ICT compliancy

Een kluwen van risico's, normenkaders, groeimodellen, wet- en regelgeving

Datum	: 03 mei 2007
Status	: Definitief
Betreft	: Afstudeerscriptie post doctorale EDP-audit opleiding VU Amsterdam
Teamnummer	: 704
Studenten	: M.G.H. van Roon & J. van Schajik
Afstudeerbegeleider	: P. Harmzen RE RA

Voorwoord

Als afsluiting van de post doctorale EDP Audit opleiding aan de Vrije Universiteit van Amsterdam hebben wij een scriptieonderzoek uitgevoerd ten behoeve van REAAL IT de IT organisatie van REAAL Verzekeringen. De scriptie heeft als onderwerp “ICT compliancy”.

Het idee voor de scriptie is ontstaan uit het feit dat banken en verzekeringsinstellingen vanuit diverse kanten wet- en regelgeving opgelegd krijgen. Voor REAAL IT is het onduidelijk of en in welke mate de diverse wetten en regels eisen stellen aan de IT-processen, -systemen en –organisatie. Daarnaast wil ze graag beschikken over een framework waarmee de organisatie kan worden getoetst op de mate van volwassenheid ten aanzien van de compliancy aan wetten en regels.

Gezien het feit dat er de afgelopen jaren veel is veranderd ten aanzien van wet- en regelgeving leek het ons interessant om de consequenties die de wetten en regels hebben voor de IT organisatie te onderzoeken.

Vanuit de Vrije Universiteit is de heer Paul Harmzen aangewezen als onze afstudeerbegeleider. Wij danken hem voor de ideeën, het doorlezen van de stukken en de begeleiding bij het afstudeertraject.

Daarnaast willen wij de interne begeleider Peter Mienes, de opdrachtgever Simon Greve en de IT auditors (Raymond Schroen, Ronald Sol, Ronald Snoep en Joost Beljaars) van SNS REAAL bedanken voor de inhoudelijke bijdrage aan het eindresultaat in de vorm van adviezen en aandachtspunten.

Tot slot bedanken wij de (gast)docenten voor de colleges van de afgelopen jaren die hebben bijgedragen aan het verbreden van onze vakkennis.

J. van Schajik
M.G.H. van Roon

Inhoudsopgave

1 Achtergrond afstudeeropdracht

§ 1.1 Inleiding

Dit hoofdstuk beschrijft de achtergronden die ten grondslag liggen aan de scriptieopdracht. Deze scriptie is gemaakt ter afronding van de postdoctorale EDP audit opleiding aan de Vrije Universiteit te Amsterdam. Het onderzoek heeft plaatsgevonden bij het verzekeringsbedrijf van SNS REAAL (verder REAAL Verzekeringen genoemd).

§ 1.2 Achtergrond

Transparantie en risicobeheersing zijn erg belangrijk in de financiële markt. Instellingen staan onder druk om omvangrijke en complexe rapportages op te (gaan) leveren aan regulerende autoriteiten en aandeelhouders. Het aankomende Solvency II verdrag, de Wet Financieel Toezicht, het voldoen aan de International Accounting Standards (IAS) en Sarbanes-Oxley wetgeving zijn onderwerpen die hun uitwerking hebben op de manier waarop ondernemingen hun bedrijfsgegevens verzamelen, vastleggen, analyseren, rapporteren en archiveren.

Mede als gevolg van het samengaan van de toezichthouders en de veranderde wet- en regelgeving zal het toezicht op het verzekeringswezen worden aangescherpt. De verwachting van het management van REAAL Verzekeringen is dat de huidige principes Interne Beheersing op termijn zullen worden vervangen door een variant van de Richtlijnen Organisatie en Beheer (ROB) van DNB. Om tijdig te kunnen voldoen aan deze aangescherpte wet- en regelgeving is in 2004 een nulmeting naar de ROB ICT uitgevoerd voor de IT organisatie van REAAL Verzekeringen. Op basis van deze nulmeting heeft REAAL IT een aantal verbeteringstrajecten uitgevoerd. In het voorjaar van 2006 heeft KPMG opnieuw een inventarisatie uitgevoerd in welke mate REAAL IT voldoet aan de IT artikelen van de ROB. Deze inventarisatie heeft aangetoond dat er een duidelijke verbetering binnen REAAL IT waarneembaar is in de aanwezigheid van expliciete beheerdoelstellingen, formele risicoanalyses, procesbeschrijvingen en controleprogramma's. Voor ieder proces die REAAL IT in haar IT processenmodel heeft gedefinieerd is een procesbeschrijving opgesteld waarin beheersdoelstellingen en beheersmaatregelen zijn uitgewerkt. Aan de hand van de beheerdoelstellingen en beheersmaatregelen is er per proces een controleprogramma opgesteld waarmee REAAL IT de werking van de maatregelen toetst. Verder wordt er periodiek binnen REAAL IT een RSA (risico self assesment) uitgevoerd waarbij het risicoprofiel wordt geactualiseerd.

REAAL IT heeft behoefte aan een volledig beeld van de wet- en regelgeving waar REAAL IT aan moet voldoen, aanvullend ten opzichte van het ROB kader. Daarnaast wil REAAL IT graag zicht hebben op de mate van compliancy ten aanzien van de van toepassing zijnde wet- en regelgeving (nulmeting en inschatting van de mate van volwassenheid). REAAL IT is specifiek geïnteresseerd in de consequenties die de Sarbanes Oxley wetgeving heeft ten aanzien van de automatisering van REAAL. Dit gezien het feit dat REAAL Verzekeringen namens ABN Amro het proces voor Bouwfonds Hypotheken uitvoert. De ABN Amro (heeft zelf een SOx verplichting) heeft REAAL Verzekeringen voor dit proces om een SAS70 verklaring gevraagd.

§ 1.3 Opdracht

Vanuit de behoefte aan een volledig beeld van de wet- en regelgeving en specifiek de Sarbanes Oxley wetgeving zijn de volgende onderzoeksvragen opgesteld, die centraal staan binnen deze afstudeerscriptie:

- Stel vast welke wet- en regelgeving van toepassing is op REAAL Verzekeringen en welke wet- en regelgeving eisen stelt aan de IT;
- Doe op basis van de van toepassing zijnde wet- en regelgeving een voorstel voor een referentiekader waarmee de eisen ten aanzien van de wet- en regelgeving getoetst kunnen worden (vaststellen mate van compliancy);
- Onderzoek welke volwassenheidsmodellen er zijn en onderbouw een voorstel voor de toepassing van één volwassenheidsmodel;
- Voeg aan het referentiekader de dimensie van volwassenheid toe waarmee de volwassenheid van de processen binnen REAAL IT kan worden vastgesteld;
- Geef aan welke consequentie de SOx wetgeving heeft voor REAAL IT.

Aanvullend op de bovengenoemde onderzoeksvragen is er gedurende het onderzoek het risicoprofiel van REAAL IT op hoofdlijnen uitgewerkt.

§ 1.4 Doelstelling

Doelstelling van het onderzoek is het voorstellen van een kader waarmee vastgesteld kan worden in welke mate REAAL IT voldoet aan wet- en regelgeving. Daarnaast schept het onderzoek duidelijkheid over de eisen die wet- en regelgeving stelt aan de IT organisatie van het verzekeringsbedrijf. Verder heeft het onderzoek als doel een voorstel te doen voor een te gebruiken volwassenheidsmodel om de getroffen IT beheersmaatregelen te kunnen koppelen aan een volwassenheidsfase. Om gericht de volwassenheid van de getroffen beheersmaatregelen te kunnen vaststellen is het onderzoek het risicoprofiel van REAAL IT op hoofdlijnen vastgesteld. Tot slot geeft het onderzoek inzicht in de consequenties die de Sarbanes Oxley wet heeft op de IT organisatie.

§ 1.5 Scope

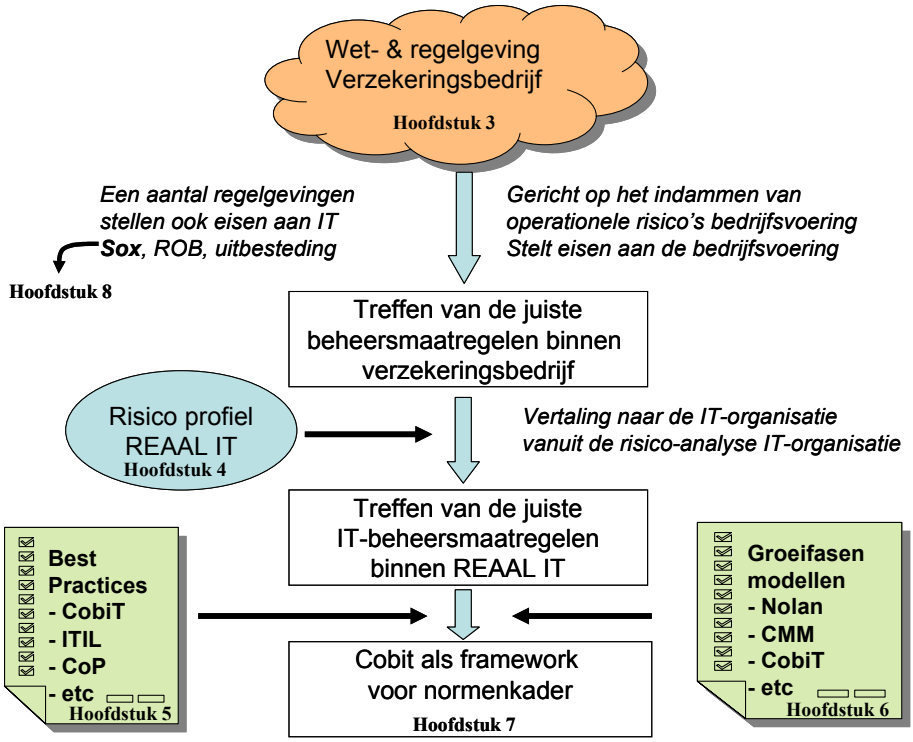
Er is relatief veel nationale- en internationale wet- en regelgeving waar organisaties mee geconfronteerd worden. Ten aanzien van het formuleren van eisen aan de IT is alleen gekeken naar die wet- en regelgeving die van toepassing is voor het verzekeringsbedrijf en eisen stellen aan General IT controls. Voor de volledigheid zullen we de overige wetgeving wel noemen.

§ 1.6 Methode van onderzoek

Dit scriptie onderzoek kenmerkt zich als een literatuurstudie naar wet- en regelgeving, best practices en interne stukken op het gebied van risico analyses en compliancy beoordelingen.

§ 1.7 Leeswijzer

In onderstaand schema is samengevat welke onderdelen in deze afstudeerscriptie worden behandeld.



In hoofdstuk 3 wordt een overzicht geschetst van de relevante regelgeving voor verzekeraars waarbij wordt ingegaan of er ook eisen aan de IT-organisatie worden gesteld.
Vervolgens is in hoofdstuk 4 het risicoprofiel beschreven van REAAL IT.
In hoofdstuk 5 is aangegeven welke gangbare best practices er zijn en welke best practices door IT-organisaties worden gehanteerd. In hoofdstuk 6 worden een aantal (binnen de IT) gangbare volwassenheidsmodellen beschreven die zijn onderzocht op toepasbaarheid.
Hoofdstuk 7 beschrijft op basis van de vorige hoofdstukken de uitwerking van het kader dat als basis dient om de compliancy voor REAAL IT te kunnen vaststellen. Tot slot wordt in hoofdstuk 8 specifiek stilgestaan bij Sarbanes – Oxley en wat de impact zou zijn als REAAL IT hier compliant aan wil zijn.

2 Samenvatting

De toenemende wet- en regelgeving vraagt om verantwoording van beheersing van bedrijfsprocessen. Beheersing van de informatievoorziening is een integraal onderdeel van de beheersing binnen de organisatie.

Deze scriptie geeft antwoord op een aantal onderzoeksvragen in het kader van ICT compliancy:

- Welke wet- en regelgeving is van toepassing op REAAL Verzekeringen en welke wet- en regelgeving stelt eisen aan de IT?;
- Doe op basis van de van toepassing zijnde wet- en regelgeving een voorstel voor een referentiekader waarmee de eisen ten aanzien van de wet- en regelgeving getoetst kunnen worden (vaststellen mate van compliancy);
- Onderzoek welke volwassenheidsmodellen er zijn en onderbouw een voorstel voor de toepassing van één volwassenheidsmodel;
- Geef aan welke consequentie de SOx wetgeving heeft voor REAAL IT.

Aanvullend op de bovengenoemde onderzoeksvragen is er gedurende het onderzoek het risicoprofiel van REAAL IT op hoofdlijn uitgewerkt.

Uit de inventarisatie van de wet- en regelgeving die van toepassing is op verzekeraars is vastgesteld dat deze voornamelijk eisen stellen aan het beheersen van de operationele risico's binnen de bedrijfsvoering. De wet- en regelgeving stelt nagenoeg geen expliciete eisen aan de ondersteunende informatievoorziening, anders dat ook hier de operationele risico's beheerst dienen te worden. De eisen die specifiek invloed hebben op de IT organisatie c.q. IT processen zijn de eisen met betrekking tot integriteits- en continuïteitsmaatregelen.

Om de operationele risico's te kunnen beheersen zijn in het onderzoek de best practices geïnventariseerd die worden toegepast om adequate beheersmaatregelen voor de informatievoorziening te treffen. Uit het onderzoek is vastgesteld dat het CobiT framework een organisatie in staat stelt om invulling te geven aan het bovenstaande verantwoordingsvereisten. CobiT is met name gericht op de beheersing van IT en biedt in de volle breedte van alle IT-processen de 'best practices' van beheersmaatregelen die binnen de IT-processen moeten worden getroffen om operationele risico's te beperken. CobiT biedt verder uitwerkingen naar andere best practices zoals ITIL, Code of Practice (Code voor Informatiebeveiliging), Prince2 en dergelijke, die een organisatie verder in staat stellen de juiste beheersmaatregelen te treffen.

Naast de best practices op het gebied van beheersing van de informatievoorziening is in het onderzoek tevens geïnventariseerd welke volwassenheidsmodellen aanwezig zijn die gehanteerd kunnen worden om de volwassenheid van de geïmplementeerde beheersmaatregelen vast te stellen. Ook hier is voor het CobiT framework gekozen aangezien deze de mate van volwassenheid van de beheersmaatregelen afdoende ondersteunt.

Vanuit de wet- en regelgeving wordt steeds meer van de bestuurder verlangd om gedocumenteerd aan te tonen dat de organisatie "in control" is. Het management is verantwoordelijk voor het implementeren en uitvoeren van de interne controle maatregelen. Het 'Trust me, Tell me, Show me and Prove me' principe moet hierbij in acht worden genomen. Deze "prove me" benadering is ook waarneembaar bij de externe toezichthouder. Met behulp van het CobiT raamwerk kan voor een IT-organisatie het niveau waarin de

beheersmaatregelen getroffen zijn uitgedrukt worden. Uitgaande van de “prove me” benadering kan gesteld worden dat het niveau van de beheersmaatregelen zoals deze getroffen zouden moeten worden vanuit de wet- en regeling, het niveau 3 conform de CobiT normering zouden moeten hebben.

Indien een organisatie als SNS REAAL SOx compliant zou willen zijn, dan wordt de lat met betrekking tot beheersbaarheid nog hoger gelegd. Niveau 4 van de CobiT normering zou dan ons inziens voor de getroffen beheersmaatregelen gelden. Voor een SOx compliancy audit dient de organisatie een bepaald traject te doorlopen waarbij:

1. De scope van het traject wordt vastgesteld;
2. een risico analyse wordt uitgevoerd op IT General- en application controls;
3. De controls worden gedocumenteerd;
4. Het ontwerp van de controls wordt geëvalueerd;
5. De controls worden getest op effectiviteit;
6. De tekortkomingen worden geprioriteerd en hersteld;
7. De effectiviteit van het gehele control programma wordt geëvalueerd.

