IS ALLEEN HET GEBRUIK VAN STANDAARDEN GENOEG OM EFFECT TE CREËREN?

# Effect creëren in de boardroom

Aansluiten bij de risicobeleving en prioriteitstelling in de boardroom is essentieel om vanuit audit of toezicht effectief te kunnen zijn. Zorgen dat bestuurs- en directieleden aandacht hebben voor verbetering en zich daarvoor inzetten, vormt de kern. Om dat te bereiken heeft het IT-Toezicht van DNB (ITD) haar aanpak vernieuwd, waarbij het gebruik van standaarden een belangrijke basis vormt. Dit artikel gaat nader in op deze aanpak.

EVERT KONING EN HANS BIKKER

## STANDAARDEN ZIJN HULPMIDDEL

In 1988 is het ITD begonnen met het hanteren van normenkaders. In dat jaar verschijnt het zogeheten 'Memorandum met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking'. Dit is een door het ITD zelf ontwikkeld kader, dat de toentertijd belangrijkste 'controls' beschrijft inzake risicoanalyse, beveiliging en continuïteit. Het memorandum voorzag in een behoefte, omdat er in de markt nog geen echte geaccepteerde standaarden voorhanden waren.

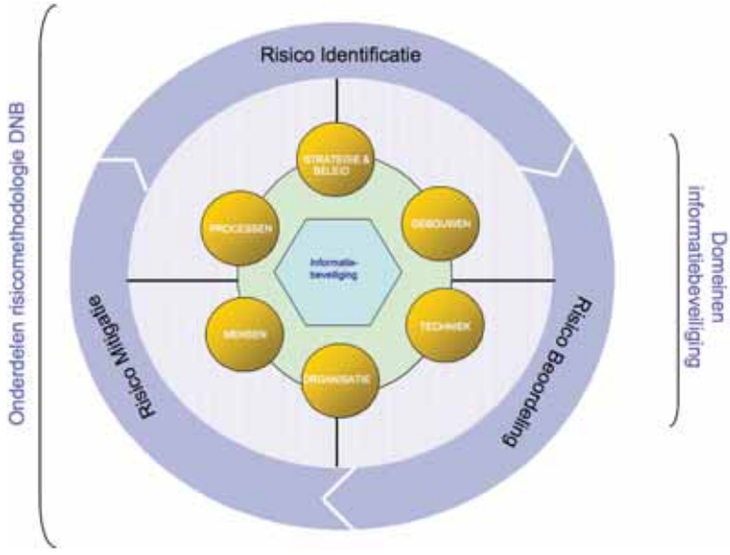
Eind vorige eeuw kwam hier verandering in. Zowel de bekendheid en het gebruik van ITIL, ISO-standaarden als van CobiT namen toe. Die ontwikkeling, versterkt door DNB's voorkeur voor *principle based* toezicht, maakte dat het ITD aansloot bij deze standaarden. De praktijk heeft het ITD namelijk geleerd dat een nadere concretisering van wet- en regelgeving van belang is om te kunnen komen tot een goed toezicht daarop. In dat kader vormt de inzet van toetsingskaders, gebaseerd op open internationale standaarden, een belangrijk hulpmiddel. Echter, het ITD schrijft het hanteren van specifieke standaarden niet voor.

Vanuit het toezichtperspectief biedt het toepassen van standaarden in de praktijk voor- en nadelen, zoals opgenomen in tabel 1. De voordelen voeren in de praktijk de boventoon, waarbij het ITD tracht de nadelen te beperken.

De implementatie van standaarden in de toezichtpraktijk is aan de hand van de hiernavolgende praktijkcasus toegelicht.

| Voordelen | Nadelen |
|---|---|
| De toepasbaarheid voor instellingen biedt efficiencyvoordeel door aan te sluiten op al gebruikte standaarden binnen de betreffende instellingen. | Het verschil tussen instellingen in ervaringsgraad met bepaalde standaarden levert mogelijk uiteenlopende interpretaties op omtrent het beheersingsniveau. |
| Vereenvoudigt de communicatie met de instellingen, koepelorganisaties, externe accountants en overige belanghebbenden. | Toetsingskaders worden meer gezien als rule-based in plaats van principle-based. Het voldoen aan een toetsingskader wordt een doel op zich. |
| Geeft richting aan de interpretatie van beheersingsvraagstukken door een nadere uitwerking te bieden. | Specifieke situaties bij instellingen kunnen deels onderbelicht blijven door het gebruik van standaard toetsingskaders. |
| De mogelijkheid tot benchmarking van uitkomsten in de tijd op instellings- en sectorniveau. | Niet alle instellingen aan de hand van een toetsingskader kunnen 'challengen' op het aanwezige beheersingsniveau. Hierdoor zou een onvoldoende ' level playing field' binnen de financiële sector kunnen ontstaan. |

