Discussierapport over de relatie tussen de Internal Audit functie en GRC

De internal auditor als spin in het GRC-web

'Samenwerking met behoud van onafhankelijkheid'

Inhoudsopgave

Eindredactie
drs. Arjan Man CIA
Michael Schoevaart RE RA
drs. Heiko van der Wijk RA CIA

Redactieraad
prof. dr. Jim Emanuels RA
prof. dr. Leen Paape RA RO CIA
prof. dr. Jan van de Poel

Stuurgroep
Joop Brakenhoff RA RO
drs. San Croonenberg RA
drs. Arjan Man CIA
drs. Arjen van Nes RO

Projectgroep
Scott Cheung RA CIA
Eddy van der Geest RE RA
drs. Carin Gorter RA
mr. Machiel Hoogendoorn RA
Michael Schoevaart RE RA
Endymion Struijs RA
Rudy Voet RA
drs. Heiko van der Wijk RA CIA

Voorwoord

Door de sinds 2008 woedende wereldwijde financiële en economische crisis is er toenemende aandacht in organisaties voor interne beheersing en voor de eis tot het voldoen aan wet- en regelgeving. Governance, Risk Management & Compliance (GRC) is 'hot'.

Deze aandacht voor GRC roept vragen op:
- Hoe kan het GRC-speelveld op een effectieve en efficiënte wijze worden georganiseerd?
- Welke mate van zekerheid wil management en bestuur over het beheersingskader en hoe vindt de verantwoording daarover plaats?

Bij de invulling, uitvoering maar vooral ook de beheersing van de diverse GRC-activiteiten binnen een organisatie moet Internal Audit haar verantwoordelijkheid nemen. Daarnaast heeft Internal Audit veel belang bij een evenwichtig, efficiënt en effectief samenspel tussen de verschillende risk- en controlfuncties binnen de organisatie.
Gezien het belang van de Internal Audit functie in het GRC-speelveld hebben de Vakgroep Intern Accountants (INTAC) van het Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) en het Instituut van Internal Auditors Nederland (IIA) opdracht gegeven om de relatie tussen GRC en Internal Audit te onderzoeken en te analyseren. Dit rapport is gebaseerd op de uitkomsten van dit onderzoek, maar gaat ook een stap verder. De werkgroep heeft (in nauw overleg èn afstemming met beide opdrachtgevers) ook een aantal inhoudelijke keuzes gemaakt in de vorm van 'good practices' die verder richting geven en zullen bijdragen aan een hoger niveau van functioneren van de Internal Audit functie. Nadere verdieping en toelichting worden opgenomen in een uitgebreider rapport dat in het najaar van 2010 op de websites van beide organisaties beschikbaar zal komen.
Een ander doel van dit project is het leveren van een bijdrage aan de discussie in het bedrijfsleven over goede vormen van samenwerking tussen GRC en de Internal Audit functie. Daarom zijn in dit rapport ook diverse conclusies en aanbevelingen geformuleerd.

Het onderzoek, gericht op commerciële organisaties in Nederland, omvat vier stappen. Begonnen is met een literatuurstudie, gevolgd door een online enquête met 67 respondenten onder GRC-professionals. Deze activiteiten hebben de basis gevormd voor een interviewronde waarin bij 22 organisaties 28 interviews zijn gehouden. Afsluitend volgde een debatsessie met deskundigen en een groot aantal professionals.

Voor definities van de gebruikte begrippen verwijzen wij naar de definities zoals vastgesteld door het IIA.

Wij nodigen u uit kennis te nemen van dit rapport en dagen u uit hiermee aan de slag te gaan. Enerzijds om de kwaliteit van de GRC-activiteiten in uw eigen organisatie te verhogen en anderzijds om de betrokkenheid van de Internal Audit functie hierbij verder te intensiveren. Tot slot hopen wij dat dit rapport stof biedt om met collega's binnen en buiten uw organisatie in discussie te gaan en daarmee bijdraagt aan de professionaliteit van onze beroepsuitoefening.

Wij willen een ieder die de enquête heeft beantwoord en/of heeft deelgenomen aan de interviews en natuurlijk de redactieraad, stuur- en projectgroep hartelijk danken voor hun medewerking aan dit onderzoek.

drs. Ingrid Doerga RA, Voorzitter Vakgroep Intern Accountants van het Koninklijk NIVRA
drs. Sander Weisz RO CIA CCSA, Voorzitter IIA Nederland

Samenvatting

De Internal Audit functie opereert in het brede speelveld dat bekend staat onder de term GRC (Governance, Risk Management & Compliance). Enerzijds is zij onderdeel van de governance van de organisatie, anderzijds heeft zij een eigen (toetsende) verantwoordelijkheid hierop. Deze verantwoordelijkheid wordt onder meer vormgegeven door richtlijnen van diverse beroepsorganisaties en door verwachtingen van belanghebbenden van binnen en buiten de organisatie. Dit maakt de Internal Audit functie de spin in het GRC-web: zij overziet, controleert, adviseert, moet soms haar tanden laten zien en is een van de weinige organisatieonderdelen die toegang heeft tot alle onderdelen van de organisatie.