Let wel de scope van SOx legt zich niet primair toe op de operationele risico’s, maar op de financiële verslaglegging. Waarbij de IT organisatie en IT processen faciliterend zijn beheerst moeten worden.

Samenvattend kan gesteld worden dat het CobiT raamwerk een goed instrument is om vast te stellen in hoeverre de operationele risico’s van de IT-organisatie beheerst worden. Op basis van het risicoprofiel van de IT-organisatie kan het instrument gericht ingezet worden. Vandaar dat aanvullend in dit onderzoek het risicoprofiel van REAAL IT op hoofdlijn is aangegeven.

Dat CobiT als overkoepelend raamwerk voor de beheersing van operationele risico’s binnen een IT-organisatie kan worden ingezet en tevens de mate van volwassenheid van de beheersmaatregelen kan worden vastgesteld is op zich niet onbekend. Het CobiT framework is goed bekend binnen de Nederlandse audit praktijk. CobiT is een de facto IT audit standaard. Wat wel opmerkelijk is, is dat de mate waarin het CobiT framework wordt toegepast aanzienlijk achter blijft (zie ook resultaat werkgroep IIA-CPP-COBIT). Met de resultaten van dit onderzoek en het voorstel om het CobiT framework voor de (toetsing van) beheersing van IT in te gaan zetten, zal de toepassing van CobiT binnen de IT auditwerkzaamheden van SNS REAAL een verdere invulling krijgen.

Als vervolg op dit scriptieonderzoek zal in maart 2007 een IT audit naar change management van REAAL IT worden uitgevoerd op basis van de aanpak zoals in deze scriptie is beschreven. Op deze wijze zal een eerste validatie plaatsvinden van de aanpak.

3. Regelgeving

Dit hoofdstuk geeft inzicht in de bestaande wet- en regelgeving die van toepassing is op het verzekeringsbedrijf. Bij de uitwerking van de wet- en regelgeving is aangegeven wat het doel is van de wetgeving, in hoeverre de wetgeving nu of in de toekomst van toepassing is voor REAAL Verzekeringen en of er expliciet eisen aan de IT-organisatie worden gesteld.

§ 3.1 Samenvatting wet- & regelgeving

In dit hoofdstuk is een analyse gemaakt op de van toepassing zijnde wet- en regelgeving voor verzekeraars en de mate waarin aandacht wordt geschonken aan IT organisaties, IT processen, IT risico of operationeel risico (hier maakt IT risico deel van uit).
De conclusie van deze analyse is dat deze wet- en regelgeving met name eisen stelt in termen van het op orde hebben van het interne risicobeheersingssysteem, het beheersen van operationele risico's, functiescheiding en het treffen van adequate beveiligingsmaatregelen van de bedrijfsvoering van een verzekeraar. Er worden nauwelijks tot geen eisen gesteld aan de processen van de IT-organisatie, anders dan dat de IT organisatie de operationele risico's van de IT processen in voldoende mate beheerst. De eisen die specifiek invloed hebben op de IT organisatie c.q. IT processen zijn de eisen met betrekking tot integriteits- en continuïteitsmaatregelen.

Voor dit onderzoek gaan wij ervan uit dat wanneer een verzekeringsbedrijf voldoet aan de eisen die de onderstaande wetten aan de IT organisatie stellen, de IT organisatie ook compliant is aan de wetten en regels die indirect eisen aan IT stellen:

- Regeling Organisatie & Beheer;
- Code Tabaksblat;
- Sarbanes Oxley;
- Solvency II;
- Wet bescherming persoonsgegevens;
- Wet Computer Criminaliteit.

Wetten c.q. regelgeving met indirecte eisen aan IT:

- IFRS;
- Wet Financieel Toezicht;
- Regeling uitbesteding.

Naast de bovengenoemde regelgeving is er een aantal wetten die specifieke eisen stelt aan IT organisatie of techniek. Vaak kennen deze wetten een eigen normenkader of specifieke eisen. Het voert voor dit onderzoek te ver om al deze eisen in één kader te omvatten. Het betreffen de volgende wetten:

- Databankenwet;
- Wetboek van Koophandel/ Burgerlijk Wetboek;
- Wet Melding Ongebruikelijke Transacties;
- Wet Elektronische Handtekeningen.

Onderstaand zijn in het kort de belangrijkste eigenschappen van de wet- en regelgeving die van toepassing is op het verzekeringsbedrijf beschreven. Daarbij is de volgende volgorde gehanteerd; eerst wet- en regelgeving zonder (specifieke) aandacht voor IT, vervolgens wet- en regelgeving met (specifieke) aandacht voor IT en tot slot wet- en regelgeving met specifieke vereisten.

Conclusie:
De huidige wet- en regelgeving (uitgezonderd de Wet Bescherming Persoonsgegevens en de Wet Computer Criminaliteit) stelt nagenoeg geen directe eisen aan de IT-organisatie, IT-processen en IT systemen. Organisaties dienen de operationele risico's beheersen. Hieronder wordt ook het IT-risico verstaan. Wanneer een organisatie SOx compliant wil worden gelden specifiekere eisen.

§ 3.2 Wet- en regelgeving zonder (specifieke) aandacht voor IT

In deze paragraaf wordt een aantal regelgevingen opgesomd waarin geen of zeer beperkte aandacht is besteed aan de IT organisatie en de mogelijke IT risico's.

§ 3.2.1 IFRS

De International Financial Reporting Standards vormt een set van afspraken over hoe bedrijven het jaarverslag moeten presenteren. De Europese Commissie heeft in een verordening aangegeven dat alle beursgenoteerde bedrijven vanaf 1 januari 2005 het jaarverslag conform de IFRS standaard moeten presenteren.

IFRS stelt eisen aan een adequate beveiliging, integriteit en controleerbaarheid. Onbevoegde toegang tot systemen en bestanden voor administraties die van belang zijn voor de controle moet nagenoeg onmogelijk zijn. De automatiseringsomgeving en de systemen dienen de functiescheidingen binnen de organisatie af te dwingen. Systemen dienen ingericht te zijn op de uitvoering van controles. Daarnaast dienen adequate herstel- of reconstructiemogelijkheden aanwezig te zijn.

IFRS stelt geen directe eisen aan het beheer van IT voorzieningen en de IT organisatie.

§ 3.2.2 Wet Financieel Toezicht

Op 1 januari 2007 is de Wet op het financieel toezicht (Wft) in werking getreden. Doel van de Wft is de wetgeving voor de financiële markten doelgericht, marktgericht en inzichtelijk te maken. De taken van DNB (prudentieel toezicht) en die van de AFM (gedragstoezicht) worden zodanig gescheiden dat er geen sprake is van overlap.

Invoering van de Wft heeft tot gevolg dat toezichtswetten zoals deze bestonden (Wet toezicht kredietwezen 1992, Wet toezicht verzekeringsbedrijf 1993, Wet toezicht effectenverkeer 1995, Wet toezicht beleggingsinstellingen, Wet toezicht natura-uitvaartverzekeringsbedrijf, Wet melding zeggenschap, Wet op het consumentenkrediet, Wet assurantiebemiddelingsbedrijf en de Wet financiële dienstverlening) op zijn gegaan in deze wet.

De WFT stelt geen directe eisen aan het beheer IT voorzieningen en de IT organisatie.

§ 3.2.3 Code Tabaksblat

De Nederlandse Corporate Governance Code vaak genoemd 'Code Tabaksblat', is een gedragscode voor beursgenoteerde ondernemingen. De gedragscode trad op 1 januari 2004 in werking. Het heeft als doel transparantie in de jaarrekening, betere verantwoording van de Raad van Commissarissen en de versterking van de zeggenschap en bescherming van aandeelhouders. De gedragscode is voor SNS REAAL, die sinds 27 mei 2006 beursgenoteerd is, ook van toepassing.
Code Tabaksblat geeft beperkt richting aan te stellen maatregelen rondom de IT voorzieningen.

§ 3.3 Wet- en regelgeving met (specifieke) aandacht voor IT

In deze paragraaf staan diverse wetten en regelingen centraal waarin aandacht is besteed aan de IT organisatie en de mogelijke IT risico's.

§ 3.3.1 Regeling Organisatie en Beheersing

De Regeling Organisatie en Beheersing (ROB) van De Nederlandsche Bank (DNB) is op 1 april 2001 van kracht geworden voor financiële instellingen. De ROB heeft als doelstelling richtlijnen en aanbevelingen te geven voor de organisatie en beheersing van bedrijfsprocessen bij financiële instellingen. SNS REAAL dient voor de bankorganisatie te voldoen aan deze regeling. De verwachting van REAAL IT is echter dat ook het verzekeringsbedrijf in de toekomst zal moeten voldoen aan een ROB gerelateerde regeling.
Op het gebied van IT stelt de ROB een aantal 'normen'. Het betreft de artikelen 54 tot en met 57. Indien sprake is van uitbesteding van (onderdelen van) de IT zijn daarnaast de artikelen 58 tot en met 64 van toepassing. Om te voldoen aan de gestelde normen in de ROB, geldt dat op genoemde gebieden de getroffen beheersmaatregelen aantoonbaar aanwezig zijn.

§ 3.3.2 Regelgeving rondom uitbesteding

Indien een verzekeringsbedrijf zaken heeft uitbesteed dient zij te voldoen aan de Regeling uitbesteding verzekeraars. DNB houdt toezicht op deze regeling. De regeling is op 22 januari 2004 in het leven geroepen door de toenmalige Pensioen en Verzekeringskamer (nu onderdeel van DNB). Volgens de regeling dient een verzekeraar de uitbestede diensten te beheersen. Uitbesteding ontslaat de verzekeraar niet van haar interne beheersingsverantwoordelijkheid. Dit in ogenschouw nemend zullen uitbestede IT diensten door REAAL IT ook vallen onder de regeling uitbesteding verzekeraars.

§ 3.3.3 Sarbanes-Oxley Act

De Sarbanes Oxley Act is ontstaan naar aanleiding van diverse boekhoudschandalen. De wet is op 30 juli 2002 van kracht geworden. De wetgeving is gericht op de verantwoordelijkheid die het bestuur van een organisatie heeft voor het onderhouden, evalueren en monitoren van de effectiviteit van de interne beheersing gericht op de financiële verslaglegging. REAAL Verzekeringen voert het hypotheekproces voor het Bouwfonds Hypotheken uit dat eigenaar is van ABN AMRO. Uit dien hoofde heeft REAAL Verzekeringen een relatie met een aan de Amerikaanse beurs genoteerd bedrijf en moet om deze reden voldoen aan SOx. Vandaar dat in het kader van deze afstudeeropdracht het SOx kader te betrokken in het onderzoek.

Hoewel SOx geen directe eisen stelt aan IT en de invalshoek financieel van aard is, speelt IT een belangrijke rol. De financiële rapporteringsprocessen worden ondersteund door IT-systemen, aangezien deze worden gebruikt voor de verwerking, opslag, overdracht en

rapportering van financiële data. De betrouwbaarheid van de financiële rapporten is dan ook afhankelijk de kwaliteit van de IT-omgeving. Het aantonen dat een organisatie SOx compliant, houdt tevens in dat aangetoond moet worden dat ook de ondersteunende IT-processen onder controle zijn. Hiertoe zijn door de PCAOB een aantal IT controledomeinen aangegeven (Program Development, Program Changes, Computer Operations en Access to Programs and Data) die in de context van SOx als belangrijke worden gezien.

Zie verder hoofdstuk 8 waar de consequenties van een SOx implementatie voor een IT-organisatie verder is uitgewerkt.

§ 3.3.4 Solvency II & Basel II

De wetgeving Solvency II bevindt zich op dit moment in de studiefase. De Quantitative Impact Study (QIS 2) is net achter de rug. De verwachting is dat de wet in 2009-2010 wordt ingevoerd. Ons inziens zal Solvency II vergelijkbaar zijn met de regelgeving Basel II die van toepassing is op banken. De Solvency wetgeving legt zich echter toe op verzekeraars.
De bedoeling van de Solvency II wetgeving is dat verzekeringsmaatschappijen dezelfde kapitaal- en risicoberekening gaan hanteren en hierover rapporteren aan de belanghebbenden. Belanghebbenden en toezichthouders kunnen dit gebruiken om de solvabiliteitspositie van de verzekeraars met elkaar te vergelijken. Als een toezichthouder van mening is dat de risico beheersing onvoldoende is kan deze bepaalde (aanvullende) eisen / maatregelen stellen.

Een aantal overeenkomsten tussen Basel II en Solvency II zijn:

- Doelstellingen zijn gelijk (internationale harmonisatie van toezicht);
- Bescherming van vreemd vermogen verstrekkers (polishouders/spaarders);
- Voorkomen van systeemrisico's;
- Drie pijlers.

Een aantal verschillen tussen Basel II en Solvency II zijn:

- Toezicht op geconsolideerd niveau (Basel) toezicht op juridische eenheden (Solvency);
- Solvabiliteitseisen zijn anders en verzekeraars hebben te maken met waarderingsregels voor technische voorzieningen.

Solvency II stelt geen directe eisen aan het beheer van IT voorzieningen en de IT organisatie.

§ 3.3.5 Wet bescherming persoonsgegevens

De wet bescherming persoonsgegevens (WBP) is op 1 september 2001 in werking getreden. De WBP stelt regels ten aanzien van de bescherming van privacy van burgers.
Organisaties die persoonsgegevens verwerken, zowel op papier als in computerbestanden (zo ook SNS REAAL) hebben een aantal plichten. Persoonsgegevens mogen, kort gezegd, verzameld en verder verwerkt worden, mits daarvoor wel bepaalde en uitdrukkelijk omschreven doelen zijn.
Voor verdere achtergronden ten aanzien van de beveiliging van persoonsgegevens zie Achtergrondstudies en Verkenningen 23 van de Registratiekamer.

Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op de naleving van de wet. Organisaties die persoonsgegevens verwerken dienen dit te melden bij het CBP.

De wet bescherming persoonsgegevens stelt eisen op het gebied van (informatie)beveiliging aan de IT voorzieningen en de IT organisatie. Daarnaast stelt de wet in het licht van beveiliging eisen aan het beheer van IT voorzieningen.

§ 3.3.6 Wet computer criminaliteit

Per 1 september 2006 is de uit 1993 stammende wetgeving over computercriminaliteit of ook wel cybercrime ingrijpend veranderd. Met name is de definitie van computervredebreuk (soms ook wel "hacken" genoemd) uitgebreid: elk opzettelijk en wederrechtelijk binnendringen in computersystemen strafbaar, ook als daarbij geen beveiliging wordt gekraakt.

Voorbeelden van computer criminaliteit zijn:

- Ongeoorloofd toegang verschaffen tot een computersysteem;
- Kopiëren van vertrouwelijke gegevens;
- Ongeoorloofd wijzigingen van computerdata;
- Ongeoorloofd uitschakelen of onbruikbaar maken van computersystemen;
- Virussen versturen;
- Fraude plegen met computers en valsheid in geschrifte met betrekking tot computerdata.

Voor SNSREAAL is de wet computer criminaliteit in zoverre van belang dat dergelijke misdaden door medewerkers (met bedrijfsmiddelen) gepleegd kunnen worden. De misdaden kunnen betrekking hebben op criminele activiteiten gericht op de eigen organisatie maar ook daarbuiten.