*Tabel 1: Voor- en nadelen van het gebruik van standaarden vanuit toezichtperspectief*




*Figuur 1: Hoofdindeling toetsingskader onderzoek Informatiebeveiliging DNB*

## EEN PRAKTIJKCASUS

Eind 2009 is het ITD een meerjarenonderzoek gestart met als doel het niveau van informatiebeveiliging binnen de financiële sector van Nederland te verhogen. Het onderzoek bestaat uit vier stappen, die in de volgende paragrafen worden toegelicht.

### Stap 1: Opstellen toetsingskader

Voor een effectieve toezichtaanpak zijn bij de uitwerking van het toetsingskader vijf ontwerpcriteria gehanteerd:

1. Het toetsingskader dient te zijn gebaseerd op een internationale standaard.
2. Instellingen moeten zelfstandig het toetsingskader kunnen invullen.
3. Niet alleen verbeterpunten, ook sterke punten moeten inzichtelijk worden gemaakt.
4. Prioriteitstelling van resultaten dient mogelijk zijn.
5. Het toetsingskader moet als basis voor benchmarking kunnen worden gehanteerd.

Rekening houdend met de bovengenoemde ontwerpcriteria is gekozen voor de internationale standaard CobiT als basis voor het toetsingskader. CobiT biedt vele voordelen, waaronder een goede aansluiting op het principle based prudentieel toezicht van DNB. Tevens biedt CobiT een brede basis aan beheersmaatregelen en bestaan er vele koppelingen met andere standaarden zoals ITIL, ISO 27000-serie en COSO ERM. Een ander voordeel is de brede toepassing van CobiT door financiële instellingen in Nederland en internationaal.

| Niveau | Label | Omschrijving |
|---|---|---|
| 0 | Non existent | Niet aanwezig, niet bewust. |
| 1 | Ad hoc, initial | Bewust van noodzaak. Aanpak niet gestructureerd, gestandaardiseerd en afhankelijk van het individu. |
| 2 | Repeatable, informal | Gestructureerde aanpak, maar niet aantoonbaar. |
| 3 | Structured and formalized | Gestructureerde aanpak organisatiebreed en aantoonbaar. |
| 4 | Implemented and periodically assessed | Niveau 3 en beheersmaatregelen worden periodiek beoordeeld op effectiviteit en zonodig aangepast. |

*Tabel 2: Omschrijving volwassenheidsniveaus*

Op basis van CobiT (versie 4.1) zijn uiteindelijk 54 beheersmaatregelen geselecteerd en gekoppeld aan controledoelstellingen, geclusterd in een zestal domeinen. In figuur 1 zijn die domeinen nader benoemd. Daarbij is een koppeling gelegd naar de risicomethodologie van DNB. Het toetsingskader is te downloaden via de website van DNB (www.dnb.nl).

Daarnaast is een volwassenheidsmodel toegepast, sterk gelieerd aan CobiT (versie 4.1), bestaande uit vijf niveaus. In tabel 2 zijn die niveaus nader beschreven, waarbij het ITD veronderstelt dat een instelling kan aantonen dat beheersmaatregelen organisatiebreed op structurele wijze werken. Dit komt binnen het volwassenheidsniveau overeen met niveau '3'.

Alvorens het toetsingskader in de praktijk te gebruiken, is dit onder meer afgestemd met de Nederlandse Vereniging van Banken (NVB), om draagvlak bij de betrokken instellingen te krijgen voor verdere stappen.

### Stap 2: Procesinrichting en pilot

Voor een efficiënte uitvoering van het onderzoek zijn diverse processtappen gestandaardiseerd en sjablonen opgesteld. Ter aanvulling is een tool gebouwd om de ingevulde toetsingskaders eenvoudig te kunnen verwerken en analyseren.