Op basis van een onderzoek bestaande uit een literatuurstudie, een online enquête onder 67 beroepsbeoefenaren, 28 interviews, en een debatsessie is een serie 'good practices' opgesteld die als referentiepunt kan dienen voor beroepsuitoefenaren, belanghebbenden en andere belangstellenden in en rondom GRC. Deze 'good practices' kunnen een eerste aanzet zijn tot nadere invulling van richtlijnen en standaarden voor Internal Audit functies zoals mogelijk te formuleren door de (internationale) beroepsorganisaties van internal auditors.

Naast de 'good practices', heeft de werkgroep een aantal conclusies geformuleerd op basis van de resultaten van het onderzoek, discussies binnen de werkgroep en gesprekken met enkele professionals:

- De aanpak van de Internal Audit functie om te komen tot een oordeel over de governance in een organisatie kan zeker nog verder geprofessionaliseerd worden.
- Het opsplitsen van GRC-verantwoordelijkheden over meerdere functies leidt tot betere beheersing in de organisatie.
- Risicomanagement is nog sterk in ontwikkeling en de Internal Audit functie heeft nog geen eenduidige aanpak voor de beoordeling ervan.
- De Internal Audit functie kijkt nog te veel naar risicomanagementprocessen en te weinig naar de uitkomsten van deze processen.
- De activiteiten als gevolg van wet- en regelgeving, ook wel genoemd 'regulatory compliance', nemen zienderogen toe en leiden tot een versterking van een 'rules oriented' cultuur ten nadele van een 'principle based' cultuur.

Het rapport bevat per conclusie enkele aanbevelingen gericht aan de diverse belanghebbenden van GRC.

Er is in Nederland vrijwel geen wetgeving die ingaat op de Internal Audit functie in relatie tot het GRC-speelveld. Naast de Corporate Governance Code is eigenlijk alleen binnen de financiële sector aanvullende wet- en regelgeving voorhanden voor GRC, zoals de Code Banken, Basel II en Solvency II.

1 Good practices

1.1 Inleiding

Governance is de combinatie van processen en structuren die het bestuur van een organisatie heeft geïmplementeerd om de activiteiten van een organisatie van informatie te voorzien, te sturen, te managen en te monitoren bij het bereiken van haar doelstellingen[1]. De Internal Audit functie (IAF), als één van de risk- en controlfuncties naast bijvoorbeeld Risk Management, Compliance en Internal Control, maakt hier een onlosmakelijk onderdeel van uit. Het geheel wordt vaak aangeduid als GRC.

Als uitgangspunt voor de verantwoordelijkheden en taken van de IAF gelden de door het IIA geformuleerde International Standards, Practice Advisories en Position Papers, aangevuld door richtlijnen van het NIVRA, specifiek voor intern accountants. De door ons opgestelde 'good practices' kunnen dienen als referentiepunt voor beroepsuitoefenaren, belanghebbenden en andere belangstellenden in en rondom GRC. Deze 'good practices' kunnen een eerste aanzet zijn tot nadere invulling van richtlijnen en standaarden voor IAF's zoals mogelijk te formuleren door de (internationale) beroepsorganisaties van internal auditors. 'Good practices' zijn uitgesproken goede voorbeelden van concrete handel- en werkwijzen waarbij praktijkervaring centraal staat. Vakgenoten krijgen hierbij ideeën met betrekking tot GRC in hun eigen professionele praktijk die zij – al dan niet met eventuele aanpassingen – in hun eigen situatie kunnen overnemen. De 'good practices' zijn afkomstig uit de enquête en interviews en zijn door de projectleden op basis van brede consensus bepaald. Een 'good practice' van één organisatie is niet noodzakelijk een 'good practice' voor een andere organisatie. Een goed begrip van de context, de randvoorwaarden en de kritieke succesfactoren is daarbij essentieel.

De vaststelling van de verantwoordelijkheden en taken van de IAF, alsmede de andere risk- en controlfuncties, zijn te allen tijde de verantwoordelijkheid van de Raad van Bestuur. De Raad van Commissarissen (eventueel gedelegeerd naar haar commissies zoals de Auditcommissie) van de organisatie houdt daar toezicht op.