§ 3.4 Wet- en regelgeving met specifieke vereisten

In deze paragraaf staat een aantal wetten centraal die specifieke eisen stellen ten aanzien van de organisatie en daarmee aan de IT. Deze eisen zijn zo specifiek dat ze niet goed tegen algemene normenkaders getoetst kunnen worden anders dan de wetgeving zelf of eisen stellen aan application controls (vallen buiten de scope van dit onderzoek).
We hebben ervoor gekozen deze wetten wel te noemen maar ze niet op te nemen in het op te kiezen kader.

§ 3.4.1 Databankenwet

De databankenwet is ingevoerd in juli 1999. De wet regelt enerzijds de auteursrechten van de databank en anderzijds gaat de wet in op doeltreffende voorzieningen betreffende beveiliging. De beveiligingsmiddelen mogen echter adequaat gebruik van de databank niet hinderen. Deze wetgeving stelt indirect eisen aan de IT organisatie ten aanzien van beveiligingsbeheer.

§ 3.4.2 Wet melding ongebruikelijke transacties

In 1994 is de Wet melding ongebruikelijke transacties ingevoerd met als doel het tegengaan van het witwassen van gelden. Het signaleren van ongebruikelijke transacties stelt enerzijds organisatorische eisen, maar deze eisen kunnen ook in de vorm van application controls in de processen worden ingebed. Deze wet stelt eisen aan de bewaarplicht. Gegevens over meldingen van ongebruikelijke transacties dienen voor een periode van vijf jaar na de melding bewaard te blijven. Dit brengt eisen ten aanzien van back-up en restore met zich mee.

§ 3.4.3 Burgerlijk wetboek/Wetboek van koophandel

Het Wetboek van koophandel is ingevoerd in 1838. Het Nederlandse handelsrecht maakt nu deel uit van het burgerlijk recht. De bepalingen zijn vanuit het Wetboek van Koophandel overgebracht naar het Burgerlijk Wetboek. Deze wetten stellen eisen aan de integriteit en de bewaar- en reproduceerbaarheid van de gegevens. Het Burgerlijk Wetboek boek 2 geeft bijvoorbeeld met artikel 10 duiding aan de directe bewaarplicht. Hieraan kan alleen worden voldaan met een specifiek elektronisch archief. Een normale back-up zal doorgaans niet voldoende zijn. Hoe langer hoe meer zal ook e-mail worden gerekend tot de officiële stukken. Aandachtspunten zijn hierbij aantoonbare authenticiteit, aantoonbaar ongewijzigd en toegankelijkheid. Dit stelt voorwaarden aan een voldoende authenticatie.

§ 3.4.4 Wet elektronische handtekeningen

De wet elektronische handtekeningen is op 21 mei 2003 in werking getreden en regelt de rechtsgevolgen van elektronische handtekeningen. Het stelt de elektronische handtekening gelijk aan de handgeschreven handtekening. De elektronische handtekening is een middel om berichten veilig en betrouwbaar via Internet te kunnen verzenden. De wet elektronische handtekening stelt eisen waaraan de handtekening moet voldoen om voldoende betrouwbaar te zijn. Bijvoorbeeld dat de handtekening is gebaseerd op een gekwalificeerd certificaat dat voldoet aan strenge eisen zoals gesteld in de telecommunicatiewet en dat de handtekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen (bijv. smartcard).

4. Risicoprofiel REAAL IT

Het vorige hoofdstuk is afgesloten met de conclusie dat de wet- en regelgeving eisen stelt aan het beheersen van de operationele risico's. Dit vertaalt zich tevens door naar het mitigeren van de operationele risico's binnen de IT processen. In dit hoofdstuk wordt eerst de IT-architectuur van REAAL Verzekeringen en vervolgens het IT-procesmodel van REAAL IT toegelicht waarna het hoofdstuk wordt afgesloten met het beeld van het risicoprofiel van REAAL IT. Dit risicoprofiel is gebaseerd op het beeld dat vanuit diverse risico analyses is gedestilleerd.

§ 4.1 IT-architectuur REAAL Verzekeringen

REAAL heeft gekozen voor productleadership als primaire focus, het ontwikkelen van innovatief producten- en dienstenaanbod met een korte time-to-market. De belangrijkste speerpunten hierin zijn Wonen, Pensioenen en Schade. Het primaire distributiekanaal van REAAL is het vrije intermediair kanaal. Een van de manieren waarop groei van het marktaandeel wordt gerealiseerd, is het aangaan van allianties en daarbij behorende insourcing en het overnemen van marktpartijen.
De IT-architectuur van REAAL Verzekeringen is er in toenemende mate op gericht om de gehele verzekeringsketen te kunnen ondersteunen. Met Mijn REAAL ondersteunt REAAL Verzekeringen de intermediair. Mijn REAAL is weer gekoppeld aan de front- en backofficeverwerking binnen REAAL Verzekeringen zelf. De systemen binnen de architectuur zijn in hoge mate geparametriseerd om alle productvariatie die REAAL Verzekeringen heeft te kunnen ondersteunen. Door de toenemende ketenafhankelijkheid die de architectuur moet waarborgen, is er een tendens dat alle systemen binnen de architectuur nodig zijn om de business blijvend te ondersteunen. Deze generieke ondersteuning maakt differentiatie naar systemen waarvan de risico's minder groot zijn niet echt mogelijk aangezien de systemen door hun vergaande geparametriseerdheid inzetbaar zijn voor alle producten en processen.

De belangrijkste business principes die als uitgangspunt voor de architectuur gelden, zijn:

- Klantgevens zijn eigendom van het verkoopkanaal;
- Het ondersteunen van commerciële vrijheid bij producten met betrekking tot het samenstellen: (multiproduct) pricing, labeling, verzending en dergelijke moet mogelijk zijn zonder grote impact op de efficiëntie;
- Front office systemen 7*24 uur beschikbaar;
- Flexibele knip tussen front, - en backoffice processen bij inrichting van distributieketens;
- Straight through processing is het patroon voor de verzekeringsprocessen;
- Alle informatie is digitaal beschikbaar in het proces.

Het flexibel inrichten van processen en de gerelateerde systeemintegratie, voor zowel interne als externe ketens, zal qua architectuurinrichting verder vormgegeven worden met op Microsoft technologie gebaseerde middelen. Deze keuze voor Microsoft is gericht op consolideren van de set van middelen voor het ontwerpen, ontwikkelen, testen, integreren, implementeren en beheren van IT systemen. De IT-principes die uitgangspunt zijn voor de architectuur, zijn de volgende:

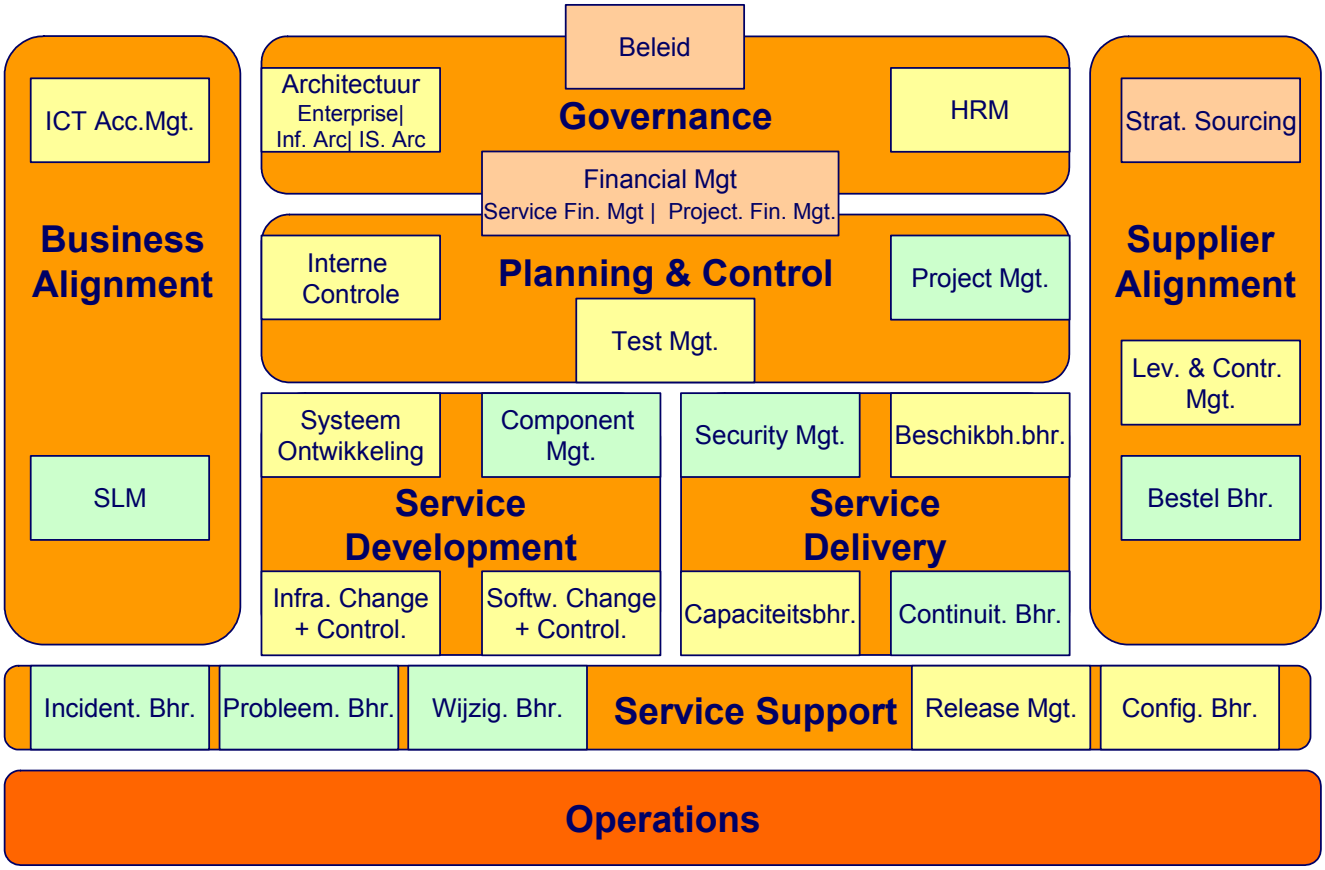
- Systeeminrichting op basis van service georiënteerde architectuur principe;
- Inzetten van standaard beheermiddelen;
- Centrale outputmanagementvoorziening voor het produceren van samengestelde commerciële output;

- Centrale management informatievoorziening;
- Centraal applicatie integratiemodel gebaseerd op marktstandaarden (.Net);
- Externe toegang tot internetomgevingen 7*24 uur beschikbaar;
- Centraal toegangsportaal voor externe partijen en gebruikers;
- Centrale voorziening voor digitale archieven.

Door het integraal ondersteunen van de business met bovengenoemde principes van de IT-architectuur ontstaat er een systeemlandschap die een integraal ondersteunend karakter heeft. Dit betekent eveneens dat voor het compliant zijn aan wet- en regelgeving voor een IT-organisatie geen differentiatie in het systeemlandschap gemaakt kan worden en de IT-organisatie, systemen en processen als geheel in beschouwing worden genomen. Het lastige hierbij is dat bij een compliancy audit, zoals bijvoorbeeld een SOx onderzoek, er geen specifiek gedeelte van de infrastructuur beoordeeld kan worden, maar de integrale architectuur, processen en organisatie onderwerp van onderzoek zijn.

§ 4.2 IT processenmodel REAAL IT

Binnen REAAL IT zijn alle onderkende processen opgenomen in het processenmodel (zie onderstaand overzicht). Dit model wordt door REAAL IT gebruikt als instrument voor kwaliteitsbewaking en dient ook als indeling voor de risico analyse die door REAAL IT is uitgevoerd (zie paragraaf 4.3).



Het REAAL IT procesmodel gaat uit van tien procesdomeinen:

1) Business: de bedrijfsprocessen van REAAL Verzekeringen (processturing buiten REAAL IT);
2) Business ICT Alignment: hoe kan REAAL IT de business het beste ondersteunen nu en in de toekomst?;
3) Governance: bepaling van beleid, de architectuur van REAAL IT;
4) Planning & control: toezicht op naleving en vertaling van het beleid, ondersteunende processen;
5) Service Development: realisatie nieuwe diensten en de daartoe benodigde systemen.
6) Service Planning: het planmatig op niveau houden van de dienstverlening, vooral gericht op de middellange termijn;
7) Service Support: ondersteuning van de levering van diensten, gericht op het heden;
8) ICT Supplier alignment: afstemming van behoeften van REAAL IT met leveranciers van producten of diensten;
9) Operations: concrete beheeractiviteiten die benodigd zijn om dienstverlening te leveren onder te verdelen in aandachtsgebieden;
10) Suppliers: leveranciers van producten of diensten (buiten REAAL IT);

De domeinen 2 t/m 9 worden aangestuurd binnen REAAL IT.

§ 4.3 Risicoprofiel REAAL IT

De hoofdactiviteit van REAAL IT is gericht op de verzorging van de geautomatiseerde ondersteuning voor de bedrijfsprocessen binnen REAAL Verzekeringen, om daarmee optimale ondersteuning te bieden aan de strategie.
Binnen REAAL wordt periodiek door Concern Audit en REAAL IT een risico analyse uitgevoerd om de operationele risico's binnen de IT processen vast te stellen.
Conform de risicotaxonomie van SNS REAAL vallen ICT Risico's onder de rubriek *operationeel risico*. DNB onderkent bijzonder belang aan het ICT risico in de Regeling Organisatie & Beheersing. In de risicoanalyse wordt enerzijds aandacht besteed aan het belang van de IT processen, en wordt anderzijds aandacht besteed aan de specifieke ICT Risico's die inhoudelijk (inherent en situationeel) van toepassing zijn.
Deze risico analyse is voor REAAL IT bedoeld om de juiste beheersmaatregelen te treffen. REAAL IT stelt zelf controleprogramma's op om de beheersmaatregelen te toetsen. De risico analyse is voor Concern Audit het uitgangspunt om de jaarplanning van de auditobjecten op te stellen.

Hieronder zijn de resultaten opgenomen van de risico analyse die voor de processen van REAAL IT zijn uitgevoerd. De risico's zijn uitgedrukt in Hoog, Midden en Laag. De risico's zijn per proces uit het IT procesmodel van REAAL IT als overkoepelend risico per proces aangegeven. Deze risico vaststelling is de resultante van het belang van het proces en de daarmee samenhangende risico, zoals hierboven kort is beschreven.

Proces	Risico
Beleid	M
Architectuur	M
Human Resource management	L
Financial management	M
Interne controle	L
Project management	M
Test management	M
ICT account management	L
Service Level Management	M
Systeemontwikkeling	M
Component management	L
Software change mgt & control	M
Infrastructuur change mgt & control	M
Capaciteitsbeheer	M
Beschikbaarheidsbeheer	M
Security management	M
Continuïteitsbeheer	H
Incidentbeheer	M
Probleembeheer	L
Configuratiebeheer	M
Wijzigingsbeheer	M
Releasemanagement	M
Strategical sourcing	M
Leveranciers & contractmanagement	M
Bestelbeheer	L
Operations	H

Op basis van de interne risico analyse zijn in hoofdstuk 7, paragraaf 7.2, deze processen afgebeeld op de processen binnen het gekozen framework.

5. Best practices binnen de IT

Dit hoofdstuk beschrijft binnen de IT-audit praktijk gehanteerde best practices. Daarnaast geeft het een overzicht van de best practices die veelvuldig binnen IT-organisaties worden ingezet voor het inrichten van beheersmaatregelen om de operationele risico's binnen de processen van een IT-organisatie in te dammen. Het hoofdstuk wordt afgesloten met een paragraaf waarin het verband wordt gelegd tussen de wet- en regelgeving zoals die in het vorige hoofdstuk staan beschreven en de raamwerkenkaders annex best practices, waardoor inzicht wordt gegeven in hoeverre de al bekende kaders de eisen vanuit de wet- en regelgeving afdekken.

