de controles.

4. Beheersingsmaatregelen dienen te zijn getroffen die waarborgen dat een adequaat testproces voor de ontwikkelde en aangekochte systemen en applicaties wordt uitgevoerd en een sign-off van het testproces plaatsvindt door IT- en business management. Hierbij dient onder meer gedacht te worden aan het uitvoeren van een gebruikersacceptatietest, het hanteren van een adequate testaanpak, het testen van systeeminterfaces en het documenteren van de testresultaten.
5. Het opzetten en onderhouden van toereikende systeem- en gebruikersdocumentatie met daarin onder meer een vastlegging van de geprogrammeerde controles.
6. Het implementeren van procedures ten aanzien van het waarborgen van de integriteit van de dataconversie.
7. Het opleiden van gebruikers op basis van een adequaat opgezet trainingsplan.
8. Het uitvoeren van een post-implementatiereview van het nieuwe systeem of de nieuwe applicatie om vast te stellen dat deze adequaat functioneert dan wel functioneren overeenkomstig de gebruikerswensen en performance-eisen.

Dit aandachtsgebied komt bij de NR2002 terug in onderstaande specifieke eis:
1. De effecteninstelling dient ervoor zorg te dragen dat veranderingen in informatiebehoeften en de daartoe benodigde aanpassingen in de automatiseringssystemen worden vastgesteld en doorgevoerd op basis van veranderingen in de doelstellingen en in het risicoprofiel van de effecteninstelling. (4.27 6)

Regeling Organisatie en Beheersing:
1. In de ROB worden geen expliciete eisen gesteld aan systeemontwikkeling. In het kader van artikel 56 en ter beheersing van de IT-risico's dient een adequate procedure voor systeemontwikkeling te zijn ingericht en kan hierbij gebruik worden gemaakt van de in SOX 404 en de NR2002 opgenomen aspecten.

Samenvatting overzicht IT-toezichteisen

Samengevat kan gesteld worden dat de ROB het meest generiek is opgesteld met betrekking tot de IT-toezichteisen. De ROB heeft ten aanzien van de IT-omgeving als uitgangspunt beheersing van IT-risico's, mede op basis van de uitvoering van een IT-risicoanalyse. In een aantal artikelen, zoals artikel 55 en 57, zijn enkele eisen in meer detail uitgewerkt, bijvoorbeeld ten aanzien van de continuïteit van de gegevensverwerking. Aanvullend is in geval van uitbesteding van IT een aantal artikelen (artikel 58 tot en met 64) gedefinieerd ter beheersing van de IT-risico's. Het beheersen van het proces van uitbesteding en daarmee samenhangende IT-risico's wordt in de NR2002 en SOX 404 niet expliciet benoemd. Impliciet geldt dat voor SOX 404 de instelling ook verantwoordelijk is voor het 'in control' zijn ten aanzien van de uitbestede (IT-)processen. Hiertoe kan de instelling van de service provider een verklaring vragen, bijvoorbeeld in de vorm van een SAS 70-rapport. Een SAS 70-rapport kent een tweetal vormen, te weten een type I- en een type II-rapport. Een type I-rapport geeft een oordeel over de situatie dat de controles en procedures zoals beschreven door de organisatie ook geïmplementeerd zijn op een bepaald moment. Een type II-rapport geeft een oordeel dat, in aanvulling op een type I-rapport, de controles en procedures ook gewerkt hebben gedurende een bepaalde periode. Deze periode omvat meestal zes tot twaalf maanden.

De eisen vanuit de NR2002 worden afgedekt via de SOX 404-eisen, met uitzondering van procedures die het mogelijk maken om uit te wijken. De SOX 404-eisen voor de verschillende aandachtsgebieden zijn, op basis van best practice-ervaringen, meer gedetailleerd uitgewerkt door instellingen. Als voorbeeld hierbij kan worden gedacht aan de uitgebreidere eisen die gesteld worden betreffende het aandachtsgebied systeemontwikkeling.

De IT-toezichteisen dienen door instellingen het meest gedetailleerd te worden uitgewerkt en geïmplementeerd ten behoeve van het voldoen aan de SOX 404-eisen.

De IT-toezichteisen dienen door instellingen het meest gedetailleerd te worden uitgewerkt en geïmplementeerd ten behoeve van het voldoen aan de SOX 404-eisen

Financiële instellingen beschikken veelal al over handboeken met procedures betreffende de inrichting en beheersing van de IT-omgeving, zoals op ITIL en ISO 17799 gebaseerde handboeken (zie ook figuur 2). Om efficiencyvoordelen te behalen is het van belang dat instellingen nagaan wat de huidig geldende en geïmplementeerde set van IT-beheersingsmaatregelen is. Deze set van IT-beheersingsmaatregelen kan als uitgangspunt gehanteerd worden in de vergelijking met de IT-toezichteisen. Een redundantie in IT-beheersingsmaatregelen kan op deze wijze worden vastgesteld en tegelijkertijd kan in het handboek worden aangegeven voor welk toezichtkader de IT-beheersingsmaatregelen van belang zijn. Omdat in het kader van de toezichthouders ook eisen gesteld worden aan de opzet, het bestaan en in geval van SOX 404 ook aan de werking van de beheersingsmaatregelen, kunnen in het handboek ook

de 'testinstructies' en de 'testfrequentie' van de IT-beheersingsmaatregelen worden aangeduid. Op basis van dit handboek zijn de IT-medewerkers in staat de vereiste compliance-activiteiten op een eenduidige wijze uit te voeren.