Om het toetsingskader en het ondersteunende proces in de praktijk te toetsen, is een pilot uitgevoerd. Hiertoe zijn enkele instellingen benaderd die veel belangstelling hadden voor het onderzoek, wat heeft geresulteerd in een verbeterde toepasbaarheid. De grootste uitdaging betrof het vaststellen van de correcte scores. Onvoldoende kennis van specifieke omstandigheden, misinterpretaties en flattering kunnen namelijk leiden tot een onjuiste inschatting van volwassenheidsniveaus door de instellingen. Deze punten zouden temeer gelden, omdat de instellingen

het toetsingskader zelf zouden gaan invullen. De pilot leidde ertoe dat binnen het onderzoeksproces twee controlemomenten zijn opgenomen:

1. De betrokken IT-toezichthouders bespreken steekproefsgewijs de uitkomsten van de ingevulde toetsingskaders met de instelling en doen zonodig een deelwaarneming.
2. Het lid binnen een Raad van Bestuur, verantwoordelijk voor IT, dient uiteindelijk het ingevulde toetsingskader te ondertekenen.

Verder bleek op basis van de pilot dat de betrokkenheid van (IT-)audit veelal de kwaliteit van de uitkomsten verhoogt. Daarom adviseert het ITD om de (IT-)auditor tijdens de *self assessment* nadrukkelijk te betrekken. Door zijn of haar onafhankelijkheid, kennis van de organisatie, ervaring met CobiT en het onderwerp Informatiebeveiliging is de (IT-)auditor prima geëquipeerd om uitkomsten juist in te schatten.

### Stap 3: Veldwerk en rapportage

Na de voorbereidende stappen is het onderzoek uitgezet bij een aantal instellingen binnen de sectoren Pensioenfondsen, Banken en Verzekeraars. Tijdens het veldwerk zijn de uitkomsten steekproefsgewijs besproken met de instellingen en is zonodig aanvullend bewijs opgevraagd. Op basis van de uitkomsten heeft het ITD een formele rapportage opgesteld. Vervolgens heeft iedere van de betreffende instellingen een verbeterplan geformuleerd om de relevante beheersmaatregelen tenminste op volwassenheidsniveau 3 te krijgen. In aanvulling op de individuele terugrapportage heeft iedere betrokken instelling een benchmarkrapportage ontvangen.

### Stap 4: Monitoring en communicatie

Uiteindelijk betekent 'effect hebben vanuit toezicht' dat de beheersing in de praktijk daadwerkelijk verbetert. Om daarvoor te zorgen, volgt het ITD op actieve wijze de voortgang van de verbeterplannen. Dit doet ITD zowel op basis van voortgangsrapportages als met periodieke gesprekken bij de betreffende instellingen. Indien de implementatie van verbeteracties onvoldoende voortgang laat zien, kan DNB overgaan tot formele handhaving. Tot dusverre zijn de ervaringen positief; instellingen zijn serieus bezig het niveau van informatiebeveiliging te verbeteren.

Naast monitoring vormt interne en externe communicatie in toenemende mate een belangrijke activiteit binnen het onderzoek Informatiebeveiliging. Communicatie biedt namelijk de gelegenheid om een groter en een meer divers publiek te benaderen en aandacht te vragen voor het onderzoek. Het levert de mogelijkheid op om, met de beschikbare toezichtcapaciteit, meer instellingen te benaderen ter realisatie van een 'level playing field'. Dit laatste wordt ondersteund door op transparante wijze kennis uit te wisselen met belanghebbende partijen zoals financiële instellingen, toezichthouders, koepelorganisaties, IT-serviceproviders en externe accountants.

Naast de individuele en benchmarkrapportages, heeft het ITD gekozen voor verscheidene aanvullende communicatievormen. Te noemen valt een seminar gericht op instellingen en externe accountants. Eveneens is een artikel geplaatst in de nieuwsbrief voor Verzekeraars en Pensioenfondsen en is recentelijk een circulaire over informatiebeveiliging[1] rondgestuurd. Blijvende aandacht voor een onderwerp is van belang om uiteindelijk effect te kunnen resulteren.

Conform de Wet op financieel toezicht (Wft) is het doel van het ITD een integere en beheerste bedrijfsvoering bij instellingen. Daarbij draait het in essentie om beïnvloeding van gedrag. In dat kader creëert alleen het gebruik van standaarden niet het gewenste effect. Evenzo blijken het benchmarken, het aangeven van de goede en verbeterpunten, het actief monitoren van verbeteracties en het periodiek communiceren van resultaten essentieel te zijn.