§ 5.1 Best practices uit de auditpraktijk

In deze paragraaf zijn de best practices zoals die in de (IT-)auditpraktijk gehanteerd worden, opgesomd. Het betreffen hier de kaders zoals COSO, CobiT, SOx normen, eisen vanuit de Wet Bescherming Persoonsgegevens en de code voor informatiebeveiliging. Het zijn kaders die gehanteerd worden om enerzijds de processen binnen een IT-organisatie genormeerd te toetsen en anderzijds voor het inrichten van de beheerprocessen.

§ 5.1.1 COSO

COSO is een management model dat is ontwikkeld door The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Dit comité heeft in 1992 naar aanleiding van een aantal boekhoudschandalen en fraudegevallen aanbevelingen gedaan en richtlijnen aangegeven ten aanzien van interne controle en interne beheersing. In 1994 is daar nog een aanvulling op gekomen en werd dit samengevoegd in het COSO-rapport. Dit rapport is bedoeld om aan organisaties een uniform en gemeenschappelijk referentiekader voor interne controle aan te bieden en om het management te ondersteunen bij de verbetering van het interne controlesysteem. In 2004 werd het model geactualiseerd, werden elementen toegevoegd en aangepast. Dit geactualiseerde model richt zich niet alleen meer op interne controle, maar op het gehele interne beheersingssysteem en staat bekend als COSO II of Enterprise Risk Management Framework (ERM).
COSO behoort tot een van de standaard referentiemodellen die door auditors worden gebruikt bij een onderzoek.

§ 5.1.2 CobiT

Control Objectives for Information and related Technology (CobiT) is een framework voor het gestructureerd inrichten en beoordelen van een IT organisatie. CobiT stelt IT managers in staat om op basis van algemeen geaccepteerde Best Practices de ICT beheermaatregelen in te richten. Daarnaast kunnen auditors op basis van het framework hun controleprogramma's beschrijven en uitvoeren.
CobiT staat momenteel in de vernieuwde belangstelling doordat in het kader van Sarbanes-Oxley vanuit het ITGI het document "control objectives for SOx" is uitgebracht. In dit document is een normering opgenomen die IT organisaties kunnen hanteren bij het vaststellen in hoeverre men SOx compliant is. Deze normering maakt gebruik van CobiT.

§ 5.1.3 Control objectives for SOx

Hoewel de invalshoek van SOx financieel is van aard, speelt IT een belangrijke rol. Veel beursgenoteerde ondernemingen zullen over het algemeen hun eigen software schrijven of gebruik maken van standaard systemen die in belangrijke mate zijn geparametriseerd voor de specifieke organisatie. Dergelijke bedrijven hebben maatwerk voor afhandeling van logistieke en interne procedures. Niet zelden zijn een aantal programmeurs in dienst die wijzigingen in

de software verzorgen op basis van eisen en wensen (wetgeving, gebruikersvraagstukken, bugs, etc.)
Als de door het bedrijf geschreven software de cijfers oplevert die accountants betrekken bij de oordeelsvorming, dan zullen de accountants zeker vragen stellen bij het tot stand komen van deze software. In veel gevallen zal het bedrijf moeten aantonen dat de software op een deugdelijke wijze is ontwikkeld en of beheerd.
Naast het feit van de verplichting tot het uitvoeren van controles waarmee aangetoond wordt dat de software op een deugdelijke wijze is ontwikkeld en of beheerd, vereist SOx bewijs dat deze geautomatiseerde controles correct en volledig zijn. Om te kunnen steunen op geautomatiseerde controles zal een onderneming ook haar algemene beheersmaatregelen rondom IT (General Controls) op orde moeten hebben om SOx compliant te worden.

Het ITGI heeft, zoals in de vorige paragraaf is aangegeven, een praktische uitwerking gemaakt op basis van het CobiT-raamwerk en in een rapport uitgebracht (control objectives for SOx). Dit rapport kan gebruikt worden bij het opstellen van een plan voor IT-controle ten behoeve van SOx.

§ 5.1.4 Code voor informatiebeveiliging

Code of practice for information security management, houdt zich bezig met informatiebeveiliging in de breedste zin van het woord. De code levert best practices, richtlijnen en algemene principes voor invoering, onderhoud en management van informatiebeveiliging. Deze code is een hulpmiddel voor organisaties van uiteenlopende omvang en type.
Deze internationale code geeft richtlijnen voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. De code kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

§ 5.1.5 Raamwerk Privacy Audit

Het raamwerk Privacy Audit is opgesteld voor het uitvoeren van Privacy Audits bij organisaties waar persoonsgegevens worden verwerkt. Het Raamwerk is geschreven voor auditors die belast zijn met de uitvoering van een Privacy audit en biedt een handvat voor het opstellen van een auditplan. Het management van een organisatie kan naar eigen keuze invulling geven aan de technische en organisatorische maatregelen ter borging van de bescherming van de persoonsgegevens. In het Raamwerk is vanuit CobiT een vertaling gemaakt naar de wijze waarop de organisatie haar (geautomatiseerde) gegevensverwerking kan inrichten en beheersen. Via deze methode zijn de eisen die uit de WBP zijn af te leiden, vertaald naar concrete technische en organisatorische en beheersmatige maatregelen en procedures.

§ 5.1.6 BCP

Van nature zijn instellingen van de financiële kerninfrastructuur gericht op het risicobeheer en beschermen van hun systemen en kritische bedrijfsprocessen. Vertrekpunt hierbij zijn continuïteitseisen zoals vastgelegd in de Regeling Organisatie en Beheer.
In 2004 is interbancair een toetsingskader business continuity planning (BCP) opgesteld dat banken, Equens (voorheen Interpay), beursinstellingen, andere marktpartijen en DNB zullen gebruiken om hun BCP-plannen concreet in te vullen en actueel te houden. SNS REAAL heeft dit toetsingskader ook voor REAAL Verzekeringen als uitgangspunt voor haar continuïteitseisen gekozen.

Het toetsingskader BCP moet een eigentijds antwoord zijn op factoren die een bedreiging kunnen vormen voor het ongestoord functioneren van het betalings- en effectenverkeer. Het kan hierbij gaan om een veelheid van oorzaken, zowel van buiten als van binnen de sector.

§ 5.2 Best practices binnen IT-organisaties

In deze paragraaf zijn de best practices zoals die binnen veel IT-organisaties worden toegepast beschreven. Het betreft hier best practices op het gebied van ontwikkeling en beheer. Deze best practices ondersteunen IT-organisaties bij het concreet inrichten van hun processen en procedures.

§ 5.2.1 ITIL

ITIL (Information Technology Infrastructure Library) is ontwikkeld als een procesraamwerk voor het inrichten van de beheerprocessen binnen een ICT organisatie. ITIL is geen methode of model, maar een set van best practices.
ITIL pretendeert best practices te geven voor het gehele beheer van de ICT infrastructuur in de breedste zin des woords (inclusief applicaties, documentatie etc.) Met name de service support en delivery sets zijn populair en voor applicatiebeheer winnen de creaties ASL en BiSL aan populariteit (zie verder de paragrafen 5.2.2. en 5.2.3).

§ 5.2.2 ASL

ASL (Application Services Library) is een procesraamwerk, ondersteund door best practices, die de processen van het beheer, onderhoud en vernieuwing van informatiesystemen en applicaties beschrijft. Het biedt een handvat bij het verbeteren van organisaties die applicatiebeheer uitvoeren.
Daar waar ITIL als beheermethodiek sterk gericht is op het beheren van IT-infrastructuren, legt ASL de nadruk op applicatiebeheer, op de processen rond het beheren en onderhouden van software en de gegevensbanken. De ITIL processen zijn voor een groot deel binnen ASL terug te vinden, met name in de hoek van de beheerprocessen en de tactische processen. ASL legt de nadruk op de ontwikkelcyclus (onderhoud / vernieuwing).

§ 5.2.3 BiSL

Business Information Service Library is een procesraamwerk voor het uitvoeren van functioneel beheer en informatiemanagement. Anders dan ASL en ITIL richt BiSL zich niet op ICT-organisaties, maar juist op de gebruikersorganisatie. In BiSL staat beschreven:

- Op welke wijze een gebruikersorganisatie ervoor kan zorgen dat informatievoorziening adequaat werkt;
- Op welke wijze men behoeften in het bedrijfsproces vertaalt naar ICT-oplossingen en niet ICT-oplossingen;
- Op welke wijze men de informatievoorziening en ICT-dienstverlening vanuit een gebruiksoptiek stuurt;
- Op welke wijze men de informatievoorziening op lange termijn vormgeeft.

Het BiSL procesraamwerk sluit aan op de procesraamwerken ASL en ITIL.

§ 5.2.4 Prince2

PRINCE2 (**PR**ojects **IN** a **C**ontrolled **E**nvironment) is een gestructureerde methode voor effectief projectmanagement. PRINCE2 is de verbeterde en uitgebreide versie van namelijk PRINCE. PRINCE was primair bedoeld voor ICT-projecten. PRINCE2 is algemener toepasbaar, maar wordt nog steeds veel gebruikt in de ICT-wereld.

PRINCE2 is toepasbaar op alle projecten en kent een grote flexibiliteit. Aspecten van de methode die niet van toepassing zijn op (of niet nuttig voor) een bepaald project, kunnen overgeslagen worden.
PRINCE2 ziet als grondbeginselen van goed projectmanagement dat een project een eindig proces is met een duidelijk begin en eind en dat projecten altijd moeten worden beheerst om succesvol te zijn. Prince2 kan als de defacto norm worden gezien voor het uitvoeren van projecten.

§ 5.2.5 RUP

Rational Unified Process of RUP is een iteratief softwareontwikkelingsproces.
RUP is gebaseerd op een aantal principes en best practices.
Gezien de tijd die het kost om grote softwaresystemen te bouwen, is het niet mogelijk om een heel systeem in één keer te maken. Iteratief ontwikkelen stelt je in staat om het project op te delen in een aantal deelproducten en deze afzonderlijk van elkaar op te leveren. RUP is erop gefocust de basisarchitectuur van een systeem in een vroeg stadium te bepalen en naarmate het systeem groter wordt zal de architectuur zich verder uitbreiden. Bij iteratief ontwikkelen is het mogelijk de componenten geleidelijk aan in kaart te brengen om ze vervolgens te ontwikkelen, kopen of hergebruiken. Zoals bij alle andere softwareprojecten zijn veranderingen in de software onvermijdelijk. RUP beschrijft een aantal methoden om deze veranderingen te beheersen en nauwkeurig te volgen. RUP is een van de beschreven software ontwikkelingsprocessen die in toenemende mate als best practice wordt toegepast.

§ 5.2.6 TMap

TMap staat voor Test Management approach en behelst een gestructureerde testaanpak voor informatiesystemen. De aanpak steunt op een viertal pijlers:

- Een aan de ontwikkelingscyclus gerelateerde fasering van testactiviteiten;
- Een goede organisatorische inbedding;
- De juiste hulpmiddelen en infrastructuur;
- Bruikbare technieken voor de testactiviteiten.

TMap is een generiek model, geschikt voor vrijwel alle testsoorten en testactiviteiten in de informatievoorziening. De beschreven aanpak wordt reeds vele jaren in een groot aantal projecten en organisaties met succes toegepast.

§ 5.3 Regelgeving versus best practices

Deze paragraaf beschrijft de relatie van de in hoofdstuk 3 weergegeven wet- en regelgeving naar best practices zoals die in dit hoofdstuk zijn vastgesteld.

§ 5.3.1 Beschouwde wet- en regelgeving vs best practices

Op basis van de in de hoofdstuk geïnventariseerde best practices is de scheiding die in dit hoofdstuk is aangebracht tussen de best practices uit de IT-organisaties (paragraaf 5.2) en de best practices uit de (IT-)auditpraktijk (paragraaf 5.1) een bewuste.
De kaders of raamwerken uit de (IT-)auditpraktijk, zoals beschreven in paragraaf 5.1, geven invulling aan verschillende IT onderwerpen zoals (IT) Governance, (informatie)beveiliging, specifiek op Sarbanex Oxley gerichte normen, privacy en de aansturing van diverse IT processen.
Deze raamwerken geven voor auditors een beter toetsbaar kader dan de best practices zoals in paragraaf 5.2 beschreven. Deze best practices gaan vaak dieper op processen en procedures in dan voor (compliancy) audits noodzakelijk is, maar kunnen wel helpen bij het verder

concretiseren van normenkaders. Er is gekozen om de toetsing in hoeverre voldaan wordt aan de eisen van de wet- en regelgeving te baseren op de kaders uit paragraaf 5.1. De wijze waarop deze normenkaders in relatie tot de wet- en regelgeving gebruikt kunnen worden is hieronder verder uitgewerkt.

Regeling organisatie en beheer
De ROB zelf geeft geen concreet normenkader dat bedrijven kunnen hanteren om aan de ROB te voldoen. Op IT gebied is een aantal hoofdnormen gesteld, deze zijn echter weinig specifiek.
Om te voldoen aan de ROB dient een verzekeringsbedrijf een IT-beleidsplan te hebben, een IT-risicoanalyse uitgevoerd te hebben, beleidsuitgangspunten vertaald en geïmplementeerd te hebben naar procedure beschrijvingen en deze na te leven, beveiligings- en continuïteitsmaatregelen te hebben getroffen en indien sprake is van uitbesteding, dienen hierop specifieke beheersmaatregelen zijn ingericht.
Het IT-beleidsplan kan getoetst worden aan normen die COSO en CobiT stellen. Ditzelfde geldt voor de vertaling naar procedures en de controle op de naleving ervan.
Beveiligingsaspecten kunnen getoetst worden tegen normen uit de Code of Practice.
Wat betreft het aspect continuïteit kan gesteund worden op kaders als het BCP. Voor het toetsen van uitbestede diensten kan gesteund worden op het COSO en CobiT kader.

Sarbanes Oxley
De Sarbanes Oxley wetgeving op zich is geen normenkader. Echter diverse organisaties hebben frameworks ontwikkeld die in meer of mindere mate concreet invulling geven aan te treffen maatregelen (controls) voor de IT Cycle. Een goed voorbeeld hiervan is het ITGI (IT Governance Institute) met de 'IT Control Objectives for Sarbanes-Oxley' met de ondertitel 'The role of IT in the Design and Implementation of Internal Control over Financial Reporting 2nd Edition September 2006'. Daarnaast steunen SOx frameworks (ook die van het ITGI) in belangrijke mate op COSO en CobiT.

Tabaksblat
De Nederlandse Corporate Governance Code richt zich in beperkte mate op het onderwerp IT. Er wordt gesteld dat de externe accountant in zijn verslag melding moet maken van aan IT gerelateerde aspecten (betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking). Intern dient de organisatie te beschikken over een risico beheersingssysteem. Tabaksblat zelf geeft hieraan beperkte richting (verwijzing naar kaders zoals COSO).

Voor dit onderzoek gaan wij ervan uit dat voor IT aspecten, de geautomatiseerde gegevensverwerking, gesteund kan worden op kaders als CobiT en/of COSO.

Solvency II
Voor Solvency II is wat betreft de eisen aan IT gekeken naar Basel II. De verwachting is dat Solvency II zal steunen op Basel II. Deze wetgeving stelt dat operationele risico's beheerst moeten worden, maar stelt geen directe eisen aan IT. Daarnaast dient de organisatie verantwoording af te leggen aan de toezichthoudende instanties. Om operationele risico's te beheersen kunnen raamwerken gebruikt worden als COSO en CobiT.