1.2 Inrichting, verantwoordelijkheden en scope

Uit ons onderzoek blijkt dat veelal het 'Three Lines of Defense model'[2] leidend is bij de inrichting van de risk- en controlfuncties. Het is in de eerste plaats het verantwoordelijke lijnmanagement dat bewaakt of de doelstellingen worden gerealiseerd en of de beheersmaatregelen om deze te bereiken effectief zijn. Dit is de 'First Line of Defense'. In veel organisaties bestaan, naast de IAF, ook andere risk- en controlfuncties zoals Risk Management, Compliance en verbijzonderde Interne Controle. Zij vormen de 'Second Line of Defense'. Zij zijn vaak (mede-)verantwoordelijk voor het ontwikkelen van beleid en dragen zorg voor de implementatie van maatregelen om het beleid te realiseren en het monitoren van de naleving daarvan. Omdat zij deel uitmaken van de interne beheersingssystemen van de organisatie, beoordeelt de IAF de effectiviteit van deze risk- en controlfuncties. Daarbij kan de IAF ook leemten en doublures tussen deze functies identificeren en daarmee de effectiviteit van het geheel aan functies verbeteren. Dit verklaart waarom de IAF als de 'Third Line of Defense' wordt aangeduid. Qua positionering merken wij verder nog op dat de IAF onafhankelijk moet zijn[3] wat betreft gedachtegang en handelen.

Good practices:

- *De positionering en taakopvatting van de IAF en de andere risk- en controlfuncties zijn in lijn met het 'Three Lines of Defense' model.*
- *De IAF rapporteert ook over GRC aan de Auditcommissie van de Raad van Commissarissen en de voorzitter van de Raad van Bestuur.*
- *De verantwoordelijkheden ten aanzien van GRC van de Auditcommissies van de Raad van Commissarissen zijn helder geformuleerd en in lijn met de bepalingen uit de Nederlandse Corporate Governance Code.*
- *De inrichting van risk- en controlfuncties is ook bij internationale organisaties tevens toegespitst op lokale wet- en regelgeving en houdt rekening met lokale 'good practices' op het gebied van GRC.*
- *Het functioneren van de IAF wordt beoordeeld door de Auditcommissie, die hierbij gebruikmaakt van input van externe kwaliteitsonderzoeken en eventueel de externe accountant en toezichthouders.*
- *De IAF kijkt meer naar de uitvoering en resultaten van de GRC-processen, dan naar de functies (de afdelingen) die deze processen uitvoeren.*

1 Vrij vertaald uit de Glossary, International Standards, IIA, oktober 2008.
2 Zie onder meer De internal auditor in Nederland, Position Paper, IIA/NIVRA, 2008. Zie verder ook hoofdstuk 2 in dit rapport.
3 Zie ook Attribute Standards 1100 en 1110, IIA.

- *Het hoofd IAF is aanwezig bij vergaderingen van de Auditcommissie en heeft zogenaamde 'private meetings' zonder aanwezigheid van management en anderen, zoals de externe accountant.*
- *De IAF draagt actief bij aan het implementeren van geautomatiseerde beheersingsmodellen ('continuous monitoring' en 'continuous assurance') in de organisatie.*
- *Het hoofd IAF is aanwezig bij vergaderingen van eventuele risk commissies.*
- *De verantwoordelijkheid van de IAF bij 'risk assessments' is beperkt; deze verantwoordelijkheid ligt in principe bij de 'first line' en 'second line'.*
- *De Risk Management functie faciliteert de totstandkoming van in control statements, de IAF levert hierbij zekerheid.*
- *De Raad van Bestuur stelt het risicoprofiel en de 'risk appetite' van de organisatie vast.*
- *Alle risk- en controlfuncties hanteren een geïntegreerd organisatiebreed risicomanagementsysteem (inclusief hetzelfde begrippenkader) voor risicodetectie en -beheersing.*
- *De IAF draagt expliciet bij aan het reduceren van de complexiteit van het risicomanagementsysteem.*

1.3 Uitvoering werkzaamheden

De Performance Standards van het IIA bevatten richtlijnen voor de uitvoering van de werkzaamheden van de IAF: 2110 over Governance, 2120 over Risk Management, 2130 over Control en 2600 over de acceptatie van risico's door het senior management. Specifieke richtlijnen met betrekking tot de Compliance functie zijn niet door het IIA geformuleerd.