Voor wat betreft de indeling van het handboek hebben wij in figuur 2 een voorbeeld van een index van het handboek opgenomen. Vanaf hoofdstuk 3 kan voor de onderverdeling per paragraaf de onderstaande indeling in de uitwerking worden gehanteerd:
- een beschrijving van de doelstelling van het proces;
- een verwijzing naar de beschikbare documentatie;
- een beschrijving van de interactie en afhankelijkheden met andere IT-beheerprocessen;
- een nadere uitwerking van de normen en procedures inclusief de testactiviteiten en de testfrequentie.

In kader 1 is als voorbeeld voor het proces fysieke (toegangs)beveiliging een nadere uitwerking van dit handboek IT Beheer & Wet- en Regelgeving opgenomen. De specifieke invulling van normen en testactiviteiten kan per instelling verschillen en dient op de specifieke situatie te worden afgestemd.

Tot slot

Gelet op de diversiteit in IT-toezichteisen is het van belang dat banken inzicht hebben in de samenhang in de IT-toezichteisen en de mate van compliance met deze eisen. Banken beschikken ter beheersing van de operationele bedrijfsvoering vaak al over een set van IT-beheersingsmaatregelen gebaseerd op onder meer ISO 17799 en/of ITIL. Veelal zijn deze standaarden geïmplementeerd en sluiten zij aan bij de geldende toezichteisen van de toezichthouders. Het kan echter van belang zijn om een overzicht te creëren waarin inzichtelijk is welke beheersingsmaatregelen en activiteiten uitgevoerd worden ten behoeve van de compliance met de IT-toezichteisen. Dit overzicht kan behulpzaam zijn bij een efficiënte en effectieve uitvoering van de compliance-activiteiten, de communicatie met de IT-medewerkers en bij het aantonen van de compliance aan de diverse toezichthouders. Bovendien geeft dit overzicht

Figuur 2. Voorbeeld van een procedurehandboek.

Inhoudsopgave

Inhoudsopgave

Fysieke (toegangs)beveiliging

Doelstelling van het proces
Het proces fysieke (toegangs)beveiliging dient voor het treffen van maatregelen ten behoeve van het veiligstellen van gebouwen, computerruimten, kluizen en apparatuur die zowel onopzettelijk als opzettelijk beschadigd kunnen worden. Maatregelen als fysieke toegangscontrole, brandbeveiliging, 'clean desk policy' en beveiliging van kabels zijn voorbeelden van maatregelen om de fysieke (toegangs)beveiliging te waarborgen.

Maatregelen als noodstroomvoorzieningen, die dienen om de robuustheid van de informatievoorziening te vergroten (en dus ook beveiliging bieden bij het uitvallen van de stroom), worden tot het Availability Management gerekend.

Documentatie
Het proces fysieke (toegangs)beveiliging is beschikbaar op de server in het tool 'xxxx'. Tevens is een hardcopy van de procedure opvraagbaar bij de procesverantwoordelijke de heer/mevrouw 'xxxxx'.

Interactie met overige IT-beheerprocessen
Zie 4.1 IT Beveiligingsbeleid en Procedures.

Normen en Procedures
Het teken (✓) geeft aan dat deze norm niet expliciet benoemd wordt in de ROB, echter dat op basis van te hanteren sound practices door invulling van deze norm ook impliciet invulling wordt gegeven aan de ROB-elementen.

Nr	Norm	ROB	NR2002	SOX 404
Norm 1a	De effecteninstelling dient zorg te dragen voor maatregelen en procedures die voorkomen dat storingen en calamiteiten optreden binnen de geautomatiseerde gegevensverwerking. Hiertoe dient de effecteninstelling te voorzien in procedures die voorzien in een fysieke en logische beveiliging van de gegevensdragers en andere computerfaciliteiten.	(✓)	4.27 4 e	
Norm 1b	Bedrijfskritische computerinstallaties en ondersteunende faciliteiten zijn geplaatst in beschermde zones. De beschermde zones zijn standaard afgesloten. Alleen geautoriseerde medewerkers hebben toegang tot de beschermde zones en zijn daar alleen aanwezig als daartoe de noodzaak bestaat. Derden hebben alleen onder begeleiding toegang tot de beschermde zones.	(✓)		Access to programs and data (APD)
Subnorm 1.1	Er dient een procedure te zijn die ingaat op het toekennen, wijzigen en intrekken van toegangsrechten tot het gebouw en de daarbinnen onderkende computerinstallaties en gescheiden zones (ook buiten kantooruren).	✓	✓	✓
Subnorm 1.2	Er dient een procedure voor fysieke (toegangs)beveiliging te zijn waarin identificatie, authenticatie en autorisatie van medewerkers (bijv. passen) worden behandeld.			
Subnorm 1.3	In de procedure fysieke (toegangs)beveiliging is het registreren van de toegang tot het gebouw, tot de computerinstallaties en de computerruimte vastgelegd.	✓	✓	✓
Subnorm 1.4	Er dient een procedure te zijn beschreven waarin het registreren en melden van beveiligingsincidenten is ondergebracht.	✓	✓	✓