Wet Computer Criminaliteit
De Wet Computer Criminaliteit legt zich toe op beveiligingsaspecten. Een organisatie moet zoveel mogelijk voorkomen dat computer criminaliteit intern plaatsvindt. Daarnaast moet een

organisatie voorkomen dat computer criminaliteit plaatsvindt met behulp van bedrijfsmiddelen. Het gaat hierbij om beveiligingsissues, om de mate van (informatie)beveiliging te toetsen kan gebruik gemaakt worden van de Code of Practice.

Wet bescherming persoonsgegevens
De Wbp geeft een concreet raamwerk dat bedrijven kunnen hanteren voor een zelftoetsing op de verwerking van persoonsgegevens. Het zogenaamde 'Raamwerk Privacy Audit'.

§ 5.3.2 Matrix regelgeving versus raamwerken en best practices

In deze paragraaf is de beschreven wet- en regelgeving afgezet tegen de gekozen raamwerken en best practices.

	Raamwerk/normenkader	COSO	Code of Practice	Control Objectives for SOX (ITG	Raamwerk Privacy Audit	CobiT	BCP normenkader
Regelgeving: direct IT eisen stellend							
Regeling Organisatie & Beheer		√	√			√	√
Code Tabaksblat		√					
Sarbanes Oxley (IT Cycle)		√		√		√	
Solvency II		√	√			√	√
Wet Bescherming Persoonsgegevens					√		
Wet Computer Criminaliteit			√				
Regelgeving indirect IT eisen stellend							
IFRS		√	√			√	√
Wet Financieel Toezicht		√				√	

§ 5.4 Conclusie

Uit de analyse van de wet- en regelgeving blijkt dat er over het algemeen beperkte tot geen (concrete) eisen worden gesteld aan IT afdelingen en IT processen. Er worden voornamelijk eisen gesteld aan de business (processen) van een verzekeraar. Verreweg de meeste wet- en regelgeving stelt dat een organisatie de operationele risico's dient te beheersen. Onder operationele risico's worden ook IT risico's verstaan.

Wij signaleren dat er vanuit de toezichthoudende instanties een verschuiving gaande is van 'tell me' naar 'prove me'. Dit betekent dat er steeds meer gedocumenteerd aangetoond moet worden welke beheersmaatregelen zijn getroffen en of de beheersmaatregelen geïmplementeerd en nageleefd worden. Ook REAAL IT zal gezien haar ondersteunende functie aan de business moeten kunnen aantonen dat zij 'in control' is wat betreft haar IT processen.

Het te ontwikkelen raamwerk dient om de bovengenoemde redenen onderwerpen te bevatten waarmee REAAL IT aan de business kan aantonen welke maatregelen zij heeft getroffen ten aanzien van de General IT Controls. De getroffen maatregelen zullen een bepaalde mate van volwassenheid kennen. Om de volwassenheid van getroffen maatregelen te kunnen vaststellen is de wens van REAAL IT om een volwassenheidsdimensie te koppelen aan het raamwerk.

Wij hebben ervoor gekozen om het raamwerk te baseren op CobiT. CobiT is zoals in dit hoofdstuk beschreven opgesteld om houvast te geven aan het treffen van beheersmaatregelen binnen de volle breedte van een IT-organisatie. Daarnaast kent CobiT relaties naar best practices zoals de Code voor Informatiebeveiliging voor de beveiligingsaspecten, ITIL, Prince2 en dergelijke. Daarnaast zijn er uitwerkingen voor bijvoorbeeld SOx gemaakt die CobiT als normenkader gebruiken.

6. Groeifasenmodellen

In dit hoofdstuk zijn de binnen de IT bekende groei- en volwassenheidsmodellen geïnventariseerd. De modellen die in dit verband relevant zijn, zijn het fasenmodel van Nolan, het IT Service CMM model, het binnen CobiT gehanteerde groeimodel en het INK managementmodel. Dit hoofdstuk beschrijft de achtergronden van deze modellen. Het hoofdstuk eindigt met het gemeenschappelijke kader dat deze modellen in zich hebben en de onderbouwing van het model dat de voorkeur heeft om toe te kunnen passen op het compliancy kader.

§ 6.1 Het fasenmodel van Nolan

Het fasenmodel van Nolan beschrijft de (volwassenheids)fasen die een organisatie doorloopt bij het gebruik van IT. Nolan stelt dat een organisatie voor een IT-toepassing altijd alle fasen doorloopt. Het fasenmodel van Nolan bestaat uit 4 volwassenheidsfasen (zie onderstaande tabel): initiation, contagion (of expansion), control (of formalization) en maturity (of integration). Zie de onderstaande tabel.
Tijdens de groei is het vaak noodzakelijk om de volledige organisatiestructuur, inclusief de informatiesystemen, te herontwerpen.
Hoewel het fasenmodel van Nolan primair is opgezet om te zien hoe de automatisering binnen een organisatie geregeld is, is zij ook toepasbaar bij de controle of een organisatie SLA's kan afsluiten op haar automatiseringsdienstverlening. Een organisatie zal zich minimaal in de 'Control'-fase moeten bevinden om ook daadwerkelijk SLA's aan te kunnen bieden.

Stage ***Gebied***	**Initiation**	**Contagion**	**Control**	**Maturity**
Management style	Los; individugeoriënteerd	Aanmoedigend	Controlerend	Strategische planning
Planning	Technologie gericht	Gestuurd door de technologie	Stuurgroepen en budgetten	Lange termijn planning
Organisatie	Weinig gebruikers.	Bevorderen IT managerfunctie; pogingen tot project management	Gecentraliseerd IT; training voor IT management	Enige decentralisatie; IT wordt taak van hoger management
Controle	Geen controle	Onvoldoende controle; informele projecttoekenningen en project management	Besparingsgericht; meer controle	Voordeelgericht; verbeterde controle

Tabel Veldtyperingen binnen Nolan's Stage Model

§ 6.2 Capability Maturity Model

Het Software Capability Maturity Model (SW-CMM) is ontwikkeld door het Carnegie Mellon Software Engineering Institute (SEI). Met het model is het mogelijk om de volwassenheid van organisaties op het gebied van software ontwikkeling te meten. In het model wordt slechts beschreven welke processen beheerst moeten worden voor een bepaald volwassenheidsniveau, de implementatie van de processen is niet beschreven. Het IT-CMM kent vijf volwassenheidsniveaus. De volwassenheidsniveaus houden in:

Niveau 1: Initial (Beginniveau)
Iedere organisatie begint op niveau 1. Dit niveau kent geen processen. De processen die plaats vinden zijn op ad hoc basis. Kennis van voorgaande processen wordt zelden toegepast.

Niveau 2: Repeatable (Herhaalbaar niveau)
De organisatie is in staat om succesvol geleverde diensten te herhalen. Om dit mogelijk te maken zijn de elementaire Service Management processen ingericht om inzicht en invloed te krijgen op de kosten, voortgang en kwaliteit van de ICT-dienstverlening.

Niveau 3: Defined (Gedefinieerd niveau)
De ICT-serviceprocessen zijn gestandaardiseerd en gedocumenteerd. De leverancier maakt gebruik van specifiek op de klant gerichte processen, die zijn afgeleid van de gestandaardiseerde processen.

Niveau 4: Managed (Gestuurd niveau)
De organisatie verricht gedetailleerde kwaliteitsmetingen. Zowel de serviceprocessen als de leveringsprocessen worden kwantitatief begrepen en beheerst.

Niveau 5: Optimizing (Geoptimaliseerd niveau)
De organisatie is in staat de processen continu te verbeteren door kwantitatieve terugkoppeling uit de processen.

§ 6.3 CobiT en volwassenheid

Binnen CobiT zijn er mogelijkheden om een assessment uit te voeren en vast te stellen wat het competentieniveau van een IT organisatie is (gerelateerd aan de key controls uit CobiT). CobiT maakt hierbij gebruik van de CMM methodologie, zoals beschreven in de vorige paragraaf. De beoordeling die wordt toegepast is gebaseerd op CMM en levert een indeling op in:

0) *Niet bestaand:* Management processen worden niet toegepast;
1) *Initieel:* Processen zijn ad hoc en niet georganiseerd;
2) *Repetitief:* Processen volgen een regulier patroon;
3) *Gedefinieerd:* Processen zijn gedocumenteerd en gecommuniceerd;
4) *Beheerst:* Processen worden gevolgd en gemeten;
5) *Geoptimaliseerd*: Best practices worden gebruikt en geautomatiseerd.

Door een assessment uit te voeren op de 34 IT processen uit het CobiT framework en een CMM evaluatie voor elk proces toe te passen, wordt een beeld verkregen van de gebieden die te verbeteren zijn.

§ 6.4 Het INK managementmodel

Het INK-managementmodel is ontwikkeld door het Instituut Nederlandse Kwaliteit (INK). Het INK-managementmodel bestaat uit een tweetal delen: ‘organisatie’ en ‘resultaat’. De ‘organisatie’ omvat interne, beheersbare factoren als leiderschap, strategie en beleid, medewerkers, middelen en processen. Het deel ‘resultaat’ omvat de waardingsfactoren: waardering door medewerkers, waardering door klanten en leveranciers, waardering door de maatschappij en de overkoepelende eindresultaten.

Het INK onderscheidt een vijftal fasen gedurende deze weg:

Fase 1: Activiteit georiënteerd
Alle werknemers proberen hun activiteiten zo goed mogelijk uit te voeren. De activiteiten staan echter los van elkaar en de invloed van de activiteiten op elkaar worden niet meegenomen in de uitvoering. Indien er klachten zijn zal de organisatie proberen deze te verhelpen.

Als er al sprake is van automatisering is dit slechts fragmentarisch en zijn de gegevens moeilijk uitwisselbaar.

Fase 2: Proces georiënteerd
De beheersing van de primaire processen staat centraal. De afzonderlijke processtappen zijn geïdentificeerd en daarmee liggen de taken en verantwoordelijkheden vast. Prestatie-indicatoren fungeren als stuurmiddel en op basis van de metingen worden processen verbeterd.
Informatie wordt door verschillende organisatieonderdelen gebruikt en loopt dwars door de organisatie heen. Er wordt begonnen met het opzetten van een uniform gegevensbeheer en er komt aandacht voor standaardisatie en optimalisatie om tot een optimale interactie van systemen te komen.

Fase 3: Systeem georiënteerd
Een verhoogde mate van klantgerichtheid zorgt ervoor dat op alle niveaus systematisch gewerkt wordt aan de verbetering van de organisatie als geheel. Door meten in de primaire processen probeert men trends te herkennen en preventief te handelen.
Doordat de organisatie steeds afhankelijker wordt van de informatievoorziening neemt de noodzaak tot standaardisering toe en wordt het belang van onderhoud, beheer en beveiliging steeds groter.

Fase 4: Keten georiënteerd
Er worden afspraken gemaakt met leveranciers en klanten die bepalend zijn voor de bedrijfsprocessen van de organisatie. Kennis en capaciteit worden maximaal benut, niet alleen van de organisatie zelf, maar ook van de leveranciers.
Technologische ontwikkelingen en communicatietechnieken maken het mogelijk om elkaar op de hoogte te houden van de stand van zaken binnen de bedrijfsketen, zonder belemmering van tijd of afstand. Ketens worden vaak 'in elkaar gedrukt', doordat schakels verkort kunnen worden in tijd, of soms zelfs geheel kunnen worden overgeslagen. Niet de technologische mogelijkheden zijn bepalend in deze fase, maar de culturele en organisatorische aspecten. Er moet gedacht worden in termen als 'partners' en 'co-makership', waarbij het gemeenschappelijk belang van de keten voorop staat.

Fase 5: Excelleren en transformeren
De organisatie ontwikkelt een maatschappelijk verantwoordelijkheidsgevoel. De zorg voor kwaliteit is alom vertegenwoordigd binnen de organisatie en signalen uit de omgeving zorgen voor een continu proces van verbetering.

Een organisatie doorloopt in haar bestaan verschillende ontwikkelingsfasen of volwassenheidsfasen. Naarmate een organisatie een hoger volwassenheidsniveau bereikt zal zij beter in staat zijn SLA’s op te stellen en na te leven.

§ 6.5 Gebruik van de modellen

Er zijn verschillende modellen toegelicht (het fasenmodel Nolan, Capability Maturity Model, CobiT en CMM, en het INK-model), die allemaal hetzelfde pad volgen: van een losse organisatie, zonder standaardisatie die werkt op basis van ad-hoc processen naar een sterk gestructureerde organisatie met gestandaardiseerde procedures en processen.
Bijsturing en verbetering zorgen voor effectiviteit op langere termijn en niet alleen op enig moment. Om gestructureerd bijsturing te kunnen beoordelen, is het toepassen van een groeifasemodel een handig hulpmiddel. Bij het kunnen vaststellen in welke mate een

organisatie voldoet aan de van toepassing zijnde wet- en regelgeving (compliancy) zien wij ook toegevoegde waarde voor het hanteren van een groeifasemodel. Alle modellen beschrijven in meer of mindere mate eenzelfde mate van fasering. Voor het bepalen van de mate waarin een organisatie compliant is stellen wij daarom een volwassenheidsmodel voor die bestaat uit 5 fasen:

1. Initieel;
2. Repetitief;
3. Gedefinieerd;
4. Beheerst;
5. Geoptimaliseerd.

Deze fasering sluit goed aan op het in CobiT gehanteerde CMM en is als zodanig ook herkenbaar voor IT-organisaties. De keuze voor het toe te passen volwassenheidsmodel om deze toe te kunnen passen op het compliancy kader versterkt de keuze voor CobiT. Wij zullen daarom het compliancy kader baseren op CobiT.

7. Referentiekader

In dit hoofdstuk vindt de synthese van de voorgaande hoofdstukken plaats. In hoofdstuk 3 is aangegeven dat het vanuit de wet- en regelgeving gaat om het beheersen van operationele risico's. Op basis van dat hoofdstuk is aangegeven dat de wet- en regelgeving voor het grootste deel eisen stelt aan de primaire processen van een verzekeraar en dat er slechts beperkt eisen gesteld worden aan de processen van de ondersteunende IT-organisatie.
Het risicoprofiel van REAAL IT is in hoofdstuk 4 geschetst en geeft inzicht welke risicogebieden onderkend zijn. Vanuit de best practices die aanwezig zijn is vervolgens in hoofdstuk 5 de keuze voor CobiT als uitgangspunt voor het inrichten van beheersmaatregelen binnen een IT-organisatie onderbouwd. Deze keuze voor CobiT geeft tevens een invulling om de volwassenheid vast te stellen zoals in hoofdstuk 6 is beschreven. In dit hoofdstuk wordt verder ingegaan welke onderdelen van het CobiT framework ingezet kunnen worden om de compliancy ten aanzien van de wet- en regelgeving voor een IT-organisatie vast te stellen. Dit leidt tot een basis normenkader waarop een werkprogramma kan worden gedefinieerd dat als leidraad dient voor het uitvoeren van een dergelijke compliancy toets.

Dit hoofdstuk behandelt achtereenvolgens: een nadere toelichting op CobiT als generiek kader, operationele risico's binnen een IT-organisatie vanuit CobiT en het uit CobiT afgeleide normenkader dat als basis voor de compliancy toets gaat dienen.