Good practices:

- *De werkzaamheden van de IAF zijn afgeleid van de organisatiedoelstellingen, de beheersingsfilosofie en beheersingskaders van de organisatie; de speerpunten van de organisatie zijn de speerpunten voor de IAF, vertaald naar risico's en controls.*
- *Bij het testen van controls wordt de scope (i.c. welke controls worden getest) vastgesteld door de reviewende partij in afstemming met het management.*
- *De IAF stelt bij haar bevindingen en aanbevelingen vast of het management ook daadwerkelijk commitment voor deze punten heeft en neemt indien nodig maatregelen als voldoende commitment ontbreekt.*
- *De IAF werkt continu en actief aan het draagvlak van haar eigen functie en van andere risk- en controlfuncties.*
- *De IAF neemt de 'cost of control' mee in haar analyse en aanbevelingen.*
- *De IAF beoordeelt regelmatig aspecten als gedrag, cultuur en managementstijl als onderdeel van haar werkzaamheden in relatie tot governance en de control environment.*
- *De IAF is zich bewust van de verschillende culturele achtergronden in haar organisatie en houdt hier rekening mee in de werkwijze en rapportage.*
- *De IAF draagt proactief bij aan het realiseren van de beoogde effecten op GRC vanuit de Europese Transparantierichtlijn over het verschaffen van uniforme informatie aan belanghebbenden van en in de organisatie.*
- *De IAF neemt maatregelen, zeker als de organisatie een geïntegreerd risicomanagemensysteem heeft, om te zorgen dat zij voldoende objectief en onafhankelijk dit systeem kan beoordelen.*
- *De IAF en GRC-functies houden de goede werking van controls voortdurend scherp in het oog.*
- *De IAF heeft er oog voor dat compliance meer inhoudt dan het formeel voldoen aan wet- en regelgeving. Niet alleen de letter, maar ook de geest is van belang; dit kan zich uiten in gedrag of uitspraken van het management en de medewerkers.*

1.4 Risicobeoordeling

Op allerlei plekken in de organisatie vinden formele en informele risicoanalyses plaats. In feite is elke handeling in een organisatie gebaseerd op een risicoanalyse, bewust dan wel onbewust. Het is de taak van elke manager om de risico's (de mogelijkheid van het plaatshebben van een gebeurtenis die mogelijk van invloed is op het realiseren van de doelstellingen) formeel in kaart te brengen, te analyseren en te managen. De Position Paper 'The Role of Internal Auditing in Enterprise-wide Risk Management' van het IIA geeft een duidelijke afbakening welke werkzaamheden de IAF zou kunnen, en niet zou moeten doen met betrekking tot integraal risicomanagement.

Good practices:

- *De IAF beoordeelt het risicomanagementproces (inclusief de transformatie van ruwe data tot informatie) op begrijpelijkheid en aggregatieniveau, naast de aspecten juistheid, betrouwbaarheid en volledigheid.*
- *De IAF beoordeelt of de risicoanalyse in het kader van integraal risicomanagement voldoende onderbouwd en aangevuld is met een gedegen financiële analyse.*

- *De IAF verleent zekerheid over de uitkomsten van het risicomanagementproces, waarbij naast een procesmatige beoordeling ook een beoordeling van de uitkomsten plaatsvindt.*
- *De IAF maakt gebruik van de inventarisaties en risicoanalyses van alle (staf-)functies (voorbeelden zijn – al dan niet verbijzonderd – functies die zich richten op sustainability, kwaliteitscontrole, innovatie, veiligheid e.d.).*
- *De IAF blijft kritisch en onafhankelijk van geest in haar beoordeling van risicomodellen en de uitkomsten daarvan; elk model is slechts een mogelijke weergave van de werkelijkheid.*
- *De IAF stimuleert dat risico's afkomstig uit verschillende bronnen integraal worden geanalyseerd, om zodoende onderlinge relaties tussen risico's zichtbaar te maken.*
- *De IAF stimuleert dat het integraal risicomanagement een stap bevat waarin risicoanalyses door verantwoordelijk management en door de operationele afdelingen (de inhoudelijk betrokkenen) zelf met elkaar geconfronteerd worden (een gecombineerde top-down en bottom-up benadering).*
- *De IAF draagt er toe bij dat risico's worden beoordeeld vanuit strategische, operationele en financiële invalshoek.*
- *De IAF stimuleert dat scenariodenken (inclusief 'worst case scenario's') een essentieel onderdeel is van de risicoanalyse.*
- *De IAF draagt ertoe bij dat zowel de Chief Financial Officer als de Chief Risk Officer integraal en consistent over risico's worden geïnformeerd.*

1.5 Communicatie en overleg

Een continu aandachtspunt voor specialisten in welke hoedanigheid dan ook is het communiceren met belanghebbenden over hun doelstellingen, functie, werkwijze en resultaten. Valkuil is dat verantwoording over de gevolgde werkwijze en vakjargon de boventoon voeren; vergeten wordt vaak dat ook de ontvanger de boodschap moet begrijpen. IAF's en andere risk- en controlfuncties verliezen dit wel eens uit het oog. Actief uitdragen van het begrippenkader, inleven in de gedachtewereld van de ontvanger en 'soft skills' van de 'audit professionals' spelen hierbij een sleutelrol. Practice Advisory 1210-1 van het IIA benoemt expliciet de noodzaak voor internal auditors tot het ontwikkelen van vaardigheden voor het omgaan met mensen, begrip van interactie tussen mensen onderling en het opbouwen van relaties met belanghebbenden, naast algemene schriftelijke en verbale capaciteiten. Communicatie door de professie naar externe belanghebbenden van de organisatie in het algemeen is hier een onlosmakelijk onderdeel van.

