

## Wet financieel toezicht en de IT organisatie Een aanpak met CobiT als start-, maar niet als eindpunt.



Drs. ing. François Zielemans<sup>1</sup>

### Inleiding

De monitoringactiviteiten van de compliance officer kunnen niet los van automatisering worden gezien. De compliance officer kan enerzijds bij zijn monitoringactiviteiten gebruik maken van geautomatiseerde systemen (denk aan tools voor het controleren van privé (effecten)transacties) en anderzijds maakt de business gebruik van veel geautomatiseerde systemen.

De compliance officer vervult geen edp audit activiteiten, maar enige achtergrondkennis van de impact van automatisering op (de verwerking van) it-eisen uit de op de Wft gebaseerde Nadere Regeling van de AFM kan bijdragen aan betere monitoring door die compliance officer. Dit artikel wil een bijdrage leveren aan die achtergrondkennis.

### CobiT

CobiT staat voor *Control Objectives for Information and related Technology* en is een standaard set leidraden ('control objectives') voor het implementeren van formele IT processen en beheersingsmechanismen en wordt gepubliceerd door het IT Governance Institute (ITGI). De oriëntatie van CobiT is gericht op het verminderen van IT risico's en dit is een van de redenen waarom het ook bruikbare elementen bevat vanuit Wft-perspectief. Immers de meeste Wft eisen zijn gericht op het verminderen van (financiële) risico's.

CobiT kan de laatste jaren op toenemende interesse rekenen van auditors en compliance officers in het kader van zekerheid verkrijgen over de mate waarin een IT organisatie voldoet aan wet- en regelgeving. Dit artikel beargumenteert dat CobiT bruikbaar is, maar dat er meer nodig is om op een *efficiënte* wijze aan de Wet financieel toezicht te voldoen.

### De Wet financieel toezicht

De Wet financieel toezicht (Wft) is op 1 januari 2007 in werking getreden en is onderdeel van het streven van de Nederlandse overheid om het financieel toezicht op een andere wijze in te richten. De Wft geeft zowel De Nederlandsche Bank (DNB) als de Autoriteit Financiële Markten (AFM) een toezichthoudende rol, maar beide kijken vanuit een ander perspectief. De DNB waarborgt dat financiële instellingen aan hun verplichtingen kunnen voldoen en de AFM beoordeelt of deelnemers aan de financiële markt correct behandeld en geïnformeerd worden.

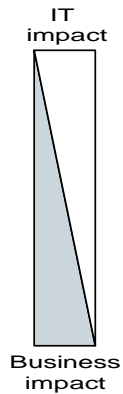
Omdat de wettekst zich op een relatief hoog abstractieniveau bevindt, is aan een deel een nadere invulling gegeven door zowel de AFM als DNB. De AFM heeft in november 2006 de *Nadere Regeling gedragstoezicht financiële ondernemingen Wft* (Nadere Regeling) gepubliceerd en dit artikel gebruikt deze Nadere Regeling als primair referentiekader om de impact van de Wft op de IT organisatie inzichtelijk te maken.

### De impact van de Wft op de IT organisatie

Een aantal eisen in de Nadere Regeling van de AFM zijn specifiek gericht op de IT organisatie van een financiële instelling, maar dezen zijn veruit in de minderheid. Dit betekent echter niet dat de impact van de Wft op de IT organisatie nihil is. Door de hoge mate van geautomatiseerde gegevensverwerking binnen financiële instellingen zijn bedrijfsproces en IT onlosmakelijk met elkaar verbonden. Hierdoor hebben verschillende, op het bedrijfsproces gerichte, Wft regelingen, indirect, ook impact op de inrichting van de IT organisatie. Door de impact van Wft op IT op deze wijze te benaderen, kan de volgende onderverdeling in categorieën worden verkregen:

---

<sup>1</sup> François Zielemans is manager bij Protiviti en gespecialiseerd in uitbestedingsvraagstukken, regieorganisaties en compliance. Hij kan bereikt worden op francois.zielemans@protiviti.nl. Dit artikel is gebaseerd op een white paper die het mitigeren van eisen vanuit regel- en wetgeving binnen de bancaire en verzekeringswereld in meer detail beschrijft. Deze white paper is beschikbaar gesteld op [www.protiviti.nl](http://www.protiviti.nl).