§ 7.1 CobiT als generiek kader

CobiT is zoals aangegeven in hoofdstuk 5 een open industriestandaard die beheersdoelstellingen levert voor beheer, controle en beveiliging van informatietechnologie, georganiseerd rond een logisch raamwerk van 34 IT-processen. CobiT heeft deze processen verdeeld over vier IT domeinen: plannen en organiseren, verwerven en implementeren, leveren en ondersteunen en monitoren en evalueren. Per IT-proces bevat CobiT één high level control objective en drie tot vijftien gedetailleerde control objectives. Deze control objectives bevatten uitspraken in verband met de gewenste resultaten of doelstellingen die moeten worden bereikt door het implementeren van specifieke beheersmaatregelen binnen de IT-organisatie en verschaffen een duidelijk beleid voor IT controle.
CobiT heeft 'management guidelines' opgesteld om deze IT-processen te kunnen controleren en meten. Deze 'guidelines' bevatten volwassenheidsmodellen, kritieke succesfactoren, Key Goal indicatoren en Key performance indicatoren voor elk proces.
Het instrument volwassenheidsmodel binnen CobiT biedt een manier om de huidige en gewenste positie te bepalen, en maakt het de IT-organisatie mogelijk om zichzelf te vergelijken met de 'best practices' en standaard richtlijnen.
Verder bevat CobiT Audit Guidelines. Deze audit guidelines bieden een eenvoudige structuur aan om de in CobiT aangereikte controls te kunnen auditen. Het biedt de auditor een uitgangssituatie om een audit te kunnen uitvoeren. Deze uitgangssituatie bevat de in opzet te nemen beheersmaatregelen per proces. Deze zijn niet uitputtend van opzet maar zullen te allen tijde voor de te beoordelen situatie concreet gemaakt moeten worden. Verder zijn er diverse aansluitingen vanuit CobiT op andere best practices gemaakt zoals Prince2, ITIL, Code of Practice, SOx etc. Dit maakt het raamwerk een prima vertrekpunt om ook gebruik te kunnen maken van best practices die aanvullende beheersmaatregelen in zich hebben.

Daarnaast kunnen met deze mappings specifieke audits binnen processen worden uitgevoerd. Om een voorbeeld te geven:
In de eerste instantie wordt bij REAAL IT door Concern Audit een audit uitgevoerd naar de mate van compliancy ten aanzien van het proces wijzigingsbeheer (het CobiT equivalent Manage Changes binnen het procesdomein Acuire & Implement). Door de organisatie is

echter aangegeven dat een audit gewenst is met meer diepgang. De organisatie heeft het wijzigingsbeheer ingericht conform ITIL. Voor deze audit kan Concern Audit gebruik maken van de high level control objective en de detailed control objectives van CobiT. Aan de hand van de door ISACA beschreven 'Mapping of ITIL with CobiT 4.0' kan een gedetailleerd normenkader worden ontwikkeld. Hierbij zullen de normen vanuit ITIL worden afgeleid en worden gekoppeld aan de detailed control objectives van CobiT.

§ 7.2 Operationele risico's in relatie tot CobiT

Om aan te kunnen tonen dat een IT-organisatie compliant is aan de wet- en regelgeving die van toepassing is voor een verzekeraar in Nederland is de betekenis hiervan in hoofdstuk 3 beschreven. Aangegeven is dat de wet- en regelgeving nagenoeg geen specifieke eisen stelt aan de IT-organisatie en haar processen, maar dat de regelgeving met name eisen aan de business stelt om de operationele risico's in te dammen. Het indammen van operationele risico's dient ook bij de IT-organisatie plaats te vinden door het nemen van adequate beheersmaatregelen. Deze beheersmaatregelen dienen getroffen te worden voor die IT-processen waarin operationele risico's worden gelopen. In hoofdstuk 4 is het risicoprofiel van REAAL IT beschreven. In dat hoofdstuk is aangegeven op welke onderdelen de IT-organisatie operationele risico's loopt. Deze inschatting is gedaan in termen van hoog, middel en laag risico's. De vertaling van de CobiT onderkende processen naar de binnen het procesmodel van REAAL IT onderkende processen is in het onderstaande overzicht weergegeven. Binnen REAAL zal afstemming moeten plaatsvinden over de mapping van de IT processen op de processen die CobiT onderkent. Onderstaand is ons voorstel opgenomen van een mogelijke mapping.

PLANNEN & ORGANISEREN		IT-proces REAAL IT
P01	Definieer IT-strategie	Beleid
P02	Definieer informatiearchitectuur	Architectuur
P03	Technologie richting	Beleid
P04	Definieer IT-processen, organisatie en samenhang	Beleid
P05	Het beheersen van IT-kosten	Financial mgt
P06	Communiceer mgt doelen & richting	Architectuur
P07	Beheers IT-personeel	HRM
P08	Kwaliteitsbeheersing	Interne controle
P09	IT Risico analyse	Interne controle
PO10	Beheers projecten	Projectmanagement
VERWERVEN EN IMPLEMENTEREN		
AI1	Identificeer IT-oplossingen	Systeemontwikkeling
AI2	Verkrijg en onderhoud applicatiesoftware	Systeemontwikkeling
AI3	Verkrijg en onderhoud infrastructuur	Infra change mgt & control
AI4	Ter beschikking stellen van IT-oplossingen	Software change mgt & control
AI5	Inkopen IT-resources	Leveranciers & contractmanagement
AI6	Beheer wijzigingen	Releasemanagement
AI7	Installeren en goedkeuren van wijzigingen	Wijzigingsbeheer
LEVEREN & ONDERSTEUNEN		
DS1	Opstellen en beheersen van servicelevels	Service level mgt
DS2	Beheersen van diensten van derden	Strategic sourcing
DS3	Beheersen van de capaciteit van IT	Capaciteitsbeheer
DS4	Verzekerd zijn van continuïteit	Continuïteitsbeheer
DS5	Verzekerd zijn van informatiebeveiliging	Security management
DS6	Identificeer en wijs IT-kosten toe	Financial mgt

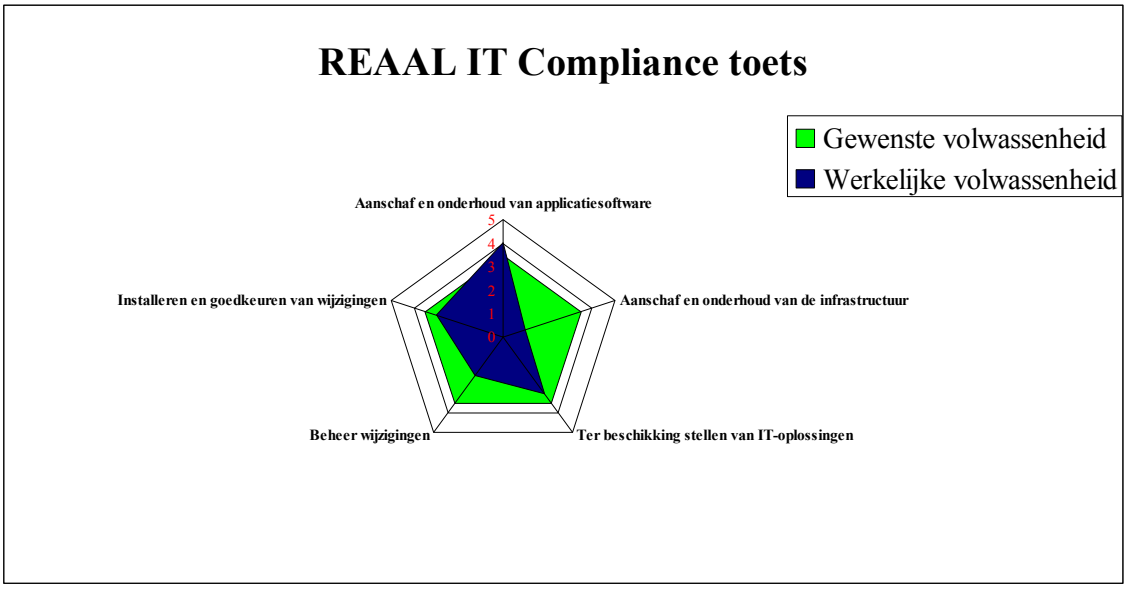
DS7	Opleiden van gebruikers	Systeemontwikkeling
DS8	Beheers incidenten en helpdesk	Incidentbeheer
DS9	Beheers je configuratie	Configuratiebeheer
DS10	Probleembeheer	Probleembeheer
DS11	Gegevensbeheer	Operations
DS12	Beheer rekencentrum	Operations
DS13	Operations management	Operations
MONITOREN & EVALUEREN		
ME1	IT-performance management	Service level management
ME2	Monitor en evalueer de interne controle van IT	Interne controle
ME3	Compliance aan wet&regelgeving	Interne controle
ME4	IT-governance	Interne controle

§ 7.3 CobiT normenkader

Op basis van de selectie van processen waarin operationele risico's worden gelopen, wordt vanuit CobiT een set van best practice beheersmaatregelen aangereikt. Vanuit de audit-guidelines zijn voor alle in CobiT onderkende IT-processen methoden en middelen aangegeven waarmee de getroffen beheersmaatregelen te toetsen zijn. In bijlage 2 is als voorbeeld voor een proces de beheersmaatregelen uitgewerkt.
Voor het toetsen in hoeverre een IT-organisatie compliant is, zijn de in CobiT aangegegeven beheersmaatregelen toereikend. Voor het uitvoeren van specifieke onderzoeken binnen de IT-organisatie kan gebruik worden gemaakt van specifiekere normenkaders zoals beschreven in hoofdstuk 5. De kracht van CobiT is dat deze specifiekere normenkaders hun zogenaamde "mapping" hebben op CobiT. In bijlage 5 zijn de reeds opgestelde mappings toegevoegd.

§ 7.4 Niveau van volwassenheid

Binnen CobiT is een volwassenheidsmodel opgenomen dat gehanteerd kan worden om de volwassenheid van beheersing van de IT-processen vast te stellen. In hoofdstuk 4 is reeds de achtergrond van volwassenheidsmodellen toegelicht. Met behulp van het CobiT volwassenheidsmodel, kan de volwassenheid van de getroffen beheersmaatregelen uitgedrukt worden in volwassenheidsniveau's. Hiermee krijgt het management inzicht in de mate en volwassenheid waarin beheersmaatregelen getroffen zijn. Dit inzicht kan vervolgens op een grafische wijze worden weergegeven door middel van een zogenaamde "spinnenwebdiagram". Een voorbeeld hiervan is hieronder opgenomen.



De compliancy toets zal op hoofdlijnen de volwassenheid van de beheersmaatregelen van de onderkende processen gaan vaststellen. Om compliant te zijn, en dit betekent dat er adequate beheersmaatregelen zijn getroffen om de operationele risico's in te dammen, zullen deze beheersmaatregelen op een dusdanig niveau moeten zijn ingeregeld binnen de processen dat er minimaal sprake is van een herhaalbaar proces. In termen van volwassenheid, is onze mening, zal het niveau, mede ingegeven door Sarbanex Oxley maar ook in toenemende mate de externe toezichthouders die veelal "Prove me" aanhangen, het niveau 3 moeten zijn. Dit betekent dat de processen en getroffen beheersmaatregelen zijn gedocumenteerd, en dat er sprake is van een formeel ingericht proces.
De SOx wetgeving stelt hierbij nog hogere eisen, namelijk dat de organisatie aantoonbaar de werking van de beheersmaatregelen toetst en hierover rapporteert. Vertaald naar het overeenkomstige CobiT niveau kan gesteld worden dat minimaal aan niveau 4 voor de getroffen beheersmaatregelen voldaan moet worden. Een lager volwassenheidsniveau impliceert voor de organisatie een veel grotere inspanning om de werking van de getroffen beheersmaatregelen te kunnen aantonen. Zie hiervoor bijlage 4 waarin de inspanningen voor de organisatie per volwassenheidsniveau zijn afgebeeld.
Het binnen CobiT gehanteerde volwassenheidsmodel geeft richting aan de volwassenheidsdefinitie die binnen organisaties zelf nog geconcretiseerd moet worden.

Het volwassenheidsmodel binnen CobiT geeft per proces per volwassenheidsniveaueen beschrijving van door de organisatie te treffen beheersmaatregelen. Deze beschrijvingen kunnen echter niet gebruikt worden als een checklist. Het volwassenheidsmodel dat CobiT biedt heeft als doel om bevindingen ten aanzien van beheersmaatregelen te adresseren en verbeteringen te treffen.
De organisatie kan het volwassenheidsmodel gebruiken om:

1. Vast te stellen waar de organisatie zich bevindt;
2. Het gewenste niveau vast te stellen;
3. Zich te vergelijken met andere organisaties binnen de branche.

De zes volwassenheidsniveau's die per proces zijn beschreven onderscheiden zich in algemene termen op de volgende wijze van elkaar:

0. *Niet bestaand:* Management processen worden niet toegepast;
1. *Initieel:* Processen zijn ad hoc en niet georganiseerd;
2. *Repetitief:* Processen volgen een regulier patroon;
3. *Gedefinieerd:* Processen zijn gedocumenteerd en gecommuniceerd;
4. *Beheerst:* Processen worden gevolgd en gemeten;
5. *Geoptimaliseerd*: Best practices worden gebruikt en geautomatiseerd.

De auditor verkrijgt op basis van de beschrijvingen van de volwassenheidsniveau's uit CobiT een beeld van de mate van beheersbaarheid. Dit beeld toetst de auditor aan het beeld wat vanuit de uitgevoerde werkzaamheden bij de compliancy toets is verkregen. De auditor let bij de beschrijvingen van de 6 fasen en de bevindingen ten aanzien van de toets op de volgende attributen:

1. Bewustzijn en communicatie;
2. Beleid, standaarden en procedures;
3. Tools en mate van automatisering;
4. Vakkundigheid en expertise;
5. Verantwoordelijkheid en aansprakelijkheid;
6. Doelstellingen en meten.

Deze attributen (CobiT terminologie) zijn gebruikt om per proces een beeld te scheppen van 6 volwassenheidsniveau's). In bijlage 3 is een overzicht opgenomen van de volwassenheidsattributen en de invulling van de attributen per volwassenheidsniveau (generieke beschrijving).

De bij de audit aangetroffen situatie wordt vergeleken met de volwassenheidsbeschrijving van het betreffende CobiT proces. Rekeninghoudend met de invulling per volwassenheidsattribuut wordt de daadwerkelijke volwassenheid van de organisatie vastgesteld. De auditor dient zijn overweging voor de keuze van een volwassenheidsfase te motiveren om discussies tussen auditee en auditor of tussen auditors te voorkomen en/of te onderbouwen.

De vertaling die voor REAAL IT zal worden gehanteerd is dat de processen minimaal het niveau 3 van volwassenheid moeten hebben. De vertaling die als uitgangspunt zal worden gebruikt is "gedocumenteerde aantoonbaarheid" van de opzet en bestaan van het proces. Een verdere uitwerking wat de gevolgen van SOx voor een IT-organisatie zijn, is in hoofdstuk 8 beschreven.

§ 7.5 Toetsing compliancy

In deze paragraaf wordt toegelicht hoe CobiT als raamwerk te gaan hanteren voor het toetsen van compliancy. In deze toelichting wordt een aanpak geschetst die gehanteerd kan worden om IT-processen te auditen. Naast de generieke opzet van de aanpak is de toelichting tevens specifiek gemaakt voor de auditomgeving van REAAL IT, aangezien als vervolg op deze scriptie de aanpak in de praktijk zal worden toegepast.

Het toetsen in hoeverre een IT-organisatie, in casu REAAL IT, compliant is aan de wet- en regelgeving volgt in hoofdlijnen het volgende stramien:
1) Vaststellen operationele risico's;
2) Vaststellen gerelateerde CobiT processen;
3) Vaststellen te verwachten beheersmaatregelen CobiT; → concretiseren normenkader
4) Vaststellen opzet en bestaan van de te toetsen beheersmaatregelen;
5) Rapporteren compliancy-toets.