Nr	Norm	Norm	Aantal tests
T 1.1	Stel vast dat een procedure aanwezig is en dat beschreven is op welke wijze het toekennen, wijzigen en intrekken van de toegang tot de computerinstallaties en de computerruimte plaatsvindt.	Norm 1a,b	1
T 1.2	Stel van een aantal gebruikers van de computerruimte vast dat de procedure is gevolgd onder meer ten aanzien van het registreren en begeleiden van derden bij de toegang tot de beschermde computerruimte.	Norm 1a,b	5
T 1.3	Stel vast wie toegang heeft tot de ruimte waar de kritieke servers staan, onder meer aan de hand van een lijst met medewerkers die lid zijn van de groep met computertoegang. Beoordeel de registratie van toegang en de reden tot deze toegang en of dit uit hoofde van hun werkzaamheden noodzakelijk is (alleen IT-personeel).	Norm 1a,b	5
T 1.4	Stel vast dat de procedure ten aanzien van het registreren en melden van beveiligingsincidenten is beschreven en werkt.	Norm 1a,b	5
T 1.5	Selecteer vijf willekeurige medewerkers en stel vast dat de toegang en uitgifte van de individuele pas tot het gebouw volgens de geldende procedure tot stand is gekomen.	Norm 1a,b	5

Kader 1. Uitwerking van een paragraaf in een procedurehandboek.

inzicht in de raakvlakken die bestaan tussen de verschillende IT-toezichteisen en kan het redundantie in de uitvoering van de compliance-activiteiten voorkomen. De in dit artikel opgenomen vergelijking tussen de IT-toezichteisen vormt een goed uitgangspunt voor het opstellen van dit overzicht. De verdere uitwerking van de compliance-activiteiten – bijvoorbeeld de uit te voeren testactiviteiten in geval van SOX 404 – dient op basis van dit overzicht een verdere invulling te krijgen.

Veelal wordt aan de meeste compliance-eisen impliciet al voldaan, gelet op de geldende maatregelen en eisen vanuit de IT-beheerhandboeken. Echter, met name voor wat betreft de aard en omvang van de werkzaamheden bestaan er verschillen. Voor SOX 404 dient onder meer ook de werking van de IT-beheersingsmaatregelen aangetoond te worden en worden daarbij hoge eisen gesteld aan bijvoorbeeld het documenteren van de testwerkzaamheden. Wanneer ten behoeve van SOX 404 bepaal-

de IT-beheersingsmaatregelen reeds geïmplementeerd zijn en getest worden, kunnen de resultaten hiervan ook gebruikt worden ten behoeve van het aantonen van de compliance voor de ROB en de NR2002. Hierbij geldt overigens wel de volgende belangrijke kanttekening. SOX 404 richt zich alleen op die systemen, applicaties en infrastructuur die van belang zijn voor de financiële verslaggeving; de ROB en NR2002 hebben betrekking op de gehele IT-omgeving en hebben daarmee een bredere scope. Met dit aspect dient rekening te worden gehouden bij de uitvoering van de compliance-activiteiten.

Op basis van de vergelijking tussen SOX 404, ROB en NR2002 is vastgesteld dat er, uitgaande van de vier SOX 404-aandachtsgebieden, raakvlakken bestaan tussen de IT-toezichteisen. Overigens is de lijst van opgenomen SOX 404-eisen niet limitatief en behoeft deze aanpassing afhankelijk van de organisatie en de lokaal geldende eisen.

Literatuur

[AFM02] Autoriteit Financiële Markten, *Nadere Regeling Gedragstoezicht Effectenverkeer 2002,* 1 september 2002.

[Beug00] B. Beugelaar RE RA, *Internet-technologie, toezicht en de rol van IT-auditors bij financiële instellingen,* Compact 2000/1.

[BTE95] Autoriteit Financiële Markten, *Besluit toezicht effectenverkeer 1995,* 1995.

[DNB04] De Nederlandsche Bank, *Handboek WtK 4201: Regeling Organisatie en Beheersing,* januari 2004.

[ITGo04] IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley: The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting,* 2004.

[KPMG04] KPMG, *KPMG IT General Controls Document – US Integrated* (5/04 Rev), 2004.

[NIVR01] NIVRA, *NIVRA Audit Alert 11: Werkzaamheden accountant in het kader van de Regeling Organisatie en Beheersing (ROB) van De Nederlandsche Bank,* 2 augustus 2001.

[PCAO04] PCAOB, *Standard number 2: An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements,* Public Company Accounting Oversight Board, 9 maart 2004.

[SEC02] SEC, *Sarbanes-Oxley Act,* Securities and Exchange Commission, www.sec.org, 2002.