- Wft eisen direct gericht op het IT domein. Voorbeelden zijn eisen die gesteld worden aan een de beveiliging van informatie en het voorkomen van ongeautoriseerde implementaties van nieuwe applicatie software.
- Wft eisen gericht op de bedrijfsprocessen, maar met indirecte impact op het IT domein. Voor deze categorie een tweetal voorbeelden: a) de eis dat *alle* financiële transacties op dagelijkse basis in de administratie gemuteerd dienen te worden heeft impact op IT processen als incident management en capaciteit management, b) de eis dat front en back office activiteiten gescheiden zijn, dient vertaald te worden in onder andere het beheer van autorisaties.
- Wft regelingen gericht op het business domein en zonder impact op de IT functie. Deze regelingen worden logischerwijs buiten beschouwing gelaten in dit artikel.

Als de IT organisatie de Wft eisen doorleest en per eis beoordeelt in welk van de drie voorgenoemde categorieën hij valt, kan de IT organisatie een totaalbeeld vormen van de totale hoeveelheid potentieel werk als gevolg van de Wft.

In de praktijk zullen verschillende eisen vanuit de Wft al afgedekt zijn door maatregelen die ingevoerd zijn als onderdeel van de gewone bedrijfsvoering of vanwege andere wetgeving. De 'Wft-to-do lijst' zal in de praktijk dan ook kleiner zijn dan de initiële lijst met daarin alle directe en indirecte eisen gesteld aan IT.

De logische volgende stap is nu bepalen welke eisen van de to-do lijst een technische oplossing vereisen en welke een organisatorische. Voorbeelden van technische oplossingen zijn het scheiden van front en back office beleggingssystemen en het automatiseren van handmatige beheersmaatregelen, door gebruik te maken van controlemechanismen in applicaties ('application controls'). Andere technische aanpassingen zijn meer functioneel van aard en vloeien voort uit bijvoorbeeld de classificatie van beleggingsklanten (klein, professioneel en tegenpartij) en communicatiekanalen met andere beleggingsinstellingen om een zo optimaal mogelijke orderuitvoering te garanderen ('best execution').

Voor die Wft eisen waar geen effectieve technische maatregel bedacht kan worden, zullen aanvullende beleidsmatige en procedurele maatregelen gedefinieerd dienen te worden.

Daar technische beheersmaatregelen zeer bedrijfsspecifiek zijn, wordt dit onderwerp niet verder uitgewerkt in dit artikel. Het tweede deel focust daarom op de mogelijkheden die bekende governance en procesmodellen bieden bij het selecteren van organisatorische beheersmaatregelen. Hierbij wordt CobiT als startpunt genomen, omdat het model ook in Nederland aan populariteit blijft winnen.

### **De (on)bruikbaarheid van CobiT**

Op basis van de eerder geïntroduceerde categorisering van Wft eisen wordt de (on)bruikbaarheid van CobiT nu kort toegelicht aan de hand van enkele voorbeelden.

- Wft eisen specifiek gericht op het IT domein. De eis dat er beleid en procedures zijn die waarborgen dat informatie altijd beschikbaar, integer en confidencieel is, wordt aangestipt door CobiT, maar op een relatief hoog abstractieniveau. Meer praktische oplossingen met betrekking tot de beschikbaarheid en veiligheid van informatiesystemen zijn terug te vinden in onder andere BS7799/ISO27001<sup>2</sup> en Code voor Informatiebeveiliging. Deze standaarden zijn meer operationeel en procesgericht en hierdoor eenvoudiger inpasbaar in de dagelijkse werkzaamheden. CobiT en ISO27001 sluiten elkaar echter niet uit, maar moeten als aanvullend op elkaar gezien worden.