Elk onderdeel is hieronder kort toegelicht.

Vaststellen operationele risico's
Indien een organisatie een terugkerend proces heeft van risico analyse, is er vaak al een beeld waar binnen de IT-organisatie operationele risico's zijn. Deze risico analyse kan na afstemming eventueel geactualiseerd worden en kan dan als startpunt gelden van de compliancy-toets. Bij REAAL IT ligt reeds een risico-analyse als uitgangspunt. Voor elk proces ligt er een RSA (risk self assesment).

Vaststellen CobiT processen (mapping)
Indien de operationele risico's niet direct zijn vertaald naar de processen zoals gehanteerd binnen het CobiT raamwerk zal deze vertaling moeten plaatsvinden. Op hoofdlijnen is dit voor de processen van REAAL IT in dit hoofdstuk in paragraaf 7.2 gedaan. Deze stap moet worden uitgevoerd om de scope vanuit CobiT vast te stellen. Deze scoping levert die IT-processen vanuit het CobiT raamwerk op die in beschouwing van de compliancy toets worden genomen. De betreffende IT-processen uit CobiT vormen het uitgangspunt voor het

vaststellen van de beheersdoelstellingen die bij de compliancy toets als uitgangspunt worden gehanteerd.

Vaststellen te verwachten beheersmaatregelen
Na de scoping van de IT-processen uit het CobiT raamwerk wordt vervolgens per IT-proces dat in de toets wordt meegenomen de beheersmaatregelen zoals aangegeven in de Audit guidelines van CobiT vastgesteld. In dit proces wordt een analyse uitgevoerd welke beheersmaatregelen mogen worden verwacht om de operationele risico's te beheersen. In deze slag worden de maatregelen concreet gemaakt naar de eigen organisatie toe. Dit betekent ook dat ze voor het IT-management concreet genoeg moeten zijn en het liefst ook herkenbaar. Deze vastgestelde beheersmaatregelen zijn het uitgangspunt voor de uitvoering van de compliancytoets. Een aantal voorbeelden van deze beheersmaatregelen zijn opgenomen in bijlage 2. Het resultaat van deze stap is een geconcretiseerd normenkader voor het betreffende proces binnen de betreffende IT-organisatie.

Concretiseren normenkader in werkprogramma
Op basis van de door CobiT aangereikte beheersdoelstellingen, worden de risico's aangegeven. Hierbij kan gebruik worden gemaakt van de binnen de organisatie aanwezige risico analyse. Vanuit de risico's worden de verwachte beheersmaatregelen vastgesteld. Hierbij wordt gebruik gemaakt van het volwassenheidsniveau dat als minimale niveau afgestemd is. Vanuit de scriptie is dat het volwassenheidsniveau 3. Zoals aangegeven is dit niveau vertaald naar het criteria "gedocumenteerde aantoonbaarheid". Voor het vaststellen van de beheersmaatregelen betekent dit dat bij het opstellen van de te verwachten beheersmaatregelen dit in de concretisering meegenomen wordt. Voor het toetsen van processen betekent dit bijvoorbeeld dat er een procesbeschrijving aanwezig moet zijn waarin de beheersmaatregelen in opgenomen zijn. Door alle beheersdoelstellingen en de vastgestelde risico's vanuit de richtinggevende volwassenheidsdefinitie van CobiT te concretiseren in de te verwachten beheersmaatregelen wordt het voor de betreffende IT-organisatie specifiek en concreet gemaakt. Het levert een normenkader op wat voor het volwassenheidsniveau 3 voor de IT-processen herbruikbaar is en de organisatie na toetsing het beeld oplevert van de mate van beheersing van de IT-processen.

Vaststellen opzet en bestaan beheersmaatregelen.
Op basis van het normenkader wordt een vaststelling in de IT-organisatie gedaan op de opzet en het bestaan van deze maatregelen. Hierbij wordt als referentie het volwassenheidsniveau 3 uit CobiT aangehouden. Indien een organisatie moet voldoen aan SOx dan zullen voor die processen die in het kader van SOx compliant moeten zijn het volwassenheidsniveau 4 aangehouden worden (en zal de werking ook aangetoond moeten worden). In de vaststelling wordt per proces de niveauduiding bepaald.
Naast het vaststellen in hoeverre de beheersmaatregelen bestaan wordt mede vastgesteld in hoeverre de risico's worden afgedekt. Het model levert hierin uiteindelijk een beeld waarin eventueel de dimensie van opzet, bestaan en werking geduid kunnen worden. Opgemerkt moet worden dat bij het toetsen van de werking vastgesteld wordt in hoeverre de risic's daadwerkelijk worden afgedekt en wat het restrisico is wat de organisatie loopt.

Rapportage
Op basis van de niveauvaststelling per proces, wordt er vervolgens per proces een zogenaamd spider-diagram opgesteld die per onderliggende controls het niveau weergeeft. Alle onderliggende controls die lager dan niveau 3 scoren geven een "non-compliancy" aan met betrekking tot de wet- en regelgeving.

Samenvatting

Het hanteren van het CobiT raamwerk voor het toetsen van de compliancy vergt het vertalen van de richtinggevende definities uit het volwassenheidsmodel en samenhang met de door CobiT aangereikte beheerdoelstellingen in een voor de organisatie specifiek gemaakt normenkader dat voor de toetsing gehanteerd kan worden. Dit normenkader geeft de IT-organisatie dan een goede houvast welke norm met betrekking tot beheersing dan wordt gebruikt. Van belang is dit normenkader af te stemmen met de IT-organisatie. Afhankelijk van de breedte cq diepgang van de audit kan gerapporteerd worden over opzet, bestaan en werking. Indien werking onderdeel is van de audit kan tevens een oordeel worden gegeven over de daadwerkelijke beheersing van het proces.

De kracht van het CobiT raamwerk zit in het aandragen van beheersdoelstellingen voor alle onderkende IT-processen en de richtinggevende definities van volwassenheid per proces. De combinatie van beide vertaald zich naar handzame diagrammen waarin de beheersing van een IT-organisatie geduid kan worden. Het voordeel van deze diagrammen is dat ze een goed communicatiemiddel zijn voor de audittee. Op diverse niveau's kan gebruik worden gemaakt van dit instrument. Het kan bijvoorbeeld gebruikt worden om de beheersing op IT-processenmodel van REAAL IT te duiden aan de directie van de IT-organisatie. Op individueel procesniveau kan gerapporteerd worden over de beheersdoelstellingen van het proces. Het concreet maken van de richting die CobiT geeft naar de eigen organisatie is hierbij wel een vereiste om het management van de IT-organisatie een concreet beeld te geven wat de mate van beheersing is waaraan getoetst wordt.

8. Impact Sarbanes Oxley voor REAAL IT

Door REAAL IT is expliciet aangegeven om bij de regelgeving ook de Sarbanes Oxley Act (SOx) te beschouwen. SNS REAAL voert processen uit van het Bouwfonds hypotheken. ABN AMRO is eigenaar van Bouwfonds Hypotheken en staat genoteerd aan de Amerikaanse beurs. Vanuit deze relatie is SNS REAAL verplicht te voldoen aan SOx voor dit proces.
In dit hoofdstuk wordt in het kort een SOx implementatie traject geschetst, daarbij is niet getracht volledig te zijn. Het geeft een idee wat een organisatie te wachten staat bij een SOx traject.

Voor SOx compliancy toetsing wordt het COSO model gebruikt met de daarin beschreven control objectives.

§ 8.1 Scope

SOx focust zich op de financiële processen en de verslaglegging hieromtrent. Voor de IT organisatie betekent dit voor SOx een focus op de IT processen die van toepassing zijn op de financiële systemen. Financiële systemen zullen echter gevoed worden door logistieke processen en bijbehorende systemen. De IT organisatie dient daarom met de business af te stemmen welke applicaties, systemen en welk deel van de infrastructuur in scope vallen. Maar zoals in hoofdstuk 4 ten aanzien van de IT-architectuur is aangegeven, zijn de IT-processen grotendeels ingericht voor alle systemen om de business processen integraal te ondersteunen.

De volgende stap is het vaststellen van de getroffen IT general controls en de application controls van de systemen in scope. Met name op het gebied van het vaststellen van de application controls is afstemming met de business vereist. Het is van belang om te bepalen wie verantwoordelijk is voor de application controls, dit voorkomt het maken van dubbele beschrijvingen en het dubbel testen van controls.
Delen van de IT kunnen zijn uitbesteed, dit ontslaat het management echter niet van de verantwoordelijkheid over de uitbestede dienst. Hieraan geeft ook de Nederlandse wet- en regelgeving invulling. De IT organisatie dient vast te stellen in welke mate IT systemen/processen zijn uitbesteed. Bij uitbestede diensten wordt veelal een SAS70 verklaring gevraagd aan de leverancier.

Een SAS70 verklaring wordt tegenwoordig veel gevraagd door organisaties met een SOx verplichting (klantorganisatie) die diensten hebben uitbesteedt aan een andere organisatie. (leverancier) SAS70 is een rapportagestandaard en is opgesteld door het AICPA (American Institute of Certified Public Accountants). Bij een certificering via SAS70 door een onafhankelijke auditor wordt onderscheid gemaakt tussen een type-1- en een type-2-verklaring. Bij een type-1-verklaring hoeft de leverancier alleen te beschrijven en te documenteren hoe de beheersdoelen worden gerealiseerd. Bij type 2 moet de leverancier aantonen dat gedurende een periode van minimaal zes maanden de beheersmaatregelen effectief hebben gefunctioneerd.

Een klantorganisatie met een SOx verplichting zal om een type 2 verklaring vragen bij de leverancier.

§ 8.2 Risico analyse

Nadat IT general controls en de application controls zijn vastgesteld wordt een risico analyse uitgevoerd. Bij het onderdeel risico analyse dienen de inherente risico's van de applicaties en onderliggende systemen (zoals onderkend in de scope) te worden vastgesteld. Op basis van de risico analyse kan de scope worden bijgesteld. Deze risico analyse is anders dan de reeds

binnen REAAL uitgevoerde risico analyse (zie paragraaf 4.3) aangezien die risico analyse bedoeld is om de operationele risico's van de IT processen vast te stellen.

§ 8.3 Documenteren controls

De volgende stap is het documenteren van de controls. Daarbij dient onderscheid te worden aangebracht in de volgende controls die SOx onderkent:

- Entity level controls (Control Environment)
- Application controls (geprogrammeerde controles in systemen)
- General IT controls

Voor het documenteren van controls gelden specifieke eisen. Op basis van de gedocumenteerde controls wordt vastgesteld welke controls relevant zijn voor het mitigeren van de geïdentificeerde risico's.

§ 8.4 Evalueren ontwerp van de controls en het testen van de effectiviteit

De IT organisatie dient op basis van de voorgaande stappen te evalueren of de beschreven controls de risico's effectief afdekken en of deze controls betrouwbaar zijn. In IT Control Objectives for Sarbanes Oxley 2nd edition is een volwassenheidsmodel opgenomen wat goed aansluit op het volwassenheidsmodel van CobiT waarbij per volwassenheidsstadium is aangegeven wat de impact van een volwassenheidsfase is bij een SOx implementatie.

Om de betrouwbaarheid van de controls te toetsen dient de frequentie van een control bekend te zijn. Op basis van het type control (handmatig of geprogrammeerd) en de frequentie van optreden (hiervoor is een model beschikbaar) dient de organisatie de controls te toetsen. Deze toetsing wordt verricht door de voor de control verantwoordelijke persoon en een tweede onafhankelijke persoon (bijvoorbeeld een IAD). Het tijdstip van de toetsing hangt sterk af van de frequentie en tijdstip van optreden.
De resultanten van de tests dienen te worden vastgelegd en per test dient bewijs te worden verzameld (prove me concept).

§ 8.5 Prioriteren en herstellen van tekortkomingen

De organisatie dient de impact van tekortkomingen inzake General IT controls te beoordelen. Daarbij dient de organisatie sterk te letten op de samenhang van tekortkomingen en het totale effect ervan. De volgende stap is het prioriteren en herstellen van de tekortkomingen.

§ 8.6 Evalueren van de effectiviteit van het control programma

Het IT management beoordeelt waar verbeteringen kunnen worden doorgevoerd om het SOx compliancy project effectiever in te steken en waar verbeteringen te treffen zijn. Hierbij worden de controls geëvalueerd (nog steeds van toepassing, relevantie, etc.). Daarnaast wordt in veel situaties gekeken in hoeverre handmatige controls vervangen kunnen worden door geautomatiseerd (verminderde druk op het testen).

Een SOx verklaring (404 verklaring) wordt over een bepaald boekjaar gegeven door een onafhankelijke partij die gemachtigd is om een dergelijke verklaring af te geven (accountantsorganisaties). Een dergelijke organisatie is nauw betrokken bij SOx trajecten. Een accountant geeft een oordeel over het control framework en de intern uitgevoerde tests. Daarnaast stelt een accountantskantoor zelf ook de controls vast door middel van een eigen onafhankelijke test.
Het uitvoeren van dergelijke tests vinden veelal aan het einde van het boekjaar plaats.

Een SOx implementatie vraagt veel van een organisatie, zowel financiële investeringen als benodigde tijd van functionarissen. Er zijn twee fasen te onderkennen. Een initiële fase waarin de documentatie op het niveau van de SOx eisen wordt gebracht en een onderhoudsfase waarbij een continue toets op de werking plaats vindt zoals hierboven beschreven.

Een goede leidraad voor een SOx implementatie specifiek voor IT organisaties vormt IT Control Objectives for Sarbanes Oxley 2nd edition dat is opgesteld door het IT Governance institute.