Good practices:

- *De IAF en GRC-functies formuleren hun opinies 'to the point', expliciet en duidelijk.*
- *De IAF heeft directe communicatielijnen met de Auditcommissie, Raad van Bestuur en senior management.*
- *De IAF stimuleert de Raad van Bestuur (en in het bijzonder de CEO en de CRO) openlijk het belang van de risk- en controlfuncties binnen de governance van de organisatie uit de dragen.*
- *De IAF stimuleert een eenduidige taal met betrekking tot risico's en controls.*
- *De IAF heeft met het lijnmanagement een relatie die zich kenmerkt door openheid en vertrouwen.*
- *De IAF stimuleert het bestuur het 'in control statement' actief onder al haar belanghebbenden te verspreiden.*
- *De IAF heeft concrete doelstellingen gericht op onderlinge samenwerking en informatie-uitwisseling met de andere risk- en controlfuncties.*
- *De IAF heeft regelmatig formeel en informeel overleg met de verschillende niveaus in de lijnorganisatie.*
- *De risk- en controlfuncties overleggen regelmatig; op de agenda staan zaken als afstemming werkzaamheden en bespreking van risicobeoordelingen.*
- *De risk- en controlfuncties hebben hun fysieke locaties dicht bij elkaar, ter versterking van de informele communicatie.*

1.6 Rapporteren en vastleggen

Rapportages zijn een belangrijk product van de IAF en vormen een kernelement van de communicatie van de IAF met haar opdrachtgevers en belanghebbenden. Ook de andere risk- en controlfuncties maken in het algemeen rapportages. Het is zorg dat al deze functies de organisatie daadwerkelijk ondersteunen en toegevoegde waarde bieden bij het formuleren van risico's en verbeteracties. Onderlinge afstemming hierbij is essentieel. Richtlijnen voor IAF's over communicatiecriteria en kwaliteit worden gegeven in Practice Advisories 2410-1 en 2420-1 van het IIA.

Good practices:

- *De organisatie heeft een gelaagd systeem van risicodashboards, waarin risico's op het juiste niveau en in voldoende mate van detail inzichtelijk worden gemaakt.*
- *De IAF zorgt ervoor dat in haar rapportages risico's helder gedefinieerd worden, met opgave van een inschatting van de kans van optreden en de impact van de mogelijke gebeurtenis.*

- *De IAF formuleert in haar rapportages concrete bevindingen met aanbevelingen die in voldoende mate richtinggevend zijn.*
- *De IAF rapporteert in duidelijke en onomwonden taal en spitst haar rapportages toe op de doelgroep.*
- *De risk- en controlfuncties en de lijn gebruiken eenzelfde tool voor het vastleggen van belangrijke controls, risico's en issues, zodat uniform taalgebruik, transparantie en coördinatie wordt bevorderd en vereenvoudigd.*
- *De risk- and controlfuncties rapporteren volgens het principe 'risks that matter'.*

1.7 Medewerkers, competentie en gedrag

Onmiskenbaar is de kwaliteit van de risk- en controlprofessionals zelf cruciaal. Deze kwaliteit omvat onder meer vakinhoud, ervaring en competenties. Het systeem van certificeringen met daaraan gekoppelde permanente educatieverplichtingen is een sprekend voorbeeld om deze kwaliteit op peil te houden. De Code of Ethics van het IIA gaat expliciet in op de vereisten inzake integriteit, objectiviteit, vertrouwelijkheid en vakbekwaamheid.

Good practices:

- *De IAF rapporteert haar bevindingen 'met rechte rug'.*
- *De IAF werkt actief aan de 'soft skills' en 'hard skills' van haar professionals en stimuleert andere risk- en controlfuncties hetzelfde te doen.*
- *De IAF haalt specifieke kennis of ervaring die noodzakelijk is voor een onderzoek van buiten haar afdeling of zelfs van buiten de organisatie, met in achtneming van de professionele normen, indien zij deze specifieke kennis niet zelf in huis heeft of om andere redenen niet in kan zetten. Het niet beschikbaar hebben van bepaalde kennis of ervaring is nooit en te nimmer een reden een onderzoek niet uit te voeren.*
- *De IAF is een 'centre of excellence' in risico's en beheersing en stelt haar kennis en kunde actief ter beschikking aan de organisatie.*
- *De IAF heeft een trainingsprogramma waarin haar medewerkers regelmatig worden bijgeschoold op kennis van de organisatie, haar processen en systemen.*
- *De IAF werkt continu aan het ontwikkelen van de kennis en kunde van haar medewerkers met betrekking tot internal auditing.*
- *De IAF wisselt actief medewerkers met de andere risk- en controlfuncties en de lijnorganisatie uit.*
- *De IAF levert een actieve bijdrage aan de kennis- en competentieontwikkeling van de medewerkers in de gehele organisatie met betrekking tot GRC.*
- *De IAF stimuleert een intensieve en frequente kennis- en ervaringuitwisseling tussen IAF's, al dan niet gefaciliteerd door haar beroepsorganisaties.*
- *De IAF maakt gebruik van een up to date kennismanagementsysteem met specifieke aandacht voor GRC.*