### VERVOLGSTAPPEN

Ook los van het continue onderzoek Informatiebeveiliging, zal het gebruik van internationale standaarden, inclusief volwassenheidsmodellen, in de praktijk van het ITD toenemen. Daarnaast zullen bestaande toetsingskaders op termijn worden aangepast in lijn met de onderliggende standaarden. CobiT 5.0 vormt bijvoorbeeld de nieuwe basis waarop het toetsingskader Informatiebeveiliging in de komende jaren zal worden geënt.

De verdergaande behoefte aan benchmarkgegevens zal het gebruik van standaarden stimuleren. Niet alleen binnen het ITD, ook bij andere toezichthouders internationaal. In dat kader is er veel belangstelling bij Europese en niet-Europese toezichthouders voor de nieuwe aanpak van het ITD. Tevens zal de samenwerking met relevante partijen, zoals externe accountants, IT-serviceproviders of de overheid, nader worden beschouwd om sectorbreed effect te creëren.

Andere aandachtspunten voor het ITD vormen de integratie van verschillende onderzoeksresultaten en de vertaling van IT-risico's naar de betekenis voor de bedrijfsvoering of -strategie. Naar verwachting zal dat leiden tot meer inzicht in de effecten van IT-risico's bij de beleidsbepalers in financiële instellingen. Kortom, een effectiever toezicht.

### TOT SLOT

Alleen vaststellen dat beheersmaatregelen ontoereikend werken, is niet de essentie van toezicht- of auditactiviteiten. Zorgen dat bestuurs- en directieleden aandacht hebben voor verbetering en zich daarvoor inzetten, vormt de kern. Daarbij is het niet genoeg alleen standaarden toe te ▶

passen. Uit de praktijkcasus bleek dat de volgende zes aanbevelingen van belang waren om betrokkenheid op bestuurs- en directieniveau te realiseren en te houden:

- *Een transparant toetsingskader*
  Een duidelijk toetsingskader bevordert een transparante communicatie en schept heldere verwachtingen.
- *Inzicht in verbeter- en goede punten*
  Naast tekortkomingen, ook de sterke punten inzichtelijk te maken.
- *Directe betrokkenheid*
  Ondertekening van het ingevulde toetsingskader door een bestuurslid, verantwoordelijk voor IT, bevordert de betrokkenheid en voorkomt vrijblijvenheid.
- *Benchmarken*
  Benchmarkinformatie die aangeeft hoe een organisatie scoort ten opzichte van de peers.
- *Doorvertaling van IT-risico's in de betekenis voor de bedrijfsvoering*
  Het koppelen van de IT-risico's aan de risk appetite en/of bedrijfsstrategie van een instelling.
- *Monitoring van verbeteracties*
  Het actief en periodiek monitoren zorgt voor een permanente aandacht voor verbeterpunten en de opvolging daarvan.

In hoeverre de vernieuwde aanpak van het ITD heeft geleid tot een grotere betrokkenheid en inzet op bestuurs- en directieniveau, zal in een vervolgartikel nader worden toegelicht. Op het moment van schrijven van dit artikel waren het onderzoek en de effectmeting namelijk nog onderhanden. ■

**Noot**

1. Link naar circulaire: http://www.toezicht.dnb.nl/binaries/Circulaire%20Info%20beveiliging.definitieve%20versie.23-11-2011_tcm50-224608.pdf


**E. (Evert) Koning** is Hoofd Expertise centrum ICT-risico's DNB. Evert werkt ruim twintig jaar bij DNB. Sinds 2004 is hij als afdelingshoofd verantwoordelijk voor het expertisecentrum ICT risico's. Als nevenfunctie is Evert bestuurslid van NOREA, de beroepsgroep van IT-auditors in Nederland. Ook is Evert examinator aan de postdoctorale IT-auditopleiding aan de VU.

**H. (Hans) Bikker** is Toezichthouder specialist Expertise centrum ICT-risico's DNB. Hans is sinds medio 2009 werkzaam bij DNB in uitvoerend toezicht. Daarnaast heeft Hans zich beziggehouden met het toepasbaar maken van standaarden in het toezichtwerk.
Hans is sinds 2009 mede verantwoordelijk voor het thema-onderzoek Informatiebeveiliging.