Ook bij het verminderen van het risico dat ongeautoriseerde software geïmplementeerd wordt, geldt dat CobiT control objectives biedt, maar dat er geen concrete maatregelen aangereikt worden. De processen Release Management en Change Management uit ITIL, ASL, CMM en ISO20000 (zie kader) bieden hier soelaas. CobiT biedt echter wederom een aantal ankerpunten, waardoor ook hier geldt dat CobiT als een overkoepelende 'paraplu' kan werken.

<sup>2</sup> zie kader voor een korte toelichting van de in dit artikel gebruikte methodieken en standaarden

Het daar waar mogelijk invoeren van programmeerbare beheersmaatregelen ('application controls') is een eis die niet door CobiT ondervangen wordt. Het automatiseren van controls is echter niet zozeer een beheersmaatregel, maar een beleidsmatig streven, waarvan de effectiviteit op een andere wijze aangetoond dient te worden.

- Wft eisen specifiek gericht op het business domein, maar met een afgeleide impact op het IT domein. Een van de Wft artikelen vereist vrij vertaald dat de financiële instelling over een operationeel management model dient te beschikken dat opgebouwd is uit onder andere de volgende onderdelen:
  - een adequate organisatiestructuur;
  - adequate allocatie van taken, mandaat en verantwoordelijkheden;
  - schriftelijke weergave van rechten en verplichtingen;
  - heldere rapportagelijnen;
  - en een adequaat systeem voor het managen van informatie en communicatie.

De Wft vereist niet expliciet dat support functies als IT aan dit artikel moeten voldoen. Maar enerzijds maakt de IT organisatie een integraal onderdeel uit van de financiële instelling en anderzijds is er de nauwe afhankelijkheid tussen bedrijfsproces en IT. Beide argumenten maken het redelijk te veronderstellen dat het betreffende artikel ook van toepassing is in de IT organisatie.

De toepasbaarheid van CobiT voor het voldoen aan de hiervoor omschreven eis is beperkt. Weliswaar voorziet CobiT in een overzicht met generieke IT functies en daarbij behorende verantwoordelijkheden, maar de Wft eis is zo specifiek dat een aantal aanvullende maatregelen noodzakelijk zijn.

Uit de voorgaande paragraaf komt naar voren dat de kunst bij de implementatie van de Wft door een IT organisatie hem zit in het slim combineren van elementen uit bestaande best practices en modellen, in plaats van het blind volgen van één methodiek.