2 Conclusies en aanbevelingen

2.1 Inleiding

Op basis van resultaten van de literatuurstudie, enquête, de interviews en de debatsessie heeft de werkgroep een aantal conclusies geformuleerd. Tevens bleek dat wij ook behoefte hadden om op enkele gebieden richtingen voor verdere ontwikkeling en aandacht te formuleren. Vandaar dat per conclusie een of meer aanbevelingen zijn geformuleerd, gericht aan verschillende belanghebbenden in het GRC-werkveld.

2.2 De aanpak van de IAF om te komen tot een oordeel over de governance in een organisatie kan zeker nog geprofessionaliseerd worden

Vele partijen spelen een rol in de governance van een organisatie en zij zijn vaak onzeker over hun onderlinge verhoudingen. De aandacht voor governance is als gevolg van de wereldwijde kredietcrisis alleen nog maar groter geworden. Risicomanagement en compliance staan continu op de voorgrond en governance fungeert daarbij als het smeermiddel om de verantwoordelijkheid van het topmanagement in te vullen en te dragen. Dit betekent ook dat duidelijk door de leiding uitgesproken moet worden wat zij als gewenst gedrag ziet en dat zij dat vervolgens ook zelf uitstraalt ('tone at the top'). Verder geeft de leiding concreet aan op welke wijze de governance-processen en -structuren dienen te worden ingevuld. De hoogste leiding van de organisatie is daarmee primair verantwoordelijk voor het constitueren, implementeren en handhaven van de governance. Er is geen algemeen geaccepteerde aanpak beschikbaar hoe de IAF zekerheid over governance kan (of moet) geven, wat voor adviesopdrachten zij wel of niet kan aannemen en hoe zij om moet gaan met de inrichting van governance (wat de verantwoordelijkheid is van de hoogste leiding waar de IAF zelf ook aan rapporteert).

Aanbevelingen:

- *Wij bevelen Auditcommissies aan om een visie over governance te ontwikkelen die aansluit bij de aard, branche, omvang en complexiteit van de organisatie, om vast te stellen in hoeverre hieraan voldaan wordt en vervolgens hierover de discussie met de leiding in de organisatie aan te gaan.*
- *Wij bevelen de beroepsorganisaties van internal auditors aan om het auditen van governance nader onder de aandacht te brengen en hier nadere instructies voor de beroepsuitoefenaren voor te (laten) ontwikkelen en mee te geven.*

2.3 Het opsplitsen van GRC-verantwoordelijkheden over meerdere functies leidt tot een betere beheersing in de organisatie

Het 'Three Lines of Defense' model wordt breed gezien als handreiking om GRC binnen de organisatie vorm te geven. Vooral in de financiële sector is dit model terug te vinden met separate functies voor Internal Audit, Risk Management en Compliance, waarbij de IAF als de 'Third Line of Defence' wordt gezien en Risk Management en Compliance functies als 'Second Line'. De wetgeving in de financiële sector schrijft deze splitsing zelfs voor, waar de sector zelf tevreden mee is. Over het algemeen functioneert dit model goed, alhoewel de uitwerking en operationalisering nog beduidend aandacht behoeft. Er zijn echter ook afdelingen die meerdere GRC-verantwoordelijkheden combineren en deze afdelingen zien daar geen bezwaar in. Valkuilen van die scheiding zijn een eenzijdige focus op het eigen vakgebied en het ontwikkelen van een geïsoleerde blik. Dit kan met de mate van volwassenheid van GRC in die organisaties te maken hebben, maar natuurlijk speelt ook de omvang van de organisatie hier een rol.

Naarmate er meer afstand ontstaat tussen de IAF en de andere risk- en controlfuncties neemt het belang van een goede communicatie tussen deze functies toe. Het versterken van de communicatie tussen deze functies verdient in veel organisaties nog veel aandacht. Een onderdeel van deze communicatie is een eenduidig en uniform begrippenstelsel, dat in veel organisaties nog geen gemeengoed is.