Bijlage 1) Geraadpleegde literatuur

Gebruikte documenten:

- Artikel: De impact van Basel II op IT, de Informatie van december 2004
- Artikel: Hefboom voor architectuur, BankingReview 2003
- Artikel: ITIL en CobiT en hun toepassing op SOx, Informatie december 2006
- International Convergence of Capital Measurement and Capital Standards – A Revised Framework – juni 2004, Bank for International Settlements (Basel Committee on Banking Supervision)
- International Convergence of Capital Measurement and Capital Standards – A Revised Framework Comprehensive version– Juni 2006, Bank for International Settlements (Basel Committee on Banking Supervision)
- Databanken wet van 8 juli 1999, geconsolideerde versie, geldig 01-09-2004, Staatsblad van het Koninkrijk der Nederlanden 08-07-1999
- Brochure Elektronische handtekening, november 2006, ECP.nl
- Certificatie dienstverleners, ECP.nl
- Juridische status van de elektronische handtekening, ECP.nl
- Wet Elektronische Handtekening, wet van 8 mei 2003, Staatsblad van het Koninkrijk der Nederlanden jaargang 2003
- Regeling Organisatie en Beheersing, Handboek WTK januari 2004, DNB
- Regeling Organisatie en Beheersing, Staatscourant 2 april 2001 nr. 65
- Considerations concerning the Outline for a Framework Directive on Solvency II, Agenda Paper for the meeting of the Insurance Committee on 8 April 2005, 23 maart 2005, Europese Commissie (Markt/2507/05)
    - Annex to document markt/2507/05 - Draft Outline of a Solvency II Framework Directive
- Policy issues for Solvency II - Possible amendments to the Framework for Consultation, maart 2005, Europese Commissie (Markt/2505/05)
    - Annex tot document Markt/2505) - Draft Amended Framework for consultation on Solvency II
- IT Control Objectives for Sarbanes Oxley, September 2006, IT Governance Institute
- Sarbanes Oxley Act of 2002, One Hundred Seventh Congress of the United States of America (second session), 23 januari 2002
- SARBANES-OXLEY SECTION 404: A Guide for Management by Internal Controls Practitioners, The Institute of Internal Auditors
- De Nederlandse corporate governance code, Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen, 9 december 2003, Commissie Corporate Governance
- Rol DNB Toezicht bij outsourcing door financiële instellingen, 12 oktober 2006, DNB
- Regeling uitbesteding verzekeraars, Staatscourant 30 januari 2004, nr. 20, Pensioen- & Verzekeringskamer
- Beleidsregel uitbesteding, januari 2002, Handboek Wtb, DNB
- Handleiding voor verwerkers van persoonsgegevens, april 2002, Ministerie van Justitie
- Handreiking bij het Raamwerk Privacy Audit, 24 mei 2005, CBP
- Quickscan Wet Bescherming Persoonsgegevens, CBP
    - Toelichting Quickscan

- Raamwerk Privacy Audit, 19 december 2000, Samenwerkingsverband Audit Aanpak / Werkgroep Privacy Audit
- Wet bescherming persoonsgegevens - versie geldig vanaf: 01-02-2006, Staatsblad 06-07-2000
- Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens – memorie van toelichting, Tweede Kamer, vergaderjaar 1997– 1998, 25 892, nr. 3
- Wet bescherming persoonsgegevens Zelfevaluatie, CBP
- Beveiliging van Persoonsgegevens - Achtergrondstudies en Verkenningen 23, april 2001, Registratiekamer
- Wijzigingen van het wetsvoorstel Computercriminaliteit II in het Wetboek van Strafrecht
- Wijzigingen van het wetsvoorstel Computercriminaliteit II in het Wetboek van Strafvordering, eJure
- Handleiding Cybercrime II Nederlandse versie, augustus 2006, Govcert.nl/KLPD
- IT-REcht in vogelvlucht - Quick reference voor IT-auditors, juni 2005, NOREA
- Wet van 12 mei 2005, houdende regels voor de financiële dienstverlening (Wet financiële dienstverlening)
- Regels voor de financiële dienstverlening (Wet financiële dienstverlening) Memorie van toelichting, Tweede Kamer, vergaderjaar 2003–2004, 29 507, nr. 3
    - Memorie van toelichting artikelsgewijs
- WFD hoofdzaken voor SNS Reaal, SNS Reaal
- Wet van 28 september 2006, houdende regels met betrekking tot de financiële markten en het toezicht daarop (Wet op het financieel toezicht), Staatsblad 2006
- Wet op het financieel toezicht- Belangrijkste wijzigingen gedragstoezicht bij invoering Wft, AFM
- Regels met betrekking tot de financiële markten en het toezicht daarop (Wet op het financieel toezicht) gewijzigd voorstel van wet, 27 juni 2006, Eerste Kamer der Staten-Generaal
- Wet van 10 juli 1995, houdende bepalingen ten aanzien van het natura-uitvaartverzekeringsbedrijf.
- Wijziging van de Wet toezicht verzekeringsbedrijf 1993 in verband met het actualiseren van de solvabiliteitseisen voor het verzekeringsbedrijf, Tweede Kamer, vergaderjaar 2002–2003, 28 838, nr. 5
- Wet van 9 maart 1994, houdende vervanging van de Wet toezicht verzekeringsbedrijf door de Wet toezicht verzekeringsbedrijf 1993
- Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit A Management Briefing from ITGI and OGC, 2005
- CobiT Mapping Overview of International IT Guidance, 2nd Edition, 2006, IT Governance Institute
- Presentatie: Compliance data retention, 9-11-2005, Verdonck, Klooster & Associates
- Artikel: Transparante processen met IT Governance, Sogeti Nederland B.V.
- Artikel: Wat is "In Control"?, Yacht
- IT-Governance Een verkenning, NOREA
- CobiT 4.0, 2005, IT Governance Institute
- Presentatie: Toetsingskader Business Continuity Planning en noodscenario’s van de financiële sector, 2006, DNB
- Toetsingskader business continuity planning betalings- en effectenverkeer, 29 november 2004, DNB

- CobiT(r) 3rd Edition Audit Guidelines, juli 2000, IT Governance Institute
- Presentatie: COBIT Perspectief van de beoordeling, 29 juni 2005, KMPG IRM
- Risicoanalyse ITF, oktober 2005, Concern Audit SNS REAAL
- Handboek FIRM, 2005, DNB
- Artikel : Solvency II en Bazel II overeenkomsten en verschillen, MAB januari/februari 2007
- FIRM: financiële instellingen risicoanalysemethode van DNB (2005)
- IT procesmodel REAAL IT
- Rapport : Inventarisatie ICT ROB compliancy REAAL IT en P&B (KPMG)
- Document IIA-CPP-COBIT inzake toepassing CobiT in de praktijk

Geraadpleegde websites:

- www.dnb.nl
- www.afm.nl
- nl.wikipedia.org
- www.cbpweb.nl
- www.justitie.nl
- www.itgi.org
- www.reaal.nl
- www.sns.nl
- www.snsreaal.nl
- www.bdo.nl
- www.isaca.org

Bijlage 2) Voorbeelduitwerking proces CobiT

CobiT	Keycontrols	Audit guideline (gebaseerd op CobiT 3.0)	Mapping CobiT op andere standaarden
Norm:P09 Domein: Plan&Organise Proces RA: Kwaliteitsmgt / Interne controle CobiT: Uitvoeren en beheersen risico analyse	Risico beheersing is volledig ingebed in de managementprocess en en wordt consistent toegepast	Assessing the compliance by: > Testing that: Er vinden regelmatig updates op risico analyses plaats om risico's tot een acceptabel niveau te brengen. Documentatie van risico analyses is voldoende beschikbaar en wordt onderhouden Het IT management en het IT personeel is betrokken bij het risico analyse proces Het management begrijpt risico gerelateerde factoren en de waarschijnlijkheid van bedreigingen Het (relevante) IT personeel begrijpt en accepteert het rest risico Rapportages inzake risico analyses worden ter review en accordering aangeboden aan het senior management. De geïdentificeerde risico's worden gemonitord en er worden tijdig risico mitigerende maatregelen getroffen. Risico's en bedreigingen geïdentificeerd door het management en risico gerelateerde attributen worden gebruikt om het voorkomen van een specifieke bedreiging te signaleren. Risico- actieplannen zijn actueel en bevatten kosten effectieve controls en beveiligingsmaatregelen om het voorkomen van risico's te mitigeren. Prioriteiten van de hoogste tot de laagste risico's bestaan voor elk risico en er zijn risico mitigerende maatregelen getroffen: - Preventieve maatregelen - Detectieve maatregelen - Correctieve maatregelen Risico's versus maatregelen zijn gedocumenteerd, actueel en gecommuniceerd naar de juiste functionarissen. Er is voldoende dekking (verzekering) voor de geaccepteerde rest risico's. Daarbij zijn bedreigingen van de volgende typen in overweging genomen: - Brand, wateroverlast, aardbevingen, stormen, terrorisme en andere mogelijke natuurrampen - Doorbreking van functiescheiding - Bedrijfsonderbreking, verliezen in omzet, verlies van klanten, etc. - Andere risico's die niet afgedekt zijn door IT- en business risico/continuïteits plannen.	CoP, Prince2

Volwassen-heidsfase 0	Volwassen-heidsfase 1	Volwassen-heidsfase 2	Volwassen-heidsfase 3	Volwassen-heidsfase 4	Volwassen-heidsfase 5
Risico analyses voor processen en business besluiten worden niet uitgevoerd. Risico beheersing wordt gezien als niet relevant voor IT.	IT risico's worden ad hoc overwogen. Risico mitigerende maatregelen worden inconsistent genomen. De organisatie is zich ervan bewust dat IT risico's belangrijk zijn en moeten worden beheerst.	Er is een risico analyses bestaan op hoog niveau en spelen een rol bij grote projecten of bij gesignaleerde problemen. Risico mitigerende processen verkeren in de opstartfase bij de geïdentificeerde risico's	Een organisatiebreed risico beheersingsbeleid bestaat en is gedocumenteerd. Besluiten volgen het risico beheersingsproces. De risico analyse methode verzekert dat belangrijke risico's worden gesignaleerd. Een risico mitigerend proces wordt gestart na het signaleren van een risico.	Het analyseren van risico's en de beheersing ervan zijn standaard procedures. Uitzonderingen op dit het risico beheersingsproces worden gerapporteerd aan het IT management. Er zijn tolerantieniveaus voor risico's gedefinieerd. Het IT management overweegt risico mitigerende strategieën. Delen van het risico beheersingsproces zijn geautomatiseerd.	Risicobeheersing is een organisatiebreed proces en is goed beheerst. Het risico analyse proces is in hoge mate geautomatiseerd. Risico beheersing is geaccepteerd en ingebed in alle business en IT processen. Het management beoordeeld voortdurend risico mitigerende strategieën.

Bijlage 3) CobiT volwassenheidsattributen

	Awareness and Communication	Policies, Standards and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
1	Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are *ad hoc* approaches to process and practices. The process and policies are undefined.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of accountability and responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2	There is awareness of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and informal understanding of policy and procedures may exist.	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility, and is usually held accountable, even if this is not formally agreed. There is confusion about responsibility when problems occur and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.
3	There is understanding of the need to act. Management is more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Skill requirements are defined and documented for all areas. A formal training plan has been developed, but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and process owners have been identified. The process owner is unlikely to have the full authority to exercise the responsibilities.	Some effectiveness goals and measures are set, but are not communicated, and there is a clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application of root cause analysis.
4	There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are in use.	Process is sound and complete; internal best practices are applied. All aspects of the process are documented and repeatable. Policies have been approved and signed off on by management. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is ensured for all critical areas and certification is encouraged. Mature training techniques are applied according to the training plan and knowledge sharing is encouraged. All internal domain experts are involved and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardised. Continuous improvement is emerging.
5	There is advanced, forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied and integrated communication tools are in use.	External best practices and standards are applied. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end management and improvement.	Standardised toolsets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and education support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.

Bijlage 4) SOx volwassenheidsniveaus

Figure 6—Control Quality

	Stage 0—Nonexistent	Stage 1—Initial/*Ad Hoc*	Stage 2—Repeatable but Intuitive	Stage 3—Defined Process	Stage 4—Managed and Measurable	Stage 5—Optimized
Characteristics	At this level, there is a complete lack of any recognizable control process or the existence of any related procedures. The organization has not even acknowledged that there is an issue to be addressed; therefore, no communication about the issue is generated.	There is some evidence that the organization recognizes that controls and related procedures are important and need to be addressed. However, controls and related policies and procedures are not in place and documented. An event and disclosure process does not exist. Employees are not aware of their responsibility for control activities. The operating effectiveness of control activities is not evaluated on a regular basis. Control deficiencies are not identified.	Controls and related policies and procedures are in place but not always fully documented. An event and disclosure process is in place but not documented. Employees may not be aware of their responsibility for control activities. The operating effectiveness of control activities is not adequately evaluated on a regular basis and the process is not documented. Control deficiencies may be identified but are not remedied in a timely manner.	Controls and related policies and procedures are in place and adequately documented. An event and disclosure process is in place and adequately documented. Employees are aware of their responsibility for control activities. The operating effectiveness of control activities is evaluated on a periodic basis (e.g., quarterly); however, the process is not fully documented. Control deficiencies are identified and remedied in a timely manner.	Controls and related policies and procedures are in place and adequately documented, and employees are aware of their responsibility for control activities. An event and disclosure process is in place and is adequately documented and monitored, but it is not always reevaluated to reflect major process or organizational changes. The operating effectiveness of control activities is evaluated on a periodic basis (e.g., weekly), and the process is adequately documented. There is limited, primarily tactical, use of technology to document processes, control objectives and activities.	Stage 5 meets all of the characteristics of stage 4. An enterprisewide control and risk management program exists such that controls and procedures are well documented and continuously reevaluated to reflect major process or organizational changes. A self-assessment process is used to evaluate the design and effectiveness of controls. Technology is leveraged to its fullest extent to document processes, control objectives and activities; identify gaps; and evaluate the effectiveness of controls.
Sarbanes-Oxley Implications	The organization has a total inability to be in compliance at even the minimum level.	Insufficient controls, policies, procedures and documentation exist to support management's assertion. The level of effort to document, test and remedy controls is very significant.	Although controls, policies and procedures are in place, insufficient documentation exists to support management's certification and assertion. The level of effort to document, test and remedy controls is significant.	Sufficient documentation exists to support management's certification and assertion. The level of effort to document, test and remedy controls may be significant depending on the organization's circumstances.	Sufficient documentation exists to support management's certification and assertion. The level of effort to document, test and remedy controls may be less significant depending on the organization's circumstances.	Implications of stage 4 remain. Improved decision making is enabled because of high-quality, timely information. Internal resources are used effectively and efficiently. Information is timely and reliable.

Bijlage 5) Mapping CobiT op best practices

Figure 11—High-level Mapping of Guidance to CobiT Processes

CobiT Process	COSO	ITIL	ISO/IEC 17799	FIPS PUB 200	ISO/IEC TR 13335	ISO/IEC 15408	PRINCE2	PMBOK	TickIT	CMMI	TOGAF 8.1	IT BPM	NIST 800-14
PO 1	+	-	-	-	-	-	-	-	-	-	-	-	-
PO 2	+	-	+	+	+	-	-	-	-	-	+	-	+
PO 3	+	+	+	+	+	-	-	-	-	-	+	+	+
PO 4	+	+	+	+	+	-	-	-	-	-	+	-	+
PO 5	+	+	-	-	-	-	+	+	-	-	-	-	-
PO 6	+	-	+	+	+	-	-	-	-	-	-	+	+
PO 7	+	-	+	+	-	-	-	-	-	-	-	-	+
PO 8	-	-	-	-	-	+	+	+	+	+	-	-	-
PO 9	+	-	+	+	+	-	+	+	-	+	-	-	+
PO 10	-	-	-	-	-	-	+	+	-	+	-	-	-
AI 1	+	-	-	-	+	-	-	-	+	-	+	-	+
AI 2	+	-	+	+	-	+	-	-	+	+	-	-	+
AI 3	+	-	+	+	-	+	-	-	+	-	-	+	+
AI 4	+	+	+	+	-	+	-	-	+	-	-	-	+
AI 5	-	-	-	-	-	-	-	+	+	-	-	-	-
AI 6	+	+	+	+	+	-	-	-	+	+	-	-	+
AI 7	+	+	+	+	+	-	-	-	+	+	-	-	+
DS 1	+	+	-	-	-	-	-	-	-	-	+	-	-
DS 2	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 3	+	+	+	+	-	-	-	-	-	-	-	-	+
DS 4	+	+	+	+	+	-	-	-	-	-	-	+	+
DS 5	+	+	+	+	+	+	-	-	-	-	-	+	+
DS 6	-	+	-	-	-	-	-	-	-	-	-	-	-
DS 7	+	-	+	+	+	-	-	-	-	+	-	-	+
DS 8	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 9	+	+	+	+	-	-	+	-	-	+	-	-	+
DS 10	-	+	-	+	-	-	-	-	-	+	-	-	+
DS 11	+	+	+	+	+	+	-	-	-	+	-	+	+
DS 12	+	-	+	+	+	+	-	-	-	-	-	+	+
DS 13	-	-	+	-	-	-	-	-	-	-	-	-	+
ME 1	-	-	+	-	-	-	-	-	+	+	-	-	+
ME 2	-	-	+	+	+	+	-	-	+	-	-	+	+
ME 3	+	-	-	-	-	-	-	-	-	-	-	-	-
ME 4	+	-	+	+	-	-	-	-	-	-	-	-	+

(+) Frequently addressed
(-) Not or rarely addressed