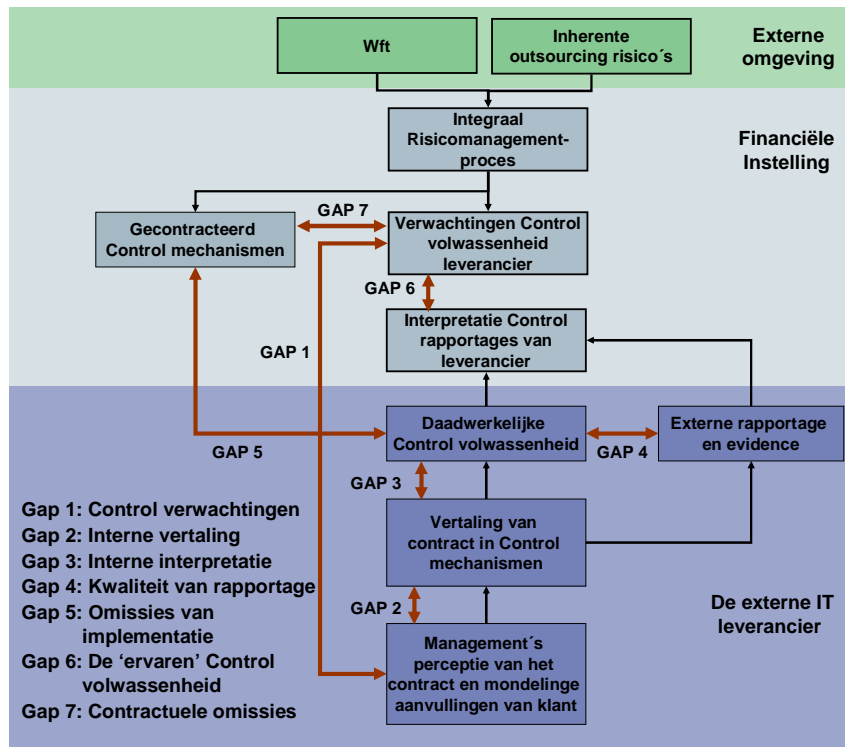
### **CobiT, Wft en outsourcing**

Een onderwerp dat nog niet aan de orde is gekomen in dit artikel, maar wel steeds relevanter wordt, is outsourcing. Het onderbrengen van IT bij een externe leverancier brengt aan de ene kant met zich mee dat aan een aantal extra Wft eisen voldaan moet worden en dwingt tevens af om op een andere manier naar de vertaling van de Wft in organisatorische en technische maatregelen te kijken. Dit laatste is echter niet eenvoudig met als gevolg dat de volgende twee, te simpele, aanpakken regelmatig gehanteerd worden als wetgeving en outsourcing ter sprake komen.

Bij de eerste aanpak wordt contractueel vastgelegd dat de externe leverancier 'Wft-compliant' moet zijn. Niets meer of minder. De financiële instelling hoopt op deze wijze van het onderwerp af te zijn en ook de externe leverancier laat het onderwerp meestal maar rusten na de financiële instelling enkele malen tevergeefs om een nadere toelichting te hebben gevraagd. Het gevolg is een soort vacuüm waarbij beide partijen (tegen beter weten in) hopen dat geen nieuws goed nieuws betekent.

Bij de tweede aanpak wordt de Wft vertaald in het integraal moeten voldoen aan bijvoorbeeld CobiT en ITIL met een daarbij behorende uitgebreide lijst met rapportage eisen. De gedachte achter deze aanpak is dat als er maar genoeg gemeten wordt er vast ook wel het juiste bij zit. Ook deze aanpak is, net als de eerste niet erg effectief noch efficiënt.

Een iets minder eenvoudige aanpak, maar wel één die leidt tot een voor beide partijen bruikbaar resultaat, volgt een tussenweg tussen beide voorgaande methoden. Deze alternatieve aanpak gaat er vanuit dat de financiële instelling een sturende en controlerende rol heeft bij het bepalen van de wijze waarop de Wft vertaald wordt in beheersingsmaatregelen. De uitvoering ligt bij de externe partij. De aanpak is schematisch weergegeven in de figuur, samen met de punten waar zaken mis kunnen gaan.



De wijze waarop een Wft eis vertaald wordt in beheersmaatregelen is idealiter afhankelijk van de (financiële) schade die mogelijk kan ontstaan indien niet wordt voldaan aan de betreffende eis. Op basis van dit 'risico' kan bepaald worden hoeveel aandacht en geld besteed moet worden aan de beheersing ervan. Dit kan ertoe leiden dat de beheersing van sommige risico's bijna volledig wordt overgelaten aan de externe leverancier (de financiële instelling stuurt op output), terwijl voor andere risico's er veel meer inzicht gewenst is in de wijze waarop de eis en het bijbehorende risico wordt geadresseerd (de financiële instelling stuurt op zowel output alsmede de inrichting van de beheersingsmaatregelen).

CobiT kan ook hierbij, indien op een slimme wijze toegepast, een rol spelen. Het integraal overnemen van CobiT is echter niet de oplossing daar het een generiek model is en het primair bedoeld is voor het aansturen van een interne IT organisatie en niet voor het managen van een externe leverancier.