Aanbevelingen:

- *Wij pleiten voor nadere richtlijnen vanuit de beroepsorganisaties van internal auditors die aangeven in welke bijzondere gevallen de combinatie van GRC-verantwoordelijkheden in één functie mogelijk is, met in achtneming van de principes van het 'Three Lines of Defense' model.*
- *Wij pleiten voor het breed toepassen van 'in control statements' in organisaties, om de verantwoordelijkheden en transparantie rondom risico's en beheersing daarvan binnen de organisatie scherp te krijgen.*
- *Wij adviseren Raden van Bestuur en Raden van Commissarissen expliciet de verantwoordelijkheid te nemen voor het realiseren van de door haar gewenste governance in de organisatie en het 'Three Lines of Defense' model hiervoor als leidraad te nemen.*

2.4 Risicomanagement is nog sterk in ontwikkeling en de IAF heeft nog geen eenduidige aanpak voor de beoordeling ervan

Risicomanagement staat in een grote belangstelling, maar is nog lang niet uitontwikkeld. Een verdere professionalisering van risicomanagement is noodzakelijk en nodig. Alleen al om de beheersing rondom allerhande productinnovaties in de financiële sector het hoofd te kunnen bieden. Zeker in de financiële sector zijn organisaties nog volop bezig om bestaande en aankomende regelgeving te verwerken in een alles omvattend beheersingskader. Er zijn vele manieren om risico's in kaart te brengen, er zijn diverse analysemodellen, de kwantificering van risico's wordt op verschillende manieren gebruikt en er is ook geen eenduidige manier van rapporteren. Dit zijn kenmerken van een vakgebied dat nog in ontwikkeling is en dat nog weinig sturing en coördinatie van bijvoorbeeld een beroepsorganisatie en impulsen op het gebied van vakontwikkeling bij universiteiten kent. Organisaties doen het op hun eigen manier. De IAF zelf heeft ook nog geen eenduidige aanpak voor het beoordelen van risicomanagement, maar we moeten ook constateren dat de kennisontwikkeling over risicomanagement binnen de IAF nog extra aandacht behoeft. Daarnaast blijft het bouwen van een robuust beheersingskader en de inbedding hiervan in de governance van de organisatie een complex en tijdrovend proces. Maar de urgentie is groot; het is maar de vraag of de IAF en de andere risk- en controlfuncties nog veel tijd zullen krijgen hun toegevoegde waarde daadwerkelijk waar te maken.

Aanbevelingen:

- *Wij adviseren de risicomanagers als beroepsgroep het vakgebied verder te professionaliseren met coördinatie, sturing, certificering en scholing.*
- *Wij adviseren de risico- en compliancemanagers in Nederland om vanuit hun optiek te komen met 'good practices' en aanbevelingen met betrekking tot de governance van de organisatie.*
- *Wij pleiten voor nadere initiatieven vanuit de beroepsorganisaties van internal auditors en vanuit de IAF's zelf om de kennis van risicomanagement bij internal auditors verder te verstreken; te denken valt aan stimuleren van promotieonderzoeken, vakstudies, standpuntbepalingen en dergelijke.*
- *Wij bevelen IAF's aan om binnen hun organisatie een bijdrage te leveren aan een brede bewustwording van de onvolkomenheden en beperkingen van het huidige instrumentarium voor risicomanagement en om de ontwikkeling van dit instrumentarium verder te stimuleren.*

2.5 De Internal Audit functie kijkt nog te veel naar risicomanagementprocessen en te weinig naar de uitkomsten van deze processen

De huidige beoordeling van risicomanagement door de IAF betreft het beoordelen van de opzet en werking van de risicomanagementprocessen. De uitkomsten van deze processen, zoals risicoregisters en risicorapportages zijn een minder eenvoudig te beoordelen. Er is geen eenduidigheid binnen het werkveld of het geven van een oordeel over de uitkomsten van de GRC-processen tot de taken van de IAF behoort. Dit is opvallend, omdat uitkomsten in de trant van 'operatie geslaagd, patiënt overleden' toch niet meer van deze tijd zijn. Dit is wellicht één van de factoren waarom de IAF in de discussies rondom de kredietcrisis maar een kleine rol speelt. Dat de Commissie De Wit de IAF meerdere malen expliciet noemt in haar rapportage is wellicht een kentering hierin.

Aanbeveling:

- *Wij pleiten ervoor dat IAF's meer aandacht geven aan het beoordelen van de uitkomsten van risicomanagementprocessen.*

2.6 De activiteiten als gevolg van wet- en regelgeving, ook wel genoemd regulatory compliance, nemen zienderogen toe en leiden tot een versterking van een 'rules oriented' cultuur ten nadele van een 'principle based' cultuur

Hoewel wij nog steeds een 'principle based' cultuur voorstaan, zien wij een toenemende aandacht voor wet- en regelgeving ontstaan. De overheid èn het publiek, naast ontwikkelingen in het buitenland, eisen een striktere handhaving en naleving van wet- en regelgeving, waarbij de overheid via horizontaal toezicht de druk daarvan bij de onder toezicht staande organisaties zelf wil neerleggen. De wijze waarop organisaties hiermee omgaan is verschillend. Sectoren met veel regelgeving gericht op het primaire proces (denk aan de financiële sector, de levensmiddelensector, de gezondheidszorg of de chemische industrie) kennen specifiek hierop gerichte functies, die wij gemakshalve samenvattend 'regulatory compliance' functies noemen. De toename aan regels zorgt echter wel voor een toenemende druk binnen organisaties om deze regels na te leven, hier op toe te zien, de effecten op cultuur en gedrag te definiëren en natuurlijk na te gaan hoe de 'regulatory compliance' activiteiten op hun beurt dan weer geaudit zouden moeten worden. Vanuit het werkveld komt echter zeer sterk naar voren dat aanvullende wet- en regelgeving niet als een versterking van GRC

en de beheersing in organisaties wordt gezien. Dit omdat gedetailleerde regels tot schijnzekerheid leiden, handhavingsproblemen oproepen en een eigen brede verantwoordelijkheid terugdringen[4].

Aanbevelingen:

- *Wij pleiten ervoor dat de beroepsorganisaties van internal auditors zich actief manifesteren als belanghebbenden bij het ontwikkelen van nieuwe wet- en regelgeving.*
- *Wij bevelen de beroepsorganisaties van internal auditors aan om met een visie te komen op het auditen van compliance en de compliance-functie.*

3 Wet- en regelgeving met betrekking tot GRC

3.1 Wet- en regelgeving algemeen

De Nederlandse Corporate Governance Code, die in december 2009 wettelijk is verankerd, is van toepassing voor iedere beursgenoteerde onderneming, financiële instellingen incluis. Hierin is een aantal 'good practice' bepalingen opgenomen voor de rol van de IAF, alsmede verantwoordelijkheden van de Raad van Bestuur en de Raad van Commissarissen bij risicomanagement. In de praktijk wordt de Nederlandse Corporate Governance Code ook door niet-beursgenoteerde, grote instellingen als 'good practice' gehanteerd.

In maart 2010 heeft het Koninklijk NIVRA een praktijkhandreiking gepubliceerd ter verduidelijking van de rol van de externe accountant bij de toetsing van in het jaarverslag opgenomen corporate governance-informatie (Praktijkhandreiking 1109). In 2009 publiceerde het IIA zijn Position Paper 'The Role of Internal Auditing in Enterprise-wide Risk Management'.

3.2 Wet- en regelgeving specifiek voor de financiële sector

De Wet op het financieel toezicht is van kracht sinds 1 januari 2007. Deze bestaat uit een samenvoeging van acht toezichtswetten en heeft de bedoeling om de wetgeving voor de financiële markten marktgericht, doelgericht en inzichtelijke te maken. Uit deze 'principle based' wet vloeien meer algemene vereisten voor 'good governance' voort.

De Code Banken is van kracht sinds 1 januari 2010. Veel principes in de Code Banken hebben betrekking op het functioneren en de rol van de Raad van Bestuur en de Raad van Commissarissen in de bancaire context. Risicobeheer krijgt in deze Code veel aandacht. De Code sluit aan op de Nederlandse Corporate Governance Code en de bestaande wet- en regelgeving.
Volgend de Code moet de IAF jaarlijks controleren of het risicoanalyseproces in opzet aanwezig is, bestaat en de werking effectief is. De principes geven verder aan dat de IAF onder meer de opzet, bestaan en werking van de governance, het risicobeheer en beheersprocessen van de bank moet vaststellen. Zij dient hierover te rapporteren aan de Raad van Bestuur en de Auditcommissie.

Andere belangrijke wetten voor financiële instellingen zijn de Bankwet, de Sanctiewet, de Wet ter voorkoming van witwassen en financieel terrorisme, Wet financiële betrekkingen buitenland en de wet kapitaalaccoord Basel II. Voor Europese (her)verzekeraars is vanaf 2012 de Solvency II richtlijn met betrekking tot de vereiste hoeveelheid kapitaal risicomanagement en interne controles van kracht. Deze opsomming is niet limitatief, maar geeft wel aan dat het belang van effectief corporate governance en risicomanagement groot is.

In maart 2010 heeft het Koninklijk NIVRA de rol van de externe accountant en de internal auditor nader toegelicht in de Praktijkhandreiking 1110, Code Banken: taken interne auditfunctie en externe accountant.

4 Zie ook de risico-regel-reflex van Margot Trappenburg in NRC Handelsblad, 15 mei 2010

Koninklijk Nederlands Instituut
van Registeraccountants

www.nivra.nl

Instituut van Internal Auditors
Nederland

www.iia.nl