### Gebruik CobiT als paraplu

Voor dit artikel kan samenvattend worden opgemerkt dat CobiT zeker bruikbaar is, maar dan vooral als overkoepeld raamwerk om een deel van de Wft beheersmaatregelen een centraal ankerpunt te geven. Door een op CobiT gebaseerde compliance raamwerk slim vorm te geven, kan het zelfs de basis gaan vormen voor het mitigeren van enig andere wet- en regelgeving (bijvoorbeeld Basel II en Solvency II). Hierbij zal opvallen dat veel beheersmaatregelen ingericht voor de Wft dezelfde zullen zijn als noodzakelijk voor Basel II en Solvency II. Goed uitgevoerd is het eindresultaat van deze aanpak lagere compliance kosten; zowel direct (IT organisatie) als indirect (interne en externe audits en SAS 70 rapporten<sup>3</sup>).

Het is aan de auditor en compliance officer om de IT organisatie zijn toegevoegde waarde te tonen door inzichten en aanbevelingen in te brengen die erop duiden dat hij eisen vanuit wet- en regelgeving slim kan combineren met de sterke en zwakke kanten van best practices als CobiT, ISO20000, CMM en ISO27001.

<sup>3</sup> Het gebruiken van SAS 70 rapporten om inzicht te verkrijgen in de mate van interne beheersing is afkomstig uit de Verenigde Staten. Er zijn twee typen SAS 70 rapporten. Type I focusteert op de mate waarin beheersmaatregelen beschreven zijn ('opzet') en Type II op de effectiviteit door middel van het uitvoeren van testen ('opzet' en 'bestaan').

### **Kader: Door de methodieken het bos niet meer zien**

De modellen, best practises, methodieken die gebruikt kunnen worden voor het inrichten van een IT organisatie zijn legio en dit artikel heeft niet het ambitieniveau om volledig te zijn in dit opzicht. De keuze voor de in dit artikel aangehaalde modellen is gemaakt vanuit het perspectief dat ze breed ingezet worden binnen veel Nederlandse organisaties.

- ITIL staat voor Information Technology Library en is in haar oorspronkelijke vorm gepubliceerd door met het CCTA (tegenwoordig OGC) in het Verenigd Koninkrijk. ITIL is een overzicht met best practices die georganiseerd zijn rondom een aantal tactische en operationele processen en gericht op het beter afstemmen van IT dienstverlening op de behoeften van de klanten. Recentelijk is versie 3 van ITIL gepubliceerd.
- ISO20000, oorspronkelijk gepubliceerd als British Standard 15000, combineert de best practice ITIL en het kwaliteitsgedachtegoed van ISO9000. Het is een formele standaard met 'controls' waartegen een organisatie gecertificeerd kan worden door een onafhankelijke auditor. ISO20000 promoot de adoptie van een integrale procesbenadering met als doel een effectieve levering van IT diensten.
- ISO27001 is de ISO versie van de British Standard 7799 en maakt onderdeel uit van de ISO20000 familie. ISO27001 biedt controls die een organisatie kan helpen risico's te managen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Net als ISO20000 is het een formele standaard en kan de organisatie zich laten certificeren.
- ASL staat voor Application Service Library en focuseert op het professionaliseren van applicatiebeheer, daar waar ITIL de nadruk legt op het beheer van de infrastructuur. ASL is public domain en is een framework met processen op strategisch, tactisch en operationeel niveau aangevuld met best practices.
- CMM is een model van het Software Engineering Institute (SEI), onderdeel van de Carnegie Mellon University. Dit instituut stelt zich ten doel organisaties die software ontwikkelen en/ of onderhouden te ondersteunen bij het verbeteren van hun softwareontwikkelingsprocessen. De eerste versie van het CMM is in opdracht van het Amerikaanse Ministerie van Defensie in 1986 ontwikkeld.